

# On Max-Plus Algebra and Its Application on Image Steganography

*by Fatmawati Fatmawati*

---

**Submission date:** 07-Feb-2020 07:58PM (UTC+0800)

**Submission ID:** 1253117152

**File name:** 5\_Kiswara\_paper\_publish.pdf (2.21M)

**Word count:** 5733

**Character count:** 25964

## Research Article

# On Max-Plus Algebra and Its Application on Image Steganography

Kiswara Agung Santoso,<sup>1</sup> Fatmawati ,<sup>2</sup> and Herry Suprajitno <sup>2</sup>

<sup>1</sup>Department of Mathematics, Faculty of Mathematics and Natural Science, Jember University, Kampus Bumi Tegal Boto, Jl. Kalimantan 37, Jember 68121, Indonesia

<sup>2</sup>Department of Mathematics, Faculty of Science and Technology, Universitas Airlangga, Kampus C, Jl. Mulyorejo, Surabaya 60115, Indonesia

Correspondence should be addressed to Fatmawati; fatma47unair@gmail.com

Received 21 December 2017; Revised 22 March 2018; Accepted 28 March 2018; Published 15 May 2018

Academic Editor: Chi-Wai Chow

Copyright © 2018 Kiswara Agung Santoso et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

We propose a new steganography method to hide an image into another image using matrix multiplication operations on max-plus algebra. This is especially interesting because the matrix used in encoding or information disguises generally has an inverse, whereas matrix multiplication operations in max-plus algebra do not have an inverse. The advantages of this method are the size of the image that can be hidden into the cover image, larger than the previous method. The proposed method has been tested on many secret images, and the results are satisfactory which have a high level of strength and a high level of security and can be used in various operating systems.

## 1. Introduction

Recently information systems are developing very quickly, especially information systems through the Internet. It happens because the Internet can be accessed by anyone, anytime, and anywhere. Access to information through the Internet does not always bring benefits but also risks to the accuracy of information. This risk is vulnerable when information is accessible by hackers.

Many efforts have been made to protect data transferred over the Internet, including encryption (protecting data before being transferred over the Internet) and authentication (verifying whether the received data is the same as the sent data). There is knowledge or art of data protecting transferred over the Internet, that is, cryptography (data encoding) and steganography (data disguise). The data to be discussed in this paper is image data.

Many steganography methods in protecting information into an image have been published. The data or information that is hidden into an image can be text data or image data. Generally, to hide text data or image data into another image, the original text and original image should be converted into

binary digits (bits). Then each digit of the original image or original text is substituted into the last bit of the cover image pixel. By using this method, information could be hidden into the cover image with little difference between the image stego image and the cover image. In this algorithm, every character (for text) or pixel (for image) is hidden into three pixels of cover image. The consequence of this method is, for the text data, the maximum number of characters that can be hidden into the cover image is one-third of the total pixels of the cover image. For image data, the image size that can be hidden into the cover image is one-third the size of the cover image (either long or wide).

In modern world, all information communication is done online. It causes the security system when data transfer becomes very important. Steganography has its own mechanism in data protecting [1, 2]. In steganography, the information to be sent is hidden into other media, so that no one knows where the information is hidden. Watermarks and fingerprints are two technologies related to steganography, where steganography tends to hide data in other media [3].

Currently research on image encoding generally focuses on the following aspects: image encoding with spatial domains,

image coding with domain transformation, image coding based on neural network, chaotic image coding, image coding based on cellular automata, and quantum technology [4]. In cryptography, encoding is the process of transforming information using certain algorithms that make it unreadable by anyone except the one who knows the special information, commonly called a key. The result of this process is called encrypted information [5]. Bouquard et al. have introduced the image encoding algorithm using affine transformation [6]. In this algorithm, the encryption and decryption process pass through two stages; that is, the first stage encodes the image using XOR operations with four key bits and the second stage encodes the encoded image using affine transformation. The conclusion of the study states that the correlation of pixel values between the original image and the encrypted image decreased after transforming the affine transform.

Tom has implemented data disguise using steganographic techniques. To make the technique safer they added a level of security by applying cryptography to confidential data before using steganography [7]. For cryptography, they use the Caesar algorithm while for steganography they use the adjacent pixel differences algorithm. Kulkarni and Jatgap substituted secret messages using a 14-square substitution algorithm [8]. Once the text was substituted, then this message was encoded with the RSA algorithm. The next step, this encoded message was hidden into an image by LSB (Least Significant Bit) method. This image works as a carrier file, which will be sent to the recipient. The receiver decrypts to get the original message by performing the same method but in reverse order. Here, it appears that they do two coding techniques, so the system becomes more powerful and secure in the face of hacker attacks. This technique makes it difficult for the troublemakers to manipulate the image and takes a long time to encrypt the message, so it is safe from various attacks through the Internet network.

In measuring quality of an image objectively, some data are statistically calculated to determine quality of the reconstruction image. Image quality could be seen from how close the relationship of image forming pixels or by looking at how much the difference in pixel values are statistically distributed. In general, to compare two images, one could use mean square error (MSE) and Peak to Signal Noise Ratio (PSNR) [9, 10]. Choudhary applied the optimization process to a stego image by using the LSB method, so that quality of the stego can get better with lower computational complexity [11]. MSE between stego image and cover image can be derived. Experimental results show that visually the stego image cannot be distinguished from the cover image. The results also showed improvement compared to the previous one.

In this paper, we propose a new steganography method to hide an image into another image using matrix multiplication operations on max-plus algebra. This is especially interesting because the matrix used in encoding or information disguises generally has an inverse, whereas matrix multiplication operations in max-plus algebra do not have an inverse. Another advantage of this method is the size of the image that can be hidden into the cover image which is greater than using the previous method.

## 2. Max-Plus Algebra

Max-plus algebra can be used to model disk events related to synchronization and time delays. The application of this theory has a very strong association with production problems [12, 13].

The max-plus algebra [7] is a sequential pair  $(R, \oplus, \otimes)$ , where  $R$  is the set of all real numbers, whereas  $\oplus$  and  $\otimes$  are binary operations on  $R$  defined as

$$\begin{aligned} a \oplus b &= \max(a, b), \\ a \otimes b &= a + b \end{aligned} \quad (1)$$

for every  $a, b \in R$ . Operations  $\oplus$  and  $\otimes$  are extensions of matrices and vectors in the same way as conventional linear algebra.

In the max-plus algebra [6], the matrix multiplier  $A \otimes B$  is defined as follows: for any matrix  $A \in R^{m \times p}$ ,  $B \in R^{p \times n}$ , we can obtain matrix  $C \in R^{m \times n}$  by the formula

$$c_{ij} = \bigoplus_{k=1}^p (a_{ik} \otimes b_{kj}) \quad (2)$$

for  $i = 1, \dots, m$ ,  $j = 1, \dots, n$ . For a square matrix with degree  $k$ , matrix  $A \in R^{n \times n}$  denoted by  $A(k)$  and was defined by recursive operation on  $k = 2, 3, \dots$

$$A(k) = A \otimes A^{(k-1)}. \quad (3)$$

The set of  $R_{\max}$  with operations  $\oplus$  and  $\otimes$  is called max-plus algebra and denoted by  $R_{\max} = (R_{\max}, \oplus, \otimes, \varepsilon, e)$ . As conventional algebra, operations  $\otimes$  have a higher priority than  $\oplus$ . For example, operation  $5 \otimes -9 \oplus 7 \otimes 1$  has an understanding like  $(5 \otimes -9) \oplus (7 \otimes 1)$ .

Note that  $(5 \otimes -9) \oplus (7 \otimes 1) = 8$ , where  $5 \otimes (-9 \oplus 7) \otimes 1 = 13$ .

In addition, there is  $-\infty$  such that  $\max(a, -\infty) = \max(-\infty, a) = a$  and  $a + (-\infty) = -\infty + a = -\infty$ . For any  $a \in R_{\max}$ , there is a small number  $\varepsilon$  such that

$$\begin{aligned} a \oplus \varepsilon &= \varepsilon \oplus a = a, \\ a \otimes \varepsilon &= \varepsilon \otimes a = \varepsilon. \end{aligned} \quad (4)$$





Let  $A \in R_e^{n \times n}$  and  $b \in R_e^n$ . In general, the system of linear equations in max-plus algebra will have no solution, if  $A$  is square matrix or if the number of columns in  $A$  is more than the number of rows in  $A$ . Therefore, subsolutions concepts are introduced [7].

Operator  $\otimes$  is a commutative operator. Except 0, every element has an inverse. The inverse of  $x$  is denoted by  $x^{-1}$  or  $1/x$ . More precisely, we denote  $x/y$  or  $x \otimes y^{-1}$ .  $x \otimes y$  multiplication could be denoted by  $xy$ . The operator allows it to be expanded to a  $m \times m$  matrix on  $R_{\max}$  [14].

Let  $A$  and  $B$  be two matrices of  $m \times m$ , operator  $\oplus$ , and we define

$$\begin{aligned} [A \oplus B]_{i,j} &= A_{i,j} \oplus B_{i,j}, \quad \forall (i, j) \in \{1, \dots, m\}^2, \\ [A \otimes B]_{i,j} &= \bigoplus_{k=1}^m A_{i,k} \otimes B_{k,j}, \quad \forall (i, j) \in \{1, \dots, m\}^2. \end{aligned} \quad (5)$$

TABLE 1: The difference between text encoding and image encoding.

Type	Secret data	Encrypt data	Remarks
Text	CSEMCKVIE	DTENDLWJF	Different
Image (RGB)	 Pixel( $P_1$ ) = (24, 45, 233)	 Pixel( $P_2$ ) = (10, 65, 198)	$P_1$ and $P_2$ are different, but visually they are difficult to distinguish
Image (Gray)	 Pixel( $P_1$ ) = (87)	 Pixel( $P_2$ ) = (114)	$P_1$ and $P_2$ are different, but visually they are difficult to distinguish

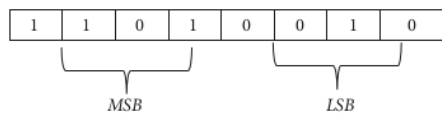


FIGURE 1: MSB and LSB bit.

It is not difficult to prove that the  $m \times m$  matrix exists in  $R_{max}$ . Based on the triangular matrix  $A$  of size  $m \times m$ , where  $A_{i,j} = 0$  for  $i > j$ , it is indicated that the set of  $m \times m$  triangular matrices exists in  $R_{max}$ , but the operator  $\otimes$  is not commutative. Furthermore, not all elements in max-plus algebra have inverse [6].

### 3. Literature Review

The image data character is very different from the text data because an image contains very large data, and all data has a very strong relationship and contains very high data loops [15].

Conceptually, the difference between text data and image data can be seen in Table 1.

An image is defined as a two-dimensional function,  $f(x, y)$ , where  $x$  and  $y$  are spatial coordinates and  $f$  is the light intensity at coordinates  $(x, y)$  known as the gray degree. An image is called a digital image if, in position  $(x, y)$ , there is an amplitude value. A digital image constitutes a finite number of elements, each of which has a particular location and a particular value. These elements are called picture elements or images of elements or pixels [16].

The pixel of an image can be converted into 8 binary digits (bits). The first to fourth bit is called LSB (Least Significant Bit) where the bit value changes in this position have no impact on the image. The fifth to eighth bit is called MSB (Most Significant Bit), where changes in bit values in this position have an effect on image. Figure 1 shows the bit positions of MSB and LSB.

The maximum deviation of an image can be found by making a grayscale histogram and calculating its area. The larger the deviation is, the better the encoding will be. To find the area of deviation image can be seen from the following formula [17]:

$$L = \frac{h_0 + h_{255}}{2} + \sum_{i=1}^{254} h_i \tag{6}$$

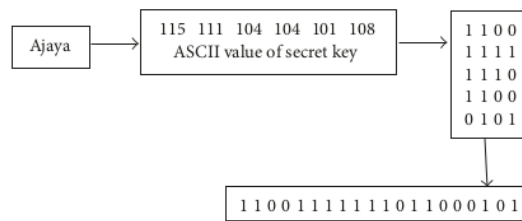


FIGURE 2: 1D array representation.

Here,

$L$  is the area of deviation;

$h_i$  is the number of pixels that have gray degree;

$i$  is the value of pixels.

A simple example of hiding data into an image is called insertion of least significant bit (LSB). For 24-bit colored images, the number of changes will be minimized so that it is difficult to distinguish by the human eye. For example, suppose we have three adjacent pixels (nine bytes) by using RGB encoding. Suppose we will hide data 10110101. Put 9 bits of data in the LSB position, so the following pixels are obtained (bold font shows the changed bits):

$$\begin{matrix} 10010101 & 00001101 & 11001001 \\ 1001011\mathbf{0} & 00001111 & 11001010 \\ 10011111 & 00010000 & 11001011 \end{matrix} \tag{7}$$

Based on the formula, here is a snippet of the steganography process (see Figure 2).

Application of stenographic LSB uses secret key. Kulkarni and Jatgap [8] take a binary representation to hide information and replace the LSB of each cover image bit. Here, a secret key is introduced to protect the hidden information by using the formula:

$$\begin{aligned} &\text{Cover image} + \text{secret key} + \text{hidden information} \\ &= \text{stego image.} \end{aligned} \tag{8}$$

To hide information, one should use cover image. Cover image is divided into three matrices (Red, Green, and Blue). Secret key is converted to 1D bit stream array. Secret key and

Red matrix are used as decision-makers to replace hidden information into the Green matrix or Blue matrix. Every bit of the secret key is operated by operators XOR with every LSB bit on the Red matrix. The result of the XOR operation is used to determine the bit of the hidden information to be replaced in the Green matrix LSB or the Blue matrix. The same process is done until all information is successfully hidden [18]. In this method, every character (plain text) or every pixel (plain image) is hidden into three pixels of cover image. As a consequence of this method, for plain text, the maximum number of characters that can be hidden into the cover image is 1/3 of the total pixel cover image. The maximum size of plain image that can be hidden is 1/3 of the size of the cover image (for length and width).

In the previous method, it is required that the size of the secret image should be smaller than the size of the cover image. In this article, we propose a new method so that the size of the secret image can be increased to the same size as the cover image.

#### 4. The Proposed Method

The following algorithm is how to hide secret image into another image with maximal size equal to cover image size:

- (1) Convert pixels from secret image and cover image into bitwise form.
- (2) Change the MSB from the pixel cover to the  $2 \times 2$  matrix form.
- (3) Find the secret image matrix using

$$\begin{aligned} \text{(a)} \quad SR_{(i,j)} &= R_{(i,j)} \otimes G_{(i,j)}, \\ \text{(b)} \quad SG_{(i,j)} &= G_{(i,j)} \otimes B_{(i,j)}, \\ \text{(c)} \quad SB_{(i,j)} &= B_{(i,j)} \otimes R_{(i,j)}, \end{aligned}$$

where

$R_{(i,j)}$  is the MSB of cover image matrix on the Red layer at position  $(i, j)$ ,  
 $G_{(i,j)}$  is the MSB of cover image matrix on the Green layer at position  $(i, j)$ ,  
 $B_{(i,j)}$  is the MSB of cover image matrix on the Blue layer at position  $(i, j)$ .

- (4) Substitute the MSB secret image into the LSB stego image with the following rules:
  - (a) If  $a_{11} > a_{12}$ , then substitute the first bit of  $MSB_{si}$  into the second bit of  $LSB_{ci}$  and substitute the second bit of  $MSB_{si}$  to the first bit of  $LSB_{ci}$ .
  - (b) If  $a_{11} \leq a_{12}$ , then substitute the first bit of  $MSB_{si}$  into the first bit of  $LSB_{ci}$  and substitute the second bit of  $MSB_{si}$  into the second bit  $LSB_{ci}$ .
  - (c) If  $a_{21} > a_{22}$ , then substitute the third bit of  $MSB_{si}$  into the fourth bit of  $LSB_{ci}$  and substitute the fourth bit of  $MSB_{si}$  into the third bit of  $LSB_{ci}$ .
  - (d) If  $a_{21} < a_{22}$ , then substitute the third bit of  $MSB_{si}$  into the third bit of  $LSB_{ci}$  and substitute the fourth bit of  $MSB_{si}$  into the fourth bit of  $LSB_{ci}$ .

TABLE 2: Example data.

Image	Layer	Value	Bit	MSB	LSB
Secret image	Red	79	00010001	0001	0001
	Green	108	01101100	0110	1100
	Blue	205	11001101	1100	1101
Cover image	Red	28	00011100	0001	1100
	Green	104	01101000	0110	1000
	Blue	146	10010010	1001	0010

Here

$a_{ij}$  is the element of matrix of the secret image at row  $I$  and column  $j$ .

$MSB_{sc}$  is the MSB of secret image.

$LSB_{st}$  is the LSB of stego image.

For more details, the proposed coding system can be illustrated through the flowchart as in Figure 3.

Here is an algorithm to display the secret image of the stego image.

- (1) Convert pixels of stego image into 8-bit form.
- (2) Calculate the secret image matrix by

$$\begin{aligned} \text{(a)} \quad SR_{(i,j)} &= R_{(i,j)} \otimes G_{(i,j)}, \\ \text{(b)} \quad SG_{(i,j)} &= G_{(i,j)} \otimes B_{(i,j)}, \\ \text{(c)} \quad SB_{(i,j)} &= B_{(i,j)} \otimes R_{(i,j)}. \end{aligned}$$

Here

$R_{(i,j)}$  is the LSB of stego image matrix on the Red layer at position  $(i, j)$ .

$G_{(i,j)}$  is the LSB of stego image matrix on the Green layer at position  $(i, j)$ .

$B_{(i,j)}$  is the LSB of stego image matrix on the Blue layer at position  $(i, j)$ .

- (3) Exchange LSB bitwise LSB of stego image with the following rules:
  - (a) If  $a_{11} > a_{12}$ , then exchange the first bit with the second bit.
  - (b) If  $a_{21} > a_{22}$ , then exchange the third bit with the fourth bit.

Here  $a_{ij}$  is the matrix element of the secret image matrix on the row  $I$  and column  $j$ .

  - (c) Convert LSB and MSB from the stego image.
  - (d) Exchange bit 1 with bit 5.
  - (e) Exchange bit 2 with bit 6.
  - (f) Exchange bit 3 with bit 7.
  - (g) Exchange bit 4 with bit 8.

For more details, decryption algorithm that can be made through the flowchart as in Figure 4.

In Table 2, the example pixel data from the secret image and the cover image is presented.

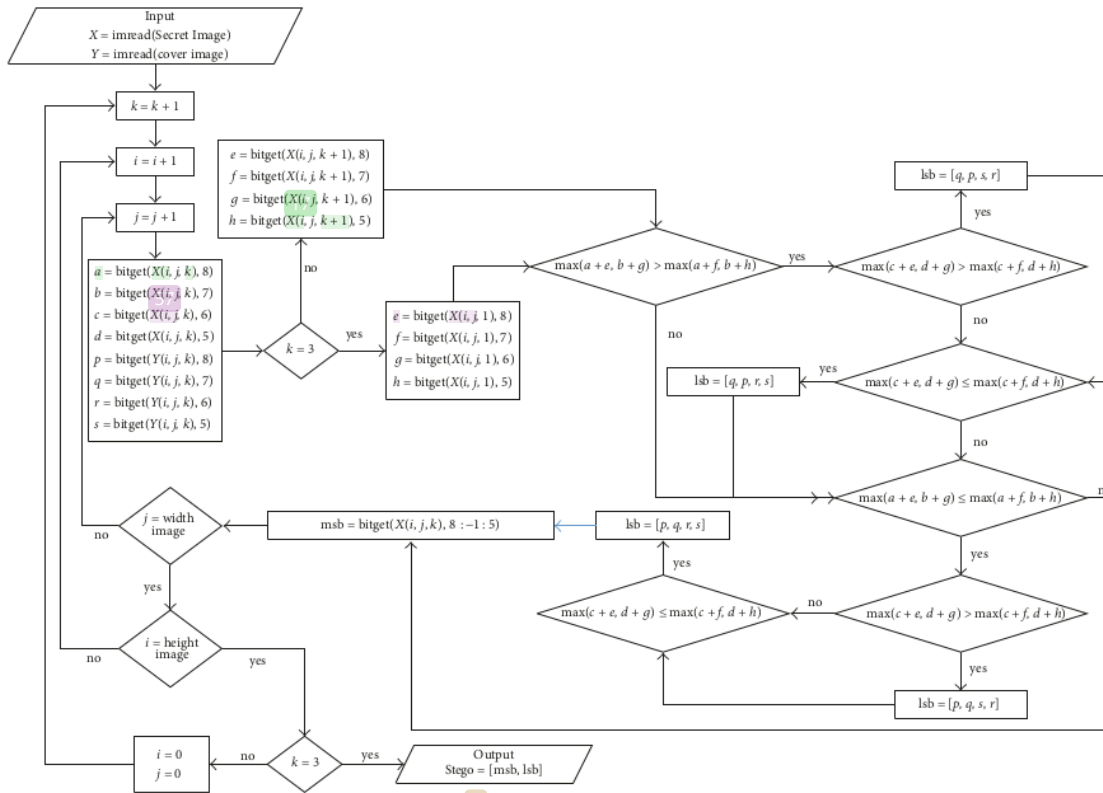


FIGURE 3: Flowcharts to hide the secret image into the cover image.

We process the following operations:  $SR = R \otimes G$   $SG = G \otimes B$   $SB = B \otimes R$ :

$$\begin{aligned}
 SR &= \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}, \\
 SG &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \\
 SB &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.
 \end{aligned}
 \tag{9}$$

In the matrix column in Table 3, if element of the left matrix is larger than element of the right matrix, then the element will be exchanged. The results of the operation process in Table 3 are given in Table 4.

### 5. Experimental Results and Analysis

To test our method, an experiment was performed. Here the test is done by using a laptop with microprocessor core i3 and Microsoft Windows 10 operating system. Computer program was created by using MATLAB R2016b and it applied to an image of good quality. The results of our algorithm are shown

TABLE 3: Operation process.

Secret image		Matrix	Stego image	
MSB	Process		Process	LSB
0001	00 01	SR: $\begin{pmatrix} a_{11} = a_{12} \\ a_{21} > a_{22} \end{pmatrix}$	00 10	0010
0110	01 10	SG: $\begin{pmatrix} a_{11} < a_{12} \\ a_{21} > a_{22} \end{pmatrix}$	01 01	0101
1100	11 00	SB: $\begin{pmatrix} a_{11} = a_{12} \\ a_{21} < a_{22} \end{pmatrix}$	11 00	1100

in Figure 5. We use the balloon image as a secret image and carrot image as the cover image. Cover image and secret image have the same size that is  $163 \times 133$ .

Figure 5 shows that the stego image (Figure 5(c)) is similar to the cover image (Figure 5(a)), although visually inside the cover image contains a secret image (Figure 5(b)). The result of stego image has a size of  $163 \times 133$ . It is proved that this method can hide the secret image that has size as same as the cover image. This needs to be demonstrated by using statistical analysis. Therefore, an ideal encoding must have power when there is an attack through its statistical model.

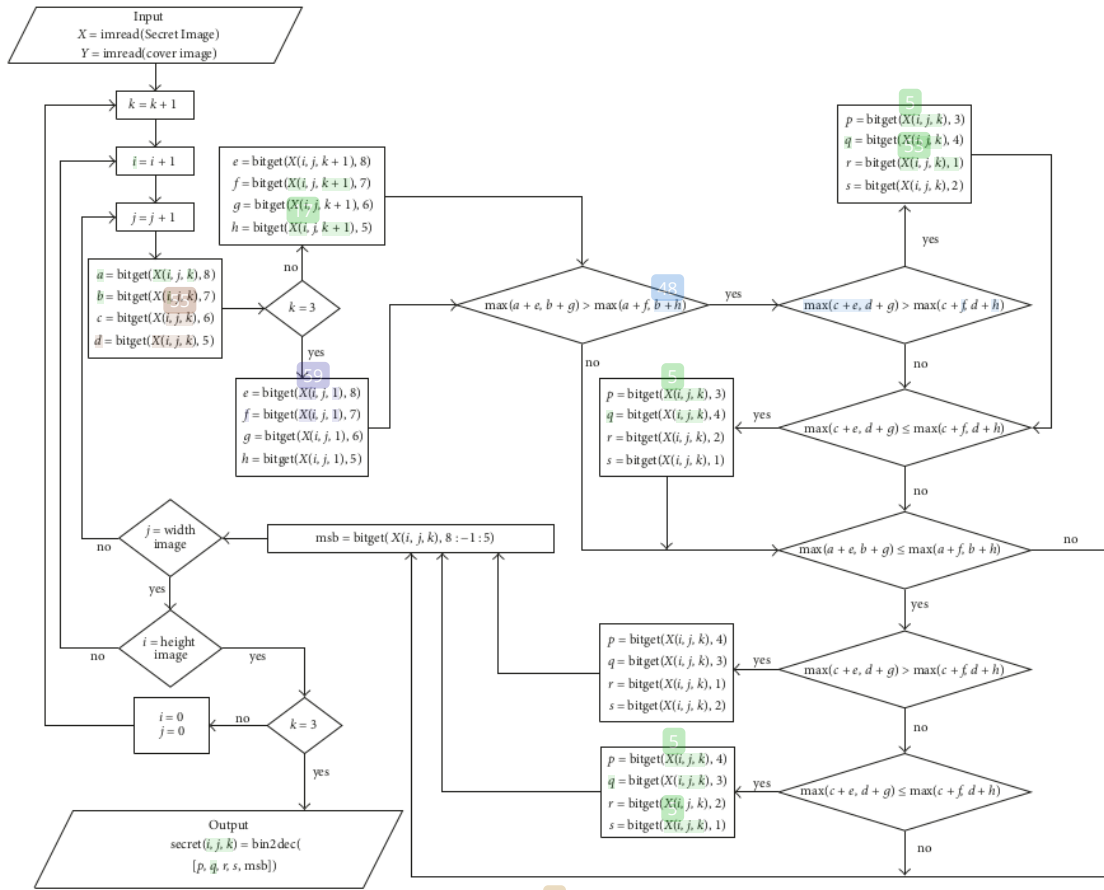


FIGURE 4: Flowchart to display the secret image of the stego image.

TABLE 4: The results.

Image	Layer	Value	Bit	MSB	LSB	Matrix
Cover	R	28	00011100	0001	1100	$R = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
	G	104	01101000	0110	1000	$G = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
	B	146	10010010	1001	0010	$B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
Secret	R	79	00010001	0001	0001	$SR = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$
	G	108	01101100	0110	1100	$SG = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$
	B	205	11001101	1100	1101	$SB = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$
Stego	R	18	00010010	0001	0010	
	G	101	01100101	0110	0101	
	B	156	10011100	1001	1100	

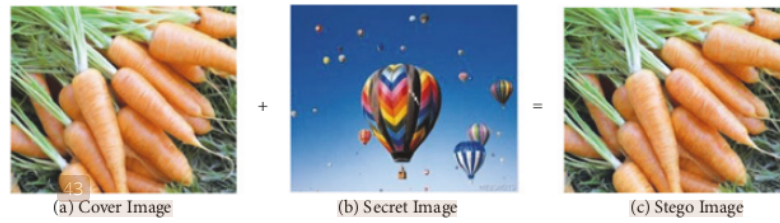


FIGURE 5: Experimental result.

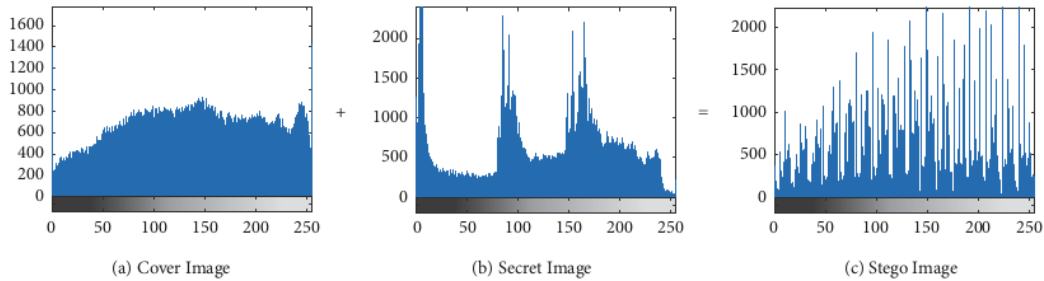


FIGURE 6: Histogram analysis.

To prove the power of this proposed method, we performed a statistical analysis by displaying a histogram and computing the correlation coefficient between two neighboring pixels on the cover image and stego image.

The abscissa histogram shows the pixel value and the ordinate showing the frequency or how often the pixel value appears. The histogram of the cover image shown in Figure 6(a) has a larger area. This area shows how often the pixel value appears in an image. Histogram of the secret image shown in Figure 6(b) has a smaller area. This shows that the cover image is clearer than the secret image. Histogram of the stego image shown in Figure 6(c) has a pattern similar to the cover image. This shows that the cover image has not significantly changed.

In addition to histogram analysis, we also analyze the correlation coefficients of two vertically neighboring pixels, two horizontally neighboring pixels, and two pixels diagonally adjacent to the stego image and cover image. First, we select 10000 pixels on a neighboring image. Then we calculate the correlation coefficient with the following formula:

$$\text{cov}(x, y) = E(x - E(x))(y - E(y)),$$

$$r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}. \tag{10}$$

Here,  $x$  and  $y$  are the values of two neighboring pixels. In numerical computation, the correlation coefficient can be calculated using the following formula [19]:

TABLE 5: The correlation coefficient.

Image	Horizontal	Vertical	Diagonal
Cover	0.97028	0.91432	0.97337
Stego	0.96014	0.91039	0.92923

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i,$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2, \tag{11}$$

$$\text{cov}(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y)).$$

Based on the proposed method, the correlation coefficient between two vertically neighboring pixels for the cover image and stego image is 0.91432 and 0.91039, respectively. Similarity of the results to the vertical and diagonal directions is shown in Table 5. It is apparent in Table 5 that there is a strong correlation between two neighboring pixels, or in other words the stego image and cover image are difficult to distinguish.

In the image processing mean square error (MSE) is often used to determine how big the image quality difference between before and after coding process. The formula is presented as follows [15]:

$$\text{MSE}_{\text{image}} = \frac{1}{MN} \sum_{y=1}^M \sum_{x=1}^N |I(x, y) - I'(x, y)|^2, \tag{12}$$





FIGURE 7: Encoding by max-plus algebra.



FIGURE 8: Encoding by previous method.

34  
where

- $M$  is the length of image (in pixel),
- $N$  is the width of image (in pixel),
- $I(x, y)$  is the initial image pixel value,
- $I'(x, y)$  is the resulting image pixel value.

Based on the calculation, the MSE between the cover image and stego image is 361.7734

Improving the visual quality of digital image can be subjective. Saying that one method provides better quality image could vary from person to person. Using same tests images, different image enhancement algorithm can be compared by peak signal to noise ratio (PSNR). The mathematical representation of the PSNR is as follows:

$$PSNR = 20 \log_{10} \left( \frac{MAX_f}{\sqrt{MSE}} \right), \quad (13)$$

where  $MAX_f$  is the maximum signal value that exists in our original "known to be good" image. Two identical images will have a zero MSE value and an infinite PSNR value so the smaller the difference between the two images, the smaller the MSE value and the larger the PSNR value [19].

From the calculation results obtained PSNR for cover image is 21.8295 and PSNR for stego image is 21.8142. Here it looks very small value difference so it can be said that the image between cover image and stego image is similar. With this similar result it can be said that the coding result goes well.

Based on analysis of time, this algorithm has the time complexity  $O(n)$ . This shows that the algorithm has execution time that increases linearly according to the number of pixels (image size).

*Comparison of Max-Plus Methods and Previous Methods.* To compare the proposed coding method with the previous



FIGURE 9: Decoding by max-plus algebra.

coding method, we use koala image (1024 × 768) as a secure image and tulips image (1024 × 768) as cover image.

From Figures 7 and 8, we can see that the encoding between the max-plus and the previous method produces the same stego image. Both methods can be used to hide the secret image that has same image size between the secret image and the cover image. Figures 9 and 10 show the results of decoding by max-plus and previous methods. Hence, we conclude that the decoding process of the Max-Plus method can return the stego image same as the secret image, while in the previous method it cannot return the stego image to the secret image perfectly but only a quarter of the part. It makes the previous method display a quarter of the secret image during the description process.

## 6. Conclusions

The proposed method has been tested on many secret images, and the results are satisfactory which have a high level of strength and a high level of security and it can be used in various operating systems. A pixel of the secret image is hidden in a cover image pixel by matrix multiplication operations in max-plus algebra, so that the message becomes safer. Maximum secret image size that can be hidden is the same as the size of cover image. This is the novelty of this

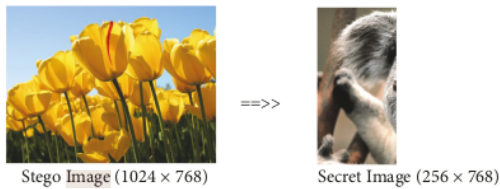


FIGURE 10: Decoding by previous method.

method where, in the previous method, size of secret image is always smaller than the cover image. In our future research, we will construct an algorithm to hide a text into an image by using max-plus algebra.

### Conflicts of Interest

The authors declare that they have no conflicts of interest.

### References

- [1] A. Khurana and B. Mehta, "Comparison of LSB and MSB based Image Steganography," *International Journal of Computer Science and Technology*, vol. 3, no. 3, pp. 870-871, 2012.
- [2] A. Sharma and V. Sharma, "Improved performance of secure data hiding algorithm using non blind steganography technique," *International Journal of Research*, vol. 2, no. 6, pp. 1-4, 2015.
- [3] S. Singh and S. Sharma, "Data Hiding using difference between adjacent pixels and bit plane swapping," *International Journal of Engineering and Computer Science*, vol. 3, no. 6, pp. 6770-6778, 2014.
- [4] P. Kori, P. Dubey, and V. Richhariya, "Double phase image encryption and decryption using logistic tent map and chaotic logistic map," *International Journal and Research Technology*, vol. 1, no. 11, pp. 33-39, 2015.
- [5] Q. Kester, "Image Encryption based on the RGB PIXEL Transposition and Shuffling," *International Journal of Computer Network and Information Security*, vol. 5, no. 7, pp. 43-50, 2013.
- [6] J.-L. Bouquard, C. Lenté, and J.-C. Billaut, "Application of an optimization problem in max-plus algebra to scheduling problems," *Discrete Applied Mathematics: The Journal of Combinatorial Algorithms, Informatics and Computational Sciences*, vol. 154, no. 15, pp. 2064-2079, 2006.
- [7] H. Tom, "Max-plus algebra and its application in spreading of information Circulant matrices," *Advances in Mathematical and Computational Methods*, pp. 188-191, 2003.
- [8] M. Kulkarni and P. Jatgap, "An efficient data hiding scheme using steganography and cryptography technique," *International Journal of Scientific and Research Publications*, vol. 5, no. 4, pp. 1-4, 2015.
- [9] A. Chandranath, "Robust steganography using LSB-XOR and image sharing," in *Proceedings of the International Conference on Computation and Communication Advancement (IC3A)*, 102, 97 pages, 2013.
- [10] J. Kaur, "A Secure Technique for hiding data under the Fingerprint Images using Modified Haar Wavelet Based Transformation," in *Proceedings of the International Journal of Innovative Technology and Exploring Engineering*, vol. 2, pp. 57-59, 2013.
- [11] K. Choudhary, "Image steganography and global terrorism," *International Journal of Scientific & Engineer Reseach*, vol. 3, no. 7, pp. 1-12, 2012.
- [12] A. Lini and D. Neenu, "Secure image encryption algorithms: A review," *International Journal of Scientific & Technology Research*, vol. 2, no. 4, pp. 186-189, 2013.
- [13] E. Menguy, J.-L. Boimond, L. Hardouin, and J.-L. Ferrier, "Just-in-time control of timed event graphs: update of reference input, presence of uncontrollable input," *Institute of Electrical and Electronics Engineers Transactions on Automatic Control*, vol. 45, no. 11, pp. 2155-2159, 2000.
- [14] B. Case, "Max-Plus Algebra : From Discrete-event Systems to Continuous Optimal Control Problems," *SIAM News*, vol. 43, no. 8, pp. 3-6, 2010.
- [15] Z. Liu, C. Guo, J. Tan et al., "Securing color image by using phase-only encoding in Fresnel domains," *Optics and Lasers in Engineering*, vol. 68, pp. 87-92, 2015.
- [16] B. De Schutter and T. V. D. Boom, "Max-plus algebra and max-plus linear discrete event systems: An introduction," in *Proceedings of the 9th International Workshop on Discrete Event Systems, WODES' 08*, pp. 36-42, Goteborg, Sweden, May 2008.
- [17] C.-M. Shin, D.-H. Seo, and S.-J. Kim, "Gray-level image encryption scheme using full phase encryption and phase-encoded exclusive-OR operations," *Optical Review*, vol. 11, no. 1, pp. 34-37, 2004.
- [18] A. Gangwar, "Improved RGB-LSB seganography using secret key," *International Journal of Computer Trend and Technology*, vol. 4, no. 2, pp. 85-89, 2013.
- [19] Z. Liu, H. Chen, W. Blondel, Z. Shen, and S. Liu, "Image security based on iterative random phase encoding in expanded fractional Fourier transform domains," *Optics and Lasers in Engineering*, vol. 105, pp. 1-5, 2018.

# On Max-Plus Algebra and Its Application on Image Steganography

---

## ORIGINALITY REPORT

---

20%

SIMILARITY INDEX

10%

INTERNET SOURCES

19%

PUBLICATIONS

0%

STUDENT PAPERS

---

## PRIMARY SOURCES

---

- |   |  |    |
|---|--|----|
| 1 | "Advances in Multimedia Information Processing — PCM 2001", Springer Nature, 2001<br>Publication   | 1% |
| 2 | Ajit Danti, G. R. Manjula. "Secured data hiding of invariant sized secrete image based on Discrete and Hybrid Wavelet transform", 2012 IEEE International Conference on Computational Intelligence and Computing Research, 2012<br>Publication | 1% |
| 3 | <a href="http://downloads.hindawi.com">downloads.hindawi.com</a><br>Internet Source  | 1% |
| 4 | <a href="http://memo.cgu.edu.tw">memo.cgu.edu.tw</a><br>Internet Source  | 1% |
| 5 | <a href="http://u.math.biu.ac.il">u.math.biu.ac.il</a><br>Internet Source  | 1% |
| 6 | Afsha Shaukat, Mahesh Chaurasia, Goutam Sanyal. "A novel image steganographic  | 1% |

technique using fast fourier transform", 2016  
International Conference on Recent Trends in  
Information Technology (ICRTIT), 2016

Publication

---

7 mafiadoc.com 1 %  
Internet Source

---

8 hal.archives-ouvertes.fr 1 %  
Internet Source

---

9 www.ni.com 1 %  
Internet Source

---

10 research.ijcaonline.org 1 %  
Internet Source

---

11 De Schutter, Bart, and Ton van den Boom. 1 %  
"Max-plus algebra and max-plus linear  
discrete event systems: An introduction",  
2008 9th International Workshop on Discrete  
Event Systems, 2008.  
Publication

---

12 Ratnadewi, Anak Agung Istri, Wuryanti 1 %  
Handayani, Ika Oktavianawati, Agung Budi  
Santoso, and Ni Nyoman Tri Puspaningsih.  
"Isolation and Hydrolysis Xylan from Soybean  
Waste with Endo- $\beta$ -1,4-D-Xylanase of Bacillus  
sp. From Soil Termite Abdomen", Agriculture  
and Agricultural Science Procedia, 2016.  
Publication

---

13

Chen, W.Y.. "Color image steganography scheme using set partitioning in hierarchical trees coding, digital Fourier transform and adaptive phase modulation", Applied Mathematics and Computation, 20070201

Publication

<1 %

14

Sridhar, Sabarish. "A Comprehensive Approach to Image Watermarking, Encryption and Steganography", Computer and Information Science, 2015.

Publication

<1 %

15

Lee, Y.P.. "High-payload image hiding with quality recovery using tri-way pixel-value differencing", Information Sciences, 20120515

Publication

<1 %

16

[fr.slideshare.net](http://fr.slideshare.net)

Internet Source

<1 %

17

Behrang Monajemi Nejad, Jorg Raisch. "Consensus-based synchronizing control for networks of timed event graphs", 22nd Mediterranean Conference on Control and Automation, 2014

Publication

<1 %

18

N Santosh Arjun, Atul Negi. "A Filtering Based Approach to Adaptive Steganography", TENCON 2006 - 2006 IEEE Region 10 Conference, 2006

Publication

<1 %

19

Masoumeh Khodaei. "Image Hiding by Using Genetic Algorithm and LSB Substitution",  
Lecture Notes in Computer Science, 2010

Publication

&lt;1 %

20

Ahmed Aliyu, Abdul H. Abdullah, Omprakash Kaiwartya, Yue Cao, Jaime Lloret, Nauman Aslam, Usman Mohammed Joda. "Towards video streaming in IoT Environments: Vehicular communication perspective",  
Computer Communications, 2018

Publication

&lt;1 %

21

Brunsch, Thomas, Laurent Hardouin, and Jörg Raisch. "Modelling Manufacturing Systems in a Dioid Framework",  
Industrial Information Technology, 2014.

Publication

&lt;1 %

22

P. Mahimah, R. Kurinji. "Zigzag pixel indicator based secret data hiding method",  
2013 IEEE International Conference on Computational Intelligence and Computing Research, 2013

Publication

&lt;1 %

23

[paper.ijcsns.org](http://paper.ijcsns.org)

Internet Source

&lt;1 %

24

G.A.D. Lopes, T.J.J. van den Boom, B. De Schutter, R. Babuška. "Modeling and Control of Legged Locomotion via Switching Max-Plus Systems",  
IFAC Proceedings Volumes, 2010

Publication

&lt;1 %

---

25

[link.springer.com](http://link.springer.com)

Internet Source

<1 %

---

26

Chitra A. Dhawale, Naveen D. Jambhekar.  
"chapter 15 Digital Image Steganography", IGI  
Global, 2017

Publication

<1 %

---

27

Emma V. Sheehan, Sarah C. Gall, Sophie L.  
Cousens, Martin J. Attrill. "Epibenthic  
Assessment of a Renewable Tidal Energy  
Site", The Scientific World Journal, 2013

Publication

<1 %

---

28

Peter Butkovic. "Simple image set of (max,+)  
linear mappings", Discrete Applied  
Mathematics, 2000

Publication

<1 %

---

29

Donghui Guo. "Multiple Image Information  
Hiding Technique Based on Chaotic  
Sequences", 2007 International Conference on  
Convergence Information Technology (ICCIT  
2007), 11/2007

Publication

<1 %

---

30

K. Kuppusamy, K. Thamodaran. "Optimized  
partial image encryption scheme using PSO",  
International Conference on Pattern  
Recognition, Informatics and Medical  
Engineering (PRIME-2012), 2012

Publication

<1 %

---

31	epdf.pub Internet Source	<1 %
32	ijraset.com Internet Source	<1 %
33	repository.dl.itc.u-tokyo.ac.jp Internet Source	<1 %
34	www.worldscientific.com Internet Source	<1 %
35	www3.combinatorics.org Internet Source	<1 %
36	Amir Farhad Nilizadeh, Ahmad Reza Naghsh Nilchi. "Steganography on RGB Images Based on a "Matrix Pattern" using Random Blocks", International Journal of Modern Education and Computer Science, 2013 Publication	<1 %
37	Asawari S. Chavan, Amrita A. Manjrekar. "Data embedding technique using secret fragment visible mosaic image for covered communication", 2015 International Conference on Information Processing (ICIP), 2015 Publication	<1 %
38	Bhaskar Panna, Sumit Kumar, Rajib Kumar Jha. "Image Encryption Based on Block-wise	<1 %



# Fractional Fourier Transform with Wavelet Transform", IETE Technical Review, 2018

Publication

---

39

Chen, W.Y.. "Color image steganography scheme using DFT, SPIHT codec, and modified differential phase-shift keying techniques", Applied Mathematics and Computation, 20080215

Publication

---

<1 %

40

Chin-Chen Chang. "Concealing a secret image using the breadth first traversal linear quadtree structure", Proceedings of the Third International Symposium on Cooperative Database Systems for Advanced Applications CODAS 2001 CODAS-01, 2000

Publication

---

<1 %

41

Manoj Sharma, Manoj Shukla, Amit Kaul. "Image hiding using unitary similarity transformation", 2011 International Conference on Image Information Processing, 2011

Publication

---

<1 %

42

[www.dcsc.tudelft.nl](http://www.dcsc.tudelft.nl)

Internet Source

---

<1 %

43

[www.ijert.org](http://www.ijert.org)

Internet Source

---

<1 %

44

"Advances in Artificial Systems for Medicine and Education II", Springer Science and Business Media LLC, 2020

Publication

<1 %

45

"Sustainable Development and Social Responsibility—Volume 2", Springer Science and Business Media LLC, 2020

Publication

<1 %

46

Biswajita Datta, Akash Roy, Romit Dutta, Samir Kumar Bandyopadhyay. "Secure Communication through Double Layer Security with Efficient Key Transmission", 2018 International Conference on Information Technology (ICIT), 2018

Publication

<1 %

47

Das, Rig, and Themrichon Tuithung. "A review on "A Novel Technique for Image Steganography Based on Block-DCT and Huffman Encoding"", International Conference on Graphic and Image Processing (ICGIP 2012), 2013.

Publication

<1 %

48

Divya Kanakanala, Swathi Routhu, Jianzhong Ruan, Xiaoqing Frank Liu, Frank Liou. "A Multi-Axis Slicing Method for Direct Laser Deposition Process", Volume 1: 36th Design Automation Conference, Parts A and B, 2010

Publication

<1 %

49

N.A. Flayh, R. Parveen, S.I. Ahson. "Wavelet based partial image encryption", 2009 International Multimedia, Signal Processing and Communication Technologies, 2009

Publication

<1 %

50

Qiangfu Zhao. "Information Hiding Based on Image Morphing", 22nd International Conference on Advanced Information Networking and Applications - Workshops (aina workshops 2008), 03/2008

Publication

<1 %

51

Richard O. Day. "Extended Multi-objective fast messy Genetic Algorithm Solving Deception Problems", Lecture Notes in Computer Science, 2005

Publication

<1 %

52

[rsisinternational.org](http://rsisinternational.org)

Internet Source

<1 %

53

[spiral.imperial.ac.uk](http://spiral.imperial.ac.uk)

Internet Source

<1 %

54

[www.scipress.com](http://www.scipress.com)

Internet Source

<1 %

55

[www.scribd.com](http://www.scribd.com)

Internet Source

<1 %

56

"Intelligent Computing", Springer Science and Business Media LLC, 2019

Publication

<1 %

57

"Network Analysis", Springer Nature, 2005

Publication

<1 %

---

58

"Progress in Advanced Computing and Intelligent Engineering", Springer Science and Business Media LLC, 2019

Publication

<1 %

---

59

Lecture Notes in Electrical Engineering, 2014.

Publication

<1 %

---

60

N. D. Jambhekar, C. A. Dhawale, R. Hegadi. "Performance Analysis of Digital Image Steganographic Algorithm", Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies - ICTCS '14, 2014

Publication

<1 %

---

61

R Palivonaite, A Aleksa, A Paunksnis, A Gelzinis, M Ragulskis. "Image hiding in time-averaged deformable moiré gratings", Journal of Optics, 2014

Publication

<1 %

---

62

Zvi Retchkiman Konigsberg. "Stability Problem for a Predator-Prey System", Lecture Notes in Computer Science, 2010

Publication

<1 %

---

63

"Integrated Intelligent Computing, Communication and Security", Springer Science and Business Media LLC, 2019

<1 %

64

César Martínez-Olvera, Jaime Mora-Vargas. "A Max-Plus Algebra Approach to Study Time Disturbance Propagation within a Robustness Improvement Context", Mathematical Problems in Engineering, 2018

Publication

<1 %

---

65

Paulo Roberto Ceridorio Correa, Esteban Mauricio Cordero, Luciana Giroto Gentil, Ethel Bayer-Santos, José Franco da Silveira. " Genetic Structure and Expression of the Surface Glycoprotein GP82, the Main Adhesin of Metacyclic Trypomastigotes ", The Scientific World Journal, 2013

Publication

<1 %

---

66

Raul Velasquez, Mihai O. Marasteanu, Joseph F. Labuz. "Microstructure Characterization of Asphalt Mixtures with 2- and 3-Point Correlation Functions", Road Materials and Pavement Design, 2011

Publication

<1 %

---

Exclude quotes Off

Exclude matches Off

Exclude bibliography On

# On Max-Plus Algebra and Its Application on Image Steganography

---

GRADEMARK REPORT

---

FINAL GRADE

**/0**

GENERAL COMMENTS

**Instructor**

---

PAGE 1

---

PAGE 2

---

PAGE 3

---

PAGE 4

---

PAGE 5

---

PAGE 6

---

PAGE 7

---

PAGE 8

---

PAGE 9

---