Digital text and digital image encryption and steganography method based on SIYu map and least significant bit

Y Satria, Suryadi MT*, D J Cahyadi
Department of Mathematics, Faculty of Mathematics and Natural Sciences, Universitas Indonesia, Depok, 16424, Indonesia

E-mail*: yadi.mt@sci.ui.ac.id

Abstract. This paper focus on keeping data and information confidentiality on digital image based on chaotic system. In this paper, we use the unmodified SIYu map for the encryption and embedding process and use 3-3-2 LSB insertion method to embed data to cover image. This paper will show how is the result of encryption process and embedding process using SIYu map. Furthermore, we will show our algorithm performance based on randomness of sequence generated by SIYu map with NIST test and entropy test, histogram analysis, goodness of fit test, quality of the stego image, quality of decrypted data, initial value sensitivity, and key space. The results show encrypted data is uniformly distributed; sequence generated by SIYu map passes all NIST test and entropy test, which means the generated sequence is random; stego image have a good quality, it can be seen from the correlation coefficient and PSNR value more than 40 dB; decrypted data has the same quality as the original data; initial value sensitivity reaches $10^{-16}$; key space reaches $2^{56} \times 10^{94}$; and add noises can be optional to increase data confidentiality. For the conclusion, our algorithm can be used to keeping data and information confidentiality on digital image.

1. Introduction
There are many methods that can protect data confidentiality, cryptography and steganography are the examples of it. Cryptography is about protecting the content of messages while steganography is about concealing their existence [1]. Cryptography and steganography based on chaotic system has been used to secure digital data as in [2], [3], [4]. For the embedding method, we use 3-3-2 LSB insertion method as in [2]. Debiprasad et al. has used logistic map for image encryption and to embed encrypted image to cover image as in [2].

In this paper we use the unmodified SIYu map from [5] to generate key stream for encrypting and embedding process. The unmodified SIYu map shown at equation (1)

$$x_{n+1} = \frac{(2r - 4)(rp x_n)(p(1 - x_n)^2)}{(1 + p(1 - x_n)^2)^2} \times 2^{12} (mod 1)$$

where $r \in (0,2) \cup (2,4)$, $p \in (0,4)$ and $x_{n} \in (0,1)$.

The SIYu map as in equation (1) is chaotic. This can be concluded by the bifurcation diagram and Lyapunov Exponent. From the figure 1 we can conclude that bifurcation diagram of SIYu map is dense and lyapunov exponent value of SIYu map for $p = 3.1$ and $x_0 = 0.4$ positive for all $r$ except for $r = 2$. 
As a result, the value of all parameter we use on this paper for encryption, embedding, extracting, and decryption are $x_0 = 0.4$, $r = 3$, and $p = 3.1$.

![Image](https://via.placeholder.com/150)

**Figure 1.** Bifurcation diagram and lyapunov exponent of SIYu map for $p = 3.1$ and $x_0 = 0.4$

2. Methodology

In this section, the methodology used will be explained. The first is encryption and embedding algorithm and the second is extracting and decryption algorithm.

2.1. Encryption and embedding algorithm

Encryption and embedding process used in this paper can be seen in figure 2. Random sequence generated 2 times, the first sequence used for encryption process and the second sequence used for insertion coordinate. Encryption method used is XOR and insertion method used is 3-3-2 LSB insertion method. The encryption process result encrypted image will be used for the insertion. The final result of this algorithm is stego image.

![Diagram](https://via.placeholder.com/150)

**Figure 2.** Encryption and embedding algorithm

2.2. Extracting and decryption algorithm

Extracting and decryption algorithm’s purpose is to get back embedded data from stego image, as can be seen in figure 3. By using same parameter and initial value as used in encryption and embedding process, the same sequences generated for the extracting and decryption so that the extracted and decrypted data will be the same as the original.
3. Result and analysis
In this section, firstly, the randomness binary sequence generated by SIYu map will be tested using NIST test and ENT suite test for sequence randomness. After that, we show the encrypting and embedding algorithm, extracting and decrypting algorithm, and analyze its result with the testing data used in this paper.

3.1. NIST randomness test and entropy estimation test
NIST randomness test and entropy estimation test used to check randomness of sequence generated by SIYu map. NIST test suite consist of 16 statistical test as described in [6] and ENT test suite as used in [7]. The result of NIST randomness test is shown on table 1 and the result of entropy test is shown on table 2.

| Type of Test                                      | P-Value    | Conclusion |
|--------------------------------------------------|------------|------------|
| Frequency Test (Monobit)                         | 0.109598   | Random     |
| Frequency Test within a Block                    | 0.398877   | Random     |
| Run Test                                         | 0.676994   | Random     |
| Longest Run of Ones in a Block                   | 0.541977   | Random     |
| Binary Matrix Rank Test                          | 0.876714   | Random     |
| Discrete Fourier Transform (Spectral) Test       | 0.403676   | Random     |
| Non-Overlapping Template Matching Test           | 0.979097   | Random     |
| Overlapping Template Matching Test               | 0.865664   | Random     |
| Maurer’s Universal Statistical Test              | 0.893903   | Random     |
| Linear Complexity Test                           | 0.559562   | Random     |
| Serial Test                                      | 0.881340   | Random     |
| Approximate Entropy Test                         | 0.249136   | Random     |
| Cummulative Sums (Forward) Test                  | 0.936330   | Random     |
| Cummulative Sums (Reverse) Test                  | 0.162317   | Random     |
| Random Excursions Test                           | 0.111240   | Random     |
| Random Excursions Varian Test                    | 0.244427\* | Random     |
| Random Excursions Varian Test                    | 0.447612\* | Random     |

*average test value
Table 2. Entropy estimation test result of number sequence generated by SIYu map

| Test name                      | P-Value   |
|--------------------------------|-----------|
| Entropy                        | 7.999296  |
| Arithmetic mean                | 127.182843|
| Monte Carlo                    | 3.145786  |
| Chi Square                     | 292.058453|
| Serial correlation coefficient | 0.000652  |

3.2. Testing data

We use text and image as our testing data. Text testing data shown in figure 4 and figure 5. We use image as testing data with 4 different pixel size as shown in figure 6. For the cover image data, we use image as shown in figure 7. The details of the data shown in table 3.

![Figure 4. Digital text data indonesiaraya.txt](image1)

![Figure 5. Digital text data sumpahpemuda.txt](image2)

![Figure 6. Digital image data lena.png](image3)

![Figure 7. Digital image data pepper.png as cover image](image4)
Table 3. List of data used

| Data Name        | Type               | Data | Size                      |
|------------------|--------------------|------|---------------------------|
| pepper.png       | Image as Cover     | 1    | 1024 × 1024 pixels        |
| lena.png         | Image              | 2    | 512 × 512 pixels          |
| lena.png         | Image              | 3    | 256 × 256 pixels          |
| lena.png         | Image              | 4    | 100 × 100 pixels          |
| lena.png         | Image              | 5    | 52 × 52 pixels            |
| indonesiaraya.txt| Text               | 6    | 1640 characters           |
| sumpahpemuda.txt | Text               | 7    | 348 characters            |

3.3. Algorithm’s result and performance

3.3.1. Histogram analysis.
The distribution of encrypted data (cipher) will be tested by using goodness of fit test as described in [8]. The examples of encrypted data can be seen on figure 8. The test result of cipher image shown on table 4 and the test result of cipher text shown on table 5.

Because of the data we use are digital texts and digital images, the degrees of freedom of goodness of fit test is 256 – 1 = 255 and we choose 1% significance level, so we obtained 310.457388 as critical value. From table 4 and table 5, all the test statistics values are less than the critical value, then we conclude that the distribution of encrypted data’s values are uniform. From the histograms of encrypted data (see on figure 10 and figure 11), we also conclude that encrypted data’s values are uniform since the histograms of encrypted data are flat-like.

Table 4. Test statistic value of cipher image

| Data | Test Statistic Value | Red        | Green       | Blue        |
|------|----------------------|------------|-------------|-------------|
|      |                      | 2          | 3           | 4           | 5           |
| 2    |                      | 246.744141 | 246.101563  | 270.701172  |
| 3    |                      | 235.500000 | 280.117188  | 251.757813  |
| 4    |                      | 245.630000 | 273.075200  | 233.753600  |
| 5    |                      | 255.526627 | 251.739644  | 211.408284  |

Table 5. Test statistic value of cipher text

| Data | Test Statistic Value |
|------|----------------------|
| 6    | 274.380488           |
| 7    | 241.977011           |
3.3.2. Stego image quality analysis.
Stego image and original cover image will be compared by Peak Signal-to-Noise Ratio (PSNR). Firstly, we want to show some stego images as the results of our algorithm that will be compared with the original cover image. From the figure 11, we conclude the stego image and the original cover image look similar, which means data successfully concealed in the stego image.

The statistics comparison used is Peak Signal-to-Noise Ratio which described in [9] with formula $PSNR = 10 \log_{10} \frac{MAX^2}{MSE}$ where $MAX = 255$ and MSE is Mean Squared Error which described in [10] with formula $MSE = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (A_{i,j} - B_{i,j})^2$, $M$ is the height of digital image and $N$ is the width of digital image and $A_{i,j}$ and $B_{i,j}$ are the $(i,j)$ value of original cover image $A$ and stego image $B$, respectively. If $PSNR = \infty$, it means the value of original cover image and stego image are exactly same and have the same quality. If PSNR values more than 40dB, it means the quality of stego image is good [10]. The result of this test shown on table 6.
Table 6. MSE and PSNR value of stego image

| Data in Stego Image | MSE    | PSNR   |
|---------------------|--------|--------|
| Data 2              | 6.02947| 40.3280|
| Data 3              | 1.50014| 46.36949|
| Data 4              | 0.22861| 54.53985|
| Data 5              | 0.06288| 60.14533|
| Data 6              | 0.01217| 67.27683|
| Data 7              | 0.00267| 73.85546|

We also compare the horizontal, vertical, and diagonal correlation coefficient of original cover image and stego image as described in [11]. We compare correlation coefficient of Data 1 (original cover image) with the stego images. Using python we obtained:

Table 7. Correlation coefficient of original cover image

|           | Horizontal | Vertical | Diagonal |
|-----------|------------|----------|----------|
|           | Red        | Green    | Blue     | Red        | Green    | Blue     | Red        | Green    | Blue     |
| Data 2    | 0.98179    | 0.99057  | 0.98328  | 0.98319    | 0.99090  | 0.98328  | 0.97159    | 0.98291  | 0.97025  |

Table 8. Correlation coefficient of stego image

| Data in stego image | Horizontal | Vertical | Diagonal |
|---------------------|------------|----------|----------|
|                     | Red        | Green    | Blue     | Red        | Green    | Blue     | Red        | Green    | Blue     |
| 2                   | 0.9817     | 0.99055  | 0.9832   | 0.98317    | 0.9908   | 0.9832   | 0.97159    | 0.9829    | 0.9702   |
| 3                   | 0.9816     | 0.9905   | 0.9832   | 0.9830     | 0.9905   | 0.9832   | 0.9714     | 0.9829    | 0.9702   |
| 4                   | 0.9809     | 0.9902   | 0.9830   | 0.9822     | 0.9905   | 0.9830   | 0.9706     | 0.9825    | 0.9700   |
| 5                   | 0.9787     | 0.9894   | 0.9825   | 0.9801     | 0.9898   | 0.9824   | 0.9682     | 0.9817    | 0.9694   |
| 6                   | 0.9817     | 0.9905   | 0.9832   | 0.9831     | 0.9908   | 0.9832   | 0.9715     | 0.9829    | 0.9702   |
| 7                   | 0.9817     | 0.9905   | 0.9832   | 0.9831     | 0.9908   | 0.9832   | 0.9715     | 0.9829    | 0.9702   |

From table 7 and table 8, we conclude the values correlation coefficient between stego image and the original cover image are similar, which means the stego image and original cover image statistically similar. From our algorithm’s results on figure 12, figure 13, figure 14, table 6, table 7, and table 8 can be concluded that our algorithm successfully keep data confidentiality visually and statistically.

3.3.3. Decrypted object quality analysis.
For decrypted digital image, we will compare its PSNR and MSE value with the original one. The result shown on table 9.

Table 9. MSE and PSNR value of extracted and decrypted digital image

| Data   | MSE    | PSNR   |
|--------|--------|--------|
| 2      | 0      | ∞      |
| 3      | 0      | ∞      |
| 4      | 0      | ∞      |
| 5      | 0      | ∞      |

For decrypted digital text, we will compare its MSE value with the original digital text. MSE value of digital text will be calculated with formula \( MSE = \frac{1}{M} \sum_{i=0}^{M-1} (A_i - B_i)^2 \) where \( M \) is total character in the text, \( A_i \) and \( B_i \) are the value of original digital text and decrypted digital text, respectively. The result shown on table 10.
From the tests result on table 9 and table 10, it can be seen that all of MSE value of extracted and decrypted data is 0, which means the extracted and decrypted data are statistically the same with the original data. We conclude that our algorithm can get the embedded data back.

3.3.4. Initial value key sensitivity analysis

In this subsection, after extraction process of Data 7 from the stego image, we will try to decrypt the encrypted Data 7 with 4 different values of $x_0$ while other parameters use the same values. For the encryption we used $x_0 = 0.4$ and for the decryption we use 4 different values as shown in table 11.

| Data | MSE |
|------|-----|
| 6    | 0   |
| 7    | 0   |

From table 11, we seen the original digital text will be obtained when $x_0 = 0.4$ and also when it reached $0.4 + 10^{-17}$. We may conclude that the sensitivity of $x_0$ from this algorithm reaches $10^{-16}$.
3.3.5. Key space analysis

In encryption algorithm using SIYu map, we use \( x_0, r, \) and \( p \) as parameters and in embedding algorithm using SIYu map we also use it. From subsection 3.3.4 we seen that sensitivity of \( x_0 \) reaches \( 10^{-16} \) (table 11) where \( x_0 \in (0, 1) \). For the \( r \) and \( p \) parameters, its sensitivity reach \( 10^{-15} \) (it can be seen on table 12 and table 13) where \( r \in (0, 2) \cup (2, 4) \) and \( p \in (0, 4) \). So the key space of our algorithm is,
\[
(10^{16})^2 \times (4 \times 10^{15})^4 = 256 \times 10^{92} = 2.56 \times 10^{94}
\]

4. Noise added experiment in encrypted data

This section explain decryption algorithm result if noise added in encrypted data. The purpose of this experiment is to get insight the quality of decrypted image if noise added in encrypted data. We will use MSE statistical test for the text and MSE and PSNR statistical test for the image.

In this experiment, the value of encrypted data will be added by random number generated so the value of encrypted data will be changed. The random number will be generated by using python. For this experiment, we will generate random integer from -2 to 2 and from -10 to 10 with designated seed so that the random number generated will be exactly the same every time generated. The size of generated image will be adjusted as the size of the data. After adding encrypted data value with random generated integer, the encrypted data will be decrypted.

We will decrypt data 4 and data 7 with random integer from -10 to 10 added in it as the example shown in figure 15 and figure 16. From figure 15, some color spots can be seen. Compared with its original image (figure 6), the quality of decrypted image is poor because of the color spot eventhough the part of original image still can be seen. From figure 16, the decrypted text completely different with the original one. For the statistical test can be seen in table 14 and table 15.

![Figure 15. Decrypted result of encrypted data 4 with random integer added in It](image)

![Figure 16. Decrypted result of encrypted data 7 with random integer added in It](image)

| Table 14. MSE value of decrypted text with random integer added |
|---------------|-----------------|-----------------|
| Data  | MSE | Added Random Integer -2 to 2 | Added Random Integer -10 to 10 |
| 6    | 170 | 635  |
| 7    | 123 | 544  |

| Table 15. MSE and PSNR value of decrypted data with random integer added |
|---------------|-----------------|-----------------|
| Data  | MSE / PSNR | Added Random Integer -2 to 2 | Added Random Integer -10 to 10 |
| 2    | 160.3171 / 26.0810 | 674.0951 / 19.8436 |
| 3    | 158.6526 / 26.1263 | 670.1817 / 19.8689 |
| 4    | 164.7867 / 25.9621 | 677.0162 / 19.8248 |
| 5    | 142.3148 / 26.5983 | 625.8968 / 20.1658 |
From table 14 and table 15, it can be seen that the quality of data that added with noises used is poor, especially for text data. We may conclude that if encrypted data added with noises it will make the decrypted data changed and the noise of data needed to be extracted first to get the original data.

5. Conclusion
From the result above we conclude that:

- Cryptography and steganography based on SIYu map with 3-3-2 LSB insertion method can be used to secure data.
- From the result of NIST test and ENT suite test, the sequences generated by SIYu map are random.
- The distribution of cipher image’s pixel values and cipher text’s character values are uniform, it can be seen from its histogram and goodness of fit test.
- The quality of stego image is good, it can be seen from its PSNR value, and correlation coefficient values of each stego image are similar with the correlation coefficient values of original cover image. It means stego image and original cover image have a similar looks.
- Extracted and decrypted digital image and digital text have the same values as the original one, it can be seen from its MSE values are equal 0, means the algorithm used in this research successfully secure the data.
- Our algorithm’s initial value key sensitivity reaches $10^{-16}$, parameters $p$ and $r$ sensitivity reach $10^{-15}$, and the key space reaches $2^{56} \times 10^{94}$.
- Encrypted data added with noises will make the decryption result poor, so it can be optional to secure data more confidential.

Acknowledgment
This research is funded by Directorate of research and community engagements Universitas Indonesia in the Hibah PUTI Proceedings scheme with contract No. NKB-929/UN2.RST/HKP.05.00/2020.

References
[1] Fabien A P P, Ross J A and Markus G K 1999 Information Hiding-A Survey Proceedings of the IEEE, special issue of protection of multimedia content 87 1062-78
[2] Debiprasad B, Kousik D, Jyotsna K M, and Paramartha D 2014 A Novel Secure Image Steganography Method Based on Chaos Theory in Spatial Domain International Journal of Security, Privacy and Trust Management (IJSPTM) 3 11-22
[3] Bhaskar M and Tarni M 2013 A Multilevel Security Scheme Using Chaos Based Encryption and Steganography for Secure Audio Communication International Journal of Research in Engineering and Technology 2 399-403
[4] Melad J S 2013 A New Technique Based on Chaotic Steganography and Encryption Text in DCT Domain for Color Image Journal of Engineering Science and Technology 8 508-20
[5] Satria Y, Suryadi MT, Ita M S, Luqman N P and Venny M 2020 The Composition of The Improved Logistic Map and The MS Map in Generating a New Chaotic Function Journal of Physics: Conference Series 1490 012046
[6] Andrew R, Juan S, et al. 2010 A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications NIST Special Publication 800-22
[7] Milad Y V, Milad J B, Peyman A and Maryam 2019 An Integer Wavelet Transform Image Steganography Method Based on 3D Sine Chaotic Map Multimedia Tools and Applications 78 9971-89
[8] Walpole R E, Myers R H, Myers S L and Ye K 2012 Probability and Statistics for Engineers & Scientists (9th edition) Boston: Prentice Hall
[9] Amit V and Iqbaldeep K 2013 Techniques and Algorithm Design for the Detection of PSNR in Digital Image International Journal of Computer Applications (0975-8887): National Conference on Structuring Innovation Through Quality SITQ 2013 33-5
[10] Abbas C, et al. 2010 Digital Image Steganography: Survey and Analysis of Current Methods *Signal Processing* **90** 727-52

[11] William M and Terry S A Second Course in Statistics Regression Analysis (7th edition) *United States: Pearson Education, Inc.*