

# The Implementation of Digital Text Coding Algorithm Through A Three Dimensional Mapping Derived From Generalized $\Delta\Delta$ -MKDV Equation Using Mathematica

Notiragayu<sup>1, a\*</sup>, and L. Zakaria<sup>2, b</sup>

<sup>1</sup>Mathematics Department, University of Lampung, Bandar Lampung, Indonesia

<sup>2</sup> Mathematics Department, University of Lampung, Bandar Lampung, Indonesia

<sup>a</sup>notiragayu@fmipa.unila.ac.id, <sup>b</sup>lazakaria.1969@fmipa.unila.ac.id

## Abstract

Encryption-decryption algorithm using a mapping can be done for encoding a digital text, such as two dimensional mapping derived from generalized  $\Delta\Delta$ -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.

**Keywords:** digital text, 3-dimensional mapping, generalized  $\Delta\Delta$ -mKdV equation, 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 the use of mapping in cryptographic algorithms for text data. The mapping option used is a 3-dimensional nonlinear mapping derived from a generalized traveling wave solution  $\Delta\Delta$ -mKdV [9].

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

Look at the following nonlinear mapping:

( ini tempat untuk persamaan 1)

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.

For example: following text data

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.

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

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  $\alpha, \eta = 0$  and make it as the key value.

Decryption Stages

1. Reuse the parameter value  $\alpha, \eta = 0$  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 Decreased From The Generalized $\Delta\Delta$ -mKdV Equation**

3.1 The 2-Dimensional Periodic Mapping Formulation Derived from the generalized  $\Delta\Delta$ -mKdV Equation

Look at the family of four mapping parameters derived from the generalized  $\Delta\Delta$ -mKdV equation follows:

$$\theta_1 V_{l,m} V_{l,m+1} - \theta_2 V_{l+1,m} V_{l+1,m+1} - \theta_3 V_{l,m} V_{l+1,m} + \theta_4 V_{l,m+1} V_{l+1,m+1} = 0, \quad (2)$$

with  $\theta_1 = \alpha_1 \beta_2 p$ ,  $\theta_2 = \alpha_4 \beta_2 p$ ,  $\theta_3 = \alpha_2 \beta_1 q$  dan  $\theta_4 = \alpha_2 \beta_4 q$ .

Using the following transformation

$$V_{l,m} = V_n, \quad \text{with } n = z_1 l + z_2 m,$$

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

$$\theta_1 V_n V_{n+z_2} - \theta_2 V_{n+z_1} V_{n+z_1+z_2} - \theta_3 V_n V_{n+z_1} + \theta_4 V_{n+z_2} V_{n+z_1+z_2} = 0 \quad (3)$$

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  $z_1 \rightarrow -z_1$ ,  $p \rightarrow -p$ , and  $z_1 \leftarrow \rightarrow z_2$ . Besides that it also fulfills the periodic nature, namely  $(i + z_2, j - z_1)$  Equation (3) is equivalent to mapping

(ini adalah tempat untuk persamaan 4)

Select  $z_1 = 1$  and  $z_2 = 2$ . The third order differential equation of equation (4) can be stated as follows:

$$\theta_1 V_n V_{n+2} - \theta_2 V_{n+1} V_{n+3} - \theta_3 V_n V_{n+1} + \theta_4 V_{n+2} V_{n+3} = 0$$

which is equivalent to the following three-dimensional mapping:

(ini adalah tempat untuk persamaan 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  $\zeta_n$  is a line in  $R^2$  that is defined as

(ini adalah tempat untuk defenisi  $\zeta_n$ )

Suppose that  $\theta$  is a parameter vector in  $R^4$ :  $(\theta_1, \theta_2, \theta_3, \theta_4)$ . Therefore, three-dimensional statements can be reduced to a two-dimensional mapping, namely:

(ini adalah tempat untuk persamaan 6)

where  $y = \sqrt[n+1]$  and  $x = \sqrt[n+2]$ . It can be checked that the mapping in equation (6)  $\sqrt[n+1]$  has an integral (there is a function  $S: \mathbb{R}^2 \rightarrow \mathbb{R}$  so that  $S(n+1) = S(\zeta n)$  for all  $n \in \mathbb{N}$ ) [8].

### 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) [10].

Look at the descriptive algorithms presented in section 2. Against the text and 4-periodic mapping given in that section, the implementation of algorithms using Mathematica is as follows.

```
str1 = " From Wolfram: Mathematica's extensive base of state - of - the - art
        algorithms, efficient handling of very long integers,";
str2 = " and powerful built-in language make it uniquely suited to both
        research and implementation of cryptographic number theory.";
StringLength[str1]
StringLength[str2]
A=ToCharacterCode[str1] ; B=ToCharacterCode[str2] ;
AccountingForm[Grid[Partition[A, 10]]] ; AccountingForm[Grid[Partition[B, 10]]]
x = A; y = B; r = 3; alpha = 0.001234;
```

THIS SECTION IS A SUBROUTIN PROGRAM NAMED **coding1** FOR ITERATION PROCESSES  $g(A, B)$  TO THE R- ITERATION.

```
xx = SetPrecision[coding1[[r - 1, 2]], 10]; yy = SetPrecision[coding1[[r - 1, 1]], 10];
AccountingForm[Grid[Partition[xx, 5]]] ; AccountingForm[Grid[Partition[yy, 5]]] ;
```

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

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

70	114	111	109	32	87	111	108	102
114	97	109	58	32	77	97	116	104
101	109	97	116	105	99	97	39	115
32	101	120	116	101	110	115	105	118
101	32	98	97	115	101	32	111	102
32	115	116	97	116	101	32	45	32
111	102	32	45	32	116	104	101	32
45	32	97	114	116	32	97	108	103
111	114	105	116	104	109	115	44	32
101	102	102	105	99	105	101	110	116
32	104	97	110	100	108	105	110	103
32	111	102	32	118	101	114	121	32
108	111	110	103	32	105	110	116	101
32	97	110	100	32	112	111	119	101
114	102	117	108	32	98	117	105	108
116	45	105	110	32	108	97	110	103
117	97	103	101	32	109	97	107	101
32	105	116	32	117	110	105	113	117
101	108	121	32	115	117	105	116	101
100	32	116	111	32	98	111	116	104
32	114	101	115	101	97	114	99	104
32	97	110	100	32	105	109	112	108
101	109	101	110	116	97	116	105	111
110	32	111	102	32	99	114	121	112
116	111	103	114	97	112	104	105	99
32	110	117	109	98	101	114	32	116

**Figure 1:** conversion results of text data to numerical data before the mapping iteration process is carried out ( $g^0$ ).

In Figure 1 given the conversion of text data to numerical data before and after mapping the first iteration's process is used.

Out(129)/AccountingForm	(0.0000005508928571)	(0.000000115994165)	(0.0000001010647011)	(0.000000132110092)	(0.000001205078125)
	(0.000000126420361)	(0.0000001001542093)	(0.00000009601618425)	(0.000000197825665)	(0.0000009495229301)
	(0.000000124720599)	(0.00000009676154390)	(0.000000196997229)	(0.000001205078125)	(0.0000001435303472)
	(0.0000001087320469)	(0.0000001013136289)	(0.0000001098646724)	(0.000000105261998)	(0.0000002513900204)
	(0.0000001211895665)	(0.00000009670546395)	(0.0000003672619048)	(0.0000001154133932)	(0.0000001311510256)
	(0.0000002876486876)	(0.0000001041789785)	(0.0000003289940171)	(0.0000001299692256)	(0.0000000998918770)
	(0.000000105261998)	(0.0000000819069307)	(0.00000010291909092)	(0.0000001106230390)	(0.0000001098353630)
	(0.0000001035408626)	(0.0000000818069307)	(0.0000003672619048)	(0.0000001085515464)	(0.0000003975515464)
	(0.00000009171311780)	(0.000000110711071)	(0.0000003672619048)	(0.0000000983156741)	(0.0000001034020446)
	(0.0000000818069307)	(0.00000009939597462)	(0.00000008791678541)	(0.0000003975515464)	(0.0000000200374823)
	(0.0000001044262972)	(0.0000000672619048)	(0.000000263984674)	(0.0000000919069307)	(0.0000001117117112)
	(0.0000003780637255)	(0.000000324383448)	(0.0000002470470470)	(0.000001205078125)	(0.0000001085503167)
	(0.0000001068938569)	(0.000000103260498)	(0.0000003707932692)	(0.0000008569444444)	(0.0000003382675439)
	(0.0000001259569256)	(0.00000009412662090)	(0.000000103260498)	(0.0000003975515464)	(0.000000113594165)
	(0.0000001154133932)	(0.000000115979089)	(0.0000000474098099)	(0.000000113594165)	(0.0000001068938268)
	(0.0000001063793103)	(0.0000003707932692)	(0.0000001078200087)	(0.0000000964445880)	(0.0000002504058442)
	(0.0000003870601852)	(0.0000001209685228)	(0.0000001109911895)	(0.000000197825665)	(0.0000001068938268)
	(0.0000001074584488)	(0.0000001211595668)	(0.0000001068938268)	(0.0000001068938268)	(0.0000000989721653)
	(0.000000340581818)	(0.0000003707932692)	(0.0000001146094548)	(0.0000001099821747)	(0.0000003886250000)
	(0.0000001154133932)	(0.000000103091010)	(0.00000009211224643)	(0.0000001068938268)	(0.00000034333440)
	(0.0000001001542093)	(0.0000001174866914)	(0.0000003382675439)	(0.0000001078105895)	(0.0000001090876948)
	(0.0000001040823212)	(0.00000009712711581)	(0.0000000898502020)	(0.0000003870601852)	(0.0000001010647011)
	(0.0000000988189588)	(0.0000001095136011)	(0.0000000984948980)	(0.0000001163602074)	(0.00000009840510367)
	(0.000000324383448)	(0.000000103260498)	(0.0000001151979099)	(0.000000120969325)	(0.0000001191857112)
Out(130)/AccountingForm	(0.00000006798017857)	(0.00000001377062760)	(0.00000001247138411)	(0.00000001397023859)	(0.0000001487066406)
	(0.000000012762726)	(0.0000001230502590)	(0.0000000147816451)	(0.00000001171121296)	(0.00000001171121296)
	(0.0000001839070144)	(0.0000001194037481)	(0.00000002430964240)	(0.0000001487066406)	(0.00000002017964484)
	(0.0000001241783488)	(0.0000001280210181)	(0.00000001355730057)	(0.00000001299723455)	(0.0000000124097452)
	(0.0000001496096711)	(0.0000001193932445)	(0.00000004532011905)	(0.00000001424201272)	(0.0000001618403656)
	(0.0000000649547796)	(0.0000001285659594)	(0.0000000467150171)	(0.00000001554208662)	(0.0000001202003236)
	(0.0000001299723455)	(0.00000004711497525)	(0.00000001270021685)	(0.00000001355536046)	(0.0000001355536046)
	(0.0000001277694244)	(0.00000004711497525)	(0.00000004532011905)	(0.0000001339510908)	(0.00000004905786082)
	(0.0000001131739874)	(0.0000001370617462)	(0.00000004532011905)	(0.00000001214028542)	(0.00000001275881230)
	(0.00000004711497525)	(0.0000001228051530)	(0.00000001048489132)	(0.00000004905786082)	(0.0000001141496252)
	(0.000000128864708)	(0.00000004532011905)	(0.00000002917157088)	(0.00000004711497525)	(0.00000001371852252)
	(0.00000004665306973)	(0.00000004102252135)	(0.00000003048560561)	(0.0000001487066406)	(0.0000001399510908)
	(0.0000001131908704)	(0.0000001299723455)	(0.0000000457589942)	(0.0000001057469444)	(0.00000004174221491)
	(0.0000001554208662)	(0.0000000161522502)	(0.00000001299723455)	(0.00000004905786082)	(0.00000001377062760)
	(0.0000001424201272)	(0.00000001421542196)	(0.00000004287038288)	(0.00000001377062760)	(0.00000001318403463)
	(0.0000000131720690)	(0.0000000457589942)	(0.00000001330498908)	(0.00000001214803251)	(0.0000000309000117)
	(0.0000000406122858)	(0.0000001492711691)	(0.00000001366651229)	(0.00000001478116971)	(0.00000001315403463)
	(0.0000001325990495)	(0.0000001498096711)	(0.00000001299723455)	(0.00000001318403463)	(0.00000001182631252)
	(0.00000004326011364)	(0.0000000457589942)	(0.00000001414200672)	(0.00000001357180036)	(0.00000004758612500)
	(0.0000001424201272)	(0.0000000127144693)	(0.00000001144069121)	(0.00000001320003467)	(0.00000004102252135)
	(0.000000129952930)	(0.00000001469415872)	(0.00000004174221491)	(0.00000001320003466)	(0.00000001366142180)
	(0.0000001284375843)	(0.00000001198548603)	(0.0000000480679293)	(0.0000000406122858)	(0.00000001247138411)
	(0.00000001181182595)	(0.00000001386333838)	(0.00000004855727041)	(0.00000001438584960)	(0.00000001214318979)
	(0.00000004102252135)	(0.00000001299723455)	(0.00000001421542196)	(0.00000001492711691)	(0.0000000120379169)

**Figure 2:** The results of the conversion of text data to numeric data with the choice of parameter values  $\eta = 0.1234$  and  $\alpha = 0.001234$ , after the mapping iteration process is carried out on  $g^2$ .

### 3.3 ENCRYPTION-DECRYPTION ALGORITHM FOR SETTING DIGITAL TEXT USING MAPPING GENERALIZED $\Delta\Delta$ -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 SUBROUTIN OF NAMED **recoding1** PROGRAMS FOR ITERATION PROCESSES  $g^{-1}$  (AA, BB) TO R-ITERATION.

Flatten[FromCharCode[Round[recoding1[[r -1]]]]].

```

Out[269]/AccountingForm=
0.0001854984308 0.0001524393045 0.0001571058138 0.0001587254614 0.0001494793180
0.0001587254614 0.0001466320929 0.0004811365548 0.0001315929039 0.0001399669978
0.0001494793180 0.0001438913061 0.0001587254614 0.0001374675871 0.0001587254614
0.0001399669978 0.0004811365548 0.0001350558750 0.0001587254614 0.0001338814761
0.0001587254614 0.0004811365548 0.0001338814761 0.0001272427252 0.0001315929039
0.0001438913061 0.0001315929039 0.0001350558750 0.0004811365548 0.0001438913061
0.0001524393045 0.0001480420169 0.0001587254614 0.0001539636975 0.0001466320929
0.0001350558750 0.0001587254614 0.0001327273255 0.0004811365548 0.0002368672270
0.0001425589792 0.0001425589792 0.0001587254614 0.0001480420169 0.0003499174944

Out[270]/AccountingForm=
0.0001338814761 0.0001524393045 0.0001480420169 0.0001587254614 0.0001350558750
0.0001315929039 0.0001338814761 0.0001399669978 0.0001272427252 0.0001587254614
0.0004811365548 0.0001438913061 0.0001466320929 0.0001327273255 0.0001587254614
0.0004811365548 0.0001571058138 0.0001587254614 0.0001399669978 0.0001272427252
0.0001587254614 0.0001438913061 0.0004811365548 0.0001571058138 0.0001524393045
0.0001350558750 0.0001571058138 0.0001315929039 0.0001587254614 0.0001327273255
0.0004811365548 0.0001587254614 0.0001412510987 0.0001587254614 0.0001425589792
0.0004811365548 0.0001438913061 0.0001524393045 0.0001571058138 0.0001587254614
0.0001466320929 0.0001438913061 0.0001587254614 0.0001399669978 0.0003347036903

```

**Figure 3:** The results of the conversion of text data to numeric data with the value of the choice parameter  $\eta = 0.05234$ ,  $\alpha = 0.7125$ ,  $\beta = 6.7111$ , after the mapping iteration process is carried out on  $g^{-1}$ .

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

## 4. Conclusions

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  $\Delta\Delta$ -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.

## Acknowledgment

This research.....

## References

- [1] R. Sadikin, Cryptography for Network Security. Andi Publisher, 2012.
- [2] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions On Information Theory, IT-31 (4), 469-472, 1985.
- [3] M. Rinaldi, a selective encryption algorithm for digital images in the frequency domain based on chaos mutations. Electrical Engineering Journal, 10 (2), 66-72, 2012.
- [4] D. H. Arinten, A. Irawan, Digital Image Cryptography System on an Intranet Network Using the Method of Combining Chaos Maps and Selective Techniques. Ultimatics, 9 (1), 59-66, 2017.
- [5] P. Ronsen, H. Arwin, S. Indra, Encryption of digital images using Arnolds map paint and nonlinear chaotic algorithm. Mikroskil SIFO Journal, 15 (2), 61-71, 2014.
- [6] F. Al-Anshori, E. Ariwibowo, Implementation of ElGamal's public key cryptographic algorithm for encryption and decryption processes for securing data files. Journal of Undergraduate Engineering, 2 (2), 1-10, 2014.
- [7] L. Zakaria, J.M. Tuwankotta, Dynamics and bifurcations in a two-dimensional maps derived from a generalized  $\Delta\Delta$  sine – Gordon equation. Far East Journal of Dynamical Systems, 28(3), 165-194, 2016.
- [8] Zakaria, Notiragayu, A. Nuryaman, S. Suharsono, The Integral Normal Form Of A Three Dimensional Traveling Wave Solution Mapping Derived From Generalized  $\Delta\Delta$ -mKdV Equation. Advances in Differential Equations and Control Processes, 19(1), 37-48, 2018.
- [9] L. Zakaria, Cryptographic Development: Encoding Text Messages Through a Mapping 2-Dimension that can be reversed, symmetric, and periodic. National



Mathematics Conference (KNM) XIX, Brawijaya University, Malang, July 24-26, 2018.

- [10] L.Shifrin,Mathematica programming: an advanced Introduction, Part I :the core language. Wolfram Media,Inc.,2008.