SEAN INSTITUTE
Sharing Knowledge
http://infor.seaninstitute.org/index.php/infokum/index
JURNAL INFOKUM, Volume 10, No.2, Juni 2022 ISSN : 2302-9706

APPLICATION OF CRT (CHINESE REMINDER THEOREM) TO SPEED UP THE PROCESS OF DATA SECURITY ON IMAGE FILES

Syaufi Arbin[1],Arpan[2], Eko Hariyanto[3]
Faculty of Science and Technology Universitas Pembangunan Panca Budi, Medan , Sumatera Utara
syaufi.arbin@yahoo.co.id, arsevent@pancabudi.ac.id, ekoharyanto@dosen.pancabudi.ac.id

Abstract

Article Info
Received, 01/06/2022
Revised, 28/06/2022
Accepted, 29/06/2022

The purpose of this study is to use the Chinese Remainder Theorem approach to create a data security application system and to improve the data security of a confidential file, particularly data that uses image files. Observation and literature review were employed in this study to acquire data. The traditional approach is used to share data, in this case a secret message in the form of text. The embedding process and the extraction process are the two fundamental procedures in message insertion utilizing the Least Significant Bit approach. The Least Significant Bit steganography technique was used to replace the secret message bits in the final bit of each color component of the image pixels, according to the results. So that the image size does not change, only one message bit (value 0 or 1) is placed into one color component of the image. Furthermore, the processing time is affected by the size of the file, the length of the key, and the computer processor performance.

Keywords: job characteristics, interpersonal relationships, affective commitment, normative commitment

1. INTRODUCTION

Information technology advancements make it simpler for consumers to interact through numerous mediums. Computer thieves use security gaps to detect and modify messages in communications that entail sending and receiving messages using developments in information technology. Security and confidentiality are very important aspects for information technology users. To avoid messages being sent to parties that are not interested, or if there is abuse of the message, encryption of the original message and insertion of the message into a medium by applying steganography science. (Mulyana, 2012).

To improve security, steganography is used, where a steganography system in such a way hides the content of information in a medium that ordinary people cannot expect, so as not to arouse suspicion in the person who sees it. Media to hide information is image formats including bitmap (bmp), gif, pcx, and jpeg. Audio formats include wav, mp3, and voc. Other formats, e.g. file text, doc, html, and pdf. The purpose of steganography is to keep or hide the existence of information.

The Chinese Remainder Theorem, in general, is the result of some congruence in number theory and its generalizations in abstract algebra. The CRT, also known in Indonesian as the Chinese Leftover Theorem, was triggered by Sun Zi's appearance in the 3rd to 5th centuries before finally being formulated in its entirety by Qin Jiushao in 1247 under the name "Da yan shu" in a book called Shushu Jiuzhang. For clarity of reading, before the CRT is discussed more deeply, there are some things that need to be known, such as GCD (Greatest Common Divisor), LCM (Least Common Multiple), and congruence relations, which use the concept of modulo. Based on the above exposure, this study aims to design a data security application system using the Chinese Remainder Theorem method and strengthen the data security of a file that is confidential, especially data that uses image files.

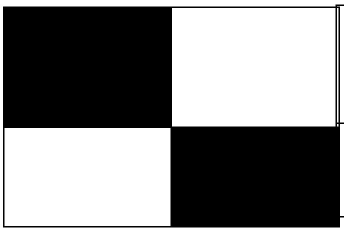
2. LITERATURE REVIEW

Digital Image

Digital imagery is a multiple picture organized by digital data in the form of an array (array) including real and complex values represented by a specific row of bits. An picture may be characterized as an M-row, N-column f (x,y) function, with x and y being spatial coordinates and amplitude f at the coordinate point (x,y) reflecting the image's intensity or grayness level at that location. (Zebua, 2017).

There are a variety of methods for storing digital pictures in memory. The sort of digital picture created is determined on the storage mechanism. Binary Image, Grayscale Image, and Color Image are three most popular digital image formats:

a. Binary Image
A binary picture (monochrome) or binary image is a digital image with just two degrees of validity for each pixel, namely 0 and 1. The values 0 and 1 signify black and white, respectively, with each pixel requiring a 1 bit storage medium.



0	1
1	0

Figures 1. Example of a 2x2 Pixel Binary Image
(Source: Putra, 2010)

b. Color Image
In a color image, each pixel has a color that is a combination of the three fundamental RGB colors (Red, Green, Blue). Each basic color has a gradation of 255 colors since each color takes 8 bits = 1 byte of storage. True color imagery is stored differently in memory than grayscale images. A byte represents each pixel in a grayscale image with 256 color gradations. While each byte in a true color image represents red, green, and blue, each pixel is represented by three bytes.

Digital Image Processing

Image processing is a discipline that studies issues such as image quality (improving contrast, color transformation, image restoration), image transformation (rotation, translation, scale, geometric transformation), performing optimal feature images for analysis, extracting information or descriptions of objects or recognizing objects contained in the image, compressing or reducing data for data storage, and so on. The input of image processing is imagery, and the output is the processed imagery. (Putra, 2010)

Digital image processing is extensively used in a variety of industries, including security, health, education, and many more. Some of the objectives of digital image processing operations are listed below.

1. Improving image quality is seen from radiometric aspects (increased contrast, color transformation, image restoration) and from geometric aspects (rotation, translation, scale, geometric transformation).
2. Perform the process of extracting information or descriptions of items from the picture, as well as the identification of objects within the image.
3. Data compression or reduction is used for data storage, data transport, and data processing time.

Method of EOF (End Of File)

The EOF (End Of File) approach uses the following algorithm: a. Read the file metadata and indicate the file's ultimate location. b. Make the CTRL-Z (marker) point at the start of the message insertion line. c. Copy and paste the message from the CTRL-Z (marker) location to the end.d. At the conclusion of the message, type the second control-z (marker). By appending pieces of the message to the end of the container picture file, this approach conceals a hidden message (Gunawan, 2013). The following is an algorithm that may be used to insert messages using the End Of File method: (Gunawan, 2013)

1. Type in the message that will be placed.
2. Use decimal codes to convert messages.
3. Input the grayscale image to be next to the message.
4. Get the validity of each pixel's degree value.
5. Add the message decimal code as the grayish degree value at the end of the image.
6. Map into a new image.

Encryption

Encryption is the process of concealing data or transforming plaintext data into a form that cannot be read or understood. Encryption has been used to protect communications in a variety of countries; however, encryption is only used by specific organizations and individuals who have a strong need for secrecy (Wahana Komputer, 2003). Although encryption can be used for security, additional approaches are still required to provide secure connections, particularly to assure message integration and authentication. Instead, an algorithm known as the cipher is utilized to perform encryption and decryption using a specified set of step processes that are performed as procedures. Encipherment is another option. The original data is stored in plaintext, while the encrypted version is known as chiphertext. Chipertext communications include all of the information found in plaintext messages, but in a format that cannot be decrypted by people or machines without the use of the correct mekanism.

Programming language

A programming language is a set of commands or instructions that a computer understands in order to complete a job. A programming language is a set of instructions for commanding a computer to accomplish certain tasks, but only in a specified manner. Programming languages also provide a set of syntactic and semantic guidelines for defining computer programs. We are familiar with Java, Visual Basic, C++, C, PHP, and other programming languages. However, the language's requirements must be tailored to the tasks and devices that make use of them.

Programming languages are divided into four generations based on their generational origins, which are as follows:

a.	1st generation	:	machine language
b.	2nd generation	:	assembly language, Assembler
c.	3rd generation	:	high level programming language, example: C and Pascal
d.	4th generation	:	4 GL (fourth-generation language), example: SQL
e.	5th generation	:	Programming Language Based Object Oriented & Web Development

Programming languages are categorized into four general categories:

1.	Object Oriented Language	:	Visual C, Delphi, Visual dBase, and FoxPro Visual are just a few examples.
2.	Low Level Language	:	Assembly language.
3.	Middle Level	:	Language C.

Language

4. High Level Language : Basic and Pascal.

Programming languages are divided into three categories based on their closeness to computer machines:

a. Machine Language, which communicates with the computer using binary language codes such as 011001011100110.
b. Low-Level Language, otherwise known as assembly language, which gives commands to computers using short codes (mnemonic codes), for example MOV, SUB, CMP, JMP, JGE, JL, LOOP, etc.
c. Intermediate Language is a computer language that uses a mixture of instructions in human words (see examples of High Level Languages below) and symbolic instructions, for example {, }, ?, <<, >>, &&.

High-Level Language, which is a computer language that uses instructions derived from elements of human language words, for example, begin, end, if, for, while, and, or, etc. Computers can understand human languages, but that requires a compiler or interpreter program. The function of a programming language is to tell a computer to be able to process the data as desired. The output of this programming language can be a special application or program. A simple example is traffic lights on the highway.

3. METHODS

Data collection

The data used in this study is:

1. Observation

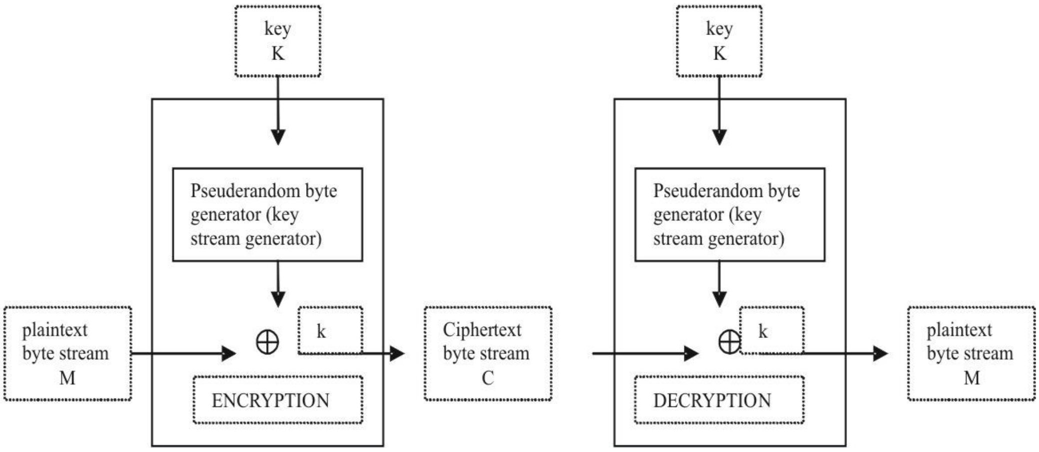
Researchers conducted firsthand observations of each user's usage of current chat programs such as WA, BBM, and Line in order to ascertain the security method that was previously implemented.

2. Library Research

It is a way to find references by collecting library materials in campus libraries as well as public libraries, as well as searching through the internet, by visiting sites such as Google Book Online, which can help discuss material.

Problem Analysis

In this case, data is exchanged in the form of private text messages using standard techniques, particularly by sharing a single keyword. The figure below illustrates how secret communications are sent using a single key.


key
K
Pseuderandom byte generator (key stream generator)
k
plaintext byte stream M
ENCRYPTION
Ciphertext byte stream C
key
K
Pseuderandom byte generator (key stream generator)
k
DECRYPTION
plaintext byte stream M

Figures 2. Analysis of Running Systems

Keyword notification from sender to recipient using media commonly used by many people.

Analyses of the Designed System's Processes

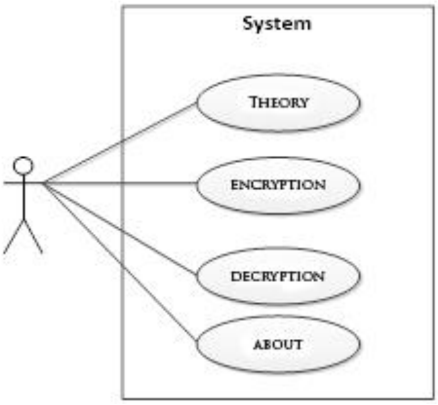
There are 2 (two) main processes in the insertion of messages using the Least Significant Bit method, namely the embedding process and the extraction process. The embedding process is the process of inserting secret messages into a medium. While the extraction process is the process of taking secret messages from a medium, In this system, the secret message is held in the form of a text databiner, which means the text of the steganography technique encryption results in the final bit value of the holding media (file image), and the media used for message insertion is a.bmp format image file,.jpg.

The process of embedding or inserting messages using the Least Significant Bit method is as follows:

a) Upload an image that will be used as a text placeholder (cover file).
b) Input the encrypted text to insert.
c) Read the binary value of each pixel in the image.
d) Insert the binary value of the text onto the binary end value of the image pixel.
e) Map into a new image.

System Planning

Object-Oriented Design, or Modeling, is the process of obtaining information from a model and displaying it graphically using a standard graphic element. The purpose of this object-oriented design is to enable higher quality communication between users, developers, analysts, testers, managers, and anyone involved in information systems development projects. The processes are shown in the use case graphic below.



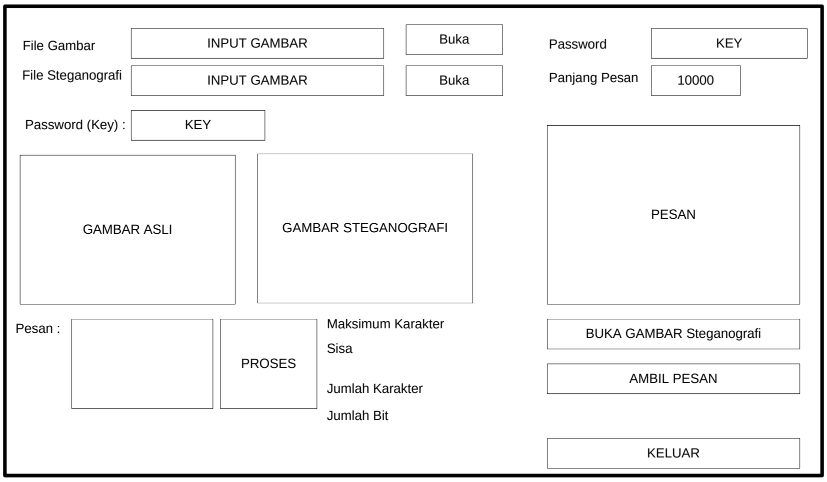
Figures 3. Use Case Diagram

Description :

The user as an actor who has a substantial use case, encryption, and about are shown in the use case diagram above. The material page shows information from the LSB about the material. The encryption page depicts the CRT-based picture encryption process, whereas the description page is the polar opposite of encryption.

Design of the Encryption Page

The user inserts the original or plaintext into the plaintext input button and then enters the key as well. After that, press the Encryption Process button, which will then display the ciphertext, or encoded writing.



Figures 4. Encryption Page Design

Description:

1. This field is used to show the name of the picture that was uploaded.
2. A button for finding the image you want to encrypt.
3. A button that is used to execute the LSB encryption procedure on the image.
4. This is used to show the outcomes of an image's encryption process.

4. RESULTS AND DISCUSSION

Least Significant Bit Algorithm (LSB)

The Least Significant Bit Algorithm is an algorithm used to insert data or retrieve data from within the storage media used. (Arjana, 2012) LSB steganography algorithm is divided into two, namely inserting text data (Embedded) and retrieving text data (Extraction).

(Pabokory, 2015)

1. Process of Inserting Text Data (Embedded)

An algorithm or set of steps for inserting text data into digital image data:

Input : C, T, KD, Pc, Pb, vM, vH, vB, toLSB, toDecimal, toBiner, xpix, Gp

Output : CT

Process :

```
for Pc = 0 To length C -1
for Pb = 0 To length C -1
        vM = C. Gp ( Pb and Pc) R
        vH = C. Gp ( Pb and Pc) G
        vB = C. Gp ( Pb and Pc) B
```

```
          T1 = Mid i, 1
          T2 = Mid i + 1, 1
          T3 = Mid i + 2, 1
          vM = toDecimal(toLSB(ToBiner(vM), T1))
           vH = toDecimal(toLSB(ToBiner(vH), T2))
          vB = toDecimal(toLSB(ToBiner(vB), T3))
            xpix = xpix + 1
            If xpix > xpx Then Exit For
           i = i + 3
          Next
                    CT ← LSB Image (an image that already contains a message)
```

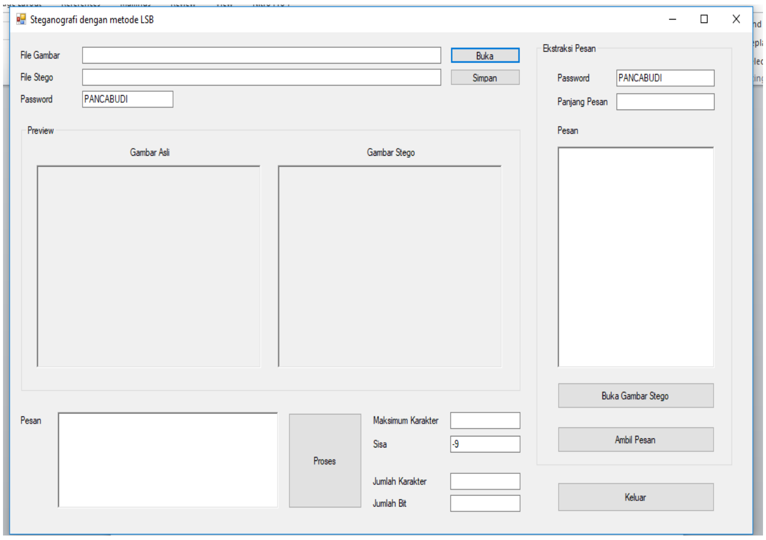
2. Process of Retrieving Text Data (Extraction)

The following is the method or procedures for reading messages from digital image data:
Input : SI, T, Pc, Pb, vM, vH, vB, toBiner, xpix, Gp, Gpes
Output : EP
Process :

```
                    For Pc = 0 To SI.Height - 1
          For Pb = 0 To SI.Height – 1
vM = SI.Gp(Pb, Pc).R
vH = SI.GP(Pb, Pc).G
vB = SI.GP(Pb, Pc).B
T = T.Mid((ToBiner(vM)), 8, 1)
T.Mid((ToBiner(vH)), 8, 1)
T.Mid((ToBiner(vB)), 8, 1)
xpix = xpix + 1
                              If xpix > xpx Then Exit For
Next
T = T + 1 * 8
Next
          EP← Extracted text messages
```

System Implementation

The implementation stage is a continuation of the system design stage. Based on the results of analysis and system design, the implementation of the system into a programming language is carried out at this stage. At this stage of implementation, software and hardware are used so that the built system can be completed properly. Furthermore, the Steganography page is the page that appears first when the system is running. Steganography page view can be seen in Figure 5.



Password: PANCABUDI

Sisa: -9

Ekstraksi Pesan – Password: PANCABUDI

Figures 5. Home Menu Page View

Description:

1. Open to search for an image file in jpg format, bmp, or png.
2. Save to save images that have been inserted as text messages.
3. Picture Box to display the original image before inserting a text message.
4. Picture Box (LSB Image) to display the original image after inserting a text message.
5. Text Box to input the message to be inserted into the image file.
6. The Button Process for processing the insertion of messages into images by the steganography method.

System Testing

The test used to test this system is a black-box testing method. Black-box testing focuses on the functional requirements of the software. Testing of the Lsb Steganography Implementation function on the Concealment of Text Messages on Digital Imagery is carried out using the Black Box method. Tests are performed on system functions to determine if they have run as expected.

1) Image Search Test Plan

Table 1 . Image Search Test Plan

Tested menu	Test details	Test type
Main Menu	Home Page View	Black box
Manage the process of hiding text messages	Image Input	Black box
	Message Input	Black box
	Password Input	Black box

2) User Testing Test Plan

Table 2. User Testing Plan

Tested menu	Test details	Test type
Password Input	Input Key On Message	Black box
Image Input	Searching Images for Message Media	Black box

Message Input	Displays messages that are in the Image.	Black box

5. CONCLUSION

After the whole process is carried out, which starts from the stages of literature study to software testing, it can be concluded as follows The Least Significant Bit steganography algorithm is performed by replacing the secret message bits in the last bit of each pixel color component of the image. One image color component is inserted only one bit of the message (worth 0 or 1) so that the image size does not change. The speed of the processing time depends on the size of the file, the length of the key and the speed of the computer processor used. The suggestions that researchers can provide for the development and improvement of this system are as follows: This research can be developed by trying to apply several other methods such as (RSA and DES algorithms) so that the detection of hidden messages in an image is more accurate and difficult to solve. In the process of concealing the pesan should be combined with other methods so that the message inserted in the image becomes more secure.

REFERENCES

[1] Arjana, P. H. (2012). Implementasi Enkripsi Data Dengan Algoritma LSB. Seminar Nasional Teknologi Informasi Dan Komunikasi (SENTIKA).

[2] Gunawan. (2013). Implementasi Hidden Message pada Citra Menggunakan Metode End of File. Universitas Widyatama.

[3] Mulyana, T. (2012). Steganografi Citra Digital Menggunakan Spreadsheet. 8(2).

[4] Pabokory, F. N. (2015). Implementasi LSB Pengamanan Data Pada Pesan Teks, Isi File Gambar Menggunakan Algoritma Advanced Encryption Standard. 10(1).

[5] Putra, D. (2010). Pengolahan Citra Digital. Andi Offset.

[6] Wahana Komputer. (2003). Memahami Model Enkripsi dan Security Data. Penerbit Andi.

[7] Zebua, T. (2017). PENGAMANAN CITRA DIGITAL BERDASARKAN MODIFIKASI ALGORITMA RC4. Jurnal Teknologi Informasi Dan Ilmu Komputer, 4(4). https://osf.io/preprints/inarxiv/nzfd4/