Plagiarism Checker X Originality Report

Similarity Found: 12%

Date: Monday, November 06, 2023
Statistics: 470 words Plagiarized / 3963 Total words
Remarks: Low Plagiarism Detected - Your Document needs Optional Improvement.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195 IMPLEMENTATION OF ELGAMAL AND LEAST SIGNIFICANT BIT (LSB) ALGORITHM FOR ENDING AND HIDDEN MESSAGES IN DIGITAL IMAGES TONNI LIMBONG1, A M H PARDEDE2, DESINTA PURBA3, LAMHOT SITORUS4 1,3,4Fakultas Ilmu Komputer, Universitas Katolik Santo Thomas Medan, Indonesia 2STMIK Kaputama, Jl. Veteran No.

4A-9A, Binjai- Sumatera Utara, Indonesia E mail: 1tonni.budidarma@gmail.com, 2akimmhp@live.com ABSTRACT Basically, confidential data needs to be stored or conveyed in a certain way so that it is not known by unauthorized foreign parties. And to overcome this problem, the science of cryptography and steganography was created.

Cryptography is the art and science of keeping messages confidential by disguising them in an encoded form that has no meaning, while steganography is the art and science of hiding secret messages inside other messages so that the whereabouts of the secret message cannot be known. Steganography keeps messages secret by hiding messages.

The current implementation of steganography uses digital media as a medium for storing or hiding messages, one of which is image media (digital image). The combination of cryptography and steganography can provide better security for secret messages, where secret messages are first encrypted using the ElGamal algorithm, then the ciphertext results from the cryptography are hidden in image media using the Least Significant Bit (LSB) steganography method.

The implementation of cryptographic algorithms and steganography methods can further increase the security of secret messages. Keywords: Ciphertext, Cryptography, ElGamal, Encryption, Steganography.

INTRODUCTION Without a guarantee of security in data transmission, of course there will be a risk when sensitive, important and valuable information is accessed by people who are not authorized and responsible, resulting in the data being misused which can be detrimental to the owner of the data.

Facing data or information security threats, security techniques are needed, and maintaining the confidentiality of messages using cryptographic and stenographic algorithms. Basically, confidential data needs to be stored or conveyed in a certain way so that it is not known by unauthorized foreign parties. And to overcome this problem, the science of cryptography and steganography was created.

Cryptography is the art and science of keeping messages confidential by disguising them in an encoded form that has no meaning, while steganography is the art and science of hiding secret messages inside other messages so that the whereabouts of the secret message cannot be known. Steganography keeps messages secret by hiding messages.

The current implementation of steganography uses digital media as a medium for _storing or hiding messages, one of which is image media (digital image). The ElGamal algorithm is a cryptographic algorithm created by Taher ElGamal in 1984. The ElGamal algorithm is an asymmetric algorithm that has a public key consisting of three pairs of numbers and a secret key consisting of two numbers.

For the same plaintext, this algorithm provides a different ciphertext each time the plaintext is encrypted. This is due to the influence of a variable that is randomly determined during the encryption process [1]. One of the digital image steganography methods is the Least Significant Bit (LSB), with the technique of hiding messages at the lowest bit location in a digital image. The message is converted into binary bits and hidden in a digital image using the LSB method [2].

The combination of cryptography and steganography can provide better security for secret messages, where secret messages are encrypted first using the ElGamal algorithm, then the cryptographic ciphertext results are hidden in image media using the Least Significant Bit (LSB) steganography method. The implementation of cryptographic

algorithms and steganography methods can further increase the security of secret messages [2].

Cryptography (cryptography) comes from the Greek: "cryptos" means "secret", while "graphein" means "to write" (writing). So, cryptography means "secret writing". There are several definitions of cryptography that have been put forward in various literature. The definition used in old books (before the 1980s) states that cryptography is the science and art of maintaining the secrecy of messages by encoding them into a form that the meaning can no longer be understood.

This definition may be appropriate in the past when cryptography was used for the security of important communications such as communications among the military, diplomats, and spies. However, currently, cryptography is more than just privacy, but also for data integrity, authentication, and non-repudiation purposes [3]. In cryptography, there are various terms or terminology.

Some important terms to know are [4]: Message, Plaintext, and Ciphertext Messages are data or information that can be read and understood. Another name for the message is plaintext or cleartext. Messages can be in the form of data or information sent (via couriers, telecommunications channels, etc.) or stored on recording media (paper, storage, etc.).

Stored messages are not only in the form of text, but can also be in the form of images, sound, video, or other binary files. In order for the message to be hidden from other parties, the message is encoded in another form that cannot be understood. The form of the encoded message is called ciphertext (ciphertext) or cryptogram (cryptogram).

Ciphertext must be able to be transformed back into the original plaintext so that the received message can be read. Sender and Recipient Data communication involves exchanging messages between two entities. The sender (sender) is an entity that sends messages to other entities. The recipient (recipient) is the entity that receives the message.

The sender certainly wants the message to be sent safely, but he believes that other parties cannot read the contents of the message he sent. The solution is to encode the message into ciphertext. Encryption and description The process of encoding plaintext into ciphertext is called encryption or enciphering (standard name according to ISO 7498-2).

Meanwhile, the process of turning ciphertext back into plaintext is called decryption or deciphering (standard name according to ISO 7498-2). Cipher and key _Cryptographic algorithms are also called ciphers, namely the rules for encrypting and decoding, or the mathematical functions used for encryption and decryption. Some encodings require different algorithms for encoding and decoding. Cryptographic System Cryptography forms a system called a cryptographic system.

A cryptographic system (cryptosystem) is a collection consisting of cryptographic algorithms, all possible plaintext and ciphertexts, and keys. Tappers Eavesdroppers are people who try to catch messages as they are being transmitted. The aim of eavesdroppers is to get as much information as possible about the cryptographic system used to communicate with the intention of breaking the ciphertext.

Cryptanalysis and cryptology Cryptography developed in such a way that it gave birth to the opposite field, namely cryptanalysis. Cryptanalysis (cryptanalysis) is the science and art of breaking ciphertext into plaintext without knowing the key used. The culprit is called a cryptanalyst. If a cryptographer (cryptographer) transforms plaintext into ciphertext with an algorithm and key, then a cryptographer tries to solve the ciphertext to find plaintext or key. Cryptology (cryptology) is the study of cryptography and cryptanalysis. Both cryptography and cryptanalysis are interrelated.

Figure 1 shows the cryptology tree. Figure 1: Cryptography and cryptanalysis are branches of cryptology Currently steganography has been widely implemented in digital media. Digital steganography uses digital media as containers, such as digital images, digital video, or audio.

Modified information is also in digital form such as text, images, audio data and video data. Digital steganography can be used in countries where information is strictly censored or in countries where

/ message encryption is prohibited. In such countries confidential information can be hidden using steganography [4]. According to more steganography is done than cryptography [5].

This is because in cryptography the scrambling/encoding of messages will result in the message changing into strange characters, which actually creates hatred for those who read it. However, in steganography, it will not be seen at all that there is a message contained in the image [6]. METHODS AND MATERIAL The analysis of the algorithm used is the analysis of the encryption and decryption process on the ElGamal cryptographic algorithm and the analysis of the process of embedding and extracting messages using the Least Significant Bit (LSB) Steganography algorithm.

After that, it will proceed to the system design stage [7].

How ElGamal Algorithm and Least Significant Bit (LSB) Work At this stage, an analysis will be carried out on the ElGamal algorithm in carrying out the process of encrypting and decrypting messages, and also an analysis of the Least Significant Bit (LSB) algorithm in carrying out the process of inserting and extracting messages [8].

How the ElGamal Algorithm Works How the Elgamal Algorithm works is explained starting from the key formation process, the encryption process and also the decryption process. Key Formation Process, The steps involved in the key formation process are as follows: Choose any prime number p. Choose 2 random numbers g and x provided that g < p and 1= x = p - 2. Calculate y with the formula y = gx mod p.

The result of this algorithm is to generate a public key (p, g, y) and a private key: pair (p, x). The steps in the key formation process in the ElGamal algorithm can be seen in full in Figure 2. _ Figure 2: ElGamal key formation process Encryption Process, The steps to perform the encryption process on the ElGamal algorithm are as follows [9]: Enter the public key (p, g, y) as well as the plaintext to be encrypted. Convert the original message (plaintext) to ASCII.

Choose a random number k, which in this case 1 = k = p – 2 Each plaintext block (m) is encrypted using a public key with the formula: a = gk mod p and b = yk.m mod p Pairs a and b are ciphertext. The entire encryption process in the ElGamal algorithm can be seen further in Figure 3.

/ Figure 4: Decryption process in the ElGamal algorithm

Figure 3: ElGamal algorithm encryption process Process Description, The steps for decrypting the ElGamal algorithm are as follows [10]: Input password and private key (p, x) Separate the values a and b in the ciphertext, provided that: a = Ciphertext of odd order b = Even-order ciphertext. Calculate m (original message) using the formula: m = b * a(p-1-x) mod p to generate plaintext.

All stages of the decryption process in the ElGamal algorithm can be seen in full in Figure 4. _How the Least Significant Bit (LSB) Algorithm Works How the Least Significant Bit (LSB) Algorithm works is explained starting from the message insertion process and also the message extraction process [11].

Message Insertion Process, The steps in carrying out the message insertion process using the LSB algorithm are as follows: Input text to be inserted into the image. Select an image file (cover image). Count the number of pixels of the image file and the length of the text. Convert each RGB value in each image pixel into 8-bit binary form Add a marker character (#) at the end of the message to be inserted.

Convert the message to be inserted into 8- bit binary form.

/

Replace the last bit of each RGB value in each digital image pixel with the message bit value to be inserted. Convert the digital image binary code that has been inserted into a message into a new RGB image value (stego image).

All stages of message insertion using the Least Significant Bit (LSB) algorithm can be seen in full in Figure 5. / Figure 5 The message insertion process uses the LSB algorithm Message Extraction Process, The steps in carrying out the message extraction process using the LSB algorithm are as follows [12]: Enter the image file (stego image) Read each pixel of the image file from start to finish.

_Convert each RGB value in each stego image pixel into 8-bit binary form Take the last bit of each RGB value in each stego image pixel, then divide each into 8 bits, then convert it into a character based on the ASCII table e. Remove the marker character at the end of the message (#), so you get the original message. The entire message extraction process using the Least Significant Bit (LSB) algorithm can be seen in full in Figure 6.

Figure 6 Message extraction process using the LSB algorithm SYSTEM ANALYSIS AND DESIGN To better understand every process that occurs in an application that is built, in the following the author will provide an example [13]. Key formation process For example, the value p = 383, g = 148, x = 338 is chosen

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Then calculate: y = gx mod p = 148338 mod 383 = 295 Thus, the public key (p, g, y) = (383, 148, 295) and the private key (p, x) = (383, 338) Message encryption process For example the message to be encrypted is the word "RAPOT", then the encryption process is as follows: Convert the original message (plaintext) to ASCII, as shown in table 1.

Table 1: Message conversion to ASCII i _Plainteks _Plainteks mi _ASCII _ _1 _R _m1 _82 _ _2 _A _m2 _65 _ _3 _P _m3 _80 _ _4 _O _m4 _79 _ _5 _T _m5 _84 _ _

Choose a random number k, which in this case 1 = k = p – 2 In this case the k value chosen is k1 = 319, k2 = 259, k3 = 353, k4 =105, k5 = 267 Each plaintext block (m) is encrypted using a public key with the formula: a = gk mod p dan b = yk.m

mod p a1 = 148319 mod 383 = 197; b1 = 295319 * 82 mod 383 = 375 a2 = 148259mod 383 = 122; b2 = 295259 * 65 mod 383 = 43 a3 = 148353 mod 383 = 85; b3 = 295353 * 80 mod 383 = 52 a4 = 148105 mod 383 = 379; b4 = 295105 * 79 mod 383 = 33 a5 = 148267 mod 383 = 340; b5 = 295267 * 84 mod 383 = 272 Pairs a and b are ciphertext. So that the ciphertext obtained is 197 375 122 43 85 52 379 33 340 272 Message insertion process, After the message is successfully encrypted, then the ciphertext will be inserted into a digital image [14]. Suppose an image is 8x12 pixels in size, with RGB values for each pixel in decimal form, as shown in table 2.

Table 2: RGB values in an 8 x 12 image _Convert each RGB value at each pixel into 8-bit binary form, as shown in table 3. Table 3: Conversion of RGB values in images into 8-bit binary

```
200, _194, _192, _198, _211, _200, _194, _192, _ _189, _185, _170, _168, _162, _189, _185,
_170, _ _203 _146 _87 _18 _7 _203 _146 _87 _ _198, _211, _201, _199, _201, _198, _209,
_201, _ _168, _162, _190, _190, _179, _168, _160, _190, _ _18 _7 _204 _151 _96 _18 _5 _204
_ _199, _201, _198, _209, _193, _189, _185, _196, _ _190, _179, _168, _160, _189, _190, _190,
_170, _ _151 _96 _18 _5 _203 _192 _170 _111 _ _
```

/ /

```
 / / R=11010100 _R=10111110 _R=10111000 _R=11010000 _R=11000010 _R=11101000
_R=11000100 _R=10111110 _R=11001110 _R=11000110 _R=11000110 _R=11001000 _
_G=01101010 _G=10111010 _G=10111110 _G=10100000 _G=10111000 _G=10100000
_G=10111110 _G=11000100 _G=10011100 _G=10111110 _G=10101000 _G=10111100 _
_B=01111111 _B=11001001 _B=10101011 _B=00000101 _B=10010011 _B=10010101
_B=10111111 _B=10110001 _B=01000001 _B=10010111 _B=00010011 _B=11001011 _
_R=00011001 _R=10111101 _R=11000100 _R=11001000 _R=11000001 _R=10111011
_R=11000111 _R=11010101 _R=11000001 _R=11001001 _R=11010010 _R=11000011 _
_G=10100010 _G=10111100 _G=10101010 _G=10111110 _G=10101010 _G=01010110
_G=10110101 _G=01101010 _G=10111100 _G=10110010 _G=10100110 _G=10111000 _
_B=01000111 _B=10111110 _B=01101110 _B=11001100 _B=01010110 _B=01000011
_B=10110010 _B=01111111 _B=11001010 _B=01100001 _B=00000110 _B=10010010 _
_R=11000101 _R=10111110 _R=11001110 _R=11000110 _R=11000111 _R=11001000
_R=11011110 _R=00011000 _R=10111101 _R=11000110 _R=11001000 _R=11000000 _
_G=10111111 _G=11000100 _G=10011100 _G=10111110 _G=10101001 _G=10111101
_G=10110110 _G=10100010 _G=10111110 _G=10101001 _G=10111110 _G=10101011 _
_B=10111110 _B=10110000 _B=01000000 _B=10010110 _B=00010010 _B=11001010
_B=10110100 _B=01000110 _B=11000000 _B=00010010 _B=11001100 _B=01010110 _
_R=11000110 _R=11010100 _R=11000000 _R=11001000 _R=11010010 _R=11000010
_R=11101000 _R=10111110 _R=10111000 _R=11010000 _R=11000110 _R=11000110 _
_G=10110101 _G=01101011 _G=10111101 _G=10110011 _G=10100111 _G=10111001
_G=10100001 _G=10111011 _G=10111111 _G=10100001 _G=10111111 _G=10101001 _
_B=10110011 _B=01111110 _B=11001011 _B=01100001 _B=00000111 _B=10010011
_B=10010101 _B=11001001 _B=10101011 _B=00000100 _B=10010111 _B=00010011 _
_R=11011110 _R=00011000 _R=10111100 _R=11000110 _R=11001000 _R=11000000
_R=10111010 _R=10111100 _R=11000100 _R=11000000 _R=11001000 _R=11010011 _
_G=10110110 _G=10100010 _G=10111110 _G=10101000 _G=10111111 _G=10101010
_G=01010111 _G=10111100 _G=10101010 _G=10111100 _G=10110010 _G=10100010 _
_B=10110101 _B=01000110 _B=11000001 _B=00010011 _B=11001101 _B=01010111
_B=01000010 _B=10111111 _B=01101111 _B=11001010 _B=01100001 _B=00000110 _
_R=11101000 _R=10111110 _R=10111001 _R=11010001 _R=11000111 _R=11000110
_R=11000101 _R=10111111 _R=11001110 _R=10111100 _R=11000111 _R=11001001 _
_G=10100000 _G=10111010 _G=10111110 _G=10100000 _G=10111110 _G=10101000
_G=10111110 _G=11000100 _G=10011100 _G=10111110 _G=10101000 _G=10111100 _
_B=10010100 _B=11001000 _B=10101010 _B=00000100 _B=10010110 _B=00010010
_B=10111110 _B=10110000 _B=01000000 _B=11000000 _B=00010010 _B=11001010 _
_R=10111011 _R=10111101 _R=11000101 _R=11000001 _R=11001001 _R=11010011
_R=11000111 _R=11010101 _R=10111111 _R=10111001 _R=11010001 _R=11000011 _
_G=01010110 _G=10111101 _G=10101011 _G=10111101 _G=10110011 _G=10100110
_G=10110100 _G=01101010 _G=10111010 _G=10111111 _G=10100001 _G=10111001 _
```

```
_B=01000010 _B=10111110 _B=01101110 _B=11001010 _B=01100001 _B=00000110
_B=10110010 _B=01111110 _B=11001000 _B=10101010 _B=00000100 _B=10010010 _
_R=11000100 _R=10111110 _R=11001111 _R=10111100 _R=11000110 _R=11001000
_R=11011110 _R=00011000 _R=10111100 _R=11000100 _R=11001001 _R=11000001 _
_G=10111111 _G=11000101 _G=10011100 _G=10111111 _G=10101000 _G=10111100
_G=10110110 _G=10100010 _G=10111100 _G=10101010 _G=10111111 _G=10101011 _
_B=10111111 _B=10110000 _B=01000000 _B=11000001 _B=00010011 _B=11001010
_B=10110100 _B=01000110 _B=10111110 _B=01101111 _B=11001101 _B=01010111 _ _
```

into 8 bits, then convert them into characters based on the ASCII table, as shown in table 8.

Table 8: Convert the last bit of stego image to ASCII character No _Binari _Ascii _Charact er _No _Binari _Ascii _Charact er _No _Binari _Ascii _Charact er _ _1 _00110 001 _49 _1 _13 _00110 100 _52 _4 _25 _00100 000 _32 _space _ _2 _00111 001 _57 _9 _14 _00110 011 _51 _3 _26 _00110 011 _51 _3 _ _3 _00110 111 _55 _7 _15 _00100 000 _32 _space _27 _00110 011 _51 _3 _ _4 _00100 000 _32 _space _16 _00111 000 _56 _8 _28 _00100 000 _32 _space _ _5 _00110 011 _51 _3 _17 _00110 101 _53 _5 _29 _00110 011 _51 _3 _ _6 _00110 111 _55 _7 _18 _00100 000 _32 _space _30 _00110 100 _52 _4 _ _7 _00110 101 _53 _5 _19 _00110 101 _53 _5 _31 _00110 000 _48 _0 _ _8 _00100 000 _32 _space _20 _00110 010 _50 _2 _32 _00100 000 _32 _space _ _ 9 _00110 001 _ 49 _ 1 _ 21 _00100 000 _ 32 _ space _ 33 _00110 010 _ 50 _ 2 _ _10 _00110 010 _50 _2 _22 _00110 011 _51 _3 _34 _00110 111 _55 _7 _ _11 _00110 010 _50 _2 _23 _00110 111 _55 _7 _35 _00110 010 _50 _2 _ _12 _00100 000 _32 _space _24 _00111 001 _57 _9 _36 _00100 011 _35 _# _ _ Remove the marking character (#) at the end of the message, so that the message (ciphertext) is obtained, namely 197 375 122 43 85 52 379 33 340 272 Message decryption process, After the message extraction process has been successfully carried out, the next step is to perform the message decryption process using the private key (383, 338) as follows: Separate the values a and b in the ciphertext, provided that: a = Ciphertext of odd order b = Even-order ciphertext So obtained: a1 = 197, a2 = 122, a3 = 85, a4 =379, a5 =340 b1 = 375, b2 = 43, b3 = 52, b4 = 33,b5 = 272 Calculate m (original message) using the formula: m = b * a(p-1-x) mod p, then convert it into ASCII characters to produce plaintext, as shown in table 9.

_Table 9: Convert m value to ASCII character i _Plainteks mi _m = b * a(p-1-x) mod p _Character _ _1 _m1 _375 * 197(383-1-338) mod 383 = 82 _R _ _2 _m2 _43 * 122(383-1-338) mod 383 = 65 _A _ _3 _m3 _52 * 85(383-1-338) mod 383 = 80 _P _ _4 _m4 _33 * 379(383-1-338) mod 383 = 79 _O _ _5 _m5 _272 * 340(383-1-338) mod 383 = 84 _T _ _ Based on the decryption process above, the initial plaintext is obtained, namely the word "RAPOT".

From the results of calculations and complete steps which have been described in detail, it can be concluded that the implementation has been successful in returning the text inserted in the image. After the analysis and design stages of the system have been completed, the next stage is system implementation. This system was built using the Visual Basic.NET programming language, with Microsoft Visual Studio 2010 software.

This system consists of 6 (six) forms, including the intro form, main form, key generation form, encryption and insertion form, extraction form and description, form about me and form about the application. CONCLUSIONS Based on the discussion and results of the research, the following conclusions are obtained: The built system can perform the process of encrypting text files, inserting, extracting and decrypting text files again so that they return to their original form.

The size of the text file inserted into the image must be smaller than the size of the image (cover image). The image file size after insertion is larger than the original image size. The existence of a secret message embedded in an image is difficult for the sense of sight to see because visually the two images look the same.

The initial message will be overwritten if another message is inserted. For further research, it is important to discuss maintaining the size of the inserted image file the same as the previous file size. Application performance needs to be improved so that it can receive different message inserts.

REFRENCES: A.

Widarma, “Kombinasi Algoritma Aes, Rc4 Dan Elgamal Dalam Skema Hybrid Untuk Keamanan Data,” Cessjournal Comput. Eng. Syst. Sains, Vol. 1, No. 1, 2016. Handrizal, F. Nurahmadi, And S. D. Siregar, “Hybrid Cryptosystem Using Elgamal Algorithm And Beaufort Cipher Algorithm For Data Security,” J. Theor. Appl. Inf. Technol., Vol. 100, No. 7, 2022. K. Vanitha, K. Anitha, Z. Rahaman, And M. Musthafa, “Analysis_Of_Cryptographic_Techniques_In Network Security,” J. Appl. Sci. Comput., Vol.

5, No. 8, 2018. R. Munir, “Algoritma Enkripsi Citra Digital Dengan Kombinasi Dua Chaos,” Chaos, Vol. 2012, No. Snati, 2012. Krisnawati, “Metode Least Significant Bit (Lsb) Dan End Of File (Eof),” Seminar, Vol. 2008, No. Semnasif, 2008. A. A. Alarood, A. A. Manaf, M. J. Alhaddad, And M. S. Atoum, “Hiding A Message In Mp3 Using Lsb With 1, 2, 3 And 4 Bits,” Int. J. Comput. Networks Commun., Vol. 8, No. 3, 2016, Doi: 10.5121/Ijcnc.2016.8305.

J. R. Jayapandiyan, C. Kavitha, And K. Sakthivel, “Enhanced Least Significant Bit Replacement Algorithm In Spatial Domain Of Steganography Using Character Sequence Optimization,” Ieee Access, Vol. 8, 2020, Doi: 10.1109/Access.2020.3009234. F. Deeba, S. Kun, F. A. Dharejo, And H. Memon, “Digital Image Watermarking Based On Ann And Least Significant Bit,” Inf.

Secur. J., Vol. 29, No. 1, 2020, Doi: 10.1080/19393555.2020.1717684. K. K. Jabbar, M. B. Tuieb, And S. A. Thajeel, “Digital Watermarking By Utilizing The Properties Of Self-Organization Map Based On Least Significant Bit And Most Significant Bit,” Int. J. Electr. Comput. Eng., Vol. 12, No. 6, 2022, Doi: 10.11591/Ijece.V12i6.Pp6545-6558. S. A. Nie, G. Sulong, R. Ali, And A.

Abel, “The Use Of Least Significant Bit (Lsb) And Knight Tour Algorithm For Image Steganography Of Cover Image,” Int. J. Electr. Comput. Eng., Vol. 9, No. 6, 2019, Doi: 10.11591/Ijece.V9i6.Pp5218-5226. E. H. J. Halboos And A. M. Albakry, “Hiding Text Using The Least Significant Bit Technique To Improve Cover Image In The Steganography System,” Bull. Electr. Eng. Informatics, Vol. 11, No.

6, 2022, Doi: 10.11591/Eei.V11i6.4337. _S. K. Salim, M. M. Msallam, And H. I. Olewi, “Hide Text In An Image Using Blowfish Algorithm And Development Of Least Significant Bit Technique,” Indones. J. Electr. Eng. Comput. Sci., Vol. 29, No. 1, 2023, Doi: 10.11591/Ijeecs.V29.I1.Pp339-347. Z. Bin Faheem Et Al., “Image Watermarking Using Least Significant Bit And Canny Edge Detection,” Sensors, Vol.

23, No. 3, 2023, Doi: 10.3390/S23031210. H. H. Liu, P. C. Su, And M. H. Hsu, “An Improved Steganography Method Based On Least-Significant-Bit Substitution And Pixel-Value Differencing,” Ksii Trans. Internet Inf. Syst., Vol. 14, No. 11, 2020, Doi: 10.3837/Tiis.2020.11.016.

INTERNET SOURCES:

1% - http://www.jatit.org/volumes/Vol98No17/15Vol98No17.pdf
<1% - http://www.jatit.org/volumes/Vol95No21/16Vol95No21.pdf
<1% - https://www.neliti.com/id/publications/282456/visualisasi-pengumuman-dan-sop-fakultas-ilmu-komputer-universitas-katolik-santo
<1% - https://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta/article/download/1135/735/
<1% - https://ejournal-medan.uph.edu/isd/article/download/184/64/368
<1% - https://link.springer.com/chapter/10.1007/978-3-031-23095-0_4
1% - https://www.itu.int/en/ITU-D/Cybersecurity/Documents/01-Introduction%20to%20Cryptography.pdf
<1% - https://www.sciencedirect.com/science/article/pii/S0045790623002483
<1% - https://www.mdpi.com/2076-3417/13/21/11771
<1% - https://www.researchgate.net/publication/341737927_Data_security_improvements_on_cloud_computing_using_cryptography_and_steganography
<1% - https://www.tandfonline.com/doi/full/10.1080/2573234X.2021.1945961
<1% - https://cryptography.fandom.com/wiki/ElGamal_encryption
<1% - https://arxiv.org/pdf/1704.02698v1
<1% - https://link.springer.com/chapter/10.1007/978-3-030-39875-0_39
<1% - http://www.jatit.org/volumes/Vol96No12/5Vol96No12.pdf
<1% - https://www.digicert.com/blog/the-history-of-cryptography
<1% - https://link.springer.com/chapter/10.1007/978-3-319-53518-0_7
<1% - https://www.researchgate.net/publication/344950501_CIPHER_ENCRYPTION_DECRYPTION
<1% - https://link.springer.com/chapter/10.1007/978-1-4842-7334-0_1
<1% - https://talenta.usu.ac.id/JoCAI/article/download/4004/3817
<1% - https://crypto.stackexchange.com/questions/57818/is-there-any-difference-between-cry

ptography-and-cryptology

<1% - https://www.kaspersky.com/resource-center/definitions/what-is-steganography

<1% - https://www.researchgate.net/publication/344322371_A_Study_of_Data_Hiding_Using_Cryptography_and_Steganography

<1% - https://dl.acm.org/doi/10.1145/2632856.2632877

<1% - https://ieeexplore.ieee.org/abstract/document/8724069/

<1% - https://www.mecs-press.org/ijmecs/ijmecs-v4-n6/IJMECS-V4-N6-4.pdf

<1% - https://journal.unnes.ac.id/nju/index.php/sji/article/viewFile/28138/pdf

<1% - https://stackoverflow.com/questions/69932895/count-total-number-of-pixels-for-each-color

<1% - https://stackoverflow.com/questions/57498254/how-to-change-the-last-bit-of-every-pixel-in-image-and-save-it-as-a-new-image

<1% - https://www.researchgate.net/figure/Least-significant-bit-algorithm-Least-significant-bit-LSB-insertion-is-a-common-simple_fig2_288630141

<1% - https://iopscience.iop.org/article/10.1088/1742-6596/1201/1/012030/pdf

<1% - https://link.springer.com/chapter/10.1007/978-981-16-4807-6_11

<1% - https://123dok.com/document/yrkj72pz-pengamanan-sqlite-database-menggunakan-kriptografi-elgamal.html

<1% - https://processing.org/tutorials/pixels/

<1% - https://ncalculators.com/digital-computation/rgb-to-hex-converter.htm

<1% - https://www.researchgate.net/publication/345992561_IMAGE_ENCRYPTION_ALGORITHM_BASED_ON_RC4_AND_HENON_MAP

<1% - https://www.researchgate.net/publication/323340842_Implementation_Cryptography_Data_Encryption_Standard_DES_and_Triple_Data_Encryption_Standard_3DES_Method_in_Communication_System_Based_Near_Field_Communication_NFC

<1% - https://www.scribd.com/document/361323222/Makalah-Kriptografi-Algoritma-ElGamal

<1% - https://www.clouddefense.ai/system-development-life-cycle/

<1% - https://stackoverflow.com/questions/14101526/the-output-image-after-cropping-is-larger-than-the-original-size

<1% - http://www.jatit.org/volumes/Vol99No18/9Vol99No18.pdf

<1% - https://repository.globethics.net/handle/20.500.12424/1376640

<1% - http://www.jatit.org/volumes/onehundred07.php

<1% - https://www.researchgate.net/publication/349185850_Security_Implementation_Using_RSA_and_Enhanced_RSA

<1% - https://informatika.stei.itb.ac.id/~rinaldi.munir/Penelitian/Makalah-Jurnal_Rekayasa_Elektrika-2012.pdf

<1% - https://ejournal-medan.uph.edu/isd/article/view/184

<1% - https://www.researchgate.net/publication/303871140_Hiding_a_message_in_MP3_using_LSB_with_1_2_3_and_4_bits/fulltext/57aa564208ae42ba52ac3cbe/303871140_Hiding_a_message_in_MP3_using_LSB_with_1_2_3_and_4_bits.pdf

1% - https://ijercse.com/viewabstract.php?id=14103&volume=Volume7&issue=Issue12

<1% - https://www.researchgate.net/publication/342930116_Enhanced_Least_Significant_Bit_Replacement_Algorithm_in_Spatial_Domain_of_Steganography_Using_Character_Sequence_Optimization/fulltext/5f0e6c9545851512999afabc/342930116_Enhanced_Least_Significant_Bit_Replacement_Algorithm_in_Spatial_Domain_of_Steganography_Using_Character_Sequence_Optimization.pdf

<1% - https://www.researchgate.net/profile/Fayaz-Dharejo/publication/338829649_Information_Security_Journal_A_Global_Perspective_Digital_image_watermarking_based_on_ANN_and_least_significant_bit_Digital_image_watermarking_based_on_ANN_and_least_significant_bit/links/5e56b7194585152ce8f26630/Information-Security-Journal-A-Global-Perspective-Digital-image-watermarking-based-on-ANN-and-least-significant-bit-Digital-image-watermarking-based-on-ANN-and-least-significant-bit.pdf?origin=publication_detail

<1% - https://ejournal.undip.ac.id/index.php/jbs/issue/view/2834

<1% - https://www.researchgate.net/profile/Munthir-Tuieb/publication/364852877_Digital_watermarking_by_utilizing_the_properties_of_self-_organization_map_based_on_least_significant_bit_and_most_significant_bit/links/635d8bd212cbac6a3e07f0df/Digital-watermarking-by-utilizing-the-properties-of-self-organization-map-based-on-least-significant-bit-and-most-significant-bit.pdf

<1% - https://www.researchgate.net/publication/365910527_International_Journal_of_Electrical_and_Computer_Engineering_a_bibliometric_analysis/fulltext/63896c642c563722f22d8e98/International-Journal-of-Electrical-and-Computer-Engineering-a-bibliometric-analysis.pdf

<1% - https://pureportal.strath.ac.uk/en/publications/the-use-of-least-significant-bit-lsb-and-k

night-tour-algorithm-fo/fingerprints/

<1% - https://ijece.iaescore.com/index.php/IJECE/article/download/20540/13247

<1% - https://beei.org/index.php/EEI/article/view/4337

<1% - https://www.researchgate.net/figure/Structure-of-Blowfish-encryption-algorithm_fig1_364833520

<1% - https://www.researchgate.net/profile/Mohammed-Majid-Msallam/publication/364833520_Hide_text_in_an_image_using_Blowfish_algorithm_and_development_of_least_significant_bit_technique/links/635f6c306e0d367d91e06634/Hide-text-in-an-image-using-Blowfish-algorithm-and-development-of-least-significant-bit-technique.pdf