The Authenticity of Image using Hash MD5 and Steganography Least Significant Bit

Nurul Khairina[1], Muhammad Khoiruddin Harahap[2], Juanda Hakim Lubis[1]

[1]Universitas Medan Area
[2]Politeknik Ganesha Medan
[1]nurulkhairina27@gmail.com, [2]choir.harahap@yahoo.com,
[3]juandahakim@gmail.com

Abstract

A creation can be considered as belonging to someone if they have a valid proof. An original creation that have been changed for certain purposes will definitely eliminate proof of ownership of the creation. A hash function is one method used to test the authenticity of data, while steganography is one method used to maintain the security of confidential data from outside parties. In this study, the Hash MD5 method will be combined with the Least Significant Bit method to test the authenticity of an image. The purpose of testing the authenticity is to find out the truth of ownership of a creation, in this case, we are testing the image. The results of this test are the status of an image that will be declared valid or invalid. Measurement of validity depends on whether there is a similarity between the value of the Hash that has been implanted and the value of the Hash obtained during the test. If the tested image has the same Hash value, then the image will be declared valid, but instead ai image is declared invalid if the image has been modified or ownership status has been changed. From the result of testing the authenticity with several images, it can prove that the combination of the Hash MD5 method with LSB has a good level of security and suitable to authenticity testing.

Keywords: *Authenticity, Hash, MD5, Stegnography, Least Significant Bit*

1. Introduction

The protection of the confidentiality of the data and the message will be a separate concentration. In the computer science, steganography is the art and a science that is used to maintain data security or confidential messages. Steganography is unique because it uses the media to maintain data confidentiality [1][2][3]. Technological sophistication accompanied by a very drastic development of science, cannot deny that security of data confidentiality is very important. This also applies to creation. A creation produced by someone must have its own ownership mark. But not infrequently, the sign can be removed for the needs of irresponsible people, so that it will eliminate the authenticity of the creation and harm the original owner. This phenomenon encourages every researcher to continue to develop ideas and research in order to continue to produce the best data security methods.

On the previous research, Muneeza et al [4] using a combination of Hash MD5 and Least Significant Bit to authenticate the integrity of digital images. On the results of this study, there is no change in image size. Besides that, The researcher can also detect images if the image has been modified by an irresponsible party. Dian et al [5] compare Hash MD5 and SHA256 to form the digital signature. The result of this research that the complexity of Hash MD5 and SHA256 are the same and the speed of Hash MD5 is better than SHA256. Krishna et al [6] implement Hash MD5 and Freeman Chain to identifying a fingerprint image. The accuracy of this method is 100%. This can be proven through the success of the method in matching input fingerprint image with the identity of the user.

Hakim et al [7] offer a new method that is modified of Hash MD5 and SHA256 to improve the security of the message. In this research, the researchers found that the

ISSN : 2580-7250

methods they offered had better complexity and security, even better than Hash MD5 and SHA256. Gurpreet et al [8] conducted research on Efficient Hash Algorithm (EHA) which is a derivative of the SHA160 method. In the test, the researcher compared it with the previous generation of hash methods, like MD2, MD5, SHA160, SHA256, SHA 384 and SHA 512. From this study, it can be seen that EHA is more efficient than previous types of hashes. Meena et al [9] conducted research using One Way Hash Function to verify data integrity in cloud computing. The results showed that the proposed method was more efficient, have better data security, and are more resistant to external attacks.

Anil et al [10] perform a combination of RSA cryptographic algorithms with LSB steganography algorithms and Hash functions. The purpose of this study is to improve data security. Layered security can be seen in the encryption process in the message before being inserted with the steganography algorithm. In this research, the researcher will combine the MD5 Hash function with the Least Significant Bit (LSB) steganography to give ownership marks and test their authenticity, this testing will be done to the image.

2. Rudimentary

2.1 Steganography

The word steganography comes from Greek which means "hidden writing". The word steganography is divided into two syllables, namely "steganos" which means "protected”, and "graphic" which means "writing" [10]. Steganography related to confidentiality of data [11] need media or cover object in the form of text, images, music, and videos to hide messages or data. Steganography is one of the data security sciences that does not invite suspicion of other parties to the existence of confidential data hidden in certain media [12]. The success of steganography in hiding confidential data can be measured with at least 3 parameters, namely security, capacity and imperceptibility [13].

2.2 Hash MD5 Algorithm

Hash MD5 was introduced by Professor Ronald L.Rivest [5] and is part of modern cryptography. Hash MD5 algorithm is a one-way hash function with the hash value 128 bit. Hash is said to be a one-way function because the message entered will be converted into a short message or “message digest” and it is difficult to return to the initial message. The Hash function is able to change input messages that have arbitrary lengths, be a short message whose length is always fixed [14] [15].

The initial message that will be processed with the Hash MD5 will be divided into 512-bit blocks, then the block is divided into 16 sub-blocks by 32 bits. The result of this Hash MD5 is a set of 4 blocks, each consisting of 32 bits, which then produces a 128-bit hash value [16]. The block diagram of Hash MD5 is as follows [17] :

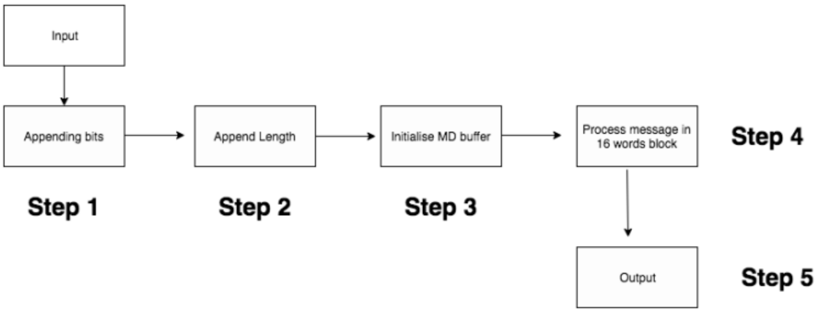

Figure 1. Block Diagram of MD5 Algorithm [17]

where :

Step 1 : “Appending Bits”, where the length of the message must be congruent with 448, modulo 512. In this process, the message bit will be extended, it will be added single “1” bit at the end of the message, which will be followed by “0” bit as needed until the message bit length matches congruent 448, modulo 512.

Step 2 : “Append Length”, where a 64-bit representation of the length of the message will be added to the message results that have been previously obtained

Step 3 : “Initialize MD Buffer”, where four 32-bit variable are initialized, They are :
A = 0x01234567
B = 0x89ABCDEF
C = 0xFEBCDA98
D = 0x76543210
These are called chaining variables.

Step 4 : “Process Messages in 16-word bitswhere there are 4 nonlinear functions that will be used to process messages, and will produce message digest. The four functions are :
$F(X,Y,Z) = (X \wedge Y) \vee ((\sim X) \wedge Z)$
$G(X,Y,Z) = (X \wedge Z) \vee (Y \wedge (\sim Z))$
$H(X,YZ) = X \oplus Y \oplus Z$
$I(X,Y,Z) = Y \oplus (X \vee (\sim Z))$
($\vee$ is OR, $\wedge$ is AND, $\oplus$ is XOR, ($\sim$is NOT)

Step 5 : “Output”, the result of the MD5 Hash is a message digest consisting of 32 bits [17].

2.3 Least Significant Bit (LSB) Method

Least Significant Bit is a term that indicates the backmost bit (8th bit). Changing the value of this bit does not have much effect on the value of a pixel. The LSB method in steganography is a simple and safe method for inserting secret messages because this method doesn't change much in stego image, so as not to arouse suspicion [18]. In the picture below, for example, we want to insert 3 binary digits "101" in 3-pixel images with a value of 200, 195, 221, then the process that occurs until the pixel image changes, is as follows :

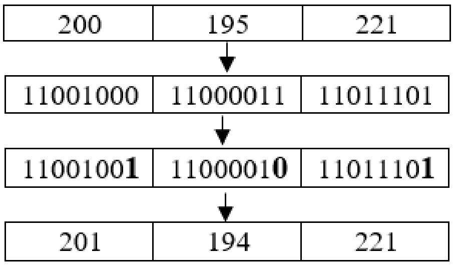

Figure 2. Least Significant Bit Process

3. Research Methodology

The proposed method in this study is as follows :

a. Requirements image size (Px * Py) > 256
b. Hash MD5 generates a 32 characters string from red pixels (see Fig. 3 below)
c. Convert Hash MD5 to a binary form that is 32 char * 8 bits = 256 pixels
d. Separate images in 2 blocks
e. The first block (B1) 256 pixels are ordered specifically for the LSB insertion location of the Hash MD5 that has been converted to binary
f. The second block (B2) the next block pixel as the source to generate the MD5 Hash

g. Comparing B1 = MD5 (B2) then the image is expressed as the original image
h. If B1 <> MD5 (B2) there is an option that the coding process will be carried out or state that the image is not original
i. To watermark the image, insert the result of point (b) to B1

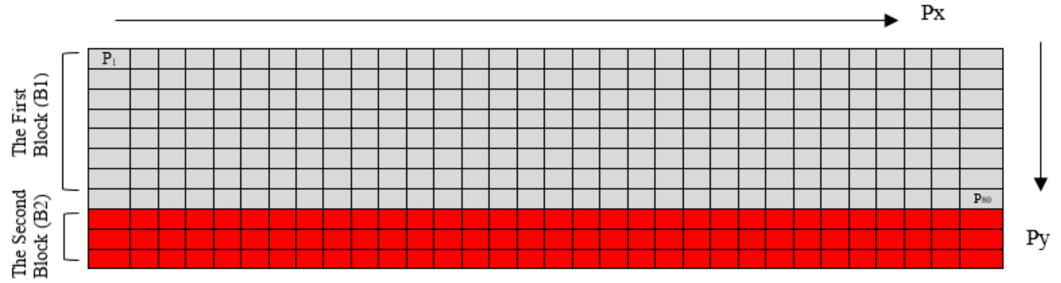

Figure 3. Scheme Image

Caption :
Gray Color: Hash MD5 Block Reserve
Red Color: Block for Generating Hash MD5

4. Result and Discussion

In this section, the researcher presents the results of research on the combination of the Hash MD5 method with the Least Significant Bit Steganography method in authenticity. Tests on this research can be seen in Table 1 below :

Table 1. The Test Results from Combination of Hash MD5 and LSB

No	Image File	File Size (KB)		Pixel Dimensi Width x Height		Embedded Hash Code Hash Code Obtained	Status for Authenticity Testing	Time Complexity (s)
		Before	After	Before	After			
1	Nurul.jpg	11.3	27.2	144 x 152	126 x 162	42393E7F121AB81B1678EAD5EB883879 42393E7F121AB81B1678EAD5EB883879	Valid	10,90
2	Sinkron.jpg	20.3	20.3	150 x 147	150 x 147	7C903E3C587BBB4C3C7F84E5EA339A52 7C903E3C587BBB4C3C7F84E5EA339A52	Valid	17.18
3	Semantika.jpg	12.8	12.8	279 x 101	279 x 101	F9E2B445F87B8824B0D8255C8FE19DB3 F9E2B445F87B8824B0D8255C8FE19DB3	Valid	05.30
4	Polgan.jpg	18.2	18.2	417 x 131	417 x 131	195DCA4ADC472F92F291BDBCF04DC3E2 195DCA4ADC472F92F291BDBCF04DC3E2	Valid	12.35
5	UMA.jpg	164	164	400 x 400	400 x 400	70A415FA1CC6B182CFC532CFE7F17503 70A415FA1CC6B182CFC532CFE7F17503	Valid	90.02

The following is the image used in the test in Table 1 above :

Figure 4. image for Authenticity Testing (a) Nurul, (b) Sinkron, (c) Semantika, (d) Polgan, (e) UMA

5. Conclusion

From the results of this study, it can be concluded that the combination of the MD5 Hash method with the LSB steganography method can test the authenticity of an image well. An image is declared valid if the Hash Code implanted is the same as the Hash Code obtained when testing authentication. And conversely, an image is declared invalid if the Hash code obtained is not the same as the embedded Hash Code.

As for suggestions for the development of this research going forward, the next researcher can combine the MD5 Hash method with other algorithms for testing authenticity, and can test the image with a more complex color arrangement.

References

[1] S. K. R. Suman, "A Secure Steganographic Method Using Modified LSB (Least Significant Bit) Substitution," *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, vol. 6, no. 8, pp. 1268-1273, 2017.

[2] H. L. Hussein, "Hiding Data in Color Image Using Least Significant Bits of Blue Sector," *Ibn Al-Haitham J. for Pure & Appl. Sci.*, vol. 31, no. 2, pp. 193-198, 2018.

[3] R. Gaur, R. Vig and AmanpreetKaur, "An Effectual Hybrid Approach Using Data Encryption Standard (DES) and Secured Hash Algorithm (SHA) for Image Steganography," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 6, no. 5, pp. 44-53, 2018.

[4] M. Wahid, N. Ahmad, M. H. Zafar, and S. Khan, "On Combining MD5 for Image Authentication using LSB Substitution in Selected Pixels," in *International Conference on Engineering and Emerging Technologies (ICEET)*, Lahore, 2018.

[5] D. Rachmawati, J. T. Tarigan, and A. B. C. Ginting, "A comparative study of Message Digest 5(MD5) and SHA256," *Journal of Physics: Conference Series*, vol. 978, pp. 1-6, 2018.

[6] K. K. Prasad and P. S. Aithal, "A Study on Fingerprint Hash Code Generation Based on MD5 Algorithm and Freeman Chain Code," *International Journal of Computational Research and Development (IJCRD)*, vol. 3, no. 1, pp. 13-22, 2018.

[7] S. Hakim and M. Fouad, "Improving Data Integrity in Communication Systems by Designing a New Security Hash Algorithm," *Journal of Information Sciences and Computing Technologies(JISCT)*, vol. 6, no. 2, pp. 638-647, 2017.

[8] G. K. Sodhi and G. S. Gaba, "An Efficient Hah Algorithm to Preserve Data Integrity," *Journal of Engineering Science and Technology*, vol. 13, no. 3, pp. 778-789, 2018.

[9] M. Kumari and R. Nath, "A Secure and Flexible One Way Hash Function for Data Integrity Verification in Cloud Computing Environment," in *International Conference on Next Generation Computing Technologies*, Dehradun, 2018.

[10] A. Kumar and R. Sharma, "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 7, pp. 363-372, 2013.

[11] N. Singh and J. Bhardwaj, "Comparative Analysis for Steganographic LSB Variants," in *International Conference on Computing, Communication and Signal Processing (ICCASP)*, Maharashtra, 2018.

[12] E. Emad, A. Safe, A. Refaat, Z. Osama, E. Sayed, and E. Mohamed, "A secure image steganography algorithm based on a least significant bit and integer wavelet transform," *Journal of Systems Engineering and Electronics,* vol. 29, no. 3, pp. 639-649, 2018.

[13] J. Bhadra, M.K.Banga and M. Murthy, "Securing Data Using Elliptic Curve Cryptography and Least Significant Bit Steganography," in *International Conference on Smart Technology for Smart Nation*, Bangalore, 2017.

[14] Hendra Pasaribu, "Combination of advanced encryption standard 256 bits with md5 to secure documents on android smartphone," *Journal of Physics: Conference Series,* vol. 1007, pp. 1-8, 2018.

[15] A. Menezes, O. P.V. and S.Vanstone, Handbook of Applied Cryptography, CRC Press,1996

[16] B. Schneier, Applied Cryptography Protocols, Algorithms, and Source Code in C. Second Edition, Jhon Wiley & Sons, Inc: California, 1996.

[17] A. Bhandari, M. Bhuiyan and P. W. C. Prasad, "Enhancement of MD5 Algorithm for Secured Web Development," *Journal of Software,* vol. 12, no. 4, pp. 240-252, 2017.

[18] S. M. Klim, "Selected Least Significant Bit Approach for Hiding Information Inside Color Image Steganography by using Magic Square," *Journal of Engineering and Sustainable Development,* vol. 21, no. 1, pp. 74-88, 2017.

Authors

1st Author
Nurul Khairina
Lecturer of Universitas Medan Area

2nd Author
Muhammad Khoiruddin Harahap
Lecturer of Politeknik Ganesha Medan

3rd Author
Juanda Hakim Lubis
Lecturer of Universitas Medan Area