ATLANTIS PRESS

Advances in Computer Science Research

Series: Advances in Computer Science Research

Proceedings of the International Conference on Mathematics, Geometry, Statistics, and Computation (IC-MaGeStiC 2021)

Session: Computation

6 articles

Proceedings Article

DOPE: MDC-2 Scheme Using PRESENT

Anjeli Lutfiani, Bety Hayat Susanti

Modification Detection Code (MDC) as an unkeyed hash function is designed to provide data integrity. Manipulation Detection Codes (MDC-2) is one of double-length (2n-bit) hash-values that requires 2 block cipher operations per block of hash input where the output size of the hash function is twice the...

Article details

Download article (PDF)

Proceedings Article

Primary Key Encryption Using Hill Cipher Chain (Case Study: STIE Mandala PMB Site)

Muhamat Abdul Rohim, Kiswara Agung Santoso, Alfian Futuhul Hadi

The condition of the world experiencing the COVID-19 pandemic has resulted in some daily activities limited by health protocols. The Indonesian government's policy in the academic field has forced STIE Mandala Jember, as one of the private universities, to implement online-based new student admissions....

Article details

Download article (PDF)

Proceedings Article

A Modification of ECDSA to Avoid the Rho Method Attack

Amira Zahra, Kiki Ariyanti Sugeng

Elliptic Curve Digital Signature Algorithm (ECDSA) is a digital signature algorithm that utilizes an elliptic curve. ECDSA consists of three steps, which are key generation, signature generation, and verification algorithm. ECDSA is used on Bitcoin transactions to generate the user's public key, private...

Article details
Download article (PDF)

Proceedings Article

Image Authentication Based on Magic Square

Kiswara Agung Santoso, Maulidyah Lailatun Najah, Moh. Hasan

Image is a digital media that is easy to change, so it is susceptible to being used for crime. Image changes may be affected by the unstable internet during transmission or deliberate manipulation of images for specific purposes. Hence, we need a tool to determine the authenticity of the image. One strategy...

Article details
Download article (PDF)

Proceedings Article

Pattern Recognition of Batik Madura Using Backpropagation Algorithm

Abduh Riski, Ega Bandawa Winata, Ahmad Kamsyakawuni

Since October 2, 2009, UNESCO has acknowledged batik as one of Indonesia's intellectual properties. Throughout the archipelago, distinct and diverse batik motifs have emerged and been produced with the passage of time; Madura batik is one of them. The Backpropagation Algorithm is used to recognize Madura...

Article details
Download article (PDF)

Proceedings Article

Hybrid Cat-Particle Swarm Optimization Algorithm on Bounded Knapsack Problem with Multiple Constraints

Kiswara Agung Santoso, Muhammad Bagus Kurniawan, Ahmad Kamsyakawuni, Abduh Riski

Optimization problems have become interesting problems to discuss, including the knapsack problem. There are many types and variations of knapsack problems. In this paper, the authors introduce a new hybrid metaheuristic algorithm to solve the modified bounded knapsack problem with multiple constraints...

Article details
Download article (PDF)

Advances in Computer Science Research, volume 96
Proceedings of the International Conference on Mathematics, Geometry, Statistics, and Computation (IC-MaGeStiC 2021)

Image Authentication Based on Magic Square

Kiswara Agung Santoso*, Maulidyah Lailatun Najah, Moh. Hasan

Department of Mathematics, University of Jember, Indonesia
**Corresponding Author. Email : kiswaras@gmail.com*

ABSTRACT
Image is a digital media that is easy to change, so it is susceptible to being used for crime. Image changes may be affected by the unstable internet during transmission or deliberate manipulation of images for specific purposes. Hence, we need a tool to determine the authenticity of the image. One strategy that can be used is to insert code into the entire image, so that any changes to the image information can be detected. The insertion process performed by dividing the image into several blocks, where the size of each block is adjusted according to the size of the magic square order 3. For the authentication process, the image that has been manipulated will be counted for each pixel. The results show that the manipulated image can be detected. The parts of the image that have changed can be identified because the pixel value doesn't satisfy the magic square rule.

Keywords: *Authentication, Image, Magic square, Pixel.*

1. INTRODUCTION

The development of more and more advanced technology has made it easier to send images. This fact can cause the risk of image security to be threatened, because the security system on the internet is not yet stable. What's more, images can also be manipulated easily for specific purposes. Therefore, it is often used as a crime usually committed by irresponsible persons [1].

Research [2-6] discusses how to detect image authenticity using cryptographic techniques by utilizing hash functions. Detection is done by comparing the hash value of the original image and the manipulated image. In [7] and [8] an image was analyzed using image forensics. The contrast difference between the original image and the manipulated image shows that there is a change in the image. At the same time, [9] detects modified image with GRB deviation. Color changes are identified by calculating the average deviation value for each RGB color. Some of the studies only focus on detecting whether the image has been tampered with or not. However, they didn't explain, which parts of the image had changed.

In this research, we propose an image authentication scheme with steganography techniques and identify the parts of the image that have changed. The method to be used is the LSB method with a magic square code order 3. This insertion process doesn't change the appearance of the image, so it can best protect the image and confirm its authenticity.

2. METHODS

Steganography is a science that studies techniques to hide secret messages on digital media, so that no one is aware of the existence of the secret message [10]. One of the most frequently used digital media is an image. An image is composed of a number of pixels that represent their presence and color. Color images are stored in a 24-bit file for the RGB (Red Blue Green) color model, where each color is represented by 8 bits. The bit is divided into 2 parts, the first 4 bits are called MSB (Most Significant Bit) and the last 4 bits are called LSB (Least Significant Bit). The following figure shows the position of the bit values.

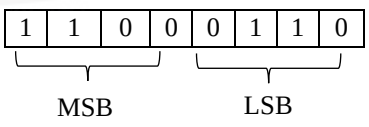

Figure 1 Position of MSB and LSB.

The image changes can be seen in the pixel change that affect the RGB base colors. So, to carry out the

authentication process, the image will be inserted with a code so that any changes in the image can be detected. The method that will be used is the LSB method, which replaces the last 4 bits of each pixel in the image with the code to be inserted. Changes in the LSB bit value won't affect the pixel value significantly, so that color changes in the image are not easily visible to the human eye [11]. The code that is inserted is magic square order 3.

A magic square is an arrangement of random numbers in cell, where the sum of each row, column, and diagonal is the same [12]. Magic square usually contains consecutive natural numbers that differ from 1 to n^2. While the number of magic constants in each row, each column, and each diagonal is called the Magic Constants, where $M_n = \frac{n(n^2+1)}{2}$ [13]. Figure 2 is an example of a magic square order 3.

6	1	8
7	5	3
2	9	4

Figure 2 Magic square order 3.

As can be seen from the above figure, a magic square order 3 is composed of natural numbers from 1 to 9. If we add these numbers horizontally, vertically, and diagonally, it will produce the same value, which is 15.

This research is divided into two processes, that is the code insertion process and the authentication process.

2.1. Code Insertion Process

The code insertion process is used to maintain image security. Each pixel in the image will be inserted with a magic square code using the LSB (Least Significant Bit) method. The LSB method has the advantage that it doesn't produce visible changes in the image and provides very high interference detection [14]. The process of inserting the code in the image can be seen as shown in Figure 3.

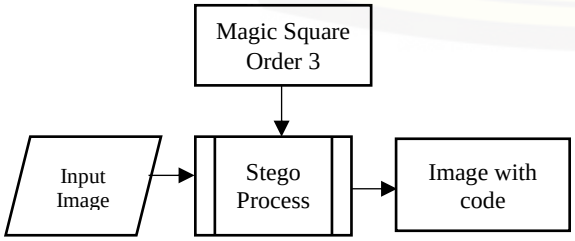

Figure 3 Code insertion.

Steps for code insertion :

a. Insert an image with a size of $h \times w$ pixels.
b. Divide the image into blocks, where each block is 3×3 pixels. So, the number of blocks $= \left\lfloor \frac{h}{3} \right\rfloor \times \left\lfloor \frac{w}{3} \right\rfloor$.
c. Convert the image pixel value to 8 bits.
d. Generate a magic square order 3 and convert the magic constant to 4 bits.
e. For each block, replace the LSB bit with the appropriate magic constant.
f. The image that has been coded is saved in the .bmp format.

PSNR is used to compare the quality of the original image with the image that has been coded. PSNR is defined as:

$$PSNR = 10\, log_{10}\left(\frac{C_{max}^2}{MSE}\right)$$

where C_{max}^2 holds the maximum pixel value in the image and MSE (Mean Square Error) is given as:

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}\left(S_{xy} - C_{xy}\right)^2$$

where x and y are the image coordinates, M and N are the dimensions of the image, S_{xy} is the code inserted image, and C_{xy} is the original image [15].

PSNR is usually expressed in decibels (dB). A PSNR value lower than 30dB indicates that the quality is quite low, that is, the distortion caused by the insertion is obvious. However, high quality should strive for 40db and above. Therefore, the greater the PSNR value of the code inserted image, the more similar the original image will be, and it will be difficult for the human eye to distinguish.

2.2. Authentication Process

The authentication process is used to check the authenticity of the image. The authentication process is carried out by identifying changes in each pixel in the image. Calculate the pixel value of the image to be tested and check whether it does satisfy the rule of magic square order 3. Systematically, we can see the image authentication process can as shown in Figure 4.

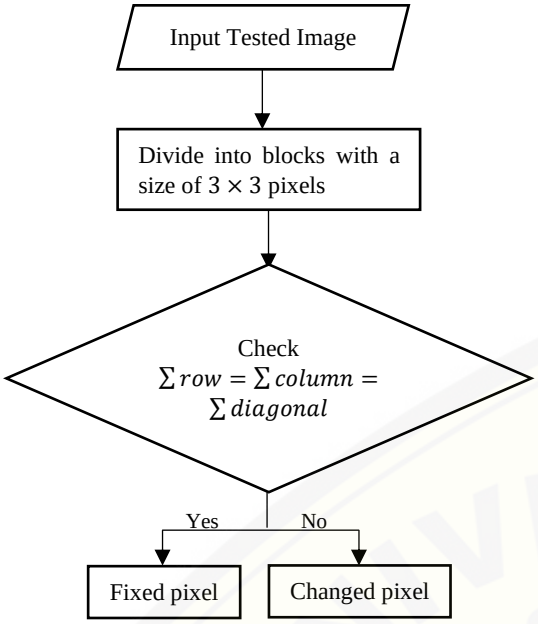

Figure 4 Authentication process.

Steps for authentication process:

a. Enter the image to be tested
b. Convert the image pixel value to 8 bits
c. Divide the image into blocks, where each block is 3 × 3 pixels
d. For each block, calculate the sum of LSB bits horizontally ($\sum row$), vertically ($\sum column$), and diagonally ($\sum diagoonal$).

   if $\sum row = \sum column = \sum diagonal$
      Fixed pixel value
   else
      Changed pixel value
   end

This research is assisted by the Matlab R2015a program in its calculations. The program will display the results of the authentication process in the form of an image. The manipulated image will be detected if it doesn't satisfy the magic square rules. In addition, the color of the changed pixels in the imagewill become white.

3. RESULTS

The object of this research is prepare an original image and two images that have been manipulated.

3.1. Code Insertion Process

The first step is to input the original image of 401 × 764 pixels.

Figure 5 Original image.

Divide the image into blocks, where each block is 3 × 3 pixels. The number of blocks formed is $\left\lfloor\frac{401}{3}\right\rfloor \times \left\lfloor\frac{764}{3}\right\rfloor = 133 \times 254$. Then, generate a magic square order 3 and convert the constant to 4 bits.

8	1	6	⇨	1000	0001	0110
3	5	7		0011	0101	0111
4	9	2		0100	1001	0010

Figure 6 Convert the magic constant to 4 bits.

Next, replace the LSB bit with the magic constant corresponding to each block. For example, take a 3 × 3 pixel sample from Figure 5.

1100**0000**	1011**1101**	1011**0100**
1011**1111**	1011**1100**	1011**0011**
1011**1011**	1011**0111**	1011**0000**
⇩		
1100**1000**	1011**0001**	1011**0110**
1011**0011**	1011**0101**	1011**0111**
1011**0100**	1011**1001**	1011**0010**

Figure 7 LSB bit insertion with constant.

Repeat the above steps until all blocks are complete. Then, save the inserted image in bmp format.

Figure 8 Image with code.

The obtained PSNR value is 53dB, which indicates that the resulting image is of good quality.

3.2. Authentication Process

The authentication process is carried out on 2 images that have been edited with the Adobe Photoshop application. The first image is the result of pasting an image of a cat with a fake head. While the second image is the result of pasting an image of a cat with a fake body.

Figure 9a Cat with a fake head.

Figure 9b Cat with a fake body.

Using the proposed technique, Figures 9a and 9b are processed to find out which parts have been manipulated. Every pixel in the image that doesn't satisfy the magic square rule order 3 will be detected, which indicates that the part has changed. The authentication results can be seen in Figure 10.

Figure 10a Result of Figure 9a.

Figure 10b Result of Figure 9b.

From Figure 10a, it can be seen that the cat's head turns white. It indicates that another image has been pasted on the head, as if it were the original image. Likewise, with image 10b, almost all parts of the image turn white, except for the cat's head. It means that only the head is original, and the other parts are patches.

This authentication scheme can be used to identify partial image changes and overall image changes. So, we can find out which parts of the image have been manipulated. This scheme is very sensitive to any changes in pixels. If there is only 1 pixel in the image that doesn't satisfy the magic square rule, the change will be detected.

4. CONCLUSION

We propose the idea of a simple image authentication scheme. This scheme can be used to determine the authenticity of the image by generating a magic square order 3. The original image is inserted with the LSB method to make it more secure. Based on the results, it can be concluded that the magic square code can be used as an image protection tool. Image that has been manipulated can be detected properly. If the pixels in the image don't satisfy the magic square rule, the change will be detected and the color will turn white. So, this scheme can make it easier for someone to authenticate the image.

REFERENCES

[1] K.N. Isnaini, H. Ashari, A.P. Kuncoro, Analisis forensic untuk mendeteksi keaslian citra digital menggunakan metode NIST (in Indonesian), Journal of Resistor, vol. 3(2), 2020, pp. 72-81.

[2] S. Hajar, Analisa metode message digest 5 (Md5) untuk mendeteksi orisinalitas citra digital (in Indonesian), Journal of Pelita Informatika: Informasi dan Informatika, vol. 9(3), 2021, pp. 142-148.

[3] I. Saputra, S.D. Nasution, Analisa algoritma SHA-256 untuk mendeteksi orisinilitas citra digital (in Indonesian), Proceedings of Seminar Nasional Riset Information Science, 2019, pp. 164-178.

[4] L.K. Bagariang, Perancangan aplikasi deteksi orisinilitas citra digital menerapkan metode whirpool (in Indonesian), Journal of Information and Scientific Technology, vol. 8(1), 2020, pp. 34-36.

[5] P.M. Simanullang, S. Sinurat, I. Saputra, Analisa metode SHA-384 untuk mendeteksi orisinalitas citra digital (in Indonesian), National Information Technology and Computer Conference, vol. 3(1), 2019, pp.187-198.

[6] J. Lahagu, Mendeteksi orisinalitas citra digital dengan menerapkan metode Adler-32 (in Indonesian), National Information Technology and Computer Conference, vol. 3(1), 2019, pp. 789-797.

[7] I. Riadi, A. Yudhana, W.Y. Sulistyo, Deteksi pemalsuan foto digital menggunakan image forensics (in Indonesian), Journal of Mobile and Forensics, vol. 1(1), 2019, pp. 13-21.

[8] T. Sari, I. Riadi, A. Fadlil, Forensik citra untuk deteksi rekayasa file menggunakan error level analysis (in Indonesian), Proceedings of Annual Research Seminar, 2016, pp. 133-138.

[9] Heriyanto, Analisa deteksi gambar termodifikasi dengan deviasi RGB (in Indonesian), Journal of Telematika, vol. 9(2), 2013, pp. 93-100.

[10] R.J. Anderson, F.A.P. Petitcolas, On the limits of steganography, Journal of IEEE on Selected Areas in Communication, vol. 16(4), 1998, pp. 474-481.

[11] K.A. Santoso, Fatmawati, H. Suprajitno, Image encryption technique based on pixel exchange and XOR operation, Proceedings of International Basic Science Conference, 2017, pp. 286-288.

[12] R. Prajapati, et al., A study on magic square, Proceedings of the 5th National Conference on Role of Engineers in Nation Building, 2017.

[13] J. Sesiano, Magic Square: Their History and Construction From Ancient Times to AD 1600, Geneva : Springer, 2019.

[14] C. Rey, J. Dugelay, A survey of watermarking algorithms for image authentication, Journal of EURASIP on Applied Signal Processing, 2002, pp. 613-621.

[15] A. Cheddad, J. Condell, K. Curran, P. Mc Kevitt, Digital image steganography: survey and anylisis of current methods, Signal Processing, vol. 90(3), 2010, pp. 727-752.