A Cryptographic Algorithm based on Max Plus Wavelet Transform

Joko Cahyono
Subiono

March 2, 2016

Introduction

- Cryptography is one of the tools to secure information.
- Many varieties of cryptographic algorithms have been constructed.
- Goswami et al proposed cryptographic algorithm based on discrete wavelet transform. They used Daubechies wavelet transform.
- Grigoriev and Shpilrain, Durcheva in their papers discussed the use of max plus algebra and min plus algebra in cryptography. Max plus algebra and min plus algebra are used for key generating.

Introduction

- Cryptography is one of the tools to secure information.
- Many varieties of cryptographic algorithms have been constructed.
- Goswami et al proposed cryptographic algorithm based on discrete wavelet transform. They used Daubechies wavelet transform.
- Grigoriev and Shpilrain, Durcheva in their papers discussed the use of max plus algebra and min plus algebra in cryptography. Max plus algebra and min plus algebra are used for key generating.

Introduction

- Cryptography is one of the tools to secure information.
- Many varieties of cryptographic algorithms have been constructed.
- Goswami et al proposed cryptographic algorithm based on discrete wavelet transform. They used Daubechies wavelet transform.
- Grigoriev and Shpilrain, Durcheva in their papers discussed the use of max plus algebra and min plus algebra in cryptography. Max plus algebra and min plus algebra are used for key generating.

Introduction

- Cryptography is one of the tools to secure information.
- Many varieties of cryptographic algorithms have been constructed.
- Goswami et al proposed cryptographic algorithm based on discrete wavelet transform. They used Daubechies wavelet transform.
- Grigoriev and Shpilrain, Durcheva in their papers discussed the use of max plus algebra and min plus algebra in cryptography. Max plus algebra and min plus algebra are used for key generating.

Introduction

- Fahim constructed wavelet transform using max plus algebra. The advantage of max plus wavelet transform is not involve floating point, so it becomes simple and efficient for computing.
- In this paper we constructed a cryptographic algorithm based on max plus wavelet transform. We used max plus wavelet transform type A. Max plus wavelet transform is used for encryption, decryption and key generating.
- The feasibility of the proposed algorithm will be tested. The analysis is done using the running time and the correlation value between plaintext and ciphertext.

Introduction

- Fahim constructed wavelet transform using max plus algebra. The advantage of max plus wavelet transform is not involve floating point, so it becomes simple and efficient for computing.
- In this paper we constructed a cryptographic algorithm based on max plus wavelet transform. We used max plus wavelet transform type A. Max plus wavelet transform is used for encryption, decryption and key generating.
- The feasibility of the proposed algorithm will be tested. The analysis is done using the running time and the correlation value between plaintext and ciphertext.

Introduction

- Fahim constructed wavelet transform using max plus algebra. The advantage of max plus wavelet transform is not involve floating point, so it becomes simple and efficient for computing.
- In this paper we constructed a cryptographic algorithm based on max plus wavelet transform. We used max plus wavelet transform type A. Max plus wavelet transform is used for encryption, decryption and key generating.
- The feasibility of the proposed algorithm will be tested. The analysis is done using the running time and the correlation value between plaintext and ciphertext.

Wavelet Transform

- The wavelet transform is used in signal processing.
- The analysis operation is done on the main signals that have high resolution to obtain the approximation signal and detail signals.
- The approximation signal represents the main signals but has a lower resolution.
- The detail signals ensure that the main signals can be recovered by the synthesis process.

Wavelet Transform

- The wavelet transform is used in signal processing.
- The analysis operation is done on the main signals that have high resolution to obtain the approximation signal and detail signals.
- The approximation signal represents the main signals but has a lower resolution.
- The detail signals ensure that the main signals can be recovered by the synthesis process.

Wavelet Transform

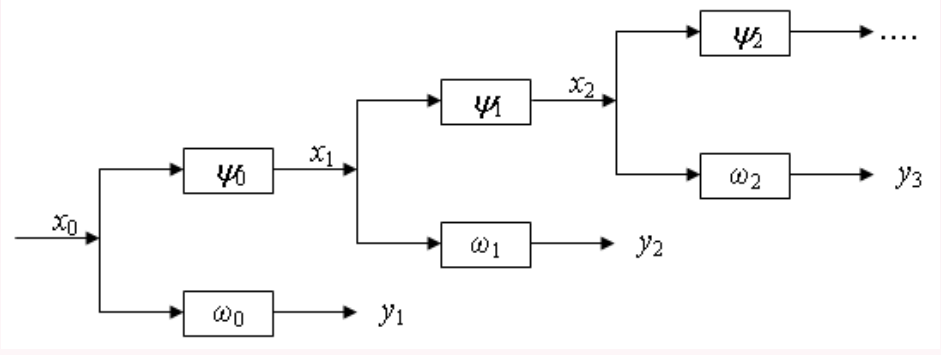
- The wavelet transform is used in signal processing.
- The analysis operation is done on the main signals that have high resolution to obtain the approximation signal and detail signals.
- The approximation signal represents the main signals but has a lower resolution.
- The detail signals ensure that the main signals can be recovered by the synthesis process.

Wavelet Transform

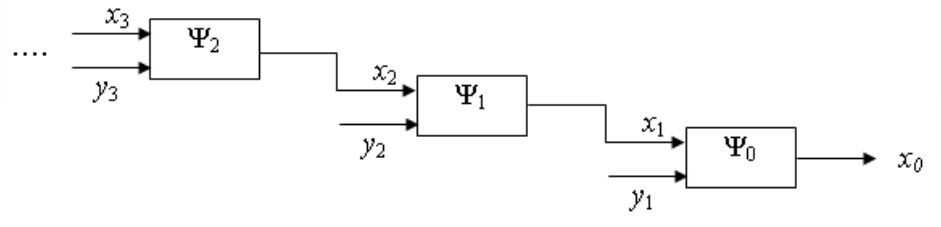
- The wavelet transform is used in signal processing.
- The analysis operation is done on the main signals that have high resolution to obtain the approximation signal and detail signals.
- The approximation signal represents the main signals but has a lower resolution.
- The detail signals ensure that the main signals can be recovered by the synthesis process.

Wavelet Transform

The Wavelet Transform Scheme Analysis Process



Synthesis Process



Max Plus Wavelet Transform

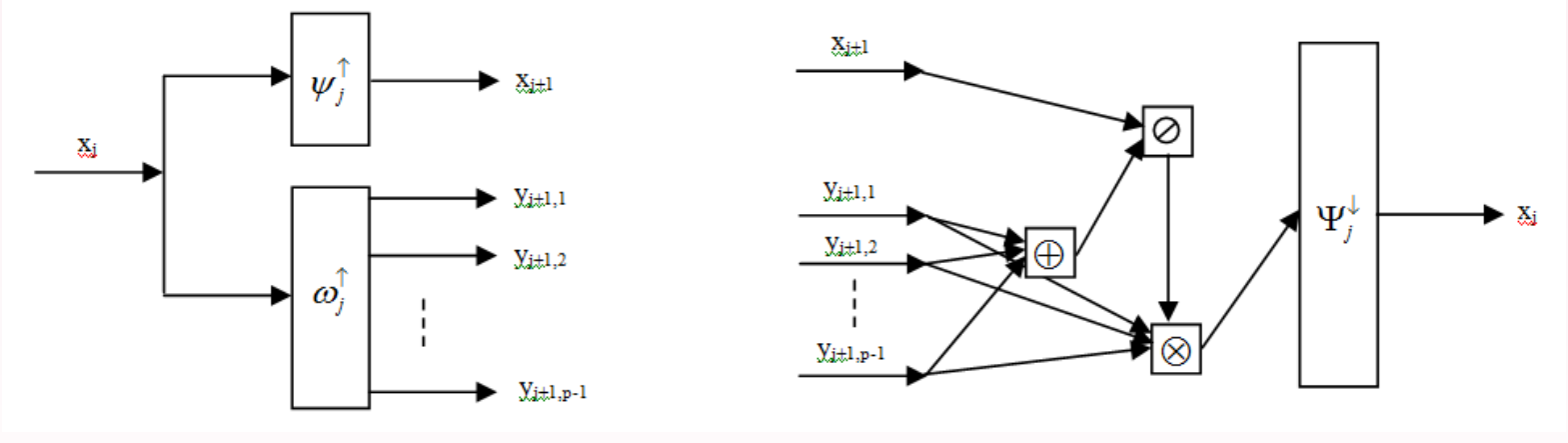
- Based on wavelet transform and max plus algebra, Fahim constructed wavelet transform using max plus algebra. Max plus algebra is algebra structure that involves only maximum and addition operation. Fahim constructed five types of max plus wavelet transform.
- In type A, there are analysis operations $\psi_j^{\uparrow}$ and $\omega_j^{\uparrow}$, and synthesis operation $\Psi_j^{\downarrow}$. In analysis operation, input are p signals, while output are an approximation signal and p-1 detail signals. In synthesis operation, input are an approximation signal and p-1 detail signals, while output are p signals.

Max Plus Wavelet Transform

- Based on wavelet transform and max plus algebra, Fahim constructed wavelet transform using max plus algebra. Max plus algebra is algebra structure that involves only maximum and addition operation. Fahim constructed five types of max plus wavelet transform.
- In type A, there are analysis operations $\psi_j^{\uparrow}$ and $\omega_j^{\uparrow}$, and synthesis operation $\Psi_j^{\downarrow}$. In analysis operation, input are p signals, while output are an approximation signal and p-1 detail signals. In synthesis operation, input are an approximation signal and p-1 detail signals, while output are p signals.

Max Plus Wavelet Transform

The Scheme of Max Plus Wavelet Transform Type A Analysis Process and Synthesis Process



Max Plus Wavelet Transform

Based on max plus wavelet transform scheme, analysis operation are constructed as follows:

$$\begin{aligned}
\psi_j^{\uparrow}(x_j)[n] &= \bigoplus_{k=0}^{p-1} x_j[pn+k] = x_{j+1}[n] \\
\omega_j^{\uparrow}(x_j)[n] &= y_{j+1}[n] \\
&= (y_{j+1,1}[n], y_{j+1,2}[n], \ldots, y_{j+1,p-1}[n]) \\
&= (\omega_{j,1}^{\uparrow}(x_j)[n], \omega_{j,2}^{\uparrow}(x_j)[n], \ldots, \omega_{j,p-1}^{\uparrow}(x_j)[n])
\end{aligned}$$

with

$$\omega_{j,r}^{\uparrow}(x_j)[n] = x_j[pn+r] \oslash x_j[pn] = y_{j+1,r}[n]$$

Max Plus Wavelet Transform

While synthesis operation are constructed as follows:

$$\begin{aligned}
\Psi_j^{\downarrow}(x_{j+1}, y_{j+1})[pn] &= x_{j+1}[n] \oslash [(\bigoplus_{k=1}^{p-1} y_{j+1,k}[n]) \oplus 0] \\
\Psi_j^{\downarrow}(x_{j+1}, y_{j+1})[pn+r] &= \Psi_j^{\downarrow}(x_{j+1}, y_{j+1})[pn] \otimes y_{j+1,r}[n], \\
&\quad \text{with } r = 1, 2, ..., p-1
\end{aligned}$$

Construction Of Cryptographic Algorithm

Encryption Technique

- The message is converted into ASCII code and then it is stored in array **PlainASCII**.
- The first element of the key is entered. It is the number of the channels used.
- The **PlainASCII** is put into the analysis process using number of the channels correspond to the key.
- The approximation signal, detail signals and the second element of the key are obtained from the analysis process. The process of key generating will explained in the next subsection.

Construction Of Cryptographic Algorithm

Encryption Technique

- The message is converted into ASCII code and then it is stored in array **PlainASCII**.
- The first element of the key is entered. It is the number of the channels used.
- The **PlainASCII** is put into the analysis process using number of the channels correspond to the key.
- The approximation signal, detail signals and the second element of the key are obtained from the analysis process. The process of key generating will explained in the next subsection.

Construction Of Cryptographic Algorithm

Encryption Technique

- The message is converted into ASCII code and then it is stored in array **PlainASCII**.
- The first element of the key is entered. It is the number of the channels used.
- The **PlainASCII** is put into the analysis process using number of the channels correspond to the key.
- The approximation signal, detail signals and the second element of the key are obtained from the analysis process. The process of key generating will explained in the next subsection.

Construction Of Cryptographic Algorithm

Encryption Technique

- The message is converted into ASCII code and then it is stored in array **PlainASCII**.
- The first element of the key is entered. It is the number of the channels used.
- The **PlainASCII** is put into the analysis process using number of the channels correspond to the key.
- The approximation signal, detail signals and the second element of the key are obtained from the analysis process. The process of key generating will explained in the next subsection.

Construction Of Cryptographic Algorithm

Encryption Technique

- The message is converted into ASCII code and then it is stored in array **PlainASCII**.
- The first element of the key is entered. It is the number of the channels used.
- The **PlainASCII** is put into the analysis process using number of the channels correspond to the key.
- The approximation signal, detail signals and the second element of the key are obtained from the analysis process. The process of key generating will explained in the next subsection.

Construction Of Cryptographic Algorithm

Encryption Technique

- The approximation signal and the absolute value of the detail signals are stored in array **CipherASCII**.
- **CipherASCII** is converted into text and then it is stored in variable **Ciphertext**.
  Then Ciphertext and the key will be sent to the receiver.

Construction Of Cryptographic Algorithm

Encryption Technique

- The approximation signal and the absolute value of the detail signals are stored in array **CipherASCII**.
- **CipherASCII** is converted into text and then it is stored in variable **Ciphertext**.
  Then Ciphertext and the key will be sent to the receiver.

Construction Of Cryptographic Algorithm

Encryption Technique

- The approximation signal and the absolute value of the detail signals are stored in array **CipherASCII**.
- **CipherASCII** is converted into text and then it is stored in variable **Ciphertext**.
  Then Ciphertext and the key will be sent to the receiver.

Construction Of Cryptographic Algorithm

Key Generating

The cryptographic key consists of two elements. The first element is the number of the channels used. The second element is the code for the detail signals. The second element of the key is generated as follows:

- The negative detail signal is given code 1, while positive is given code 0.
- Every 8 number of the code will be transformed to a binary number, and also for the rest of the code.
- The binary numbers are converted into integers. The integers are the second element of the key.

Construction Of Cryptographic Algorithm

Key Generating

The cryptographic key consists of two elements. The first element is the number of the channels used. The second element is the code for the detail signals. The second element of the key is generated as follows:

- The negative detail signal is given code 1, while positive is given code 0.
- Every 8 number of the code will be transformed to a binary number, and also for the rest of the code.
- The binary numbers are converted into integers. The integers are the second element of the key.

Construction Of Cryptographic Algorithm

Key Generating

The cryptographic key consists of two elements. The first element is the number of the channels used. The second element is the code for the detail signals. The second element of the key is generated as follows:

- The negative detail signal is given code 1, while positive is given code 0.
- Every 8 number of the code will be transformed to a binary number, and also for the rest of the code.
- The binary numbers are converted into integers. The integers are the second element of the key.

Construction Of Cryptographic Algorithm

Key Generating

The cryptographic key consists of two elements. The first element is the number of the channels used. The second element is the code for the detail signals. The second element of the key is generated as follows:

- The negative detail signal is given code 1, while positive is given code 0.
- Every 8 number of the code will be transformed to a binary number, and also for the rest of the code.
- The binary numbers are converted into integers. The integers are the second element of the key.

Construction Of Cryptographic Algorithm

Decryption Technique

- The encrypted message (Ciphertext) is converted into ASCII code and then it is stored in array **CipherASCII**.
- The cryptographic key is entered.
- The first element of the key is extracted to get the number of the channels used. The rest of the key is taken as the second element of the key. It is converted into binary number.
- The detail signals can be obtained using the binary number. While the approximation signal is the first number of CipherASCII.

Construction Of Cryptographic Algorithm

Decryption Technique

- The encrypted message (Ciphertext) is converted into ASCII code and then it is stored in array **CipherASCII**.
- The cryptographic key is entered.
- The first element of the key is extracted to get the number of the channels used. The rest of the key is taken as the second element of the key. It is converted into binary number.
- The detail signals can be obtained using the binary number. While the approximation signal is the first number of CipherASCII.

Construction Of Cryptographic Algorithm

Decryption Technique

- The encrypted message (Ciphertext) is converted into ASCII code and then it is stored in array **CipherASCII**.
- The cryptographic key is entered.
- The first element of the key is extracted to get the number of the channels used. The rest of the key is taken as the second element of the key. It is converted into binary number.
- The detail signals can be obtained using the binary number. While the approximation signal is the first number of CipherASCII.

Construction Of Cryptographic Algorithm

Decryption Technique

- The encrypted message (Ciphertext) is converted into ASCII code and then it is stored in array **CipherASCII**.
- The cryptographic key is entered.
- The first element of the key is extracted to get the number of the channels used. The rest of the key is taken as the second element of the key. It is converted into binary number.
- The detail signals can be obtained using the binary number. While the approximation signal is the first number of CipherASCII.

Construction Of Cryptographic Algorithm

Decryption Technique

- The encrypted message (Ciphertext) is converted into ASCII code and then it is stored in array **CipherASCII**.
- The cryptographic key is entered.
- The first element of the key is extracted to get the number of the channels used. The rest of the key is taken as the second element of the key. It is converted into binary number.
- The detail signals can be obtained using the binary number. While the approximation signal is the first number of CipherASCII.

Construction Of Cryptographic Algorithm

Decryption Technique

- The approximation signal and detail signals are put into the synthesis process using number of the channels correspond to the key.
- The main signals are obtained from the synthesis process and these are stored in array **PlainASCII**.
- The original messages can be retrieved by transform **PlainASCII** to their corresponding ASCII characters.

Construction Of Cryptographic Algorithm

Decryption Technique

- The approximation signal and detail signals are put into the synthesis process using number of the channels correspond to the key.
- The main signals are obtained from the synthesis process and these are stored in array **PlainASCII**.
- The original messages can be retrieved by transform **PlainASCII** to their corresponding ASCII characters.

Construction Of Cryptographic Algorithm

Decryption Technique

- The approximation signal and detail signals are put into the synthesis process using number of the channels correspond to the key.
- The main signals are obtained from the synthesis process and these are stored in array **PlainASCII**.
- The original messages can be retrieved by transform **PlainASCII** to their corresponding ASCII characters.

Construction Of Cryptographic Algorithm

Decryption Technique

- The approximation signal and detail signals are put into the synthesis process using number of the channels correspond to the key.
- The main signals are obtained from the synthesis process and these are stored in array **PlainASCII**.
- The original messages can be retrieved by transform **PlainASCII** to their corresponding ASCII characters.

Results And Discussion

- This program works perfectly for the text format i.e. **.txt** files.
- For example, the original message ”**Shabieq El-Fathin Attaraufaa’** ”.
- Using the first element of the key [2 3 5], be obtained the ciphertext ”’ **(++I&!%K+& ”4=5!$qG93!nS31**/ ”’ and the second element of the key i.e. [11 216 194 29].
- Decryption process is done by the key i.e. [2 3 5 11 216 194 29].

Results And Discussion

- This program works perfectly for the text format i.e. **.txt** files.
- For example, the original message ”**Shabieq El-Fathin Attaraufaa’** ”.
- Using the first element of the key [2 3 5], be obtained the ciphertext ”’ **(++I&!%K+& ”4=5!$qG93!nS31**/ ”’ and the second element of the key i.e. [11 216 194 29].
- Decryption process is done by the key i.e. [2 3 5 11 216 194 29].

Results And Discussion

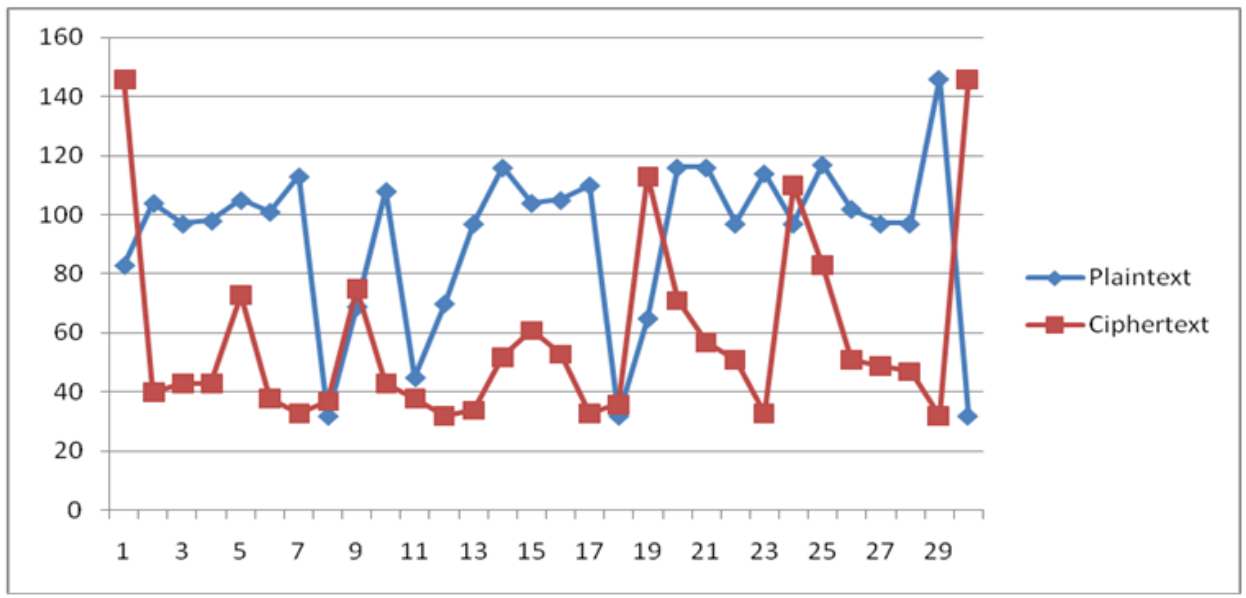
- This program works perfectly for the text format i.e. **.txt** files.
- For example, the original message ”**Shabieq El-Fathin Attaraufaa’** ”.
- Using the first element of the key [2 3 5], be obtained the ciphertext ”’ **(++I&!%K+& ”4=5!$qG93!nS31**/ ”” and the second element of the key i.e. [11 216 194 29].
- Decryption process is done by the key i.e. [2 3 5 11 216 194 29].

Results And Discussion

- This program works perfectly for the text format i.e. **.txt** files.
- For example, the original message ”**Shabieq El-Fathin Attaraufaa’** ”.
- Using the first element of the key [2 3 5], be obtained the ciphertext ”’ **(++I&!%K+& ”4=5!$qG93!nS31**/ ”” and the second element of the key i.e. [11 216 194 29].
- Decryption process is done by the key i.e. [2 3 5 11 216 194 29].

Results And Discussion

The Contrast between Plaintext and Ciphertext



Results And Discussion

- One of the cryptographic algorithm criteria is the level of confusion and diffusion.
- The level of confusion can be determined by calculate the correlation value between the plaintext and ciphertext.
- The correlation value in this experiment is 0.126543374.
- Each character on the plaintext transforms to different character in the ciphertext, and there is no direct relationship between the plaintext and the ciphertext.
- The message has some repeated characters, and every time the resulted cipher is different from the other.
- These indicate that the proposed algorithm has high confusion and diffusion.

Results And Discussion

- One of the cryptographic algorithm criteria is the level of confusion and diffusion.
- The level of confusion can be determined by calculate the correlation value between the plaintext and ciphertext.
- The correlation value in this experiment is 0.126543374.
- Each character on the plaintext transforms to different character in the ciphertext, and there is no direct relationship between the plaintext and the ciphertext.
- The message has some repeated characters, and every time the resulted cipher is different from the other.
- These indicate that the proposed algorithm has high confusion and diffusion.

Results And Discussion

- One of the cryptographic algorithm criteria is the level of confusion and diffusion.
- The level of confusion can be determined by calculate the correlation value between the plaintext and ciphertext.
- The correlation value in this experiment is 0.126543374.
- Each character on the plaintext transforms to different character in the ciphertext, and there is no direct relationship between the plaintext and the ciphertext.
- The message has some repeated characters, and every time the resulted cipher is different from the other.
- These indicate that the proposed algorithm has high confusion and diffusion.

Results And Discussion

- One of the cryptographic algorithm criteria is the level of confusion and diffusion.
- The level of confusion can be determined by calculate the correlation value between the plaintext and ciphertext.
- The correlation value in this experiment is 0.126543374.
- Each character on the plaintext transforms to different character in the ciphertext, and there is no direct relationship between the plaintext and the ciphertext.
- The message has some repeated characters, and every time the resulted cipher is different from the other.
- These indicate that the proposed algorithm has high confusion and diffusion.

Results And Discussion

- One of the cryptographic algorithm criteria is the level of confusion and diffusion.
- The level of confusion can be determined by calculate the correlation value between the plaintext and ciphertext.
- The correlation value in this experiment is 0.126543374.
- Each character on the plaintext transforms to different character in the ciphertext, and there is no direct relationship between the plaintext and the ciphertext.
- The message has some repeated characters, and every time the resulted cipher is different from the other.
- These indicate that the proposed algorithm has high confusion and diffusion.

Results And Discussion

- One of the cryptographic algorithm criteria is the level of confusion and diffusion.
- The level of confusion can be determined by calculate the correlation value between the plaintext and ciphertext.
- The correlation value in this experiment is 0.126543374.
- Each character on the plaintext transforms to different character in the ciphertext, and there is no direct relationship between the plaintext and the ciphertext.
- The message has some repeated characters, and every time the resulted cipher is different from the other.
- These indicate that the proposed algorithm has high confusion and diffusion.

Results And Discussion

The Correlation Value between Plaintext and Ciphertext

Length of Text	Correlation Value
30	0.126543374
100	0.05135685
300	0.094886202
600	0.035254875
1000	0.023059525
3000	0.016014888
6000	0.009566434
10000	0.00004862

Results And Discussion

Encryption and Decryption Time

Length of Text	Encryption Time (Second)	Decryption Time (Second)
30	0.016	0.015
100	0.031	0.016
300	0.047	0.046
600	0.093	0.078
1000	0.172	0.125
3000	0.515	0.484
6000	1.451	1.388
10000	2.262	2.09

Conclusions

- The max plus wavelet transform can be used for construct a cryptographic algorithm.
- Encryption and decryption time are fast and increase linearly along with increasing length of the text.
- These show that the proposed algorithm is efficient in the running time.
- This cryptographic algorithm has small correlation value between plaintext and ciphertext, this meaning almost no linear correlation between the plaintext and ciphertext.
- Each character in the plaintext will be several different characters in the ciphertext.
- These show that the proposed algorithm has high level of confusion and diffusion.

Conclusions

- The max plus wavelet transform can be used for construct a cryptographic algorithm.
- Encryption and decryption time are fast and increase linearly along with increasing length of the text.
- These show that the proposed algorithm is efficient in the running time.
- This cryptographic algorithm has small correlation value between plaintext and ciphertext, this meaning almost no linear correlation between the plaintext and ciphertext.
- Each character in the plaintext will be several different characters in the ciphertext.
- These show that the proposed algorithm has high level of confusion and diffusion.

Conclusions

- The max plus wavelet transform can be used for construct a cryptographic algorithm.
- Encryption and decryption time are fast and increase linearly along with increasing length of the text.
- These show that the proposed algorithm is efficient in the running time.
- This cryptographic algorithm has small correlation value between plaintext and ciphertext, this meaning almost no linear correlation between the plaintext and ciphertext.
- Each character in the plaintext will be several different characters in the ciphertext.
- These show that the proposed algorithm has high level of confusion and diffusion.

Conclusions

- The max plus wavelet transform can be used for construct a cryptographic algorithm.
- Encryption and decryption time are fast and increase linearly along with increasing length of the text.
- These show that the proposed algorithm is efficient in the running time.
- This cryptographic algorithm has small correlation value between plaintext and ciphertext, this meaning almost no linear correlation between the plaintext and ciphertext.
- Each character in the plaintext will be several different characters in the ciphertext.
- These show that the proposed algorithm has high level of confusion and diffusion.

Conclusions

- The max plus wavelet transform can be used for construct a cryptographic algorithm.
- Encryption and decryption time are fast and increase linearly along with increasing length of the text.
- These show that the proposed algorithm is efficient in the running time.
- This cryptographic algorithm has small correlation value between plaintext and ciphertext, this meaning almost no linear correlation between the plaintext and ciphertext.
- Each character in the plaintext will be several different characters in the ciphertext.
- These show that the proposed algorithm has high level of confusion and diffusion.

Conclusions

- The max plus wavelet transform can be used for construct a cryptographic algorithm.
- Encryption and decryption time are fast and increase linearly along with increasing length of the text.
- These show that the proposed algorithm is efficient in the running time.
- This cryptographic algorithm has small correlation value between plaintext and ciphertext, this meaning almost no linear correlation between the plaintext and ciphertext.
- Each character in the plaintext will be several different characters in the ciphertext.
- These show that the proposed algorithm has high level of confusion and diffusion.

REFERENCES

- D. Goswami, N. Rahman, J. Biswas, A. Koul, R.L. Tamang, A.K. Bhattacharjee, 2011, **A Discrete Wavelet Transform based Cryptographic algorithm**, *International Journal of Computer Science and Network Security*, Vol. 11, No. 4.
- K. Fahim, 2014, **Konstruksi Transformasi Wavelet Menggunakan Aljabar Max Plus**, Master's Thesis in Department of Mathematics, Sepuluh Nopember Institute of Technology, Surabaya.
- D. Grigoriev, V. Shpilrain, 2013, **Tropical Cryptography**, *International Association for Cryptologic Research*.
- M. Durcheva, 2015, **Some applications of idempotent semirings in Public Key Cryptography**, *ACM Communication in Computer Algebra*, 19.

REFERENCES

- D. Goswami, N. Rahman, J. Biswas, A. Koul, R.L. Tamang, A.K. Bhattacharjee, 2011, **A Discrete Wavelet Transform based Cryptographic algorithm**, *International Journal of Computer Science and Network Security*, Vol. 11, No. 4.
- K. Fahim, 2014, **Konstruksi Transformasi Wavelet Menggunakan Aljabar Max Plus**, Master's Thesis in Department of Mathematics, Sepuluh Nopember Institute of Technology, Surabaya.
- D. Grigoriev, V. Shpilrain, 2013, **Tropical Cryptography**, *International Association for Cryptologic Research*.
- M. Durcheva, 2015, **Some applications of idempotent semirings in Public Key Cryptography**, *ACM Communication in Computer Algebra*, 19.

REFERENCES

- D. Goswami, N. Rahman, J. Biswas, A. Koul, R.L. Tamang, A.K. Bhattacharjee, 2011, **A Discrete Wavelet Transform based Cryptographic algorithm**, *International Journal of Computer Science and Network Security*, Vol. 11, No. 4.
- K. Fahim, 2014, **Konstruksi Transformasi Wavelet Menggunakan Aljabar Max Plus**, Master's Thesis in Department of Mathematics, Sepuluh Nopember Institute of Technology, Surabaya.
- D. Grigoriev, V. Shpilrain, 2013, **Tropical Cryptography**, *International Association for Cryptologic Research*.
- M. Durcheva, 2015, **Some applications of idempotent semirings in Public Key Cryptography**, *ACM Communication in Computer Algebra*, 19.

REFERENCES

- D. Goswami, N. Rahman, J. Biswas, A. Koul, R.L. Tamang, A.K. Bhattacharjee, 2011, **A Discrete Wavelet Transform based Cryptographic algorithm**, *International Journal of Computer Science and Network Security*, Vol. 11, No. 4.
- K. Fahim, 2014, **Konstruksi Transformasi Wavelet Menggunakan Aljabar Max Plus**, Master's Thesis in Department of Mathematics, Sepuluh Nopember Institute of Technology, Surabaya.
- D. Grigoriev, V. Shpilrain, 2013, **Tropical Cryptography**, *International Association for Cryptologic Research*.
- M. Durcheva, 2015, **Some applications of idempotent semirings in Public Key Cryptography**, *ACM Communication in Computer Algebra*, 19.

REFERENCES

- S. Kromodimoeljo, 2010, **Teori Dan Aplikasi Kriptografi**, SPK IT Consulting.
- C. E. Shannon, 1949, **Communication Theory Of Secrecy Systems**, *Bell Systems Technical Journal*, Vol. 28.
- Subiono, 2015, **Aljabar Min Max Plus Dan Terapannya**, Department of Mathematics, Sepuluh Nopember Institute of Technology, Surabaya.

REFERENCES

- S. Kromodimoeljo, 2010, **Teori Dan Aplikasi Kriptografi**, SPK IT Consulting.
- C. E. Shannon, 1949, **Communication Theory Of Secrecy Systems**, *Bell Systems Technical Journal*, Vol. 28.
- Subiono, 2015, **Aljabar Min Max Plus Dan Terapannya**, Department of Mathematics, Sepuluh Nopember Institute of Technology, Surabaya.

REFERENCES

- S. Kromodimoeljo, 2010, **Teori Dan Aplikasi Kriptografi**, SPK IT Consulting.
- C. E. Shannon, 1949, **Communication Theory Of Secrecy Systems**, *Bell Systems Technical Journal*, Vol. 28.
- Subiono, 2015, **Aljabar Min Max Plus Dan Terapannya**, Department of Mathematics, Sepuluh Nopember Institute of Technology, Surabaya.