STEGANOGRAPHY APPLICATION ON VIDEO WITH LEAST SIGNIFICANT BIT (LSB) METHOD

ASEP BUDIMAN
10103211

UNIVERSITAS KOMPUTER INDONESIA (UNIKOM)
Jl. Dipati ukur no.102-106 Tlp. 2503054 Fax. 2533754 Bandung 40132
Email : asbud01@gmail.com

Steganography is a technique to hide an information which secret or sensive into a media. Secret data is hidden by the way of embedded at a media like citra, audio, and video so that not seen that in the media hidden an information message.

Method Least Significant Bit is a method steganography which can embedding a file in to embed cover like image, audio, and video with change the lower bit-bit from a cover embed so the changes on the steganography that produced will not be visible even the file has been embeded

Steganography at video merges steganography at image and audio, basically video is alliance image which "peripatetic" and audio, which more difficult to be detected and can embedding secret data more if it is compared with steganography at image.

Keyword: *Steganography video, video, least significant bit, LSB.*

CHAPTER I
Introduction

1.1 Background problem

Information Technology Growth (TI) at this time give human amenity to conduct its activity. Entered sent sent information in the form of file became commonplace in computerization era at this time. Many range from to file is referred in secret and of vital importance, and may not known by other party. And along with Information Technology growth referred [as], growing expand also badness technique that have the shape of mutilation and also data theft by party that not have authority to the data referred [as]. There are some attack form to data and information, like hacker, cracker, trojan force attack, and others. In consequence,, today has been conducted various of efforts to care of data security and overcome attacks is referred.

Previous already there is a way of to care of data security that recognized by the name of cryptography. With cryptography of secret data maintained its security, nevertheless form chipertext that randomized will be easy detected and awake third party of file secretness referred. For that applied deep steganography greek means "message are hided" (covered writing) in effort care of data secretness. Steganography is one of way to hide a message/secret data in data or message other emergent not contain anything, except to one who understands the key. In the field of computer security, steganography are used to hide secret data when encryption process can not be conducted or at the same time by encryption process. Thus, although success encryption are broken (dechiper) message/secret data remain not to be seen. At steganografi message are disguised in the form of that relative safe until not happened suspicion is referred [as]. Steganografi can be used at many data form, that is image, audio, and video.

Steganography that expanded at this time is steganography at image and audio, nevertheless steganografi at image and audio still frequently haves weakness like stand-out display change at image and voice trouble that happened at steganografi audio. In other hand much softwares that can detect data and information parenthetic at image and audio.

Rely on various of existing weaknesses at steganography at image and audio is referred, in this Final Projects will be discussed steganography at video. Steganography at video join steganography at image and audio, basically video is aliance from mobile image with audio, that

more difficult detected. This condition because of video can hide more data and video is stream from image until distortion at one of frame image not seen easily by human eyes.

In steganography this video uses method Least Significant Bit (LSB). This condition because of at method Least Significant Bit (LSB) this can keep text file at lowest beet from frame-frame video until the result of video steganografi will not looked to be happen change.

1.2 Identification Problem

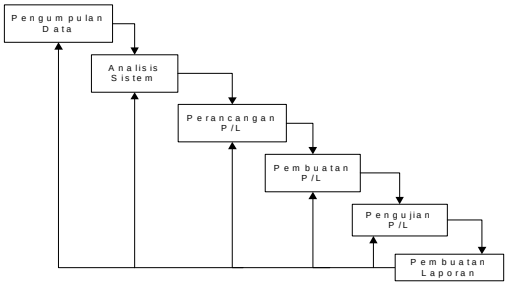
Base problems background above, then problem that formulated that is how develop an application steganography to hide secret message and can protect its data security parenthetic at video by using method Least Significant Bit (LSB) until its data secretness are fixed secured and in kasak eye not happens change at video referred though has been inserted data.

1.3 Purposes and objectives

Intention from Final Projects writing this is the to develop technique steganography image and audio that already exist developed next become technique steganography video that can hide and protect parenthetic data security video avi by using method Least Significant Bit (LSB).
Whereas target that will be reached by in research this is the :

1. To develop a software that can hide and protect parenthetic security of secret information into digital video.
2. For informational how technique steganography method Least Significant Bit (LSB) can be applied in digital video security.
3. To manipulate digital video data that inside existed secret information until

2. Method of software development



Picture 1.1 Diagrams method waterfall

secret message are referred [as] ignorable the existance and in kasak eye not happens its change at digital video manipulation result.

4. Technique steganography by using method Least Significant Bit (LSB) so that can close over existing weakness at technique steganography that has been built previous by using other method.

1.4 Definition Problem

In this Final Projects making, to overcome existing problems then compiler limits problems as follows :

1. Video that used as the insertion media only video avi that have not yet terkompres.
2. Bundle or secret data parenthetic at video have the format of any but its size should be able to be small from accomodation power from video or 1/8 from frame video.
3. Language pemograman that used by is language Pascal.
4. Format of video file that produced by from program steganografhy this is the format *.avi.
5. Bundle or secret data parenthetic or hidden at video but a single file.

1.5 Methodologies Research

Methodologies as used in Final Projects writing this is the as follows :

1. Data collecting Phase

Data collecting Method as used in research this is the as follows :

a. Study to library

Bibliography Study is conducted to look for information about steganography its video and process. Bibliography Source is taken away from steganography related to books video and information that also can be obtained/got from internet.

Step that will be conducted in this system development by using method waterfall like showed at picture 1.1 that is :

Explanation of each phase from process at diagram waterfall above shall be as follows:

a. Data collecting
   Data collecting [of] have the shape of literature or have the shape of erudite masterpieces related to research conducted
b. System analysis
   System analysis will be specified with concerned about information capacities and data processing process networked.
c. Software Design
   Design of data processing Software covers data structure, menu and operation procedure.
d. Software Making
   Making of data processing Software will be conducted with the usage of language correct pemograman, effective and efficient with concerned about computerization technology.
e. Software Testing
   Testing to data processing Software will be conducted with systematic that is in partial at making step and testing final integrated in totally to ensure that pemograman that designed have fulfilled desired result.
f. Making Laporan
   Research Result that conducted will be documented for furthermore need to development hereinafter if required.

1.6 Systematic Writing

This Systematic way of research proposal writing is made arrangements for give public picture about research run. Systematic way of Final Projects writing this is the as follows :

CHAPTER I INTRODUCTION

Elaborate about problems background, try formulate problems nucleus/core faced, determine target and application usefulness built, be next followed with problem demarcation, assumption, and writing systematic way.

CHAPTER II. THEORY BASE

Discuss various of elementary concepts and related to theories research topic that conducted and things that useful in process of problems analysis and overview to similar researches that has been conducted previous entered sintesisnya.

CHAPTER III. SYSTEM ANALYSIS AND DESIGN

This Chapter elaborates about analysis and design about technique Steganography as [the] digital video security with menggunaka method Least Significant Bit (LSB).

CHAPTER IV. DESIGN AND IMPLEMENTATION

This Chapter discusses hit implementation and step performed within research, result of analysis testing hits program characteristic that has been made till conclusion withdrawal.

CHAPTER V. CONCLUSION AND SUGGESTION

Contain conclusion and suggestion that have been obtained/got from result of Final Projects writing.

CHAPTER II
THEORY BASE

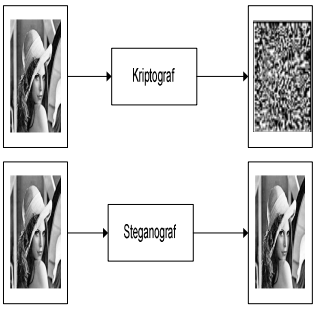
2.1 Steganography

Steganography indigenous to greek that is Steganós that mean hide and Graptos with the meaning article until as a whole that means is article that disebunyikan. In general steganografi is one of way to hide a secret message (hiding message) in data or message other emergent not contain anything, until existence (eksistensi) message are not detected by human sense except to one who understands the key.

Steganography requires two propertieses: container of (cover) and secret data that will be hidden. Digital Steganografi uses digital media as cover, for example image, voice, text, and video. Secret Data that hidden also can be in the form of image, voice, text, or video. Media that has been inserted data is called stegodata or stegofile. Process of data concealment into media called insertion (embedding), whereas process on the contrary called extraction (extraction).

In the field of computer security, steganografi differed from cryptography where steganografi are used to hide data of encryption moment secret can not be conducted or at the same time with encryption. Thus, although success encryption are broken (decipher) message / secret data remain not to be seen and message “disguised” in the form of that

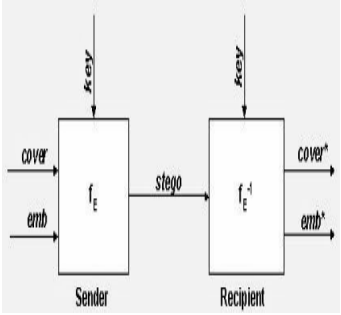
relative “safe” until not happened that suspicion. Whereas at cryptography, where third party can detect existence of data (chipertext) because the result of cryptography have the shape of different data from form in origin and usually its data as if mussy but can be returned to form initialy. Illustration hits cryptography difference and steganografi can be seen at pictute 2.1.



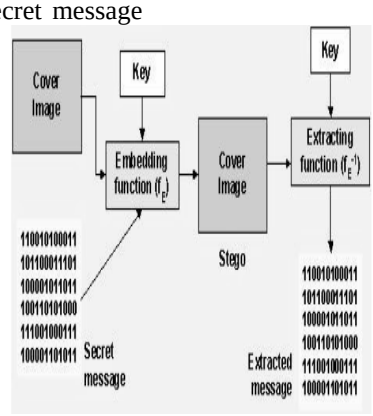
Picture 2.1 Ilustrasis cryptography and steganography

Steganography also discusses how a message can be inserted into a media bundle until third party not realize it. Steganografi exploits limitation of human sense system like eye and ear. With existence of this limitation method this steganografi can be applied at various of digital medias. Output Result from this steganografi have perception form in common by form in origin, it is of course perception here limited to by human sense ability, but is not by computer or processor peripheral digital other.

Picture 2.2 System steganography



Picture 2.2 show a system steganography public where dibagian message consignor (sender), dilakukkan process embedding (fE) message that will be sent in secret (emb) into data cover as [the] place meyimpannya (cover), by using certain key (key), until produced data by message hided in it (stego). In part of message receiver (recipient), dilakukkan process extracting (fE-1) at stego to dissociate secret message (emb) and depositor data (cover) mentioned by using key in common like at process mentioned embedding. Thus only one who knew this key just that can mengekstrak mentioned secret message. Mentioned process can be represented on a more clear at picture 2.3 below/under.



Gambar 2.3 Graphical Version of a Steganographic System

2.1.1 History Steganography

Steganography had been used since yore for the sake of politics, military, diplomatic, and for the sake of person as a means of. Some usage examples steganografi:

1. Steganography at slave body: At greek era Kuno, Herodotus (greek historian) submit message by shave of slave head and mentato its head by message referred. Later, its hair moment grows [again], slave is delivered at its location and hair moment return digunduli then message will be read.
2. Steganography in wax;candle layer: Still at greek era Kuno, secret message are carved at wood then given wax;candle layer to close over message are referred , that way message can be [submitted/sent] without incuring suspicion.
3. Steganography at paper: At World War II, government the United States writes secret message at its ARMY that capture by Germany by using unseen ink above or in empty part other message and to detect it are used water.
4. Steganography with microdots: Still at World War II, spy agent uses microdots to deliver information. The usage of this technique commonly use at microfilm chip that must enlarged around 200 times.
5. Steganography digital world: At one particular guidance that conducted by FBI at the end of September 2001, assistant of FBI director, Ron Dick states possibility ploughmans plane at attack 11 September to buildings World Trade Center use internet technology like website spurious company or porn website, e-mail, chat rooms, bulletin boards to co-ordinate attack.

2.1.2 Steganalysis

Steganalysis is a technique or that used to express message existence is hided or disguised from steganografi. Steganalysis becomes a separate mystery to be able to known how technique to conduct description process or resolving or the invention of message is referred. There is some softwares that can conduct analysis existence of the usage of technique steganografi. In praktiknya way of technique resolving are what used in steganalysis by it self in empirik gyrates range from to :

1. Analysis from change that conducted to meta file data is referred.
2. Analysis from file features has used certain software for steganografi.
3. Compare to genuiness file, last looked for its difference and pattern that used until by this way not only can be known file has experienced of process steganografi can be also known message hidden.

But technique steganalysis not applicable to knows message that will if in the reality message will will experience of cryptography or pengkodean reorders. Thus a good way to conduct steganografi is by undertaking assumption that one would know that there is message that will until will next security with cryptography. Cryptography Election also don't be conducted ineptly and use that has been proven like 3DES and SHA-1.

2.1.3 Benefit Stenaganography

Steganography is a double-edged knife, he/she can be used for good reasons, but can be also used as badness medium. Steganography also can be used as one of method watermarking at image for proteksi copyrights, like also digital watermarking (fingerprinting). Steganography also can be used as substitution hash.

And advanced, like mentioned previously, steganography applicable to hides secret information, to protect it from theft and from one who [have] no business to know it. Unhappily, steganography also applicable to steals data that hidden at other data so it's can be sent to other party, that [have] no business, without that suspect. Steganography also can be used by terrorists to communicate one another. Referring to information system security, steganography only is one of the much implementable ways to hide secret message. Steganography more compatible used at the same time with other method referred [as] to create security that endue. For example steganography can be used [together/ along] with encryption. Windows and Unix also uses steganography in implementation hidden directory.

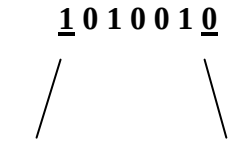
2.1.4 Media Steganography

Steganography uses a cover, its target as the camouflage from message that

actually. Much digital bundle formats that can be made media to hide message. At modern-day like at this time, steganografi usually conducted by entangle bundles like text, image, sound and video.

2.1.5 Least Significant Bit (LSB)

Method most commonly steganografi at type of image bundle is least significant beet (LSB). This Method hides data by change at least data beets means in cover with beets of secret data. At beet formation in a byte (1 byte = 8 beets), there is harshest beet (most significant beet (MSB) and at least beet means least significant beet (LSB).



Beet that suited for changed is beet LSB, because change is referred only alter value byte one higher or one inferior to value previously. Take example at cover image, byte are referred state ruddle, then one-bit change LSB not alters ruddle referred in mean, more than anything else human eyes can not differentiate small change. For example, for example existed data raster original image file that will be used as cover as follows:

00100111 11101001 11001000
00100111 11001000 11101001
11001000 00100111 11101001

Whereas binary representation letter a is 01000001, by insert it into pixel above then will be produced

00100110 11101001 11001000
00100110 11001000 11101000
11001000 00100111 11101001

Seen only three low beets that change (boldface), for human eyes eyesight very impossible to be able to differentiate the color of image file that has been filled secret message in comparison with file of genuiness image before inserted by secret message.

CHAPTER III
ANALYSIS AND DESIGN

System Analysis and design to water down in comprehending and compile step hereinafter that will the of decomposition from an intact system into parts of its component with a view to identify and evaluation bunches of troubles until found weakness, opportunity, and resistance that happened and expected needs so it's can be proposed its repair.

3.1 Analysis Problem

This Analysis covers all problemses that happened at technique steganography this video like how insertion process / embed message at video, process of message extraction, usage password to add security, and process of video quality measurement to know how video difference produced.

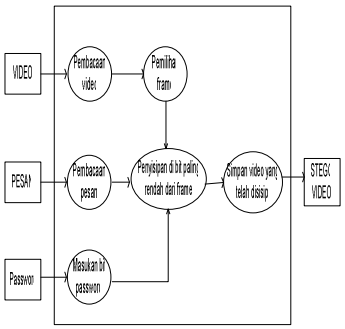
At steganografi video by using method LSB hides beets from secret bundle at segment beets frame video. This Concealment basically give influence to bundle cover frame video, but because change that happened very small until not caught by human sense. For example, for image fairish bitmap 24-bit 256 x 256 piksels are existed 65536 piksels and every fairish pikselnya 3 bytes (R=1 byte, G=1 byte and B=1 byte), mean entirely there is 65536 x 3 = 196608 bytes. Because in every byte only can hide 1 beet at LSB-nya, then maximum size of secret bundle that can be kept at image referred [as] is 196608/ 8 = 24576 bytes or 1/8 from image size referred [as].

3.1.1 Message Embed at video

System for message insertion at video, require input have the shape of video as the insertion media, message that wish inserted,

and password as the protector. Video that useded as the media of message insertion only video that (*.avi) that have not yet terkompresi. Aktifitas that will be conducted at process of message insertion this is the as follows :

1. Conduct read to video file that *.avi to prepare video file is referred that will be used as media of message insertion. Video File is referred turned into set of frame-frame. Every frame in video turned into a file BMP.
2. Conduct read to text file to prepare beets of text file that will be inserted at video. Parenthetic message into video can have the format of any but its size not exceeds power of repository accomodation from video referred .
3. Insert beets of message file into lowest beet from one of frame video that used as the insertion place that produced by at the first step, password are inserted at first frame whereas to order secret will be inserted at next frame.
4. Join return set of frame-frame is referred as that has been inserted message until become video that contain message.



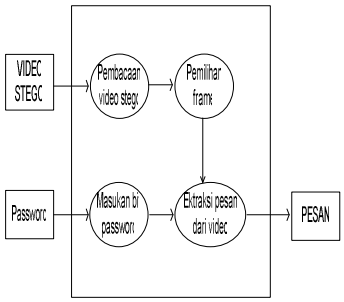
Picture 3.1 Diagrams process of message embed

3.1.2 Embeding message Extraction at video

System to extract message at video need two input unit that is videos that contain message, and password that inputted as [the] its protector. This Video had format in common when insertion that is video that *.avi.

Process of message extraction by the start of election frame and koefesien at video that will be read. Later, message inside read, become message in the form of disorder, password that inputted will become determinant of message [the] truth, where random number consecution that generated by password will arrange how message sequence is referred [as]. Only password that used [by] when insertion that can produce genuiness message [again]. Aktifitas that conducted at process this is the as follows:

1. Conduct read to video file that has been inserted message that produced [by] at process of message insertion. Video File is referred [as] turned into set of frame-frame. Every frame in video referred turned into set of file BMP.
2. Check input password what/wheter already equal to password that kept in file first BMP. If same then continued to process hereinafter, otherwise same then will present mistake message.
3. Detect data beet at second frame and so on that contain code of message data.
4. Write down data beets that has been extracted become a file.



Picture 3.2 Diagrams process of message extraction

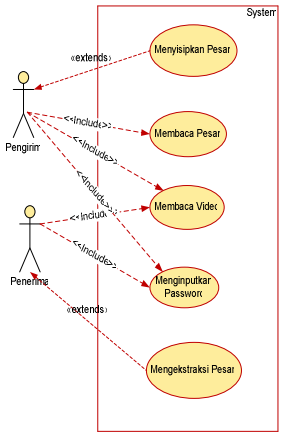
3.2 Design System

System Design is a process that depict how a system is built to fulfill need at analysis phase. System Design bent on to give system picture that will be made. In other word system design is defined as [the] depiction or sketch making from some elements that disjointed into one intact unity and. In other hand also design bent on to be more instruct system that terinci, that is clear and complete design making in the future will be used for simulation making. Application this steganography is made plainly, until expected user can easily use application this steganography.

.

3.2.1 Use case Diagram

Diagram use-case (use-case diagram) is one of diagram to model aspect of system behavior. Each diagram use-case shows a group of use-cases, actor and its relation/link. Diagram of vital importance use-case for memvisualisasikan, menspesifikasikan, and document need of system behavior. Diagram use-case also is centers modeling of system behavior, sub system and class. Use case also can be used mendeskripsikan interaction between system user and system it self, by give a narasi on how system is referred useded.



Gambar 3.3 use case *steganography* video

Software steganography this video haves 5 units use case and 2 actor units. Consignor Actor is user that conduct insertion/embed secret message into video, whereas receiver actor is user that conduct extraction of secret message that has been inserted into video.

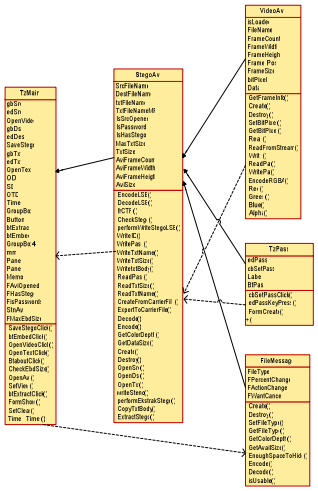
Use case inserts message are used to conduct insert message data into video. Whereas use case reads message are used to conduct message read and validasi message size to power of video accomodation. Then second this use case are only used when insertion process.

Whereas for use case message extraction are used to extract return message that has been inserted into video, then this use case shall only be used at extraction process.

Use case reads video is used to conduct read to video and validasi video size and wether video referred has contained message or have not yet. And use case menginputkan password are used when process of message insertion also when process of message extraction, until second this use case exist ons both process.

3.2.2 Class Diagram

Class diagram is used for mendeskripsikan object types in system and many static relation/link that existed in system referred. Class diagram also can show properties and operation a class and boundaries that existed in object relation/link referred.



Picture 3.4 classes application diagram steganography video

Its explanation :

- Process Penyisipan

At insertion process require 3 input classes that is : VideoAvi class, FileMessage class, and TzPass class.

Where class “VideoAvi” handle all process to video like validasi video format and amount frame video entered, searching frame correct video for made insertion media and to determine capacities of accomodation power from video. Class “FileMessage” arrange read of text file that will diembed and to check wether size of text file referred [as] in accordance with power of video accomodation. Class “TzPass” to keep password was as [the] protector from process embed that can be used as password when extract it [again]. Class “StegoAvi” is class that arrange process of message insertion into video, and also used to keep the result of insertion process.

- Process Ekstraksi

At extraction process membutukan 2 input class that is classes VideoAvi and TzPass class.

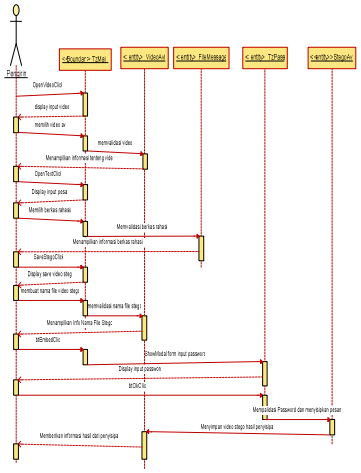
Where Kelas “VideoAvi” used to conduct read and checking to video that inputted what/wheter has contained message or not. Class ”TzPass” used conduct read was to password that inputted what/wheter equal to password was that inputkan when insertion process. If same then video is referred [as] can diekstrak, otherwise same then video stego is referred [as] not can diekstrak. Class ”FileMessage” used to keep text [of] file the result of process of video extract stego. Class ”StegoAvi” used to process ektraksi text file from video stego

3.2.3 *Sequence Diagram*

In methodologies of object orientation to show how an object communicates with other object with concerned about time sequence that modeled didalam sequence diagram.

Sequence diagram consist of objects that presented in study inside load name from object, object recognition, read object that represented by arrow line and time (time) that represented with vertical progression.

3.2.3.1 Sequence Diagram Process Embeding

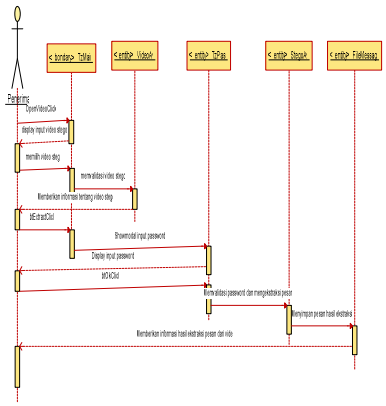


Gambar 3.5 Sequence Diagram Process Embeding

Explanation from picture 3.5 as follows :

1. User click consignor button OpenVideo at TzMain, later, system will present [screen/sail] of video input browser to select video inputted.
2. User consignor selects video that will in inputkan and click button open at [screen/sail] of video input browser, later, system will call VideoAvi class for memvalidasi video and informational from video that select referred to the user consignor.
3. User click consignor button OpenText at TzMain, later, system will present screen/sail of file input browser message to select message that will be inserted into video.
4. User consignor selects message file that will be inserted at video and click button open at of file input browser message, later, system will call FileMessage class for memvalidasi message file and informational from message file that selected referred.
5. User click consignor button SaveStego, later, system will present browser [screen/sail] save file stego, User consignor made file name and address folder to keep last insertion result click button save, later, system will call next VideoAvi class for memvalidasi from file name stego and informational address and name of insertion result file to the user consignor.
6. User click consignor button btEmbed, later, system presents form input password that used as the security, last user content consignor password and click button O.K., last system will call TzPass class for menginputkan and memvalidasi password is conceived of password insertion.
7. Later, system will call StegoAvi class to insert message into video, then keep video stego and present information the result of insertion process are referred.

3.2.3.2 Sequence Diagram Proses Ekstraction



Picture 3.6 Sequence Diagram Proses Ekstraction

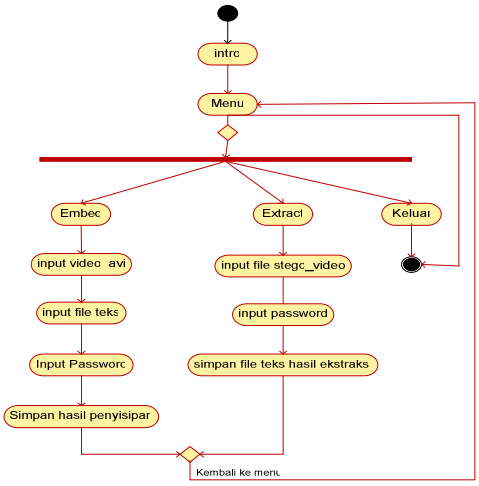
Explanation from picture 3.6 as follows :

1. User click receiver button OpenVideo at TzMain, later, system will present of video input browser stego to select video stego.
2. User receiver selects video file stego that will in inputkan and click button open at of video input browser stego, later, system will call VideoAvi class for memvalidasi wether video referred has had message or not and informational from video stego that select referred.
3. User click receiver button btExtract at TzMain, later, system presents browser save text file to make file name and select address folder to keep text file the result of extraction are referred, last user click receiver button save, later, system will call FileMessage class for memvalidasi name of message file and informational address of message file the result of extraction are referred. Later, system presents form input password.
4. User input receiver password in common with password when insertion, last click button O.K. at form input password, later, system will call TzPass class was for memvalidasi password that inputted what/wheter equal to password when insertion.
5. System will call StegoAvi class to extract message from video. Last system calls FileMessage class to keep message the result of extraction process and informational to the user receiver.

3.4.2.4 *Activity Diagram*

Activity diagram is designed to show what happened during a process and operation take place. Activity diagram is a extension from state diagram. State diagram shows state-state an object and activity representation are expressed as state that attributed to line instructs.

Every activity represented with a rounded rectangle. Processing at one particular activity that will be delivered to next activity automatically to conduct next activity. Line instructs state activity transfer from an activity to activity next. Following is activity diagram from application steganography video, visible at picture 3.7



Picture 3.7 Activities diagram from application steganography video

CHAPTER IV
IMPLEMENTATION DAN TESTING

4.1 IMPLEMENTATION

This Step is conducted after design finishes conducted and hereinafter will implementation at programming language that will be used. Implementation Target is to apply design that has been conducted to application until user can give input to growing of application steganography video that has been built.

4.1.1 Peripheral support That used

In course of its making and testing, application steganography this video it is of course requires hardware and software. Following is explanation from hardware and software that useded.

4.1.1.1 Hardware

In course of its making and testing, application this steganografi it is of course requires hardware and software. Following is explanation from hardware and software that useded.

1. Processor AMD Athlon 64, 2.0Ghz.
2. RAM 1 Giga.
3. VGA 256 MB.
4. Hardisk 80 GB.
5. Mouse dan keyboard.

4.1.1.2 Software

Software as used in making and application testing steganografi this is the as follows :

1. Borland Delphi 7.0
2. Windows media player
3. Virtual Dup
4. Win AVI Video Converter

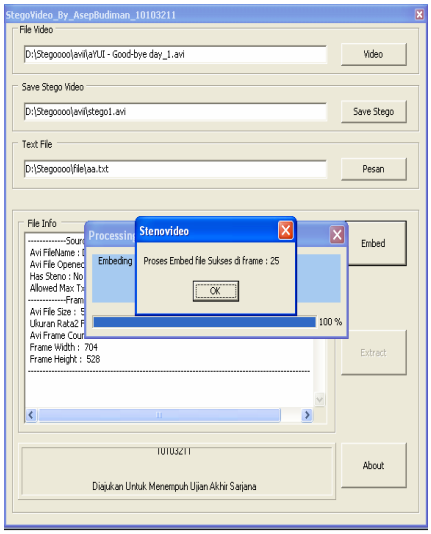
4.2 System Testing

System Testing is processes hereinafter after software implementation finishes conducted. This Testing is conducted to test secret bundle and video avi that useded.

4.2.1 Testing for comparison Size File message

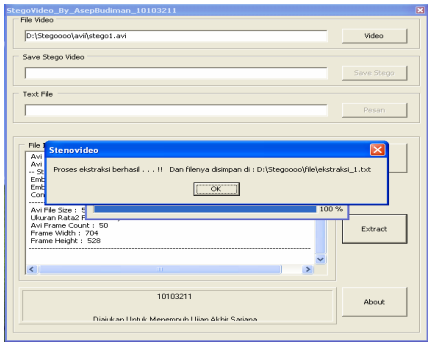
Testing that conducted here that is by compare to content and size from secret bundle before and after conducted process steganografi. This Testing can be told succeed if content and bundle size before and after conducted process steganografi must same precisely either its content or file size.

For example bundle file by the name of file (D:\Stegoooo\file\aa.txt) of the size 1kb are inserted to video by the name of file (D:\Stegoooo\avii\aYUI pin-cushion Good-bye day_1.avi) of the size 54499kb and success insertion process in frame 25th by the name of file stego(D:\Stegoooo\avii\stego1.avi) fairish 54499kb.



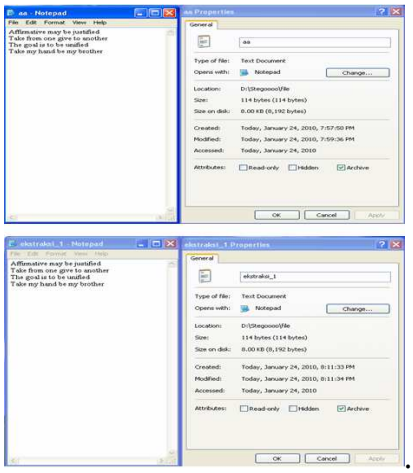
Picture 4.1 Proseses insertion result

Later, file stego (D:\Stegoooo\avii\stego1.avi) that will contain message will next diekstrak until produce new message file by the name of file (D:\Stegoooo\file\ekstraksi_1.txt) of the size 1kb.



Picture 4.2 Proseses extraction result

The result of this testing indicates that content and size of all a success bundle process same precisely by previous secret bundle until this testing can be told succeed.



Picture 4.3 size bundle file and file of extraction result

4.2.2 Pengujian Terhadap Kondisi dan Ukuran video

At this testing will be compared to condition and size frame from video before and after conducted insertion process. Comparison is conducted by give kuisioner to ten one whos not have colour blind disease. Testing at this video told succeed if video condition after conducted insertion process not experiences of big difference is compared to video in origin. In other word, video from bundle that produced [by] difficult to differentiated with video from bundle in origin. For this testing used file stego from testing 4.2.2.



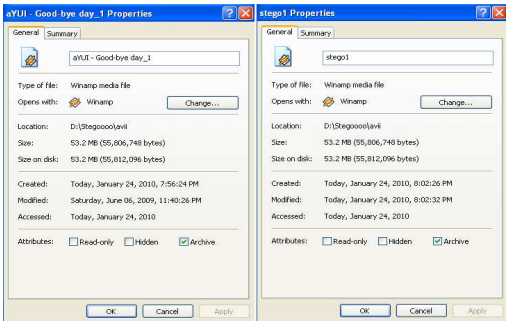
Picture 4.4 Video (D:\Stegoooo\avii\aYUI-Good-bye day_1) frame 25



Picture 4.5 Video (D:\Stegoooo\avii\stego1.avi) frame 25 that have been inserted secret bundle

From perception result that conducted by ten one whos not have colour blind disease is referred [as] entirely conclude that both picture referred [as] seen there is no change though has experienced of process steganografi with tersimpannya text bundle.

Link technique steganografi as used in Final Projects research this is the by using substitution technique at LSB, then theoretically bundle size stego will not differ from genuiness bundle.



Picture 4.5 size video file with file stego that has been inserted message

At picture 4.5 seen size (size) from genuiness video with video stego not experiences of change though has experienced of process steganografi with tersimpannya text bundle in it.

4.3 Conclusion result testing

Base testing that has been conducted, got that application steganography this video can keep text bundles with any format but size of text bundle is referred [as] not exceed accomodation power covers frame video and can extract return file of secret bundle that has been inserted into video.

Testing that conducted to video resolution that is to know accomodation power from video referred [as]. If video avi that have its resolution big then will have big accomodation power conversely if video avi that its resolution small then will have small accomodation power.

Testing that conducted to video indicate that video stego that produced [by] from insertion process not differ and its size not at all changes though has experienced of process of text bundle repository in it. And bundle file that produced [by] from result of file extraction incorruptible stego either content or big its size same as with parenthetic file of genuiness bundle into video. Without berubahnya quality and video size significant stego from video in origin, big possibility others will not know that there is an information in video is referred [as].

CHAPTER V
CONCLUSION AND SUGGESTION

5.1 CONCLUSION

Analysis Having taken steps and system implementation that continued with system testing, then from implementation result and testing referred [as] then can be taken some conclusions as follows:

1. Technique Implementation steganography at video with method Least Significant Bit (LSB) success avi are conducted.
2. By using password at insertion process and extraction then parenthetic security of secret bundle data at video can maintain safely.
3. With technique steganography, though video that has been inserted secret bundle keep be opened with various of sorfware player video.
4. Ever greater parenthetic size of secret bundle then growing looked to be change that happened at cover frame video.

5.2 SUGGESTION

Application steganography video that built this still in rough. This Application still must developed next so that can insert at various of video formats that already compresion and can insert secret bundle in size big.

DAFTAR PUSTAKA

1 Budhi Irawan, *Jaringan komputer*, Graha Ilmu, Yogyakarta, 2005.

2 B.Girod, J.Chakareski, (2002), Advances in Network adaptive Video Streaming, Stanford University .

3 Munir, Rinaldi (2004), *Bahan kuliah ke 7 IF5054 Kriptografi: Steganografi dan watermarking*, Departemen Teknik Informatika Institut Teknologi Bandung, Bandung.

4 Krenn, Robert (2004), *Steganography and Steganalysis.* http://www.krenn.nl/univ/cry/steg/ article.pdf (9 maret 2009 Pukul 21.00)

5 Hirohisa. Hioki, ”A data embeding method using BPCS Principle with new complexity measures” Faculty of Integrated Human Studies, Kyoto University.

6 E.Kawaguchi and R.O.Eason, “Principle and applicationsof BPCS-Steganography,” *Proceedings of SPIE: Multimedia Systems and Applications*

7 http://www.en.wikipedia.org/steganography (12Maret 2009 jam 10:00)

8 http://www.planet-source-code.com (12 Maret 2009 Pukul 10.00)