The Implementation of Digital Text Coding Algorithm Through A Three Dimensional Mapping Derived From Generalized \(\Delta\Delta\)-mKdV Equation Using Mathematica

Notiragayu\(^1\) and L Zakaria\(^1\)

\(^1\) Mathematics Department, University of Lampung, Bandar Lampung, Indonesia

Abstract. Encryption-decryption algorithm using a mapping can be done for encoding a digital text, such as two dimensional mapping \(\Delta\Delta\)-sine Gordon equation. In this article, we will be given an encryption-decryption algorithm to a digital text through a three dimensional mapping that derived from the generalized \(\Delta\Delta\)-mKdV equation. Implementation of Encryption-decryption algorithm in this article using MATHEMATICA.

1. Introduction

Cryptography is an attempt to secure digital data files (etc. text and images). Cryptography, based on security keys, can be classified into two types of keys, symmetric keys and asymmetric keys [1]. An efficient and effective encryption-decryption algorithm is a necessity in cryptography for data security. A simple encryption-description algorithm is implemented into a computer programming and produces a high degree of difficulty in finding the security key for opening the data is an absolute thing in Cryptography. Encryption-decryption algorithm which involves mathematics in it can be found in ElGamal's article (1985) and the articles in the reference [2]. Among Cryptographic encryption-decryption algorithms that use mathematical concepts, there is a Cryptographic encoding algorithm that involves mapping. For encoding in an image for example, Rinaldi (2012) has introduced the use of Arnold Cat Map (ACM) linear mapping [3]. Meanwhile, Arinten and Hidayat (2017) use Logistic Map (LM). Likewise with Ronsen, Arwin, and Indra (2014), they used ACM and Nonlinear Chaotic Algorithm (NCA) in coding for an image [4,5]. Thus a mapping can be used as a means of building cryptographic encoding for a digital data (image).

With regard to digital text data, popular cryptographic algorithms used are public key algorithms, commonly referred to as asymmetric keys, for example the ElGamal public key [6]. While the use of a mapping for cryptographic algorithms text data is relatively little published.

In this article, we will discuss an application of map in cryptographic algorithms for text data. The mapping is a part of the nonlinear mapping derived from a generalized traveling wave solution \(\Delta\Delta\)-mKdV [7].

This article is divided into four sections. In the first section an illustration of a descriptive algorithm is provided for cryptographic coding of text data using a 2-dimensional periodic nonlinear method. The second part, in the form of case studies, discusses cryptographic algorithms of text data using 2-dimensional mapping derived from the equation of a generalized traveling wave solution \(\Delta\Delta\)-sine Gordon. In the third part, the implementation of the cryptographic algorithm of text data into the Mathematic programming language. In the fourth section, the conclusions are briefly described in the results obtained in the previous section.
2. Encryption-Decryption Algorithm For Digital Text Submission Using Mapping: An Illustration

Consider the following nonlinear mapping:

\[ \gamma_{n+1} = g_0(\gamma_n) \]  

(1)

where

\[ g_0 : \mathbb{R}^2 \rightarrow \mathbb{R}^2 \]

\[ (x, y) \mapsto \left( \frac{\alpha}{x}, \eta \right) \frac{x}{y} \]

It can be examined that equation (1) is a 3-periodic nonlinear mapping with the parameter values \( \alpha \) and \( \eta \) set as any but not zero.

Example:

Consider the following text data.

\textit{From Wolfram:} Mathematica’s extensive base of state-of-the-art algorithms, efficient handling of very long integers, and powerful built-in language make it uniquely suited to both research and implementation of cryptographic number theory.

We are coding the text data using mapping (1) whose symmetrical key is selected from \( \alpha \) and \( \eta \). Descriptively, the encryption-decryption algorithm for example text like this can be done in the following way.

2.1. Encryption stage

1. Grouping Text into two parts, for example parts \( x(n) \) and \( y(n) \) with \( n \in \mathbb{N} \) are the values of numeric data associated with text data. And assume the length of the text data \( l \) is the same that is \( l(x) = l(y) = m \in \mathbb{N} \).
2. Convert text data to numeric data. The ASCII code can be used or uses a self-made encoding.
3. Do the mapping iteration process as much as \( r \) times with the provisions of \( g^0 < g^r; r \in \mathbb{N} \).
4. Select the parameter value \( \alpha, \eta \neq 0 \) and make it as the key value.

2.2. Decryption Stages

1. Reuse the parameter value \( \alpha, \eta \neq 0 \) which is the key value at encryption.
2. Perform the mapping iteration process provided until it reaches the \( r \) iteration, that is \( g^r; r \in \mathbb{N} \).
3. Convert numeric data into text data.
4. Finish.

The implementation of the descriptive algorithm above using Mathematica is given in the next section.

3. Digital Text Description-Encryption Algorithm Using A Mapping Derived From Generalized \( \Delta\Delta \)-mKdV Equation

3.1. The 2-Dimensional Periodic Mapping Formulation Derived from Generalized \( \Delta\Delta \)-mKdV Equation

In this section, we will follow a technique for a generalized sine-Gordon equation (see [8]). Look at the family of four mapping parameters derived from the generalized \( \Delta\Delta \)-mKdV equation follows:
\[ \theta_{1} V_{l,m} V_{l,m+1} - \theta_{2} V_{l+1,m} V_{l+1,m+1} - \theta_{3} V_{l,m} V_{l+1,m} + \theta_{4} V_{l,m+1} V_{l+1,m+1} = 0, \] (2)

with \( \theta_{1} = \alpha_{1} \beta_{2} p, \ \theta_{2} = \alpha_{4} \beta_{2} p, \ \theta_{3} = \alpha_{3} \beta_{2} q \) and \( \theta_{4} = \alpha_{2} \beta_{2} q \).

Using the following transformation

\[ V_{l,m} = V_{n} \quad \text{where} \quad n = z_{1}l + z_{2}m, \]

where the parameter values of \( z_{1} \) and \( z_{2} \) are relatively prime integers, we can reduce the form of the current wave solution (2), namely

\[ \theta_{1} V_{n+1} V_{n+2} - \theta_{2} V_{n+3} V_{n+3} - \theta_{3} V_{n+1} V_{n+1} + \theta_{4} V_{n+2} V_{n+2} = 0 \] (3)

Equation (3) is a form of traveling wave solution from \( \Delta \Delta - mKdV \). It can be examined that the equation (3) is invariant for a transformation \( z_{11} \rightarrow z_{11} - p \) and \( z_{12} \rightarrow z_{12} \). Besides that it also fulfills the periodic nature, namely \( (i + z_{2}, j - z_{1}) \). Equation (3) is equivalent to mapping

\[ V'_{z_{1}+z_{2}-1} = V_{0} \left( \frac{\theta_{1} V_{z_{1}} - \theta_{1} V_{z_{2}}}{\theta_{1} V_{z_{1}} - \theta_{1} V_{z_{2}}} \right) \]

\[ V'_{z_{1}+z_{2}} = V_{z_{1}+z_{2}-1} \]

\[ \vdots \]

\[ V'_{i} = V_{2} \]

\[ V'_{j} = V_{l} \% \]

Select \( z_{1} = 1 \) and \( z_{2} = 2 \). The third order difference equation of equation (4) can be stated as follows:

\[ \theta_{1} V_{n+2} V_{n+3} - \theta_{2} V_{n+1} V_{n+3} - \theta_{3} V_{n+1} V_{n+1} + \theta_{4} V_{n+2} V_{n+2} = 0 \]

which is equivalent to the following three-dimensional mapping:

\[ V'_{n+2} = V_{n} \left( \frac{\theta_{1} V_{n+3} - \theta_{1} V_{n+1}}{\theta_{1} V_{n+2} - \theta_{1} V_{n+3}} \right) \]

\[ V'_{n+1} = V_{n+2} \]

\[ V'_{n} = V_{n+1} \] (5)

The equation in (5) is usually given a three-dimensional mapping derived from the generalized \( \Delta \Delta - mKdV \) equation.

Look at equation (5). Suppose that \( \xi_{n} \) is a line in \( \mathbb{R}^{2} \) that is defined as

\[ \xi_{n} = \begin{pmatrix} V_{n+2} \\ V_{n+1} \\ V_{n} \end{pmatrix} \]

Suppose that \( \theta \) is a parameter vector in \( \mathbb{R}^{4} : (\theta_{1}, \theta_{2}, \theta_{3}, \theta_{4}) \). Therefore, three-dimensional statements can be reduced to a two-dimensional mapping, namely:

\[ \xi_{n+1} = g_{\theta}(\xi_{n}) \]

where
\[ g_0 : \mathbb{R}^2 \rightarrow \mathbb{R}^2 \]
\[(x, y) \mapsto \left( \frac{-1}{xy} \left( \theta_4 x - \theta_1 \right), x \right). \quad (6)\]

where \( y = \frac{V_{n+1}}{V_n} \) and \( x = \frac{V_{n+2}}{V_n} \). It can be checked that the mapping in equation (6) has an integral (there is a function \( S : \mathbb{R}^2 \rightarrow \mathbb{R} \) so that \( S(\zeta_{n+1}) = S(\zeta_n) \) for all \( n \in \mathbb{N} \) [8]). If \( \alpha = \frac{\theta_1}{\theta_4}, \beta = \frac{\theta_2}{\theta_4}, \) and \( \lambda = \frac{\theta_3}{\theta_4} \), then the map in equation (6) can be written as

\[ g_{(\alpha, \beta, \lambda)} : \mathbb{R}^2 \rightarrow \mathbb{R}^2 \]
\[(x, y) \mapsto \left( \frac{\alpha \left(1 - \lambda x\right)}{xy \left(\beta x - 1\right)}, x \right). \quad (7)\]

### 3.2. Implementation of Digital Text Data Encryption Algorithms Based on 2-Dimensional Mapping Using Mathematica

To implement a cryptographic algorithm into a computer program, a number of software can be used, such as Matlab and Mathematica. In this article, we will use Mathematica that its rules and technical writing of this program in full in a reference written by Shifrin (2008) [9].

Look at the descriptive algorithms presented in section two. Against the text and 4-periodic mapping given in that section, the implementation of algorithms using Mathematica is as follows.

\[\text{str1} = "\text{FromWolfram: Mathematica’s extensive base of state-of-the-art algorithms, efficient handling of very long integers, }\];
\[\text{str2} = "\text{and powerful built-in language make it uniquely suited to both research and implementation of cryptographic number theory. }\];

\text{StringLength[str1]}
\text{StringLength[str2]}
\text{A = ToCharacterCode[str1];}
\text{B = ToCharacterCode[str2];}
\text{AccountingForm[Grid[Partition[A, 10]]];}
\text{AccountingForm[Grid[Partition[B, 10]]];}
\text{x = A; y = B; r = 3; \alpha = 0.0001523; \lambda = \beta = 8.1037277;}

\begin{verbatim}
THIS SECTION IS A SUBRUTIN PROGRAM NAMED coding1 FOR ITERATION PROCESSES \ g (A, B) TO THE r- ITERATION.
\end{verbatim}

\text{xx = SetPrecision[ coding1[[r - 1, 2]], 10];}
\text{yy = SetPrecision[ coding1[[r - 1, 1]], 10];}
\text{AccountingForm[Grid[Partition[xx, 5]];}
\text{AccountingForm[Grid[Partition[yy, 5]];}

THIS PART IS A SUBROUTIN PROGRAM NAMED recoding1 FOR ITERATION PROCESSES $g^{-1}(A, B)$ TO R-ITERATION.

```
Flatten[FromCharacterCode[Round[recoding1[[r-1]]]]]
```

Figure 1. Conversion results of text data A (left) and B (right) to numerical data before the mapping iteration process is carried out ($g^0$).

Figure 1 shows the result of the conversion of program outputs text data into numerical data using ASCII code (based on $g^0$). Another output of the program, for parameter values $\alpha = 0.0001523$ and $\lambda = \beta = 8.1037277$, we have the following numerical data.

![Table of numerical data for Figure 1](image1.png)

Figure 2. The results of the conversion of text data to numeric data with the choice of parameter values $\alpha = 0.0001523$ and $\lambda = \beta = 8.1037277$, after the iteration of the mapping (7) process is carried out on $g^2$. 

![Table of numerical data for Figure 2](image2.png)
3.3. Encryption-Description Algorithm For Setting Digital Text Using Mapping Generalized ΔΔ-mKdV Equation

Review the implementation of the algorithm using Mathematica which was given in the previous section. By using the transparent properties found in mapping (6), the periodic mapping iteration process can be replaced by an iteration invers mapping process, namely:

**THIS SECTION IS A SUBRUTIN OF NAMED recoding1 PROGRAMS FOR ITERATION PROCESSES g⁻¹ (AA, BB) TO r-ITERATION.**

\[
\text{Flatten[FromCharacterCode[Round[recoding1[[r-1]]]]].}
\]

**Figure 3.** The results of the conversion of text data to numeric data with the value of the choice parameter \( \lambda = 0.05234, \alpha = 0.7125, \) and \( \beta = 6.7111 \), after the iteration of the mapping (7) process is carried out on \( g^8 \).

With algorithms and implementation of similar algorithms, for mapping (7) with a choice of key values in the form of the choice parameter value \( \lambda = 0.05234, \alpha = 0.7125, \) and \( \beta = 6.7111 \) as given in figure 3.

**4. Conclusion**

From the results obtained and discussed in the previous section, it can be concluded that the 3-dimensional mapping reduced to 2-dimensional mapping derived from the ΔΔ-mKdV equation can be used to design a text cryptography relatively easily. As the purpose of cryptography is data security, then the choice of a reversible mapping option can be used as an alternative choice of digital text encoding with a symmetric key selected non-zero parameter values. The results of this study, because the statement involved is a mapping that is reversing symmetry, then for the mapping and procedure of cryptographic algorithms used for an image, the request requires a measure preserving nature, and this will be an interesting advanced topic to study.

**Acknowledgments**

The authors would like to thank The Directorate of Research and Community Services at Kemenristek Dikti RI for funded this research through DIPA FMIPA Research Grants 2017 of Lampung University and also thanks to the Head of Institute of Research and Community Services of Lampung University whom supported this research.
References

[1] Sadikin R 2012 *Kriptografi untuk Keamanan Jaringan* (Yogyakarta: Andi Publisher) p 392
[2] El Gamal T 1985 A Public key crypto system and a signature scheme based on discrete logarithms *IEEE Transactions On Information Theory* 31 4 pp 469-472
[3] Rinaldi M 2012 A selective encryption algorithm for digital images in the frequency domain based on chaos mutations *Electrical Engineering Journal* 10 2 pp 66-72
[4] Arinten D H and Irawan A 2017 Digital image cryptography system on an intranet network using the method of combining chaos maps and selective techniques *Ultimatics* 9 1 pp59-66
[5] Ronsen P, Arwin H and Indra S 2014 Encryption of digital images using Arnolds map paint and nonlinear chaotic algorithm *Mikroskil SIFO Journal* 15 2 pp 61-71
[6] Al-Anshori F and Ariwibowo E 2014 Implementation of elGamal's public key cryptographic algorithm for encryption and decryption processes for securing data files *Journal of Undergraduate Engineering* 2 2 pp 1-10
[7] Zakaria L, Notiragayu, A Nuryaman dan S Suharsono 2018 The integral normal form of a three dimensional traveling wave solution mapping derived from generalized ∆Δ-mKdV equation *Advances in Differential Equations and Control Processes* 19 1 pp 37-4
[8] Zakaria L and Tuwankotta J M 2016 Dynamics and bifurcations in a two-dimensional maps derived from a generalized ∆Δ-sine Gordon equation *Far East Journal of Dynamical Systems* 28 3 pp 165-194
[9] Shifrin L 2008 *Mathematica® Programming: an Advanced Introduction, Part I: the core language* (California: Wolfram Media Inc) pp 408