Jurnal Ilmiah Komputer dan Informatika (KOMPUTA)
Edisi. .. Volume. ... Bulan 20.. ISSN : 2089-9033

STEGANOGRAPHY APPLICATION DEVELOPMENT ON VIDEO USING SPREAD SPECTRUM METHODS AND LOKI97 ALGORITHM FOR DATA SECURITY

Steven A. Barande[1]

[1]Teknik Informatika – Universitas Komputer Indonesia
Jalan Dipatiukur 112-114 Bandung
E-mail : wildpb_13@yahoo.co.id

ABSTRACT

Cryptography is a technique for encrypting messages, namely changing the original message into irregular shapes. While Steganography is concealment techniques message. Steganography requires two properties, that is the message that will be inserted and the media as a container message. Cryptography and steganography both have shortcomings, the cryptographic techniques changed the original message to forms of irregular, so it is still arousing suspicion to the viewer. While the technique of steganography if the location of the message in the media reservoir can be revealed its existence, then this information will be known.

Based on the problems that have been studied, the purpose of this thesis is to build on the video steganography applications using spread spectrum and loki97 algorithms for data security. Spread Spectrum method takes advantage of the frequency domain of an *image*. Step first performed in Spread Spectrum steganography method is to transform the *image* into the frequency domain. But those that do not use the transformation coefficients in the media and only use Pseudo Random Number Generator as plant seeds randomization message in concealing information. LOKI97 algorithms including the type of symmetric algorithm and block cipher. Thus these algorithms use the same key when the encryption and decryption as well as inputs and outputs in the form of a block with a certain number of bits.

Based on the implementation and results of the testing it can be concluded as follows. Merger cryptography and steganography in this study resulted in an application that helps users to increase data security so that confidential data or information is maintained.

Keywords: Steganography, cryptography, LOKI97

1. INTRODUCTION

Messages or information has to be something very important since thousands of years ago. To protect messages from unauthorized parties to use some of the techniques or methods to protect the confidentiality of messages, such as cryptographic techniques and steganography techniques.

Cryptography is a technique for encrypting messages, namely changing the original message (plaintext) into irregular shapes (ciphertext). While Steganography is concealment techniques message. Steganography requires two properties, that is the message that will be inserted and the media as a container message. Cryptography and steganography both have shortcomings, the cryptographic techniques changed the original message to forms of irregular, so it is still arousing suspicion to the viewer. While the technique of steganography if the location of the message in the media reservoir can be revealed its existence, then the information or the message will be immediately known. By combining these two techniques intended to increase the security level of the message or information.

2. THEORETICAL BASIS

2.1. Information System Security

Information security system has four fundamental objectives :

1. *Confidentiality*
   Information on the computer system confidential, accessible only by authorized parties, the integrity and consistency of data in the system is maintained. So that the efforts of people who want to steal such information would be useless.
2. *Availability* Ensure the legitimate user to always be able to access information and resources are authorized. To ensure that people who are entitled to access information that has become due.
3. *Integrity*
   Ensure consistency and ensure the data is in accordance with the original, so that the efforts of others who try to change the data will soon be known.
4. *Legitimate Use*
   Guaranteeing that resources can not be used by unauthorized people.

2.2 Digital Video

Video is the technology of sending electronic signals of a moving *image*. Digital video is basically composed of a series of frames. The series of frames are displayed on the screen at a certain speed, depending on the given frame rate (in frames / second) if the frame rate is high enough, the human eye can not capture *image*s per frame, but caught as a series of mutually connected. Each frame is a picture / *image* (*image*) digitally.

A digital *image* is presented with a matrix, each element present intensity value. If I is a two-dimensional matrix, I (x, y) is the intensity value corresponding to the line position x and y columns in the matrix. The points where the *image* sampling is referred to as picture elements or commonly known as pixels. Digital Video characteristics determined by the resolution (resolution) or the dimensions of the frame (frame dimension), the depth of pixels (pixel depth), and the frame rate (frame rate). These characteristics will determine the quality of the video and the number of bits required to store or transmit it [2].

2.3 Steganography

2.3.1 History of Steganography

Steganography comes from the Greek, namely "Steganos" which means "hidden writing". Steganography is already known by the Greeks for a long time. Herodatus, a Greek ruler, sent a secret Oesan using slave or a soldier's head as a medium. How, hair Dibotaki, then a secret message written on the scalp of slaves. After the slave hair grows quite a lot (which means covering a secret message), the slave sent a message to bring the place of destination secret Oesan head. Place Dibotaki slave receiver head back to read messages hidden behind her hair [1].

2.3.2 *Spread Spectrum* Method

Spread Spectrum method was first introduced in mid 1950. Spread Spectrum is a transmission technique using pseudo-noise code, sebaga modulator waveform to spread the signal energy in a communication path (bandwidth) that is greater than the signal communication path information. By the receiver, the signal is recovered using a pseudo-noise code replica synchronized. Spread Spectrum use wideband, noise-like signal. Because it is noise-like, spread spectrum is difficult to be detected, cut, or pitch-modulation. It this is what causes the spread spectrum used for military communications for years.

How to insert a secret message or steps into a cover-object also varies, as research conducted in 2006 which uses the transformation of the media using FFT computation (Fast Fourier Transform) [12]. But those that do not use the transformation coefficients in the media and only use Pseudo Random Number. Spread Spectrum method used in such research multiplying the message bits by the pseudorandom generator that had previously been in the scatterplot with scalar multiplier.

2.4 LOKI97 Algorithms

LOKI97 algorithms including the type of symmetric algorithm and block cipher. Thus these algorithms use the same key when the encryption and decryption as well as inputs and outputs in the form of a block with a certain number of bits.

LOKI97 LOKI97 is an algorithm that uses data block size of 128 bits and using a key that can vary ie 128.192 and 256 bits. LOKI97 the algorithm implementation using the following elements:

2.4.1 Feistel Network

Feistel Network is a common method used in cryptographic algorithms block cipher. The main part of the feistel network is a function of f, i.e. the function mapping input string becomes the string output. At each iteration, the input block is the source for the function f, and then, the output of the XOR function f with the destination block, after which both the interchangeable blocks. LOKI97 algorithm uses 16 iterationsData Computation

LOKI97 perform data encryption plaintext with a block size of 128 bits to generate ciphetext with a size of 128 bits . Data computing will divide the 128 -bit plaintext into two - 64 is L and R.

2.4.2 Key Schedule

LOKI97 use their key scheduling based on feistel network, operates on four 64 bit data. By using the function f is f (A, B) as the calculation data to give a fairly non-linear and ensure that the calculation can be done with a key. Key scheduling can be initialized to the size vary i.e. 128 bit, 192 bit and 256 bit, based on the size of the keys that can be used in 4 64 bit data [K4 40 | K3 | K2 | K1].

2.4.3 F function (A,B)

Function f (A, B) non linear will receive two 64 bit input values of A and B, process them by using two S box, to produce output of 64 bits. Three permutations are used to ensure the maximal avalanche on the functionality for all the bits.

2.4.4 S-Box

It is a substitution table used on most block cipher algorithm. S-box was first used in Lucifer, DES and then after that many algorithms that use the LOKI97 using two pieces of S-box that was built with either 8 x 8 bit permutation and key.

2.5 *Unified Modelling Language* (UML)

The Unified Modelling Language (UML) is a tool for visualizing and documenting the results of the analysis and design that contains syntax in visual system as a model. UML has three main categories namely structure diagrams, behaviour diagrams and interaction diagrams. Where each of these categories has a diagram that describes the system architecture and integrated [9].

***1) Class* diagram**

Class diagram describes the static structure of the class in your system and describes the attributes, operations and relationships between classes. Class diagram helps in visualizing the structure of the classes of a system and is a type of diagram that is most widely used.

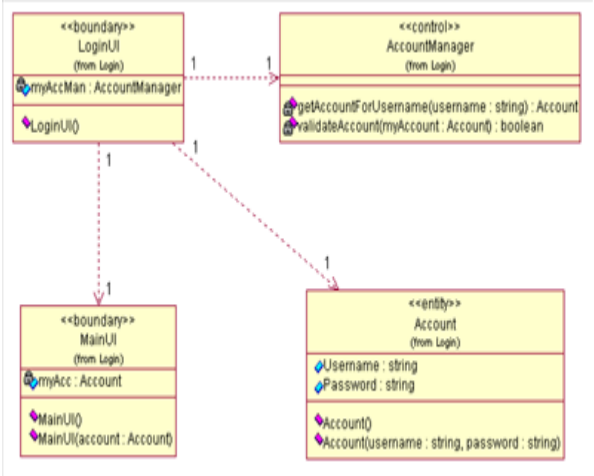


Image 2.1 Class Diagram

***2) Activity* diagram**

Describe the activities, object, state, transition state and event. In other words the activity workflow diagram illustrating the behavior of the system for the activity of

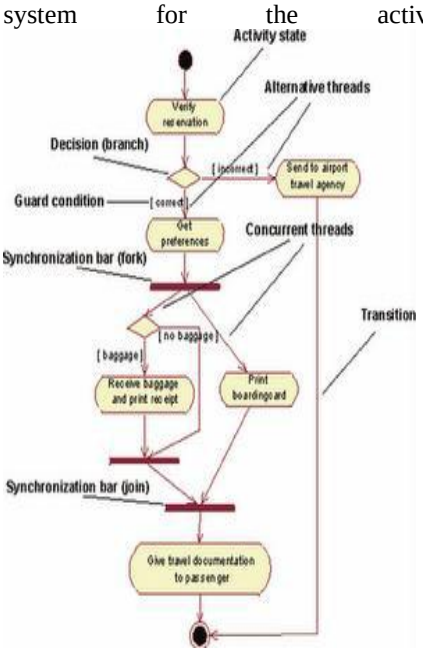


Image 2.2 Activity Diagram

***3) Use case* diagram**

Diagram depicting the actor, the use case and his associate as a sequence of actions that provide measurable value to an actor. A use case is described as a horizontal ellipse in a UML use case diagram. Use Case has two terms, namely a System use case; interaction with the system and Business use case; business interaction with consumers or real events.

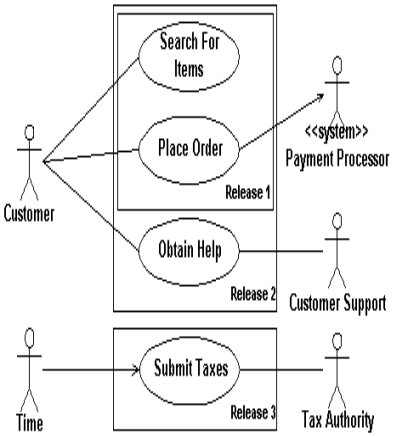


Image 2.1 *Use Case* Diagram

***4) Sequence* diagram**

Sequence diagram describes the interaction of objects that are arranged based on the time sequence. In easy a sequence diagram is a picture gradually, including chronology (sequence) changes are logically supposed to do to produce something in accordance with use case diagrams

2.6 Java Technology

Java is a technology introduced by Sun Microsystems in the mid-1990s. According to the definition of Sun, Java is the name for a set of technologies for creating and running the software on a computer or on a stand alone network environment. Java stands above a machine interpreter named Java Virtual Machine (JVM). JVM bytecode will read this in the class files of a program as a direct representation of a program that contains the machine language. Therefore, the Java language is referred to as a portable programming language because it can run on many different operating systems, as long as the operating system there is a JVM. The Java platform consists of a set of libraries, JVM, the class loader that is packaged in a regular Java environments, and a compiler, debuger, and other devices that are packaged in the Java Development Kit (JDK) [11].

3. CONTENTS OF RESEARCH

3.1 System Analysis

System Analysis ia a step whom purposefully was did to know. Analysis of the system is one which aims to identify and observe what is involved in a system . Discussion that exist on the analysis of this system is the analysis of problems , analysis of algorithms , non - functional requirements analysis , and functional analysis .

3.1.1. Problem Analysis

In securing an information or confidential data, technique or method that is often used is the cryptographic techniques and techniques of steganography, however good cryptography or

steganography each has a shortage. Encoding data with cryptographic techniques results in a data which is irregular so it would cause suspicion for the party concerned, whereas the concealment of data with the technique of steganography becomes a problem when the layout of the message in the media can be known, so that the data or information has been inserted may be released by the party which is not berkentingan.

3.1.2 Algorithms Analysis

Analysis of Algorithms are used to determine the process flow of the algorithm used to can be applicable into the application to be built . The application development using LOKI97 algorithm for encryption and decryption as the security of the information to be inserted . While steganography method used is Spread Spectrum method for the insertion and extraction of information .

The stages are carried out in each process is as follows :

The stages in the process of steganography applications to be built in general can be seen in Figure 3.1

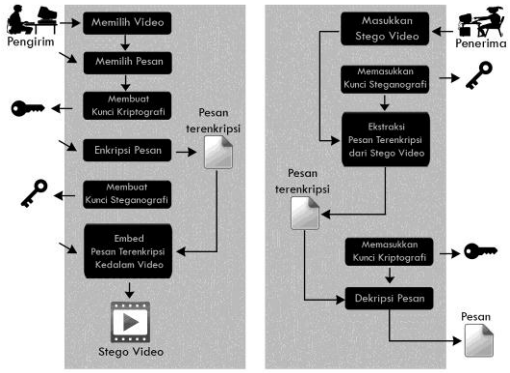


Image 3.1 General description of the application

3.1.2.1 LOKI97 Algorithms Analysis

LOKI97 algorithm is cryptographic algorithms that use the size of symmetrical ciphers using block. So this algorithm using the same key for encryption and decryption process. The algorithm LOKI97 there are two process, namely the process of scheduling the key and the encryption process.

3.1.2.1.1 Analysis Of The Key Scheduling

LOKI97 using key scheduling based on feistel network, operates on four 64 bit data. By using the function f is f (A, B) as the calculation data to give a fairly non-linear and ensure that the calculation can be done with a key. Key scheduling is initialized with a size of 256 bit, based on the size of the keys that can be used in 4 64 bit data [K40 | K30 | K20 | K10]. With 256 bit key [Ka | KB | KC | Kd], [K40 | K30 | K20 | K10] = [Ka | KB | KC | KD]
total to 48 iterations required to key scheduling.

3.1.2.1.2 Encryption Analysis

In using a block encryption, the first step is the calculation of data by dividing the two input block size of 128 bits of the plaintext into two 64 bit data i.e. [L | R] consist of L0 = L; R0 = R. This process will have 16 times the iteration in the feistel network. Each iteration uses the XOR operation and operating + 64 bit value for data with the output of non linear complex function *f* (A, B) that will result in the value of the maximum of all the avalanche of input bits as follows:

$$R_i = L_{i-1} \text{ xor } f\,(R_{i-1} + SK_{3i-2}, SK_{3i-1})$$
$$L_i = R_{i-1} + SK_{3i-2} + SK_{3i}$$

The result of the process of encryption of 128 bit data input plaintext into ciphertext 128 bit output is as follows: [R16 | L16]. The process of decryption algorithm LOKI97 is the antithesis of the encryption process. For a description of the process that is to divide the ciphertext with 2 fruity 64 bits of data: [R16 | L16] after dividing into two ciphertext then the inverse of the encryption process 16 times iteration. Then the retrieved results description of 128 bit plaintext value, namely:$L_i = R_i$ xor f (L_i - SK_{3i-}, SK_{3i-1})

$R_i = L_i - SK_{3i} - SK_{3i-2}$

Thus generating plainteks beginning prior to the encryption process, namely:

$[R_0|L_0]$

3.1.2.2 Analisis Metode *Spread Spectrum*

Spread Spectrum method used in this study did not use the function transformation of the media. Messages inserted by way of spread with the scalar multiplier then do randomization message by using a random number generator as a pseudorandom key. The concept of this method is to randomize the position bit bit spooler files and messages using Linear Congruental Linear formulas and function XOR (Exclusive OR) then pasted on the end bit pixel frame.

3.1.2.2.1 Analysis of embedding process

Prior to deployment process (spreading), the process does is change the hexadecimal to message then to binary. Then binary messages scattered with four pengalinya, scalar quantities will result in a new segment of the next step is the generation with the generation seedlings pseudonoise determined based on key input after obtaining the value of the keyword (101), then that value is used as the initial seed the random number generation. Calculation of random number generation corresponding random numbers generation formula LCG (Linear Congruential Generator).

an example done five times the spread and the result is "44 83 74 5 8" if modified in binary 01010011 01001010 00101100 became "00000101 00001000". To get the results of the modulation, the message will be segments is modulated with a pseudonoise signals using function XOR (Exclusive

OR). The result of the modulation process which will be inserted into the bit-bit *image*s.

3.1.2.2.1 Analysis Of The Extraction Process

On the process of the extraction process is the reverse of the process of embedding. Enter keywords such as at the time the process of embedding. Next on the body pictures done screening process in order to get bit-bit modulation results after all bit-bit modulation results obtained, then conducted the process of with demodulasi pseudonoise signals of the same keywords on the process of modulation in order to gain bit-bit correlated. The next process is de-spreading is by dividing the results of four demodulasi, which is useful for menyusutkan results demodulasi into the actual content of the message. The end result "01100101 01110100 01110011 01110100" is the same messages when the segment is hidden on the process of embedding. The result is then converted into a kebentuk character will be the original form.

3.1.3 Analysis of Non- Functional Requirements

Analysis of nonfunctional requirements is a step in which an application builder to analyze the resources needed to use the application to be built.

3.1.3.1 user analysis

Users who will be using steganography application consists of a sender and a receiver with such skills needs in Table 3.1 .

Table 3.1 Application User Needs

Tipe Pengguna	Hak Akses	Tingkat Keterampilan	Jenis pelatihan
Pengirim	Dapat melakukan operasi enkripsi pesan dan penyisipan pesan kedalam video	Dapat mengoperasikan komputer dan memahami konsep steganografi dan kriptografi.	Tidak diperlukan pelatihan khusus.
Penerima	Dapat melakukan operasi dekripsi pesan dan ekstrak pesan video.	Dapat mengoperasikan komputer dan memahami konsep steganografi dan kriptografi.	Tidak diperlukan pelatihan khusus.

4. CLOSING

4.1 Conclusion

Conclusions based on the results of the analysis, design, implementation and testing of the system is done as follows:

1. The majority of respondents approve applications allow a user encrypts and hides in the data or confidential information into the video.
2. Based on the results of the questionnaire, these applications meet the criteria-criteria of cryptography and steganography, so aim to improve data security in order to maintain the confidentiality of the data has been fulfilled.

Bibliography

[1] Munir, Rinaldi. 2006. *Kriptografi*. Informatika, Bandung.

[2] Izza Anshory, Indah Sulistiyowati. Simulasi Penerapan MPEG-4 Untuk Pengiriman Video Melalui Jaringan Wireless. Universitas Muhamadiyah Sidoarjo, Sidoarjo.

[3] A.A. Ngurah Pradnya Adhika. Enkripsi Dan Dekripsi Audio Format AMR Dengan Algoritma Kriptografi LOKI97. Universitas Udayana, Denpasar.

[4] M.A. Ineke Pakereng, Yos Richard Beeh, Sonny Endrawan. 2010. Perbandingan *Steganografi* Metode *Spread Spectrum* Dan *Least Significant Bit* (LSB) Antara Proses Waktu Dan Ukuran *File Image*. Universitas Kristen Duta Wacana, Yogyakarta.

[5] Aries Pratiarso, Mike Yuliana, Hadi, M. Zen Samsono Hadi, Fatchul Bahri H., Brahim W. 2012. Analisa PSNR Pada Teknik Steganografi Menggunakan *Spread Spectrum.* Politeknik Elektronika Negeri Surabaya, Surabaya.

[6] Sri Hartati Monalisa. 2014. Steganografi Pada Citra Untuk Pengamanan Data Menggunakan Metode *Spread Spectrum*. STMIK Budidarma, Medan.

[7] Asep Budiman. Aplikasi Steganografi Pada Video Dengan Metode *Least Significant Bit* (LSB). Universitas Komputer Indonesia, Bandung.

[8] Paryati. 2008. Keamanan Sistem Informasi. UPN, Yogyakarta.

[9] Haviluddin. 2011. Memahami Penggunaan UML *(Unified Modelling Language)*. Universitas Mulawarman, Samarinda.

[10] Mahmuddin Yunus, Agus Harjoko. 2014. Penyembunyian Data Pada *File* Video Menggunakan Metode LSB dan DCT. UGM, Yogyakarta.

[11] Farrell, Joyce. 2012. *Java Programming*. Course Technology, United State of America.

[12] Riko Arlando Saragih. 2006. Metode Parity Coding Versus Metode Spread Spectrum Pada Audio Steganography. Universitas Kristen Maranatha, Bandung.

[13] Dinny Devi Triana. Skala Pengukuran sebagai Alat Evaluasi dalam Menilai Tari Karya Mahasiswa. Universitas Negeri Jakarta. Jakarta