Secure Data Transmission by Using Video Steganography

Mohd Fikri Bin Mustafa
Universiti Kuala Lumpur
Malaysian Institute of Information Technology
Kuala Lumpur, Malaysia.
fikri.mustafa93@gmail.com

Delina Mei Yin Beh
Universiti Kuala Lumpur
Malaysian Institute of Information Technology
Kuala Lumpur, Malaysia
delina@unikl.edu.my

***Abstract*—** It is very essential to transmit important data like banking and military information in a secure manner. Video Steganography is the process of hiding some secret information inside a video. The addition of this information to the video is not recognizable by the human eye as the change of a pixel color is negligible. With the development of the technology, people have tend to figure out methods which are not only capable in hiding a message, but also capable of hiding the existence of a message. Steganography was introduced as a result of such research work. The proposed technique applies combination of insertion of metadata and blowfish encryption to embed the information into mp4 video files. The proposed method will hide secret information at random path of video metadata. The secret message will be encrypted using blowfish before hiding it into video metadata. When steganographed by this method, the probability of finding the hidden information by an attacker is lesser when compared to the normal method of hiding information frame-by-frame in a sequential manner. It also reduces the computational time taken for the extraction process and can hide huge amount of payload without effecting the steganography criteria.

Keywords—steganography, video, metadata, blowfish encryption

I. INTRODUCTION

Data security deals with the protection of the secret data from eavesdroppers and unauthorized users. Cryptography and steganography are the two techniques used to deal with data security. The main objective of cryptography is to secure communications by changing the data into a form so that it cannot be understood by an eavesdropper. On the other hand, steganography techniques tend to hide the existence of the message itself, which makes it difficult or an observer to figure out where exactly the message is.

Steganography is not new term but it has been used thousands of years back. It is a technique to allow two people to communicate secretly by hiding the presence of any secret message within the cover media. In steganography the secret message is hidden under any other file also known as the carrier. This file can be in digital Text, Image, Audio or Video format.

Video Steganography is a technique to hide any type of files or information into digital video format. Video is the combination of pictures is used as carrier for hidden information. Currently H.264/mp4 video standard due to its excellent compression efficiency and good network affinity has become mainstream video compression standard, so the research of information hiding algorithm based on H.264 /.mp4 standard video is of great significance

II. RELATED WORKS

A. Steganography Overview

Steganography has been widely used in historical times, especially before cryptographic systems were developed. Examples of historical usage include hidden messages in wax tablets in ancient Greece, people wrote messages on the wood, and then covered it with wax so that it looked like an ordinary, unused tablet. Hidden messages on messenger's body: also in ancient Greece. Herodotus tells the story of a message tattooed on a slave's shaved head, hidden by the growth of his hair, and exposed by shaving his head again. The message allegedly carried a warning to Greece about Persian invasion plans. This method has obvious drawbacks. It is impossible to send a message as quickly as the slave can travel, because it takes months to grow hair, a slave can only be used once for this purpose [1] . Modern steganography entered the world in 1985 with the advent of the Personal Computer applied to classical steganography problems. Development following that was slow, but has since taken off, based upon the number of steganography programs available today there is a lot of improvement in term of security.

B. Type of Steganography

Steganography is basically a technique to hide the secret information in cover file which may be in the form of audio, video, image or even text. In steganography, secret information is hidden in such a way that nobody other than intended person knows the existence of the information within the cover file.

I) Pure Steganography

Pure Steganography is defined as a steganographic system that does not require the exchange of a cipher such as a stego-key. This method of Steganography is the least secure means by which to communicate secretly because the sender and receiver

can rely only upon the presumption that no other parties are aware of this secret message. Using open systems such as the Internet, we know this is not the case at all

II) Secret Key Steganography

Secret Key Steganography is defined as a steganographic system that requires the exchange of a secret key (stego-key) prior to communication. Secret key Steganography takes a cover message and embeds the secret message inside of it by using a secret key (stego-key). Only the parties who know the secret key can reverse the process and read the secret message. Unlike Pure Steganography where a perceived invisible communication channel is present, Secret Key Steganography exchanges a (stego-key), which makes it more susceptible to interception. The benefit to Secret Key Steganography is even if it is intercepted only parties who know the secret key can extract the secret message.

III) Public Key Steganography

Public Key Steganography takes the concepts from Public Key Cryptography as explained below. Public Key Steganography is defined as a steganographic system that uses a public key and a private key to secure the communication between the parties wanting to communicate secretly. The sender will use the public key during the encoding process and only the private key, which has a direct mathematical relationship with the public key, can decipher the secret message. Public Key Steganography provides a more robust way of implementing a steganographic system because it can utilize a much more robust and researched technology in Public Key Cryptography. It also has multiple levels of security in that unwanted parties must first suspect the use of Steganography and then they would have to find a way to crack the algorithm used by the public key system before they could intercept the secret message.

C. Steganography Medium

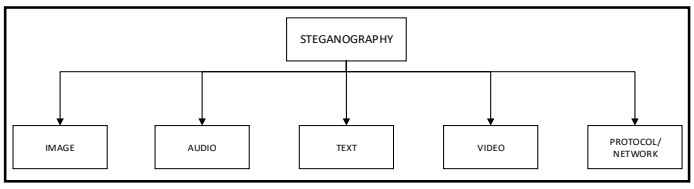

Figure 1 : Steganography medium

I) Encoding Secret Message in Image

Coding secret messages in digital images is by far the most widely used of all methods in the digital world of todays. This is because it can take advantage of the limited power of the human visual system (HVS). Almost any plain text, cipher text, image and any other media that can be encoded into a bit stream can be hidden in a digital image. Two of the more popular digital image encoding techniques used today. They are least significant bit (LSB) encoding and masking and filtering techniques.

II) Encoding Secret Message in Audio

Encoding secret messages in audio is the most challenging technique to use when dealing with Steganography. This is because the human auditory system (HAS) has such a dynamic range that it can listen over. The only weakness in the (HAS) comes at trying to differentiate sounds (loud sounds drown out quiet sounds) and this is what must be exploited to encode secret messages in audio without being detected.

III) Encoding Secret Message in Text

Encoding secret messages in text can be a very challenging task. This is because text files have a very small amount of redundant data to replace with a secret message. Another drawback is the ease of which text based Steganography can be altered by an unwanted parties by just changing the text itself or reformatting the text to some other form (from .TXT to .PDF, etc.). There are numerous methods by which to accomplish text based on Steganography [2]

IV) Encoding Secret Message in Video

It is a technique to hide any type of files or information into digital video format. Video i.e. the combination of pictures is used as carrier for hidden information. The discrete cosine transform i.e. DCT change the values e.g., 8.667 to 9 which is used to hide the information in each of the images in the video, which is not justified by the human eye. It is used such as H.264, Mp4, MPEG, AVI or other video formats. Figure 2 below shows example of video steganography flow.

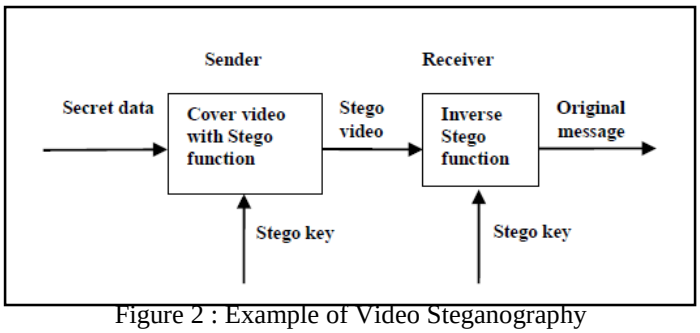

Figure 2 : Example of Video Steganography

D. Steganography Technique

I) Transform Domain

Transformations are used to hide information in the images. In the frequency domain, the process of embedding data of a signal is much stronger than embedding principles that operate in the time domain [3]. The transform domain techniques over the spatial domain techniques is to hides the information in the images that are less exposed to compression, image processing and cropping. Some transform domain techniques are not depending on the image format and they run the lossless and lossy format conversions. Transform domain techniques are classified into various categories such as Discrete Fourier transformation (DFT), discrete cosine transformation (DCT), Discrete Wavelet transformation (DWT)

II) Spital Domain

A spatial domain Steganography technique refers to methods in which data hiding is performed directly on the pixel value of cover image in such a way that the effect of message is not visible on the cover image [4] . The spatial domain methods are classified into three categories, Least Significant Bit (LSB), Pixel Value Differencing (PVD), and Binary Pattern Complexity (BPC)

III) Vector Embedding

A vector embedding method that uses robust algorithm with codec standard (MPEG-1 and MPEG -2) .This method embeds audio information to pixels of frames in host video. It is based on the H.264/AVC Video coding standard. The algorithm designed a motion vector component feature to control embedding, and also to be the secret carrier [5]. The information embedded will not significantly affect the video sequence's visual invisibility and statistical invisibility. The algorithm has a large embedding capacity with high carrier utilization, and can be implementing fast and effectively.

IV) Insertion at Metadata

Java MP4 parser is a java API to read, write and create MP4 container. Typical task for the MP4 parser are muxing video/video into an MP4 file, append recordings that use same encoding setting, adding/changing metadata and shorten recordings by omitting frames. H264 and AAC are most typical codec for MP4 files. Typical issue with this technique is audio and video are not in sync.

V) Masking and Filtering

This approach is used to hides the data by marking an image. This approach is valuable where watermarks become a portion of the image. The data will be embedded where the more significant part of the image rather than hiding it into the noisy portion. The watermarking techniques are more integrated into the image and it can be applied without the fear of destruction of the image. This technique is used in 24 bit and grey scale images

E. Factors Include in Steganography

The effectiveness of steganography technique can be determined by comparing cover-video with the stego video. The various factors are:

I) Robustness

Robustness refers to the ability of embedded data to remain intact if the stego- video undergoes transformations, such as linear and non-linear filtering, sharpening or blurring, addition of random noise, rotations and scaling, cropping or decimation, lossy compression.

II) Imperceptibility

The imperceptibility means invisibility of a steganography algorithm. Because it is the first and foremost requirement, since the strength of steganography lies in its ability to be unnoticed by the human eye.

III) Bit Error Rate (BER)

The hidden information can be successfully recovered from the communication channel. It must be ideal but for the real communication channel, the error comes while retrieving hidden information and this is measured by BER. It is the ratio of the number of errors to the total no of bits sent in an image.

IV) Mean Square Error

It is computed by performing byte by byte comparisons of the two images. The representation of pixel with 8 bits and the representation of grey level images up to 256 levels. The distortion in the image can be measured using MSE. Let I be the cover image, K be the stego image and m*n be the total number of pixels

F. Types of Encryption

There are have two popular type of encryption. Are made up from encryption application (EA), encryption protocols (EP) and encryption Algorithms. And then symmetric cryptography and asymmetric cryptography are some technique of type encryption from sender to receiver. Categorizing are cryptography requires one to know on encryption.

I) Data Encryption Standard

DES is the increase in power and decrease in cost of computing has made its 56-bit key functionally obsolete for highly sensitive information. It considered acceptable for low security application

II) Triple DES

Triple DES or other word is 3DES as sometimes. It run DES three times on the data in three phase: encrypt, decrypt and then encrypt again. It actually doesn't give a threefold increase in the strength of the cipher, but it still gives an effective key length of 168-bit.

III) Advanced Encryption Standard (AES)

AES are significant encryption because they used an open competition to decide on the standard. AES is rapidly becoming the new standard for encryption. It offers up to a 256-bit cipher key. AES is implemented in either 128-bit or 192-bit mode for performance considerations.

IV) Rivest-Shamir-Adleman (RSA)

RSA is public-key encryption technology developed by RSA Data security. The RSA algorithm is based on the difficulty in factoring very large numbers (Rabin, 1998). That mean is fall

to mathematic method. RSA encryption prime factorization as the trap door for encryption. RSA is standard encryption method for important data, especially data for transmitted over the internet.

V) Blowfish

Blowfish is a block cipher proposed by Bruce Schneier, and deployed in some software. Blowfish can use huge keys and is believed secure, except with regards to its block size, which is 64 bits, just like DES and 3DES. Blowfish security has been extensively tested and proven. As a public domain cipher, Blowfish has been subject to a significant amount of cryptanalysis, and full Blowfish encryption has never been broken [6]

G. Comparison of Encryption Technique

Encryption technique is divided into 2 categories, Symmetric and Asymmetric, In Symmetric technique, both sender and receiver use a shared key to encrypt or decrypt the data. The problem with this technique is that if the key is known to others. In Asymmetric technique, both sender and receiver use a separate key to encrypt and decrypt the data. For this project im using Blowfish Encryption technique, Blowfish is the most commonly used algorithm around the world, developed by Bruce Schneier, the president of Counterpane Systems, a firm that deals with cryptography and security. Blowfish is known to be the secret-key cipher that uses a variable number of bits ranging from 16 - 448 bits and encrypts the data 16 times to make it impossible for a hacker to decrypt it. Until now, no attack has been discovered to break the blowfish encryption (Bruce Schneier, n.d)

Table 1 : Comparison of Encryption Technique

Encryption	Info	keys	Type
AES	.Efficient in both software and hardware	128 to 256 bits	Symmetric
RSA	It can be used both for encryption and for digital signatures	1024- bits	Asymmetric
DES	Old data encryption standard	64- bits	Symmetric
Blowfish	Algorithm design to replace DES	64-bits	Symmetric
Twofish	Improvement from Blowfish	256- bits	Symmetric

H. Existing System

I) Our Secret

Our Secret is freeware software that user can use to hide message and documents in video. It has very simple interface and can hide multiple messages or documents in a single video file. The disadvantages of Our Secret is they are not provided encryption to the data

II) MSU Stego Video

MSU StegoVideo also freeware software, the advantage of this software is data that had been hide can be recovered even video was compressed again by another codec but its not provide encryption to the data

III) DeEgger Embedder

DeEgger Embedder is an lightweight freeware Steganography software. It has simple interface where user can easily drag and drop the carrier file and secret file. The limitation for this software is they are not protected by password, attacker migheasily steal the data (Waqas Ahmed, 2012)

I. Comparison of existing system of Video Steganography

Table 2 : Comparison of Existing Sysem

Tools	Encryption	Video Format	Methods	Keys
Video Stega	Yes	MP4	Insertion	Yes
Our Secret	No	3GP,MP4,MPG,VOB	-	Yes
MSU StegoVideo	No	AVI	Transposition	Yes
DeEgger Embedder	No	AVI,MP4	-	No

III. PROJECT DEVELOPMENT

The product (application) is named as Video Stega, Which is the combination of steganography and cryptography together as one application. The application is implementing Windows Operating system. The product function is to hide data (text) in an video files, this process include encryption of the data subject to be hidden. The user can also decrypt and review back the hidden data; this process is called steganography.

Furthermore, the application can hide the secret data without changing the video quality. To prove this progression, there is a tools that can view and compare the video quality of the video before and after steganography happen. If the graph shows constantly pattern, the quality of the video remain same. There is also another tools used to proved that the secret data has been successfully encoded inside the video metadata, the tools will compare the both video and produce a result whether the video is identical or not. If the result is not identical, it will prove there is hidden data presence in the video files.

A. System Structure

Sytem structure will describe about the workflow of the Video Steganography applications . This system will be implemented based on diagrams and flowchart proposed in Chapter 3. Figure 3 and Figure 4 depicted the proposed flowchart while Figure 5 and Figure 6 depicted the block diagram that will show flow of the system and represent the flow from one activity to another activity, diagram as proposed will describe a set of standard notation for the modelling of real object and systems and use

the intuitive symbols to represent the system elements. The diagram shows each of the flow system processes.

I) Encode Flowchart

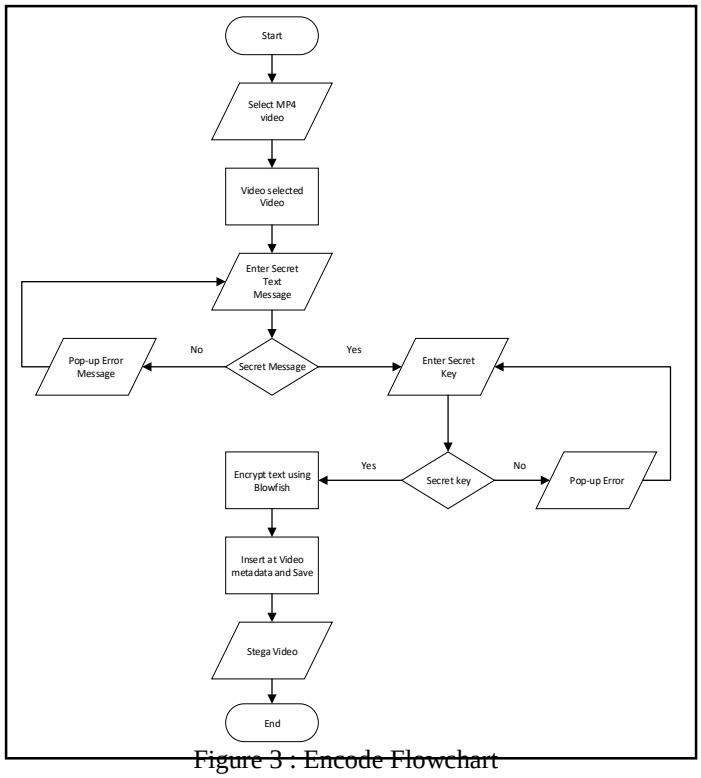

Figure 3 : Encode Flowchart

II) Decode Flowchart

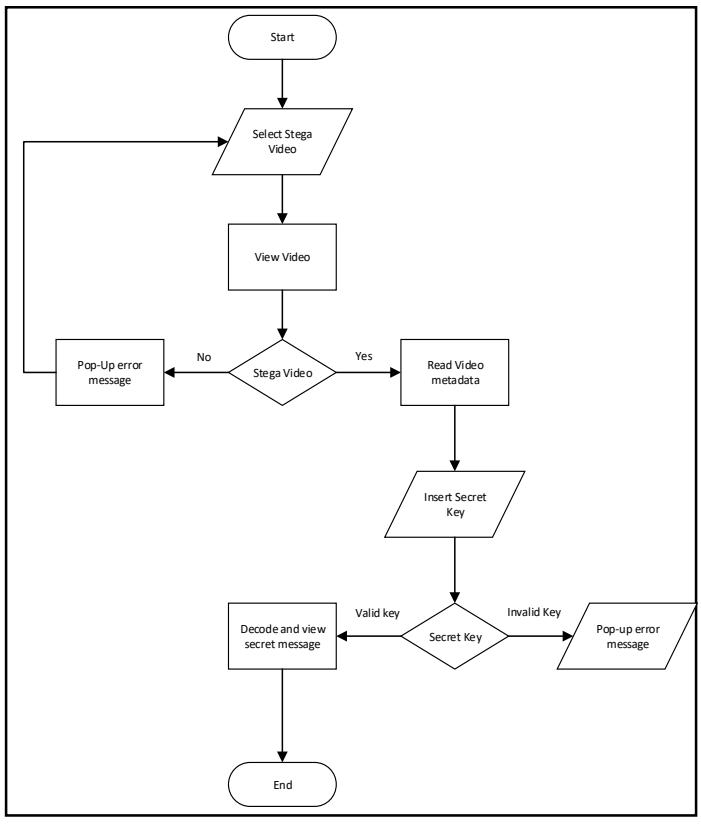

Figure 4 : Decode Flowchart

III) Encode Block Diagram

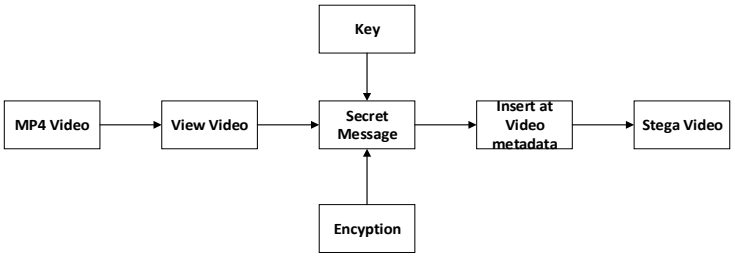

Figure 5 : Encode Block Diagram

IV) Decode Block Diagram

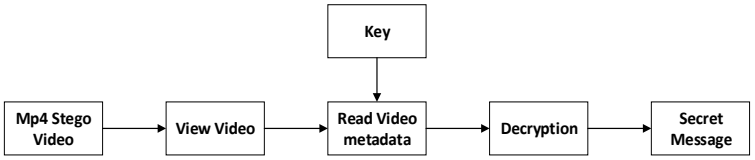

Figure 6 : Decode Block Diagram

B. Result and Discussion

the testing phase which explain about the testing method that is used to test the Video Steganography application. Testing is important phase to make sure the application is free from errors and to gain confidence with the system functionality with security and integrity. In general, testing is about finding out how well something works and testing is work level of knowledge or skills has been acquired. The developer will be able to fix the issues if there have any errors found during do the testing. However the test result important because this is to ensure the functionality of the system achieved the project objective or not.

System testing is to test the whole system of development projects. For this testing, there are four types of testing which is Data Integrity testing, Video Quality testing, Secret Data validation testing and payload testing. Each of the testing were performed using Open Source Software.

I) Data Integrity Testing – Autopsy 4.4.0

Data integrity testing is performed to test the visibility of secret data and key after encoded happen by using Autopsy 4.4.0. Autopsy is a forensic tools that will analyse the video files, list all findings and produce result. As a result in table 3 below the tools cannot find or detect the secret message and key.

Table 3 :Data Integrity Testing – Autopsy 4.4.0

No	Video Size (MB)	Visibility
1.	2	Visible
2.	5	Visible
3.	10	Visible
4.	20	Visible
5.	30	Visible

II) Data Integrity Testing – HxD

Data integrity testing is performed to test the visibility of secret data and key after encoded happen by using HxD hex editor. Hxd functions is almost similar to Autopsy which is a forensic tools that will analyse the video files, list all hex and and string value. As a result the tools cannot find or detect the secret message and key, this is depicted in Table 4

Table 4 :Data Integrity Testing – HxD

No	Video Size (MB)	Visibility
1.	2	Visible
2.	5	Visible
3.	10	Visible
4.	20	Visible
5.	30	Visible

III) Video Quality Testing

Video quality testing was performed by using MSU Video Quality Measurement Tools Free 9.1. This software will test the quality of video before and after encoded happen, it will compare based on Peak Signal to Noise Ratio (PSNR) of the video files. The tools will compare the noise inside the video if any changes happened.

Table 5 : Video Quality Testing

No	Video Size (MB)	Before	After
1.	2	Unchanged	Unchanged
2.	5	Unchanged	Unchanged
3.	10	Unchanged	Unchanged
4.	20	Unchanged	Unchanged
5.	30	Unchanged	Unchanged

As the result in table 5 above, the quality of the video before and after the encoded remain the same. So the encoded technique that has been implemented will not change the quality of the video.

Figure 7 : Comparison of noise of Video Files

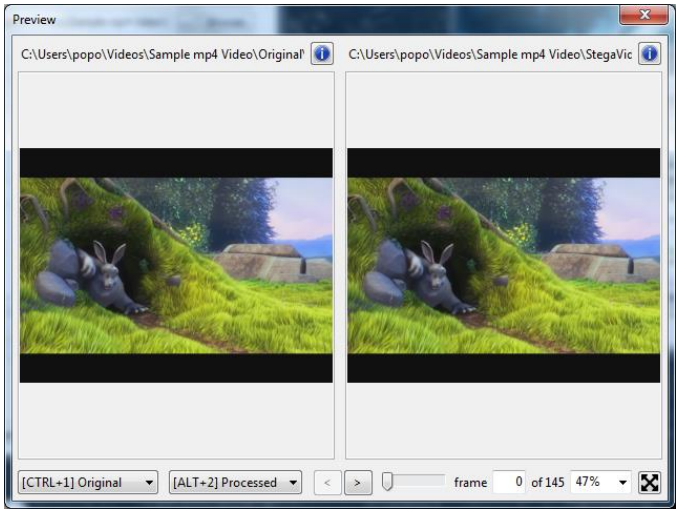

Figure 8 : Frame Comparison of Video Files

Figure 8 above shows frame comparison between original and processed of video files

IV) Secret Data Validation Testing

WinMerge is an Open Source differencing and merging tool for Windows. WinMerge can compare both folders and files, presenting differences in a visual text format that is easy to understand and handle. This software is used to proof the validation of encoded message. As the result based on Table 6 below proofed that the files are not identical which means the encoded is successfull.

Table 6 : Secret Data Validation Testing

No	Video Size (MB)	Before	After
1.	2	Unchanged	Changed
2.	5	Unchanged	Changed
3.	10	Unchanged	Changed
4.	20	Unchanged	Changed
5.	30	Unchanged	Changed

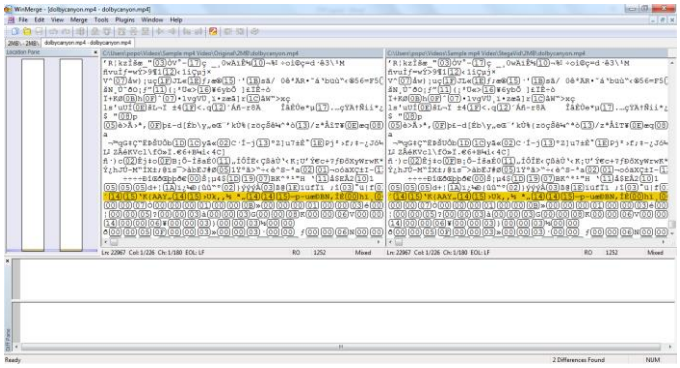

Figure 9 : Location of the secret message in Video Files

V) Payload Testing

Payload testing is performed to test the amount of secret data can be hide inside the video metadata based on steganography criteria, which is size before and after the steganography

happen. The testing conducted between 20 to 3200 number words. As the result the size different meet the Steganography criteria as shows in Table 7 below

Table 7 : Payload Testing

No	No of words	Size Before(MB)	Size After(MB)	Size Different(MB)
1.	20	5.00	5.13	0.13
2.	50	5.00	5.13	0.13
3.	100	5.00	5.13	0.13
4.	200	5.00	5.13	0.13
5.	300	5.00	5.13	0.13
6.	400	5.00	5.14	0.14
7.	800	5.00	5.14	0.14
8.	1600	5.00	5.16	0.16
9.	3200	5.00	5.18	0.18

Table III.2 : Security Testing

IV. FUTURE RECOMMENDATION

For future recommendation, it is recommended to improve the system for future development by extend the future and overcome the current problems in terms of functionality for video steganography tools. In addition, video steganography tools could be further improvised by first extending the application to a wider variety of different video format and provide variety of secret message other than text, such as image and audio.

REFERENCES

[1] M. Dixit, N. Bhide, S. Khankhoje and R. Ukarande, "Video Steganography," 2015 International Conference on Pervasive Computing (ICPC), Pune, 2015, pp. 1-4. doi: 10.1109/PERVASIVE.2015.7087159

[2] Y. Zhang, M. Zhang, X. Yang, D. Guo and L. Liu, "Novel video steganography algorithm based on secret sharing and error-correcting code for H.264/AVC," in Tsinghua Science and Technology, vol. 22, no. 2, pp. 198-209, April 2017. doi: 10.23919/TST.2017.7889641

[3] K. Hossain and R. Parekh, "An approach towards image, audio and video steganography," 2016 Second International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN), Kolkata, 2016, pp.302-307. doi: 10.1109/ICRCICN.2016.7813675

[4] D. Job and V. Paul, "An efficient video Steganography technique for secured data transmission," 2016 International Conference on Data Mining and Advanced Computing (SAPIENCE), Ernakulam, 2016, pp. 298-305. doi: 10.1109/SAPIENCE.2016.7684125

[5] P. Yadav, N. Mishra and S. Sharma, "A secure video steganography with encryption based on LSB technique," 2013 IEEE International Conference on Computational Intelligence and Computing Research, Enathi, 2013, pp. 1-5. doi: 10.1109/ICCIC.2013.6724212

[6] Bruce Schneier (n.d). The Blowfish Encryption Algorithm. Retrived from https://www.schneier.com/academic/blowfish/