MEU جامعة الشرق الأوسط
MIDDLE EAST UNIVERSITY
Amman - Jordan

Secure Data Hiding Technique Using Batch Video Steganography

تقنية إخفاء البيانات بطريقة آمنة باستخدام حزم الفيديو

By
Sara Ahmad Alrefai

Supervisor

Dr Mudhafar Al-Jarrah

A Thesis Submitted in Partial Fulfilment of the Requirements for The Master's Degree in Computer Science

Department of Computer Science

Faculty of Information Technology

Middle East University

May 2019

Authorization

I Sara Ahmad Mohammad Ali Alrefai authorize Middle East University to provide and electronic copies of my thesis to the libraries, organization, or bodies and institutions concerned in research and scientific studies upon request.

Name: Sara Ahmad Mohammad Ali Alrefai

Date: 3/6/2019

Signature: Sara

23/6/2019.

Examination Committee Decision

This is to certify that the thesis entitled "Secure Data Hiding Technique Using Batch Video Steganography" was successfully defended and approved on 2/6/2019.

Examination Committee Members	Signature
(Supervisor and Chairman of Examination Committee) **Dr. Mudhafar Aljarrah** *Associate Professor, Department of Computer Science* *Middle East University*	2019/6/19
(Internal Committee Member) **Dr. Abdelrahman Abu Arqoub** *Associate Professor, Department of Computer Science* *Middle East University*	22.06.2019
(External Committee Member) **Dr.Adnan Hnaif** *Associate Professor, Department of Computer Science* *Al Zaytoonah University*	٢٠١٩/٦/٢٢

Acknowledgement

(وَمَا تَوْفِيقِي إِلَّا بِاللَّهِ ۚ عَلَيْهِ تَوَكَّلْتُ وَإِلَيْهِ أُنِيبُ)

First and foremost, I would like to thank God Almighty for giving me the strength, knowledge, ability and opportunity to undertake this research study and to persevere and complete it satisfactorily. Without his blessings, this achievement would not have been possible.

I would like to thank my thesis supervisor Dr. Mudhafar Aljarrah of the Department of Computer Science at Middle East University. The door to Dr. Aljarrah\s office was always open whenever I ran into a trouble spot or had a question about my research or writing. He consistently allowed this thesis to be my own work but steered me in the right direction whenever he thought I needed it.

I would also like to thank the members of my thesis examination committee, Dr Abdelrahman Abu Arqoub and Dr Adnan Hnaif, who provided me with their valuable comments and input, which enriched the form and content of my thesis.

The researcher
Sara Alrefai

بسم الله الرحمن الرحيم

"وقل ربي زدني علماً"

Dedication

This thesis is dedicated to:

The sake of Allah, my Creator and my Master,

My great teacher and messenger, Mohammed (May Allah bless

and grant him), who taught us the purpose of life,

My homeland Jordan, the warmest womb.

My great parents, who never stop giving of themselves in countless ways.

My beloveds' brothers Hashim and Mohammad, my pretty sisters Seema, Viviana, Saba, who

stands by me when things look bleak…

I dedicate this research.

Contents

List of figures

List of tables

List of Abbreviations

ABS	Adaptive Batch Steganography
AES	Advance encryption standard
AVI	Audio Video Interleaved
DCT	Discrete Cosine Transformation
DWT	Discrete Wavelet Transformation
FZDH	Forbidden Zone Data Hiding
IP	Internet Protocol
JPEG	Joint Photographic Experts Group
KL	Kullback–Leibler divergence
LSB	Least Significant Bit
MAX	Maximum
MD5	Hash function producing a 128-bit hash value
MPEG	Moving Picture Experts Group
MSB	Most Significant Bit
MSE	Mean Square Error
OSI	Open Systems Interconnection
PSNR	Peak Signal to Noise Ratio
RGB	Red Green Blue
RSA	Rivest Shamir Adleman
SSIM	measurement of structural similarity
SHA-1	Secure Hash Algorithm 1
TCP	Transmission Control Protocol
BVS	Batching Video Steganography

Secure Data Hiding Technique Using Batch Video Steganography

By Sara Alrefai

Supervisor: Dr Mudhafar Al-Jarrah

Abstract

Steganography is the art of masking the secret information and denying its existence in such way no one can detect, by covering confidential information inside an innocent cover, no one can know what is hidden in the carrier except the concerned sender and receiver. The Steganography approach is facing two challenges. First, the size of data that needs to be hidden is becoming larger as in multimedia files. Second, Steganalysis techniques are becoming more sophisticated which poses a threat that an intelligent Steganalyzer can extract the hidden data. There are many multimedia file types can be used as a cover in steganography systems like text, images, audio and video, but the video is considered the best choice for cover because it provides higher embedding capacity, and nowadays it is widely exchanged in social media. This thesis proposes a novel batch video steganography system (BVS) for secure and high capacity information hiding, using the batching technique to split the secret payloads into a batch of fragments where each fragment is stored in a different video cover. The LSB replacement technique is used for embedding within frames of the selected video covers. To strengthen the security of the hidden data, each byte of the secret data is split into bit pairs and each pair is hidden in a different cover. The experimental work showed the embedding of various secret data file types. The peak signal to noise ratio (PSNR) was used to evaluate the imperceptibility of the stego frames with respect to the original frames which gave an average value of more than 49 decibel. The results showed that the system can embed any type of data in AVI video batches with lower opportunity to notice the effect of embedding of the secret payload, especially that with moving frames in a video film it is less likely to observe a change.

Keywords: Steganography, AVI video, batching, security, hide, embedding, extract, LSB, PSNR, warden, BVS, system, capacity, warden.

تقنية اخفاء المعلومات بطريقة امنة باستخدام حزم الفيديو

إعداد: سارا الرفاعي

إشراف: الدكتور مظفر الجراح

الملخص

ستيجانوجرافي هو فن إخفاء المعلومات السرية وإنكار وجودها بطريقة لا يمكن لأحد أن يكتشفها، وذلك عن طريق تغطية المعلومات السرية داخل غلاف بريء، بحيث لا يمكن لأحد أن يعرف ما هي المعلومات السرية إلا المرسل والمستقبل المعني. يولحه النظام تحديين ، التحدي الأول هو أنه اذا كانت البيانات التي نريد إخفاءها كبيرة كما هو الحال في ملفات الوسائط المتعددة، ثانياً أصبحت تقنيات تحليل ملف الغطاء أكثر تطوراً مما يشكل تهديداً على البيانات، بإستطاعة المحلل الذكي استخراج البيانات المخفية. هناك العديد من أنواع الوسائط المتعددة التي يمكن استخدامها في أنظمة إخفاء المعلومات مثل النصوص والصور والصوت والفيديو، لكن الفيديو يعتبر أداة فعالة وهامة لأنه يوفر سعة تضمين أعلى ويتم تبادله في الوقت الحاضر على نطاق واسع في وسائل التواصل الإجتماعي. تقترح هذه الأطروحة نظامًا جديدًا لإخفاء المعلومات بكفاءة عالية من خلال تقنية حزم الفيديو لتوزيع الحمولة السرية على أغلفة فيديو متعددة، ذلك لتوزيع الحمل على أكثر من كائن الذي سيساعد من استيعاب حمولة أكبر من البيانات السرية مع الحد الأدنى من الشكوك، تم استخدام تقنية استبدال LSB 2 لعملية تضمين البتات الأقل أهمية من ملف الفيديو الأصلي ببتات الملف السري المراد تضمينها لتعزيز أمان البيانات المخفية كما تساهم عملية توزيع الحمولة على أكثر من غطاء على تصعيب عملية استخراج البيانات السرية على المراقب، لانه يتم تقسيم كل بايت من البيانات السرية إلى أزواج بت ويتم إخفاء كل زوج في ملف فيديو مختلف. أظهر العمل التجريبي تضمين أنواع مختلفة من ملفات البيانات السرية. تم استخدام إشارة الذروة إلى الضوضاء (PSNR) لتقييم عدم الادراك الحسي للإطارات مقارنةً مع الإطارات الأصلية اللتي أعطت قيمة حوالي49 ديسبل . أظهرت نتيجة النظام أنه يمكن تضمين أي نوع من البيانات في حزم فيديومن نوع AVI مع فرصة أقل من الشكوك بوجود حمولة سرية، خصوصاً بوجود الإطارات المتحركة في فيلم الفيديو، يكون من غير المحتمل أن يتم ملاحظة أي تغيير.

الكلمات المفتاحية : ستجانوجرافي، إخفاء البيانات، حزم ، فيديو ،غلاف ، حمولة ، نشر ، تضمين ، استخراج ، غطاء ،توزيع ، استبدال ، السعة ، المراقبين

Chapter One

1.1 Introduction

This chapter will address the primary topics, focusing on the problem statement, the significance of the work, the goal and objectives and the questions that must be answered using rational answers.

1.2 Research Context

This thesis deals with securing the transmitted information using digital video medium to avoid detection or extraction by observers, such practice of securing data is called “steganography” (Petitcolas.A, Anderson.R, Khan.M, 1999).

Furthermore, the research focuses on the partitioning and distribution of secret data into a batch of fragments, which help to increase the hiding capacity as well as protecting secret data from extraction.

1.3 Background

In recent years, communication of confidential data is a major issue everywhere, to increase the information security a nonconventional approach called steganography is proposed (Saleh. M.A, 2018).

Confidentiality and privacy are required for many fields, such as medical, military, education, even for peoples between each other's, hence the importance of the data concealment science by coating and embedding the secret data within another regular file, it can be applied to graphics, video files, audios, and texts (Sumathi, C.P, Santanam.T, Umamaheswari G 2013).

Kakde.V, Pawar.S, (2014) mentioned that the hidden message could be invisible ink between the visible lines of a secret letter. Steganography is based on the Greek word Stegano which means covered or reticent, the word was revived after being a misnomer for 150 years. It was brought to a close early in the nineteenth century, labelled an obsolete synonym of cryptography, but was revived in the eighteen as a form of digital cryptography. Sending data in public communication is not secure therefore, hiding secret data for a more secure communication insulates information from one unauthorized user or one unintended recipient.

According to Thampi.S.M, (2004) Steganography is sometimes used when encryption is not permitted, or generally used to complete encryption, so even if the encrypted file is deciphered, the hidden message is still not seen, unlike cryptography the art of secret writing, secret messages do not attract attention to themselves. Clearly visible encrypted messages no matter how unbreakable will arouse suspicion and may themselves be incriminated in countries in which encryption is illegal. Thus, whereas cryptography disguises a message to conceal its contents, steganography protects both communicating parties and the contents of the messages (Behal.S, Kaur.N, 2014)

Table.1.1 Comparison of secret communication techniques

Secret communication Technique	Confidentiality	Integrity	Un-removability
Encryption	Yes	No	Yes
Digital signature	No	Yes -No	No
steganography	Yes -No	Yes -No	Yes

A comparison of the secret communication technique (Channalli.S, Jadhav.A, 2009) shows the different confidentiality, integrity and un-removability levels of the secret data between different communication technology like encryption, digital signatures and steganography as Table.1.1 shows.

Shukla.A.k, Dixit.G. (2017) The main goals of steganography are to communicate securely in a completely undetectable manner, provide a cryptic communication to hide a secret message and to avoid drawing suspicion to the transmission of a hidden data in a way that no one apart from the intended recipient, even to be known that a message has been sent.

(Jayaram P, Ranganatha.H., Anupama H.S, 2011) mentioned that a good steganography technique should ensure that embedded data remain immune and recoverable, and offer unavailability of hidden data against compression, interception, modification or removal etc.

The Renaissance and revival of steganography can be attributed to some points:

I. The increased need to protect the intellectual property rights of digital content owners.

II. The government bans on digital cryptography. Individuals and companies who seek confidently look to steganography as a viable alternative, since combining cryptography and steganography can help in avoiding suspicion and protect privacy.

III. The trend toward electronic communication and humans desire to conceal messages from curious eyes, with rapid advancement in technology, coding software is getting effective in hiding information in the image, video, audio, or text files.

Despite the wide good use of the technique, there is always a misuse. Terrorists can use cryptography and steganography to keep their communication secret and to coordinate attacks.

This sound disgraceful, and the fact the obvious uses of steganography is for things like spying.

As reported by Sandhu.M, Kaur.J, Kuar S, (2016) in The New York Times published an article On October 2001, Allegation that AL Qaeda used steganography to encode messages into images and send it by email, and maybe by USENET to proceed September 11, 2001, the horrible terrorist attack.

1.4 Problem Statement

The field of information hiding or steganography, which serves to protect the security of data exchanged over communication networks, faces two main challenges. First, the size of the secret data that needs to be hidden inside cover media has increased tremendously, from small text documents and images in the past, to large databases and video media in recent years. Second, the steganalysis techniques have become more sophisticated, with the help of machine learning and image analysis, which is increasing the possibility of not only discovering the existence of a hidden data but also to be able to extract the hidden secret data. The work in this thesis aims to deal with the two problems, through increasing the hiding capacity of the cover media and using techniques that will prevent the attackers from getting any useful information while attempting to extract the hidden data.

1.5 Goal and Objectives

The goal of this research is to enhance the steganography approach as a mechanism for protecting confidential data transmitted over networks, through increasing the hiding capacity and strengthening the secrecy of the hidden data.

The following objectives are taken into consideration.

1- To design and implement a strong steganography system to embed a large payload into a batch of identical video covers and to enhance the security of the embedded data.

2-To slice and embed the secret data within different video covers in such a way that it should not be possible to get any meaning information if an attacker manages to extract the embedded data in one video cover.

3- To embed the secret data within successive frames of a video cover, and to utilize the appropriate embedding technique that will provide high embedding capacity without affecting the imperceptibility.

4- To ensure that the resulting stego videos will be identical in size with the cover videos.

5- To experiment with embedding and extracting various multimedia files in batches of video covers, and to measure the statistical imperceptibility of the stego videos.

1.6 Motivation

The information security confidentiality and integrity always had significant attention from the researchers and is considered as a critical issue. Therefore, it is necessary to enhance the complicated of detecting the embedded data, and capability to hide the existence of confidential message to get rid of desire unauthorized persons from becoming aware of the existence of a message. The great advantage of video is the large size of payload that can be hidden inside a video. A video is a moving stream of images and sounds. Therefore, any small but other noticeable distortions might go unobserved by humans because of the continued flow of information and the fast movement of frames.

1.7 Contribution

The expected strengthening of data security by embedding secret information in a video covers through the batching technique, which provides a steadfast and impermeable mean of communication to share important or sensitive information with specific recipients with minimal doubts that a secret message is hidden within.

1.8 Scope of work

The scope of the project is to design and implement a technical solution that will fulfill the research goal of increasing the hiding capacity and strengthening the protection of the hidden data from unauthorized access. To meet the requirements, the BVS system was developed. The proposed system employs a suitable algorithm for embedding the payload in the frames of multiple video files, using the LSB replacement technique which provides higher embedding capacity compared with other embedding techniques. The BVS system partitions the secret data into bit pair fragments and embeds the fragments in frames of different video files so as to prevent the extraction of the secret data in a legible form by an attacker. The work included testing the BVS system using several types of multimedia files as secret data, and evaluating the distortion effect of data embedding by measuring the distortion metrics of the video cover before and after the embedding process.

1.9 Thesis organization

The rest of this thesis is organised as follow:

Chapter Two presents the literature review, an overview of the perception of steganography in general, and related work. Chapter Three presents the methodology, objectives and design of the proposed model, outlines of the system, and flow charts to show the embedding and extracting modules and the results expected of the proposed system. Chapter Four comprehends the experimental results and discussion which introduced the introduction, objectives of the experimental work, the dataset of the cover video and the payload, batch embedding, Extraction module, least significant bit technique, experimental calculations, error Analysis measures, the PSNR results average, video quality evaluation, result and discussion of the reference work and the proposed work. Chapter Five presents the conclusion and suggests future works.

Chapter Two
Literature review

2.1 Introduction

This chapter shows an analysis of the concepts of steganography science, embedding algorithms, batching technique, video processing, and some related work in different steganography types.

2.2 Steganography overview

Considering the constant growth of all types of well-known digital attacks that are lurking on the internet, information security is the most critical issue at the present time. (Folk C, Hurley D.C, Kaplow, W.K, Payne.J.F, 2015)

People around the world transmit a huge number of multimedia files through the internet, sending files that might contain critical information through the internet is a sensitive matter, here the importance of steganography lies to cover personal information or sensitive data in a medium to prevent attackers from observing any differences between the original file and the stego-file. No changes or loss of the quality of data occurs during a steganography mechanism. (Sheelu, Ahuja.B, 2013)

Steganography is the art of inconspicuous hiding data within other data. The main target of steganography is to mask information well. (Channalli.S, Jadhav. A ,2009)

This technique can be used for ethical motives, to embed a message in Facebook photos for example, but these methods can be used atrociously. For security defenders, the question is how to tell the difference between a video that has been modified for legitimate reasons and the one that has been changed to secretly contain malicious information.

The main goal of steganography is to transfer steadily in a completely imperceptible way, such that no one can dubious that it bears some top-secret information. Different cryptography, which secures data by transforming it into another unreadable format, steganography makes data unseen by hiding (or embedding) them in alternative media. Thus, cryptography is the science of undisguised secret writing while steganography as ulterior secret writing. (Kahlon.J.S, Bhardwaj.V, 2016)

2.3 History of Steganography

The word steganography is not a new term, steganography has been used for hundreds of years, it came from a Greek word which means (cover or hide) we can go far back in history and find examples in which steganography has been used, during the World War, the spies used invisible inks, these were fluid such as milk, fruit juice or urine that was getting darker when heated. (Kavitha.R, Murugan.A, 2008)

2.4 Types of Steganography:

A. Text Steganography

In this approach, the secret message is hidden in the text by changing the ninth bit of every word, perhaps it is the most difficult type of steganography due to the lack of redundant information in a text, but this method might be preferred because it has simpler communication and smaller memory occupation. (Sinha.S, Gupta.P, 2016)

B. Image Steganography

This technique is more popular than other steganography methods. Hiding information straight message insertion may encode every bit of information in images, the messages may also be distributed randomly throughout the images. (Singh.N, Bhati.B.S, Raw, 2012)

C. Audio Steganography

Secret messages are embedded in digital sounds, the payload is hidden by slightly altering the binary sequence of a sound file. Audio steganography can be problematic and can be useful for transmitting covert information in an innocuous cover audio signal.

Echo Hiding, Phase Coding, Parity Coding, Spread Spectrum and Tone insertion, are some type of audio steganography technique. (Kaur and Behal, 2014)

D. Video Steganography

In this technique, we can easily hide a large data file into the video file, the video file is generally a collection of images and sounds, Video file is generally a collection of images and sounds.noticeable distortion might go by unobserved by humans because of the continuous flow of information. (Singh.N, Bhati.B.S, Raw, 2012)

The great advantages of video over other media are a large amount of data that can be hidden by utilizing a large number of video frames in a few second video clip, the fact that it is a moving stream of images and sounds (Sinha.S, Gupta.P, 2016)

E. Protocol Steganography

In this technique, steganography can be used in the layer of the OSI network model and cover channels protocols. Steganography refers to the technique of embedding information within messages and network control protocol used in network transmission. The information is added in the TCP / IP header and sent in the network. (Singh.N, Bhati.B.S, Raw, 2012)

2.5 Technique of steganography

1- Spatial domain

Images are represented by pixels where simple watermarks could be embedded by modifying the pixel values or the least significant bit (LSB) values. The raw data is directly loaded into the image pixels. Some of its algorithms are LSB and spread spectrum modulation (SSM) based technique.

Significant bits of the cover object is replaced without modifying the complete cover object. It is a simple method for data hiding. (Olalekan.O, Adenrele.A, 2014)

i) Least Significant Bit (LSB)

Rejani. R, Murugan. D, and Krishan D.V (2015) This is the most common, simple approach for embedding data in a cover image. The least significant bit (8th bit) of one or all the bytes in an image is changed to a bit of the payload. When we use a 24-bit image, three colour bits components are used, red, green, and blue; each byte store 3 bits in every pixel. An 800 × 600-pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data. The LSB is a very simple and useful method, it is also the most used in steganography, it is based on using the least significant bit and replacing the embedded data instead of the original bits directly, usually used from right to left. Hiding capacity can be increased by using up to 4 least significant bits in each pixel which is also quite hard to detect.

ii) Most Significant Bit (MSB)

This method is similar to the LSB method with few modifications; it uses the most significant bits instead of using the least significant bit. (Rajani. R, Murugan. D, and Krishan D.V, 2015)

iii) FZDH (Forbidden Zone Data Hiding)

This technique can be used instead of LSB and watermarking, no changes are available at the time of data hiding process, and no alteration is allowed in a host signal during message embedding step which is useful as authentication tools. (Esen.E and Alatan.A.A, 2011)

2- Frequency Domain:

i) Discrete Cosine Transformation (DCT):

This method converts the uncompressed image into JPEG compressed type, based on data hiding used in the JPEG compression algorithm to transform successive 8x8-pixel blocks of the image from the spatial domain to 64 DCT coefficients each in the frequency domain. The main advantage of this method is its ability to minimize the block like appearance resulting when boundaries between the 8x8 sub-images become visible, known as blocking artefact. (Olalekan.O, Adenrele.A, 2014)

ii) Discrete Wavelet Transformation (DWT):

It gives the best result of image transformation. It splits the signal into a set of basic function. There are two types of wavelet transformation one is continuous and the other is discrete. This is the new idea in the application of wavelets, in this, the information is stored in the wavelet coefficients of an image, instead of changing bits of the actual pixels. It also performs local analysis and multi-resolution analysis. DWT transforms the object in the wavelet domain and then processes the coefficients and performs the inverse wavelet transform to show the original format of the stego object. (Olalekan.O, Adenrele.A, 2014)

2.6 Linguistic Steganography

Olalekan.O, Adenrele.A (2014)The linguistic technique is used to hiding the message within the cover text in a non-obvious way such that the presence of a message is imperceptible to an outsider; it is divided into two types:

A) Semagrams

It only uses symbols and signs to hide information. It is further categorized in two ways:

i) Visual Semagrams

A visual semagram uses physical objects, used every day, to send a message, for example, the positioning of items on a website. (Olalekan.O, Adenrele.A, 2014)

ii) Text Semagrams

This type is used to hiding a message by modifying the appearance of the carrier text, or by changing font size and type, or by adding extra space between words and by using different flourished in letters or handwritten text (Olalekan.O, Adenrele .A, 2014)

B) Open Code:

In this approach, the payload is embedded in legitimate paraphrases in the cover text in the way such that it appears not obvious to an unsuspecting observer. It can be achieved by two ways, as Jargon which is understood only by a group of peoples and Cipher which uses some concealed cyphers to hide a message openly in the carrier medium, or as a subset of Jargon codes which are cue codes, where certain prearranged phrases convey meaning (Olalekan.O, Adenrele .A, 2014)

2.7 Steganalytic tools

There are several Steganalytic tools available at hand like Photo Title, 2 Mosaic and StirMark Benchmark etc. These three steganalytic tools can remove steganographic content out any image. This is achieved by destroying the secret message by two techniques; break apart and resample. StegDetect, StegBreak, StegSpy identify the information embedded via the following tools - Jsteg-shell, JPhide, and Outguess 0.13b, Invisible Secrets, F5, appendix, Camouflage, Hiderman, JPHIde and Seek, Masker, JPegX, Steganography Analyzer Real-Time Scanner is the best available steganalysis software in the market at the moment, which can analyze all the network traffic to look for traces of steganographic communication. (Mandal.P.C, 2012)

2.8 PSNR (Peak signal to noise)

This thesis will rely on the PSNR tool, were the quality of the images is very important, and the best tool to evaluate the images is the human eyes, but this is not enough, there must be a tool using full reference metrics; a distortion that where occurred in the image during transmission, capturing, or compression algorithms (sender, or reviver side).

PSNR is the tool that can check how much the image was being distorted if the image quality increases it results in an increased value of structural similarity (SSIM) and peak signal to noise (PSNR), but the value of mean square error gets reduced (MSE).

The criteria of the relation between (PSNR) and (SSIM) remains the same but the values get changed because of variation in the complexity of the image. The measurement of structural similarity (SSIM) gives better results for the image quality estimation, but it fails on highly blurred images. (Pinki, Mehra.R, 2016)

When the value of the peak signal noise ratio increases the resulting image is very smooth to the eye perception. If the value of the structural similarity index increases, that image approaches to its original image. Highly distorted images give a high value of the mean square error, less the value of peak signal to noise ratio and worst values for the structural similarity index.

The conclusion can be derived from the following graph and table is, PSNR and SSIM are immediately relative to each other, PSNR and MSE are reciprocally relative to each other, Figure 2.1 is showed below is representing the graphical illustration of the image quality.

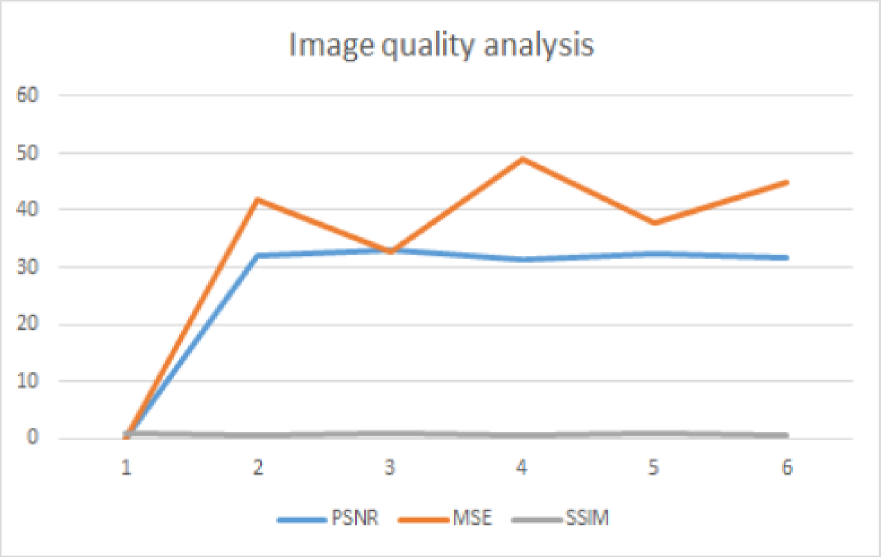


Fig.2.1 Graphical illustration of PSNR, MSE, SSIM. (Pinki, Mehra.R, 2016)

2.9 Related work

1- Saxena.A, Sharma, S. (2017) This paper proposed video steganography, which is similar to this thesis, that the author was utilized video frames to hide confidential data in AVI video file, the aim is to hide the heavy amount of payload into the video files. As shown in the following figure 2.2 and 2.3 video steganography embedding and extraction algorithms with secret key this is called secret key steganography.

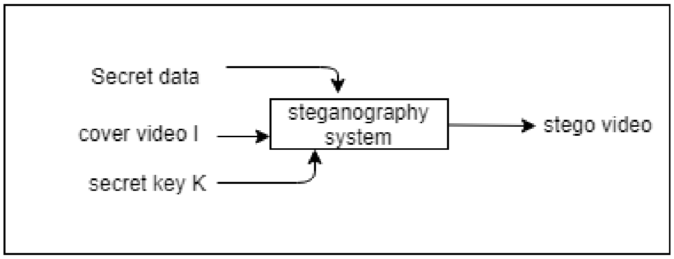


Fig.2.2 General block diagram example of video steganography embedding algorithm which includes a secret key to reach the secret data (Saxena.A, Sharma, S ,2017)

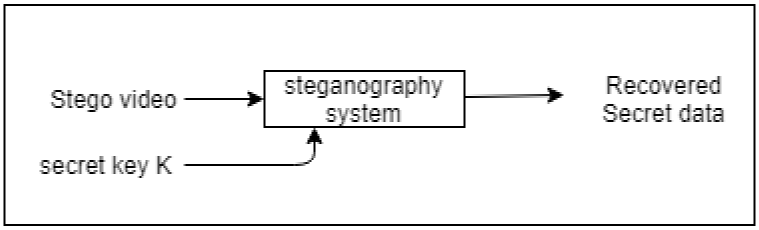


Fig.2.3 General block diagram example of video steganography extraction algorithm, to recover secret data should insert the secret key, (Saxena.A, Sharma, S ,2017)

In this steganography system, the AVI file is applied as the carrier, video files carrying audio frequency are divided into video and audio frames, video frames are in the type of images, hence image steganography is applied with video frames, as audio is separated or took out from a video data file, it is an audio file and audio steganography is applied at audio files, as both audio and video frames applied as the carrier, capability of steganography is raised. The secret information could be image and audio or text. In this system, secret image and audio signals are covered in the video files. the advantage of these techniques is their robustness, it resists processes such as filtering, cropping, rotation, and compression. the secret data is not found by the third party, hence the scheme is secure. In this steganography system, a random frame selection method and pixel swapping method are applied to improve the safety of the system.

2- Kulkarni.A.D, Bansal.E, Rajasjree.B Rasika.R, Madhuri.L.(2015) these authors give a developed data security method, to hold the quality of the cover image and for decrease the size of video before transmission, in this work, two-stage techniques are applied to plant secret text data into a video clip. The first level is image steganography by applying LSB technique, the second level is video steganography applying DCT method, the sizing of the video is modified after embedding technique. So lossless compressing method is applied, the advantages of this technique are increased information security, the visual quality of stego video stays the same and sizing of the final stego video is decreased for fast transmission.

3- Nikam.G , Gupta.A, Kalal.V , Waghmare,P (2017) this paper was suggested to hide secret payloads without affecting the visual quality and the content of the video file cover, polynomial equation were used to hide the secret payload using LSB substitution algorithm, in this embedding system they read the cover video, were the video has been segmented into frames and they compute the histogram value for each frame, after that they embed the hidden data into the frames to get the stego file, then they combine each frame to get the video and send to the other side with whom you want to communicate. In extracting algorithm, first, read the stego video and segment the stego video into frames, then read the recovery parameters of frame1 and determine appropriate frames, extracting or de-embed the hidden or secret data form frame, gaining the secret message and get back the hidden message sent from another receiver side.

4- Pal .S, Bandyopadhyay.S.K. (2016) the authors suggest encrypting and then hide the payload into a video file. In the sending purpose, he used the LSB method the researcher pointed out the advantages of LSB coding that LSB allows a huge volume of data given in audio or text format to be encoded and data are found in the other side (receiving) in a loss-less way, the quality of the proposed method was tested in the measured with respect to two parameters (MSE and PSNR) .

The experimental result illustrates that the stego signal generated by the proposed method are perceptually indistinguishable from the original cover file. The author here prefers to hide data in a video rather than the constant image, because of the huge size of the video which it had a higher capacity than a constant image, and also more data can be concealed into the video.

5- Throughout my study, I relied also on papers for batching technique which started as a Competition and lasted more than ten years between the warden and the stenographer at Oxford University.

Ker.A (2006) in this paper they motivated and defined the problems of batch steganography and pooled Steganalysis, giving a menu of techniques for the latter and examining the implications for the former, the pooled Steganalysis methods have been benchmarked for a particular type of steganography, with results in line with the theoretical predictions. The conclusion, that in many cases the Stenographer should cluster the embedding data in a small number of cover objects, seems rather counterintuitive. In future work, the researcher pointed out that he wants to consider letting the Steganographer to vary the amount of data embedded in each object (this results in a larger combination), and to deal with objects of varying capacity. More information on the individual Steganalysis response, as it depends on object size and other object parameters, will be needed here. Finally, they would like to prove a general result of how steganographic capacity upsurges, given the expectations they made in this paper, including all covers being the same size.

6- Ker.A (2007-a) This paper supposes that the Steganographer has to choose a spread fixed number of data between a large number of covers. Assuming the existence of Steganalysis methods for each object, and the observer's effort to reveal the payload by pooling the indication from all the objects, but that requests a correct pooling methodology, and it depends heavily on Steganographer that how will choose the correct way to distribute the payload in the objects. This paper achieves the details of specific methods for observers that can count the number of objects of which the detection statistic surpasses a certain threshold. These attempts of the pooling method lead to a challenging game between the observer (Warden) and Steganographer. The key to this dilemma is exciting, suggesting that steganographer should focus on putting the payloads in a few covers as possible, or on the contrary, but don't use the intermediate strategy at all.

7- Ker et al., (2015) Here, the pooled steganalysis problem exposes an essentially game-theoretic condition. When a (batch) steganographer hides all their payload in one object, a certain type of detector is optimal; but when they spread their payload in many objects, a different detector is optimal. These statements can be proved in artificial models and observed in practice. Indeed, the same can be said of single images; if the embedded always hides in noisy areas, the detector can focus its attention there, and vice versa. Game theory offers an interesting perspective from which to study steganography. If both steganographer and steganalyst know the cover source and are computationally unconstrained, the steganographer can embed perfectly; with a shorter key. If the steganographer is computationally bounded, but not the steganalyst, the best they can do, subject to their constraints is to minimize the KL divergence. Another way to frame this is to play a minimax strategy against the best possible detector. This may not add a lot of insight into the lab. But once we step out into the real world, where knowledge of the cover source is incomplete and computational constraints defy finding globally optimal distortion functions or detectors, then the game theory becomes very useful. It offers a wealth of solution concepts for situations where no maximin or minimax strategies exist. A popular one is the notion of a Nash equilibrium. It essentially says that among two sets of strategies, one for the steganographer (choice of embedding operation, distortion function, parameters, etc.) and another for the steganalyst (feature space, detector, parameters such as local weights, etc.), there exist combinations where no player can improve his or her outcome unilaterally. Although exploitation of game theory for steganography has just begun, and we are aware of only four independent approaches, it seems to be a promising framework which allows us to justify certain design choices; such as payload distribution in batch steganography or distortion functions in adaptive steganography.

8- Sajedi.H, Jamzad.M (2009) In this paper the researcher mentioned that in batch steganography, the steganographer embeds secret data in multiple cover images. Previous works in batch steganography are theoretical and consider some unreal assumptions for simplicity. Accordingly, in this paper, Adaptive Batch Steganography ABS, a new approach for practical multiple-cover steganography is proposed by defining and using the embedding capacity of an image. Using ABS, we determined the upper bound of secure embedding rate in every image by defining embedding capacity in the presence of multiple steganalyzers as a property of an image regarding the constraints of the used steganography method. Previous works in defining embedding capacity have considered it as a property of a steganography method. However, such definitions for embedding capacity cannot guarantee the security of embedding in a certain image because images with similar properties in embedding capacity analysis viewpoint may have unequal thresholds for secure embedding due to their different contents. We showed that, in ABS, the embedding capacity of an image set is the sum of embedding capacity of each image in the set. ABS is an SBS method because it cares to prevent embedding data in a cover image more than its embedding capacity. In addition, ABS attempt to embed a large payload efficiently in the least number of cover images. We hope that batch steganography in its full content brings solutions to the current dead ends to image steganography such as limitations in embedding capacity. In future, they are going to offer suitable image sets to hide large payload.

9- Ker. A. (2007-b) This paper proves that the covers of uniform size and quantitative steganalysis methods satisfying certain assumption "secure" steganographic capacity are proportional only to the sequence root of the number of covers.

Steganalysis aims to detect the original file from the stego file, it's clear that the larger payloads are easier to detect. Determining the maximum payload for which risk of detection is acceptable is a fundamental problem in steganography and steganalysis. our ability grows quickly to distinguish covers from uncovered with the distortion of the object.

The theorem we have presented here is of theoretical importance-it is the first to show explicitly how capacity is influenced by the number the covers. The second is pooled steganalysis, it is too difficult because it cannot really be assumed that the Warden knows the values of p1….pn, but only how the performance of a pooling strategy can mainly rely on the embedding strategy.

10- Ker. A and Pevný.T .(2012) in this paper they are focusing on the embedding of payload in a single cover or detecting of payload in one object belonging to one user. The main objective here is what the best way is to spread the payload between multiple covers and pooled steganalysis. However, they examine the universal pooled steganalyzer in two respects; the first one, they confirm that the method is applicable to a different number of steganographic embedding methods. The second one, throughout testing different payloads allocation technique against the universal steganalyzer, takes into account the reverse process of how to distribute the payload in different covers. Here they focus on the practical solution which can be implemented without a new program (software) or any prior knowledge, and they test on real-world data. Distribution of payloads in a small number of covers is the less is exposed to dangers. In this paper, they present additional investigation which explains this phenomenon and clarify the nonlinear relationship between embedding distortion and payload. Taking into consideration, consequence blind steganalysis, this is a worthy issue for both batch steganography and pooled steganalysis. The valuable lesson of the whole study is that a greedy embedding strategy, which focusses payloads in a few covers of the largest possible capacity, is able to be exploited by a property of the detector.

Table 2.1, Table 2.2 below shows summarizes of the brief description of related work in video steganography, batching technique and some technical approach were used in the video steganography in general.

Table 2.1 Related work in video steganography

Author & year	**Paper title**	**Technique used**
Sapate.P, Patil.V, Pardeshi. M and Michael.A (2016)	A Review Paper on Video Steganography	The paper presents various techniques of video steganography, is used for hiding the secret information (text, image, and video) in video file using LSB algorithm, where random frame selection algorithm and pixel swapping algorithm is used to improve the security of this method.
Choudry. K.N and Wanjari.A . (2015)	A Survey Paper on Video Steganography	This paper presents a review work in different steganography methods, Weighting the video and images steganography, in this method least significant bit of the frames of host video is used to carry the secret information
Wajgade. V.M and Kumar.S. (2013)	Enhancing Data Security Using Video Steganography	In this paper they presented several ways of hiding the secret data inside the cover medium such as image, audio and video by LSB algorithm, they use (AES) Advance encryption standard and SHA-1 for generating a secret hash function or key.
Chandel.B , Jain.S. (2016)	Gurmukhi Text Hiding using Steganography in Video	Effective selection of the AVI video as cover media, LSB algorithm were used to identify embedding secret message with minimum imperceptibility, high embedding capacity, high embedding efficiency with optimum data hiding locations, low computational cost of data retrieval and data embedding rate, high security, different video files extension, different types of secret message like video inside video, image inside video, audio inside video and so on.

Ramalingam, M and Isa, N.A. (2015)	A Steganography Approach over Video Images to Improve Security	The experimental results proved the quality of the video images is maintained well by the Least Significant Bit substitution technique. From the results, it is concluded that the proposed method allows embedding of the payload of different length in the cover-video images without varying the size of the original video images. The hidden payload is extracted without any errors.
Goyal.H, Bansal.P (2015)	An Analytical Study on Video Steganography Techniques	The algorithms are based on various formats such as Joint Photographic Expert (JPEG), Bit Map format (BMP), Graphics Interchange Format (GIF), Audio Video Interleave (AVI). Video Steganography is a vital and rapidly growing research area. It is a form of security through ambiguities and puzzles. Also, the authors refer that 4 LSB method embedding capacity is 4 times as that to 1 LSB method.
Chitra.S, Thoti.N , (2013)	Implementation of Video Steganography Using Hash Function in LSB Technique	This paper is suggesting the AVI video file to conceal secret data regardless of its type; however, it can work with any type of video format. the Performance analysis of the proposed technique after comparison with the LSB technique is quite encouraging
Al salihi.I , Kahyan. S.K, (2017)	A comparative study of LSB based Video Steganography technique	This paper was compared between two hiding technique The first method, improved LSB image steganography technique uses Bit-Inverse in 24 Bit colour image, and the second LSB image steganography approach uses RGB colours components, they improve payload capacity of image steganography and provide more security to the stego video through using the RGB pixel component weighted to hide a particular text message in a video, secured hiding with a minimum mean square error and a result gives maximum PSNR. Also, this will increase the payload capacity with minimal distortions in the host video.

Table2.2 Related work in batch technique approach in video steganography

Author & year	**Paper title**	**Technique used**
Ker.A (2006)	Batch Steganography and Pooled Steganalysis	In this paper the author suggests that the steganographer should spread the embedding in a small number of cover objects, they used the LSB replacement algorithm. The Experiments have been conducted on numerous steganalysis, and frequent attacks show that pooled steganalysis can give very reliable detection of even small proportionate payloads.
Ker.A (2007-a)	Batch Steganography and the Threshold Game	This research is like a game between the Warden and Steganographer. The conclusion that the author suggests the Steganographer that should always focus the payload in a few covers as possible, or the opposite completely, but never accepts an intermediate strategy. LSB replacement technique was used here.
Ker.A (2007-b)	A Capacity Result for Batch Steganography	In this paper, the author proves that, with respect to a natural definition of secure capacity, it is clear that larger payloads are more easily detectable. Determining the maximum payload for which risk of detection is acceptable is a fundamental problem in steganography and steganalysis
Ker.A , Pevný.T (2012)	Batch Steganography in the Real World	The steady experience of this paper can summarize that a greedy embedding approach, which focusses payloads in as rare covers of largest possible capacity, is able to exploit a property of the Wardens. The property is owing to a nonlinear relationship between (unavoidably normalized) features and payload size, which is an important insight for both embedders and wardens. DCT algorithm has been implemented in this paper

Chapter Three

Methodology and the proposed method

3.1 Introduction

In this chapter will discuss the methodology of the BVS system, what the steps to hide the secret payload is and how to extract the secret payload from the video batches. The methodology adopted in this thesis is based on experimental work for embedding a secret payload within video batches using the 2-LSB algorithm. The proposed model is implemented by C# programming language. Implementation of the BVS system into two modules: Embedding process which deals with storing the secret Payload in a multi video cover, and extraction process deals with extracting the secret Message as well as checking the integrity of the extracted secret message compared to the original secret message.

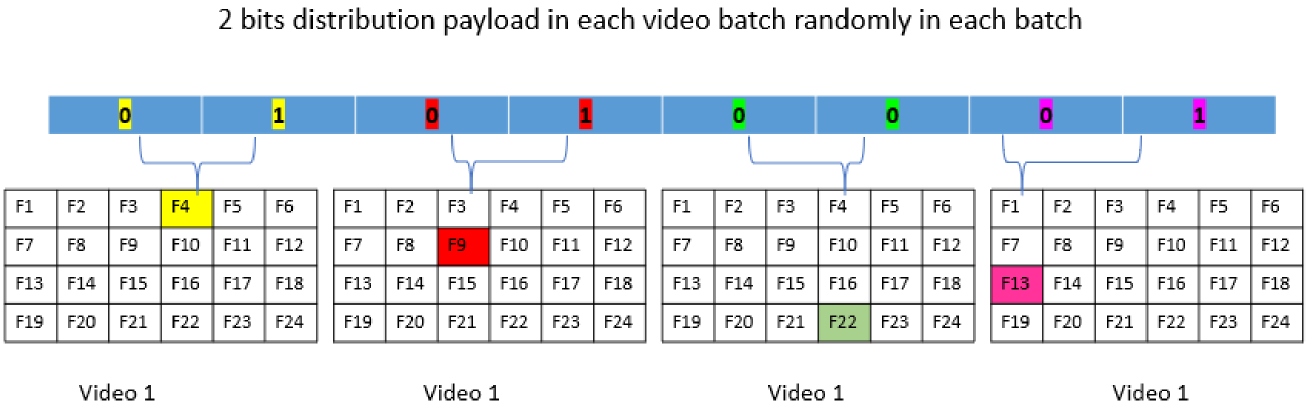
3.2 Methodology Approach

The research methodology approach of this proposal is experimental, where a technical solution for the research problem will be designed and experimental evaluation will be performed. The research contributes to finding solutions for how to send data in a confidential manner without perceptive of observers. The method of batch steganography will be extended to deal with the embedding of any type of data in AVI format video files.

3.3 Design of the proposed method

To achieve the required objectives of embedding secret data in the video file, the BVS system will split the hidden data into multiple video files, using the 2LSB algorithm. It will not be possible for the observer to extract the hidden data if its existence is detected, each byte of the secret data is split into pairs of bits and each pair is hidden in different covers, into two, four or eight covers, depending on the required embedding ratio. Frames and pixels from each RGB channels are selected to improve the safety of the BVS system, in which no pattern can lead the Warden to sequence or trace to detect.

A sample result of batch video steganography system using byte distribution technique, this vertical slice technique slice the byte into pairs of bits as shown in figure 3.1.


2 bits distribution payload in each video batch randomly in each batch
0
1
0
1
0
0
0
1
Video 1
Video 1
Video 1
Video 1

F1	F2	F3	F4	F5	F6
F7	F8	F9	F10	F11	F12
F13	F14	F15	F16	F17	F18
F19	F20	F21	F22	F23	F24

F1	F2	F3	F4	F5	F6
F7	F8	F9	F10	F11	F12
F13	F14	F15	F16	F17	F18
F19	F20	F21	F22	F23	F24

F1	F2	F3	F4	F5	F6
F7	F8	F9	F10	F11	F12
F13	F14	F15	F16	F17	F18
F19	F20	F21	F22	F23	F24

F1	F2	F3	F4	F5	F6
F7	F8	F9	F10	F11	F12
F13	F14	F15	F16	F17	F18
F19	F20	F21	F22	F23	F24

Fig 3.1 Sample result of video Steganography distributing byte

3.4 Implementation of the proposed system

The BVS system presents video steganography for data embedding and extracting embedded data, in video files using the 2-LSB replacement technique. The following section illustrates this process in detail and figures 3.2 and 3.3 will explain the process in the flowchart diagram.

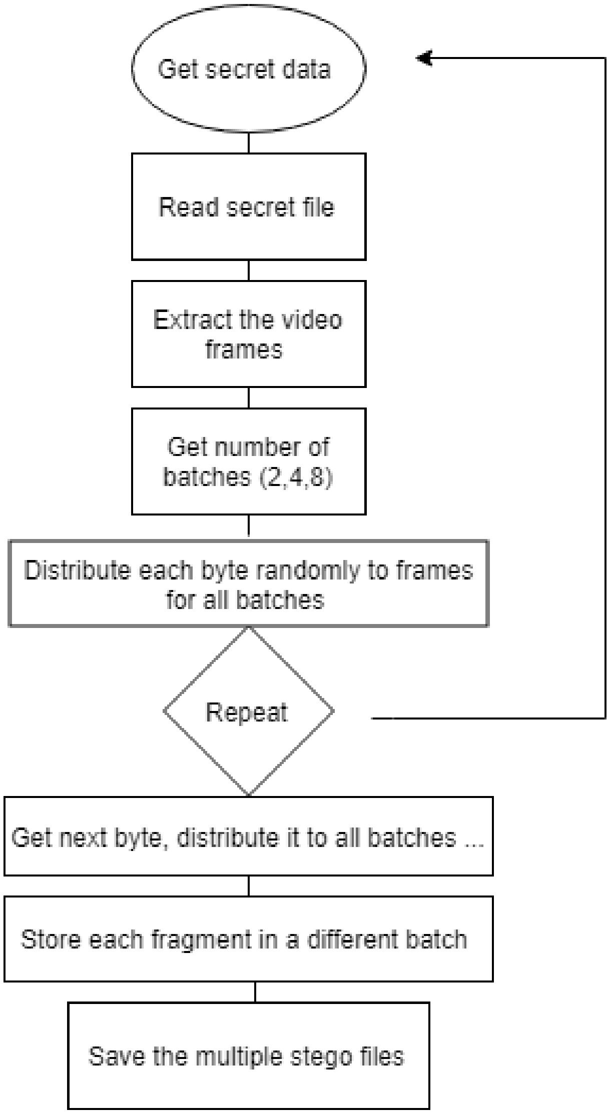
The proposed module for hiding a secret message in an input AVI video file is implemented as follow:

- ✓ Get the input secret data.
- ✓ Read secret data file and calculate size.
- ✓ Extract the video file (Original file) into frames. Decomposition of input video into red, green and blue colour component frames.
- ✓ Get the number of batches required to cover the secret data 2,4 or 8 covers, depend on the payload size.
- ✓ Conversion of the secret message into binary form, then distribute each byte to frames for all batches, repeat until all the secret data is distributed and embedded into the batches.
- ✓ Store each frame in a different batch.
- ✓ Save the multiple stego videos copies.

To get the secret data payload from output batch video, implemented as follow steps:

- ✓ Extract each segment of bits into byte from the multiple video files.
- ✓ Combine all distributed byte together
- ✓ Output the extracted secret file from all video batches and combine them in one file
- ✓ The extracted file should be identical to the original secret file.

The steps in the flowcharts below to understand the embedding and extraction process As shown in figure 3.2 and 3.3.


Get secret data
Read secret file
Extract the video frames
Get number of batches (2,4,8)
Distribute each byte randomly to frames for all batches
Repeat
Get next byte, distribute it to all batches ...
Store each fragment in a different batch
Save the multiple stego files

3.2 Embedding process .

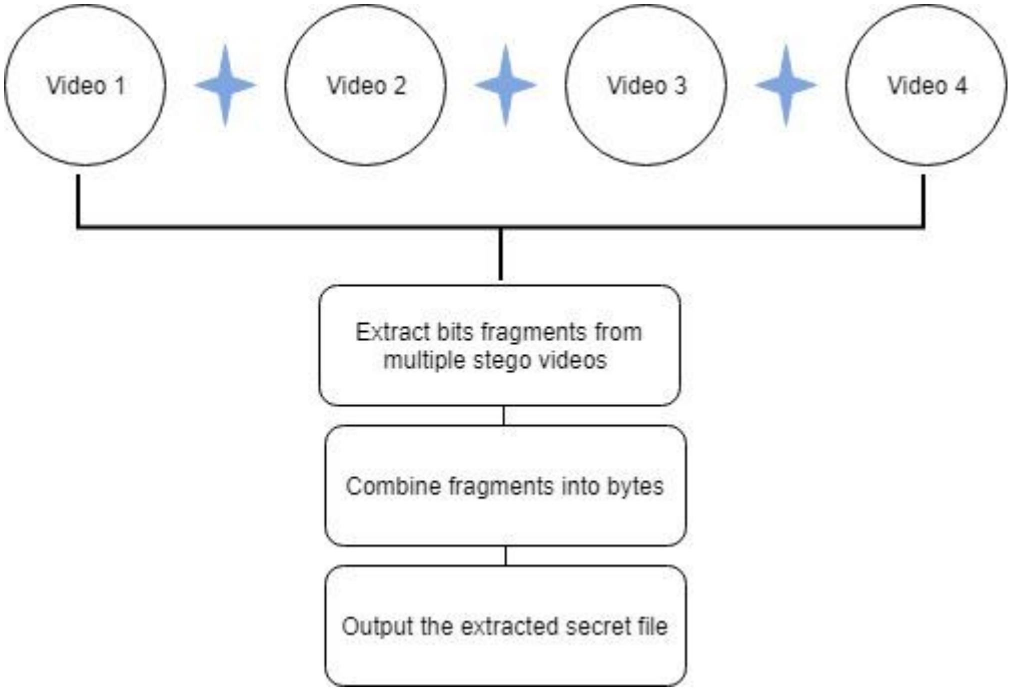

Video 1
Video 2
Video 3
Video 4
Extract bits fragments from multiple stego videos
Combine fragments into bytes
Output the extracted secret file

Fig 3.3 Extracting module

3.5 The results expected of the proposed system

As compared to all previous related studies in steganography, taking advantages, avoiding disadvantages and develop special touches on them, the proposed BVS system is considered with powerful, embedding capacity achieved higher than expected without loud distortion in video quality, and high-security level with lower imperceptibility aspects., this shows that the BVS system is not disposed to be attacked by hackers and observers. The system is very steady and platform independent, the approach proposed in the implementation attained the same output file size as the file input, this means that file size does not increase in size after embedding.

Chapter Four
Experimental result and discussion

4.1 Introduction

This chapter presents the batch video steganography system (BVS) implementation and the experimental work and result. The system embeds bytes of the secret data into bytes of frames of the cover videos, which is two covers in our experiment but can be more. Each byte of the secret data is split into pairs of bits and each pair is hidden in different covers, i.e. the secret data bytes are split over two covers so that is it not possible to extract useful information if the secret data is extracted by a warden. The proposed system is implemented in C# programming language, with the possibility of experimenting on another language like MATLAB or PYTHON. The experimental work included embedding various media data types (Text, Image, Video) within the RGB channels of each cover. To extract the embedded payload from the batch of covers, that were used in the embedding system, the payload bytes are formed by merging four pairs of bits into bytes, where the bit pairs are extracted from the bytes of the two covers interchangeably. The extracted bytes are stored in the recovered payload file. Evaluation of the imperceptibility is done using the PSNR metric.

4.2 Objectives of the experimental work

The experimental work aims to provide a way to hide data in a safe way using the proposed model.

Selecting the media which will cover the secret data (AVI video), then select the secret data payload (text, image, video file), the experimental work can be applied in the future to different file types, after that split the payload of the secret data into the video batch, the choice of the number of the covers can be two or more depending on the payload size, hiding capacity of the cover media and security requirements (more covers per batch increases security but less convenient for the user).

Distribute each byte of the secret data in different frames in the batch of videos, then check the stego-files distortion using PSNR metric, making sure that each of the stego files have the same size in bytes as the original cover, finally extract the secret data from the two stego files and check that the extracted file is identical to the original secret file.

4.3 The Experimental dataset

A- Cover medium (video)

The AVI video file type which is uncompressed and this type is chosen because it provides higher hiding capacity compared with compressed video files such as MPEG or MP4. We need to utilize all the data bits in frames of the video file. The main objective of choosing the video as a cover medium is shortened in this question: how to hide big secret data without compromising imperceptibility? It is a difficult task to hide a big amount of data without raising suspicion of alert observers, the video can accommodate the inclusion of a large amount of data without realization by the Human Visual System. Moreover, the fast movement of frames helps to smooth and conceal the distortion that is introduced by the data embedding. Information of any type and format can be hidden in the frames forest of a video file. Table 4.1 show examples of the size in bytes of a few seconds AVI video files before and after embedding.

Table 4.1 Result evaluation between the original video file and the stego-file without any difference in file size.

Video file (original cover)	Resolution (W*H)	Original Video size	Number of frames	Stego Video Size	Length
Test1.avi	320*240 19.9 MB	19.9 MB	75 frames	19.9 MB	3/ second
Test2.avi	320*240 25.7 MB	25.7 MB	100 frames	25.7 MB	4/seconds
Test5.avi	320*240 22.4 MB	22.4 MB	100 frames	22.4 MB	4/seconds

B- Secret data

The experimental work was tested on three different file formats: text, image and video. After embedding the secret data in the video batches the receiver should run the extraction program to get the frames that hold the secret data and extract the secret message. Figure 4.1 and 4.2 show the result after embedding a text file in a video.

Fig 4.1 stego-file (cover1)

Fig 4.2 stego-file (cover 2)

4.4 Sending process

In the sending process the sender will input the video file and the secret data, then extraction the video frames from the cover video, after that embedding the secret data in the two covers by distributing each byte into pairs of bits in each cover will distribute 2bits interchangeably to the frames in video cover until all data were embedded, save the two covers and the output will be a two stego video, as shown in the block diagram in figure 4.3

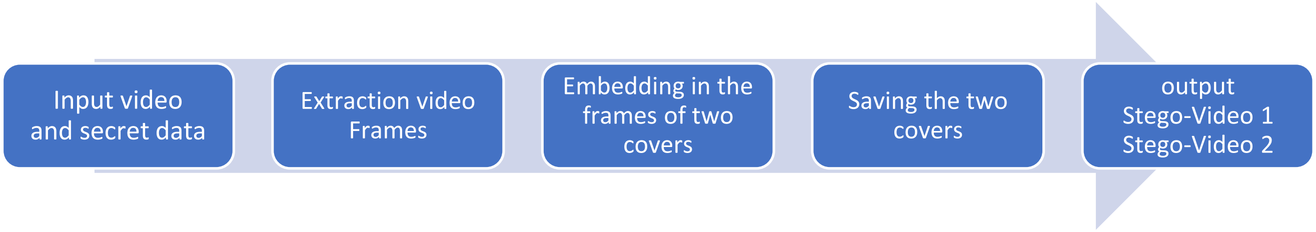

Input video and secret data
Extraction video Frames
Embedding in the frames of two covers
Saving the two covers
output Stego-Video 1 Stego-Video 2

Figure 4.3 Block Diagram of Transmitting Systems.

4.5 Receiving process

The receiving process is the opposite of the sending process which the receiver will input the two stego files, then combine the secret data from video frames from the two batches and save the extracted files which are identical to the original secret data, the block diagram in figure 4.4 below shows the steps of the extraction method.

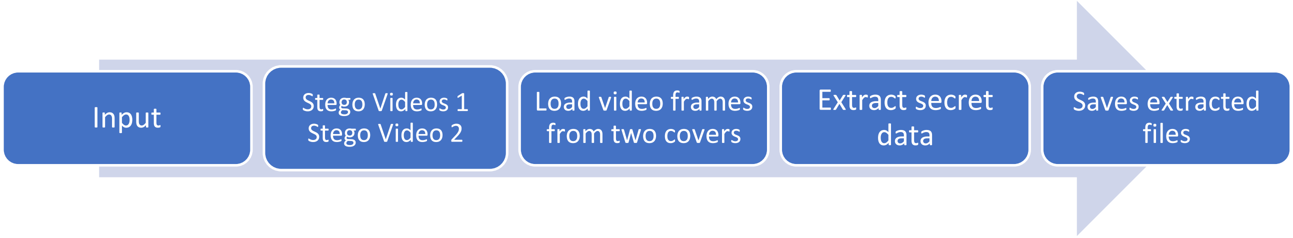
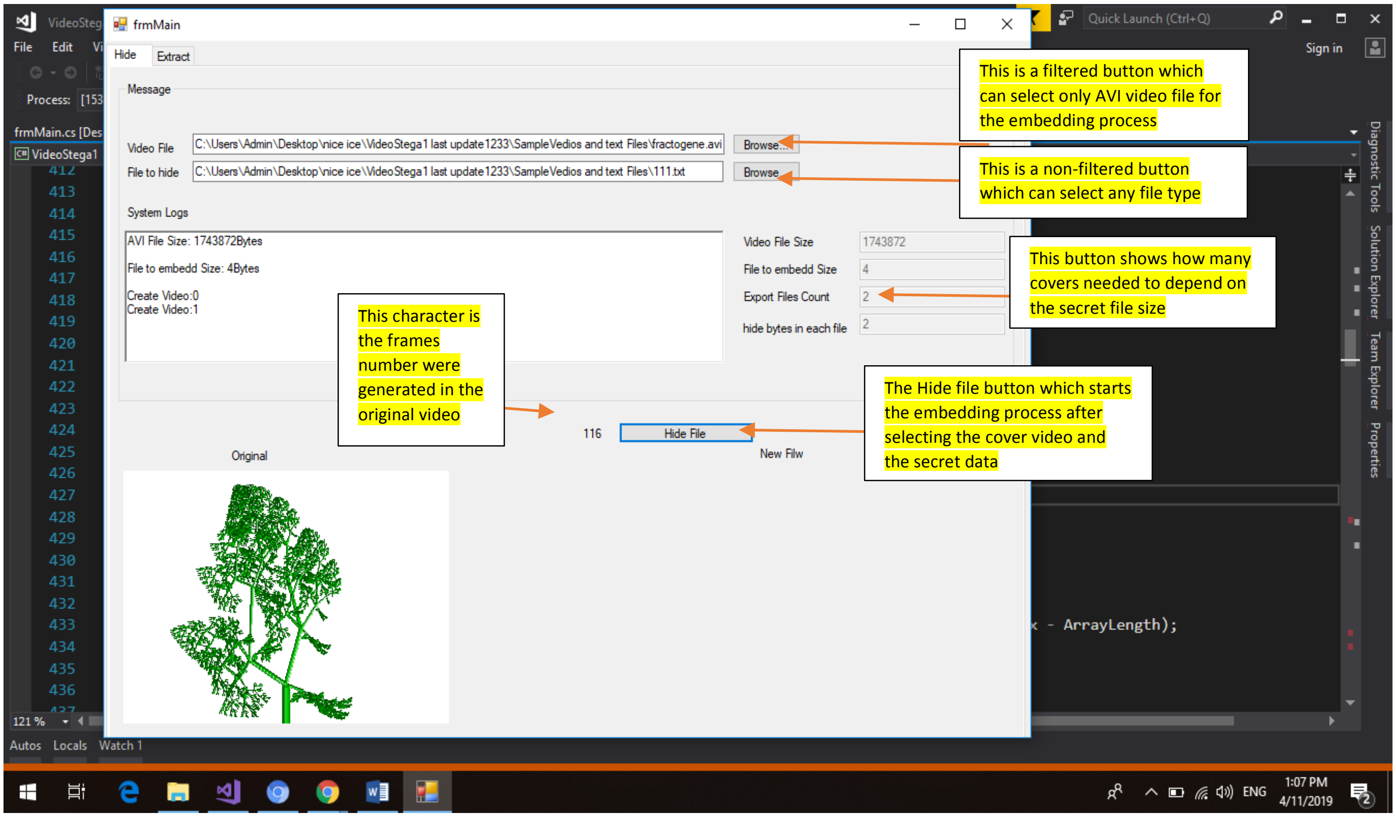


Figure 4.4 Bloch diagram shows the extracting method

4.6 Batch embedding

In this module the AVI video file was embedded with another file type, the spatial domain 2-LSB replacement technique in each byte was used. According to the secret data payload, the secret data will split in a multi video covers, and spread 2 bit per byte from the secret data in a multi covers, which means that even if the Warden guess existing of secret data in a the stego-video it will be difficult to guess the confusing distribution technique which segmented in a hundred frames, and without any pattern can connect him with an obvious trace. The peak signal noise ratio (PSNR), which is an average metrics to compare imperceptibility of the stego-video to the original video, is also considered, where the precision is the original data, and the clatter is different while embedding the secret data, figure 4.5 shows embedding module interface demo of hiding process with a text file, the text file was distributed in two covers depending on its size.



Video File: C:\Users\Admin\Desktop\nice ice\VideoStega1 last update1233\SampleVedios and text Files\fractogene.avi

File to hide: C:\Users\Admin\Desktop\nice ice\VideoStega1 last update1233\SampleVedios and text Files\111.txt

```
AVI File Size: 1743872Bytes

File to embedd Size: 4Bytes

Create Video:0
Create Video:1
```

Video File Size: 1743872

File to embedd Size: 4

Export Files Count: 2

hide bytes in each file: 2

116

This is a filtered button which can select only AVI video file for the embedding process

This is a non-filtered button which can select any file type

This button shows how many covers needed to depend on the secret file size

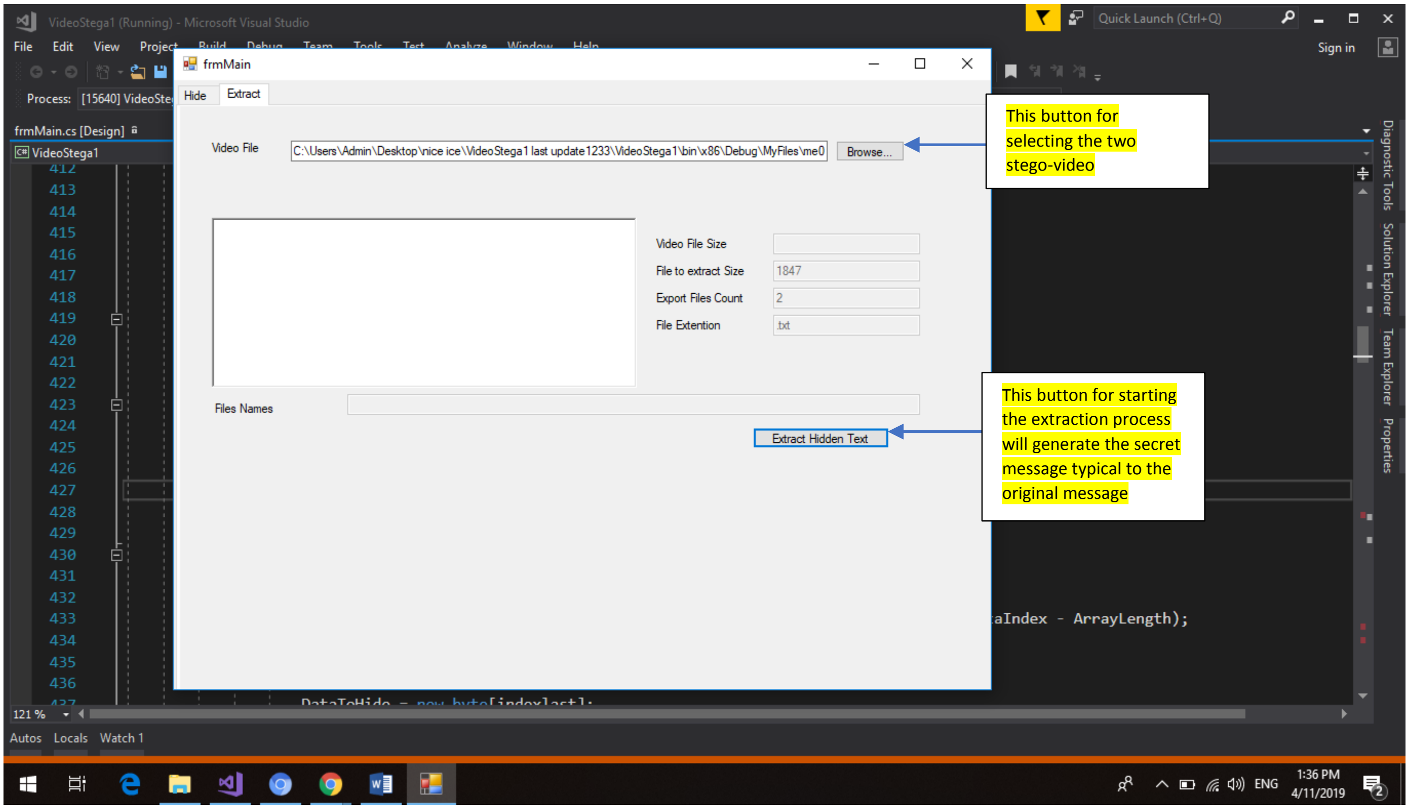
This character is the frames number were generated in the original video

The Hide file button which starts the embedding process after selecting the cover video and the secret data

Fig .4.5 Embedding module

4.7 Extraction module

The experimental work was implemented and tested in reverse technique and the result is the two stego video was extracted to generate the secret text message as shown in figure 4.6 extraction module interface demo.



Video File: C:\Users\Admin\Desktop\nice ice\VideoStega1 last update1233\VideoStega1\bin\x86\Debug\MyFiles\me0

Video File Size:

File to extract Size: 1847

Export Files Count: 2

File Extention: .txt

This button for selecting the two stego-video

This button for starting the extraction process will generate the secret message typical to the original message

Fig 4.6. Extraction module interfaces demo.

4.8 Least significant bit technique

The LSB replacement technique is one of the spatial domain methods and it is a simple algorithm. The changes in value in the LSB technique is imperceptible as LSB is the lowest bit in a sequence of binary numbers. The LSB based steganography is one of the steganographic methods which is used to embed the secret data into the least significant bits of the pixel values in a cover image. e.g. 211 can be hidden in the first eight bytes of three pixels in a 24-bit image. Pixels:

(00100110 11100001 11101000) (01100111 11001010 11101101) (11011001 10100111 11101000)

211: 11010011 result:

(0010011**1** 11100001 11101000) (01100111 11001010 1110110**0**) (11011001 10100111 11101000)

Here number 211 is embedded into first eight bytes of the grid and only 2 bits are changed. Well, it's on in the two significant bits. The Advantages of spatial domain LSB technique; the first there is a fewer chance for degradation of the original image, the second is hiding capacity is huge i.e. more data can be stored in an image.

4.9 Data Layout of the Secret File

The secret multimedia file which will be embedded in the video cover is processed as a stream of bytes, where each byte pixel is split into four two-bit fragments (bit pairs), and each fragment will be stored in 2-LSB bits of bytes of the cover image, the useless bits from the original byte were replaced by the secret byte . As shown in figure 4.7

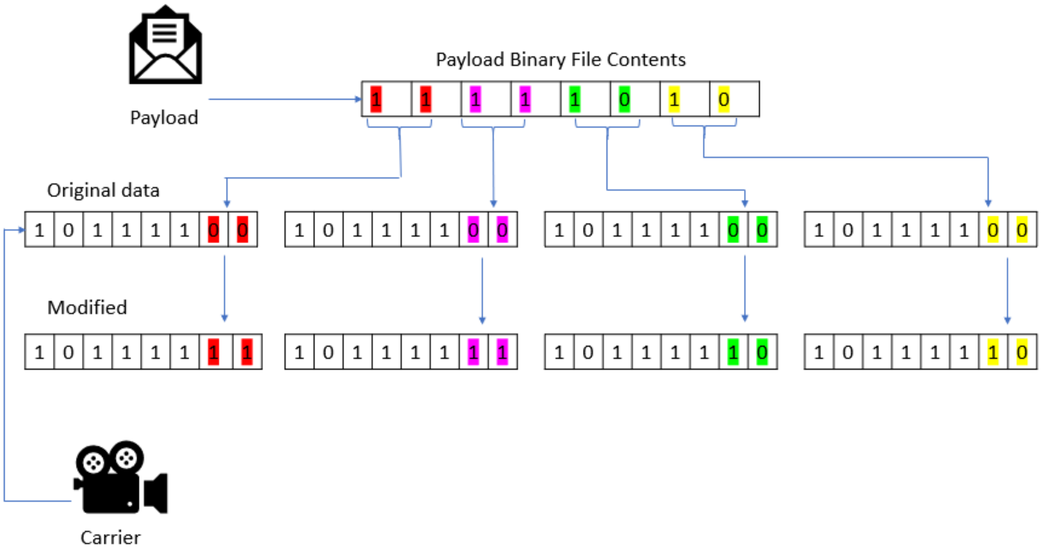


Figure 4.7 The 2-LSB replacement algorithm were used in the embedding process

4.10 Experimental calculations

Calculating the required hiding capacity of each video cover, for storing a specific secret data file size in two covers, by embedding 2bits per colour channel of each frame, we follow steps below:

- Determine secret data size in bytes: S
- Required cover hiding capacity = S / 2
- Actual cover hiding capacity CHC = W x H x C x F / 4
- Where W = frame width
- H = frame height
- C = number of colour channels that are used for embedding, which is 3 in this work
- F = number of frames in the video = Time in seconds x Frame per Second the divisor 4 is used because each byte of the secret byte requires 4 bytes of cover. Therefore, the actual hiding capacity per cover should be equal to or greater than the required hiding.

Example:

Given a cover with the following measure:

- Time = 20 seconds
- FPS = 20 x 25 = 500 frame
- Width = 480, Height = 270 pixels
- CHC = 320 x 240 x 3 x 500 / 4 = 28,800,000 bytes = 28.125 MB.

Therefore, the two covers can store a secret file of 56 MB. An area of 100 bytes of the first frame needs to be reserved for header information which includes secret file name, secret file name size and secret file size in bytes.

4.11 Error Analysis Measures

MSE the Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two-error metrics used to comparing image distortion quality. The MSE represents the cumulative squared error between the stego image and the original image, whereas PSNR represents a measure of the peak error. whenever is lower value of MSE, there is the lower error.

PSNR is an image quality model that refers to the level of accuracy in which different imaging systems capture, process, store, compress, transmit and display the signals that form an image. This model output is calculated for every frame of a video sequence, and this quality measure of every frame of an entire video sequence. To compute the PSNR, the block first calculates the mean-squared error using the equation below, “m” and “n” are the number of rows and columns in the input images, respectively. Then the block computes the PSNR using the following equation, MAX is the maximum value of the pixel in the original image. For example, if the input image has a double-precision floating point data type, then MAX is 1. If it has an 8-bit unsigned integer data type, MAX is 255, etc.

$$PSNR = 10log_{10}\,(\frac{MAX_1^2}{MSE})\ \ldots\ldots\ (1)$$

PSNR is used to scale the MSE according to the image range. We have used the Peak Signal-to-Noise Ratio (PSNR) to measure the quality of the stego images in the frames. The value of PSNR gives better result because our proposed method changes a very small number of bits of the image. The PSNR block computes the peak signal-to-noise ratio, in decibels, between two images. This ratio is often used as a quality measurement between the original and a compressed image.

Whenever the PSNR is higher, the quality of the compressed or reconstructed image is better. (Chitra.S, Thoti.N , 2013)

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^{2} \ldots\ldots (2)$$

4.12 The PSNR results in average

The researcher takes about the average of the PSNR to check the video quality distortion measurement in video embedding process as shown in table 4.2, figure 4.8 and figure4.9.

Table 4.2 PNSR results

Name of video	Resolution (W*H)	Number of frames	PSNR AVG before embedding	Secret payload name	Secret message size	PSNR AVG after embedding
Test 5	320*240 (23,505,408 bytes)	100	54.76 db	Cookie.avi	320*240 5,347,840 bytes	49.17 db

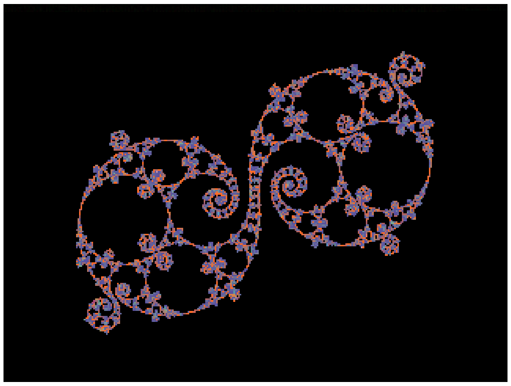


Fig 4.8 Clean frame PSNR=52.42 db

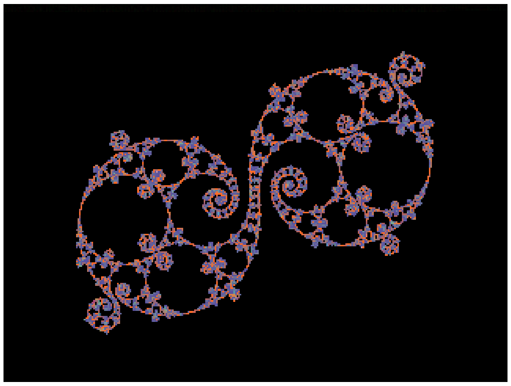


Fig.4.9 Stego-frame PSNR=46.65 db

4.13 Video Quality Evaluation

The PSNR (Peak Signal to Noise Ratio) is the standard metric for evaluating the quality of images in steganography. In this work, we take the average of the PSNR values of the individual frames that were used for embedding as the PSNR value of the video file. Embedding in 2 bits per colour channel resulted in of about 50 in PSNR values. To have higher PSNR we can embed in 1 LSB.

4.14 Retrieving secret data

The retrieved data from the extraction BVS system must be identical to the original confidential data as determined in figure 4.10 and 4.11.

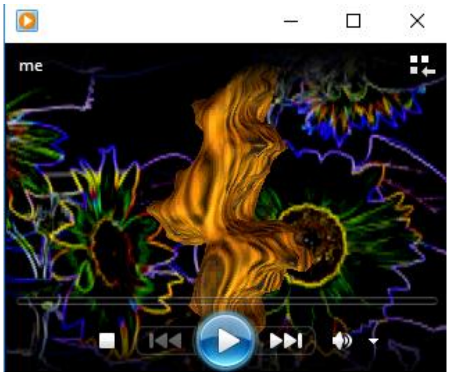


Fig. 4.10 Secret video

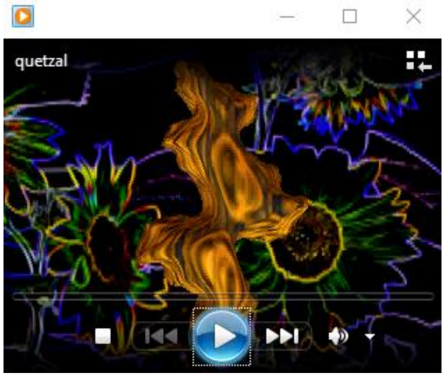
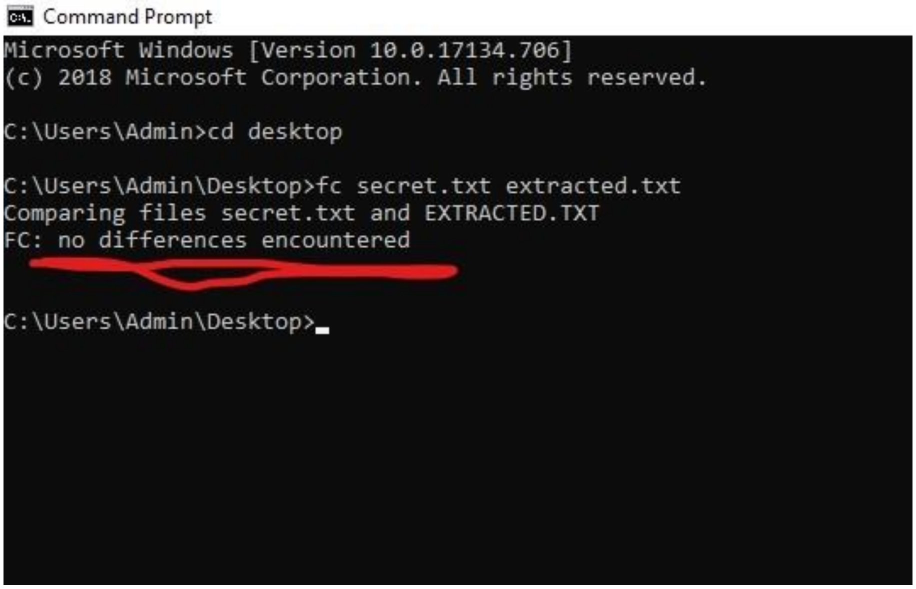


Fig. 4.11 Retrieved video

4.14 Results and discussion

This section presents our indicated target of batch video steganography using the 2-LSB technique which can conceal a huge amount of data in a small video file, the original file and the stego file have the same size and duration which achieve the security and integrity of the file by distributing the secret file in a multi video covers. Also, the extracted file is tested and compared with the original secret data using the CMD, considering there is no difference between them, as shown in figure 4.12 below



```
Microsoft Windows [Version 10.0.17134.706]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Admin>cd desktop

C:\Users\Admin\Desktop>fc secret.txt extracted.txt
Comparing files secret.txt and EXTRACTED.TXT
FC: no differences encountered

C:\Users\Admin\Desktop>
```

Figure 4.12 shows file compare using CMD, it is no difference between the secret.txt and the extracted.txt file

In this embedding system, the embedding process with no difference between the original video file is ensured, and without any difference between the original secret message and the extracted message after the extracting process. Which is the result indicating our target, insecurity and integrity, and is what we are looking for.

Chapter Five
Conclusion and future work

5.1 Conclusion

This thesis presented a steganography model combined with the batch technique to hide secret data within multiple video covers which provides a highly secure method for data hiding and communication. In this thesis, we have presented a new system combining video steganography with the batch technique.

The proposed BVS system provides high capacity, security and high imperceptibility aspects. Using the batch technique prevents the observer from capturing the secret data if he manages to get one of the stego files and extract the embedded bits. The proposed batch technique is more secure than other techniques that store contiguous bytes of the payload data into segments where each segment is stored in one cover of the batch. In the proposed technique, the payload file is sliced vertically into 2-bit slices, and each slice is stored in a separate stego file, thereby scattering the payload data as bit pairs in different stego files. The proposed BVS system is tested by taking payloads from various media formats and hiding them in images/frames of the cover video, the stego files output in size and duration were identical to the original video. The steganography algorithm that was used is the spatial domain 2-LSB method, which provides higher hiding capacity than transform domain, and is considered to provide visual imperceptibility. It is possible to increase hiding capacity by increasing the number of LSB bits to 4, or to lower it to 1-LSB or less to enhance imperceptibility. It is also possible to use other embedding techniques in combination with the batch technique.

The LSB embedding is done in the three RGB channels, so replacing 2 bits per channel (bpc), but it is possible to embed in one or two channels only to enhance imperceptibility.

The obtained PSNR distortion metric is 48, which represent the average of PSNR values of the stego frames, which is considered acceptable with regard to imperceptibility, and it can be raised to 50+ if we use 1-LSB embedding.

1. Increasing the hiding capacity by increasing the number of stego files in a batch without the need to increase the number of embedded bits per channel so that to reduce the distortion in the frames.

2. Strengthening security of the hidden data in case the observer attempts to extract it from one of the stego files, as not only the data is partitioned into two or more stegos, but the vertical slicing of the secret data makes it harder to reassemble the slices into the original secret data file without prior knowledge of the slicing method. In addition, security will be enhanced when each setgo of a batch is sent via a different communication channel.

5.2 Suggestion for future work

There is no complete research, but each research work can provide new ideas for another work. Based on the outcome of the present research, the following ideas are humbly suggested for future work:

- It would be of great value if the system was implemented as a mobile application to improve the privacy and security of multimedia files that are exchanged on mobile devices.
- It is possible to hide two separate secret files in a common batch of stego files, to further enhance the security aspect.

- The rate of distortion can be reduced by using a lower number of bits per colour channel (1 LSB, 0.5 LSB, 0.05 LSB, etc).
- Alternative steganography techniques can be used, such as DCT or DWT, in combination with the batch technique.
- Extending the work to compressed video file types for cover, such as MPEG and MP4.
- Adding a checksum per stego video to enhance the integrity of the secret data through detecting possible alterations by a hacker or due to communication problems.

References

Al-Salihi,I ., & Kayhan, S.K. (2017). ***A comparative study of LSB based Video steganography technique***. Proceedings of IASTEM International Conference, Turkey. Available: http://www.worldresearchlibrary.org/up_proc/pdf/883-15009732081-5.pdf

Chandel.B.,& Jain, S. (2016). ***Text Hiding using Steganography in Video***. International Journal of Computer Applications, (0975–8887).India. Available: http://ijirr.com/sites/default/files/issues-pdf/1237.pdf

Channalli,S., & Jadhav,A. (2009). ***Steganography an Art of Hiding Data.*** International Journal on Computer Science and Engineering, 137-141, India, Available: https://arxiv.org/abs/0912.2319

Chitra,S.,& Thoti,N. (2013**). *Implementation of video steganography using hash function in LSB technique***. International Journal of Engineering Research & Technology (IJERT), 2278-0181. India. Available: file:///C:/Users/Admin/Downloads/journalpaper%20(1).pdf

Choudry, K.N., & Wanjari, A. (2015). ***A Survey Paper on Video Steganography.*** International Journal of Computer Science and Information Technologies (IJCSIT), 2335-2338. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.734.8297&rep=rep1&type=pdf

Esen, E., & Alatan, A.A. (2011). ***Robust Video Data Hiding Using Forbidden Zone Data Hiding and Selective Embedding***. *IEEE Transactions on Circuits and Systems for Video Technology*, 21(8):1130-1138. Available: http://www.cluster2.hostgator.co.in/files/writeable/uploads/hostgator12698/file/robustvideodatahidingusingforbiddenzonedatahiding.pdf

Fabian, A.P., Petitcolas., Anderson, J., & Khan, M.G. (1999). ***Information Hiding-A Survey Fabien***. Proceedings of the IEEE, special issue on the protection of multimedia content, 87(7): 1062–1078. Available: https://www.petitcolas.net/fabien/publications/ieee99-infohiding.pdf

Folk, C., Hurley, D.C., Kaplow, W.K & Payne, F.X (2015). ***THE SECURITY IMPLICATIONS OF THE INTERNET OF THINGS***, AFCEA International Cyber Committee, USA. Available: https://www.mitre.org/sites/default/files/publications/afcea-white-paper-security-implications-internet-of-things.pdf

Goyal, H., & Bansal, P. (2015)***. An Analytical study on video steganography technique.*** International Journal of Advanced Research in Computer Science, 0976-5697. Available: file:///C:/Users/Admin/Downloads/2481-4937-1-SM%20(2).pdf

Jayaram, P ., Ranganatha, H.R .,& Anupama, H.S , (2011) ***INFORMATION HIDING USING AUDIO STEGANOGRAPHY – A SURVEY,*** The International Journal of Multimedia & Its Applications (IJMA).2011.3308 86 INDIA. Available: http://aircconline.com/ijma/V3N3/3311ijma08.pdf

Kahlon, J.S ., & Bhardwaj,V. (2016), ***A Secure Image Steganography Using Bit Shift Encryption & MLSB Approach***, International Journal of Science and Research (IJSR) Licensed Under Creative Commons Attribution CC BY, Available: https://pdfs.semanticscholar.org/6b27/afc7b2fd665a52a7203a8d85e366965b9057.pdf

Kaur, N., & Behal, S. (2014). ***A Survey on various types of Steganography and Analysis of Hiding Techniques***. International Journal of Engineering Trends and Technology (IJETT), 2231-5381, India, Available: file:///C:/Users/Admin/Downloads/ASurveyonvarioustypesofSteganographyandAnalysis_May2014Navneet%20(1).pdf

Kavitha, R., & Murugan, A. (2008). ***Lossless Steganography on AVI File using Swapping Algorithm.*** International Conference on Computational Intelligence and Multimedia Applications., India. Available : file:///C:/Users/Admin/Downloads/losslessstegano-ieee%20(3).pdf

Ker, A.D.(2006)**. *batch steganography and pooled steganalysis***. Part of the Lecture Notes in Computer Science book series (LNCS, volume 4437) UK. Available : http://www.cs.ox.ac.uk/people/andrew.ker/docs/ADK18D.pdf

Ker,A.D. (2007-a). ***Batch Steganography and the Threshold Game.*** SPIE/IS&T EI 2007 ***UK.*** Avaialble: https://www.cs.ox.ac.uk/andrew.ker/docs/ADK21B.pdf

Ker,A.D. (2007-b). ***A capacity result for batch steganography***. IEEE SIGNAL PROCESSING LETTERS, 1070-9908.UK. Available:

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.156.9194&rep=rep1&type=pdf

Ker, A.D., & Pevný, T. (2012). ***Batch Steganography in the real World***. Published on MM&Sec '12 Proceedings of the on Multimedia and security, Pages 1-10, UK. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.918.4286&rep=rep1&type=pdf

Ker,A.D., Bas,P .,Böhme,R., Cogranne,R .,Craver,S .,Filler,T ., Fridrich,J ., &Pevný.T. (2015). ***Moving Steganography and Steganalysis from the Laboratory into the Real World Conference.*** Proceedings of the first ACM workshop on Information hiding and multimedia security, 45-58. Uk. Available: http://www.ws.binghamton.edu/fridrich/Research/ih067-ker.pdf

Kulkarni, A.D., Bansal, E., Rajashree, H., Rasika, J,. & Madhuri, L. (2015). ***Improved Data Security Using Video Steganography.*** International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 2278 – 1323 .Available: http://ijarcet.org/wp-content/uploads/IJARCET-VOL-4-ISSUE-10-3903-3905.pdf

Mandal, P.C. (2012). ***Modern Steganographic technique: A survey.*** International Journal of Computer Science & Engineering Technology (IJCSET), 2229-3345 India, Available: http://www.ijcset.com/docs/IJCSET12-03-09-047.pdf

Nikam, G., Gupta, A., Kalal, V., & Waghmare, P. (2017) ***A Survey of Video Steganography Techniques,*** Journal of Network Communications and Emerging Technologies (JNCET) 2395-5317, India.Available: file:///C:/Users/Admin/Downloads/StegnographyVol-7-issue-5-M-07.pdf

Olalekan,O .,& Adenrele,A. (2014) , ***A survey of various types of steganography and analysis of hiding techniques***, International Journal o Engineering Trends and Technology (IJETT), Nigeria. Available: https://www.academia.edu/38039824/A_Survey_on_various_types_of_Steganography_and_Analysis_of_Hiding_Techniques

Pal, S.,& Bandyopadhyay, S.k (2016). ***Various methods of video steganography.*** International Journal of Information Research and Review (IJIRR), 2569-2573. India. Available: http://ijirr.com/sites/default/files/issues-pdf/1237.pdf

Pawar, S.,& Kakde, V. (2014). ***Review on Steganography for Hiding Data***. International Journal of Computer Science and Mobile Computing, 225-229, India. Available: https://www.academia.edu/6704398/REVIEW_ON_STEGANOGRAPHY_FOR_HIDING_DATA_

Pinki., & Mehra, R. (2016). ***Estimation of Image Quality under Different Distortions***. International Journal Of Engineering And Computer Science 17291-17296. Chandigarh, Available: file:///C:/Users/Admin/Downloads/Estimation_of_the_Image_Quality_under_Different_Di%20(2).pdf

Rejani, R., Murugan, D.,& Krishnan, D.V.(2015). ***Comparative Study of Spatial Domain Image Steganography Techniques,*** , International Journal Advanced Networking and Applications 0975-0290 India. Available: https://www.ijana.in/papers/V7I2-2.pdf

Ramalingam, M., Isa, N.A., Ramalingam, M., & Isa, N.A. (2015)***, A Steganography Approach over Video Images to Improve Security*** Indian Journal of Science and Technology. 0974-5645.India, Available: file:///C:/Users/Admin/Downloads/53100-86546-3-PB%20(1).pdf

Saxena,A. & Suraj,S.(2017***). A review of different methodologies for video steganography***. International Journal of Innovative Science and Research Technology ,2456-2165.India . Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.156.9194&rep=rep1&type=pdf

Shukla,A.K., & Dixit.G **.*, Data Hiding Using Steganography***, (2017) International Journal for Innovations in Engineering, Science and Management ISSN 2347 - 7911, India . Available: https://pdfs.semanticscholar.org/c7f9/fa4a6ea7881d23f6f0217498f520ef2aed4a.pdf

Sumathi, C.P., Santanam, T., & Umamaheswari, G.(2013). ***A Study of Various Steganographic Techniques Used for Information Hiding*** International Journal of Computer Science & Engineering Survey (IJCSES) 2013.46029 , India. Available: https://www.academia.edu/10458439/A_Study_of_Various_Steganographic_Techniques_Used_for_Information_Hiding

Saleh, M.A.(2018), ***Image Steganography Techniques A Review Paper***, International Journal of Advanced Research in Computer and Communication Engineering 2278-1021 Kingdom of Saudi Arabia, Available: https://ijarcce.com/wpcontent/uploads/2018/10/IJARCCE.2018.7910.pdf

Sajedi,H ., & Jamzad,M. (2009). ***Adaptive batch steganography considering image embedding capacity***. 48(8), 087002.Iran . Avalable: file:///C:/Users/Admin/Downloads/p_ABS-OE%20(1).pdf

Sandhu, M., Kaur, J., & Kaur, S. (2016).***Encoding and Decoding of Image using Steganography Technique.*** International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE), 2278-909X India, Available: http://ijarece.org/wp-content/uploads/2016/06/IJARECE-VOL-5-ISSUE-6-1699-1702.pdf

Sapate,P., Patil,V ., Pardeshi,M., & Nichal,A. (2016). ***A Review Paper on Video Steganography***. International Advanced Research Journal in Science, Engineering and Technology, 2393-8021.India Available: file:///C:/Users/Admin/Downloads/18AReviewPaperonVideoSteganography.pdf

Singh, N., Bhati, B.S., Raw, R.S.(2012). ***Digital images steganalysis for computer forensic investigation***, India, Available: file:///C:/Users/Admin/Downloads/Digital_Image_Steganalysis_for_Computer_Forensic_I%20(2).pdf

Sheelu ., &Ahuja, B. An Overview of Steganography (2013) Journal of Computer Engineering (IOSR-JCE), 2278-0661 India, Available: https://www.academia.edu/4814244/An_Overview_of_Steganography

Sinha,S., & Gupta,P.(2016) ***IMAGE STEGANOGRAPHY USING DESYNCHRONIZATION*** International Journal of Computer Science and Mobile Computing A Monthly Journal of Computer Science and Information Technology 2320–088X IJCSMC, pg.55 – 61, Available: https://ijcsmc.com/docs/papers/February2016/V5I2201614.pdf

Thampi, S.M. (2004**).** ***Information Hiding Techniques: A Tutorial Review***. ISTE-STTP on Network Security & Cryptography, India . Available: file:///C:/Users/Admin/Downloads/0802.3746%20(1).pdf

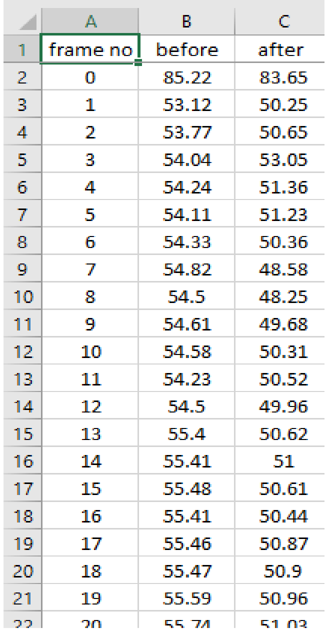
Upadhyay, R., Thakur, Y.S., & Sakravdia, D.K (2015), ***A Comparative Study of Un-optimized and Optimized Video Steganography*** International Journal of Computer Science and Information Technologies, (IJCSIT) 3753-3757. Available: http://ijcsit.com/docs/Volume%206/vol6issue04/ijcsit20150604102.pdf

Wajgade,V.M ,.& Kumar,S (2013). ***Enhancing Data security using video steganography.*** International Journal of Emerging Technology and Advanced Engineering. 2250-2459, India. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.413.6576&rep=rep1&type=pdf

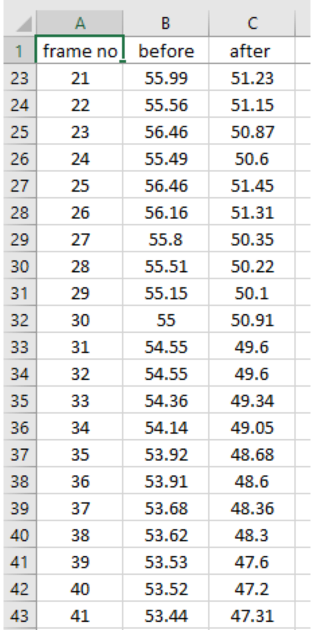
Appendix

Sample of PSNR accuracy results of the video payload

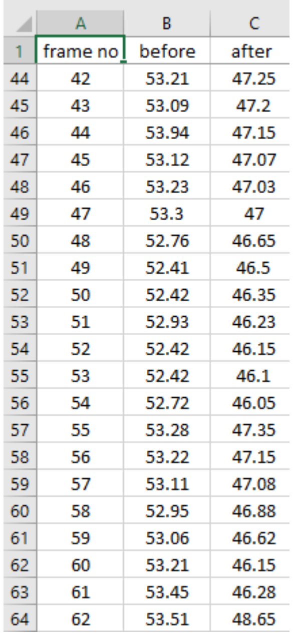
PSNR results before and after embedding using the 2LSB technique. The results were checked and tested on Video Quality Estimator. The PSNR for the entire video is calculated as the average of PSNR values of the frames.



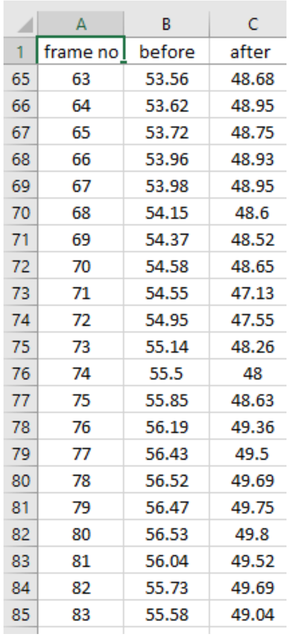
	A	B	C
1	frame no	before	after
2	0	85.22	83.65
3	1	53.12	50.25
4	2	53.77	50.65
5	3	54.04	53.05
6	4	54.24	51.36
7	5	54.11	51.23
8	6	54.33	50.36
9	7	54.82	48.58
10	8	54.5	48.25
11	9	54.61	49.68
12	10	54.58	50.31
13	11	54.23	50.52
14	12	54.5	49.96
15	13	55.4	50.62
16	14	55.41	51
17	15	55.48	50.61
18	16	55.41	50.44
19	17	55.46	50.87
20	18	55.47	50.9
21	19	55.59	50.96
22	20	55.74	51.03



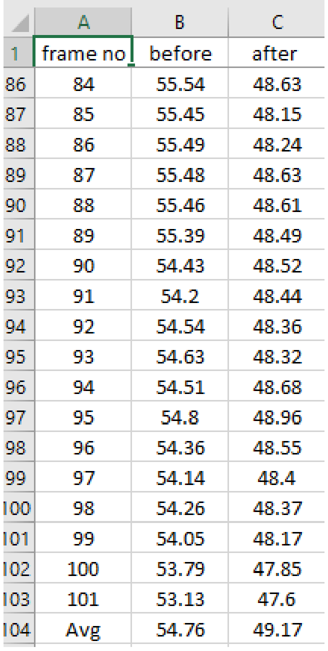
	A	B	C
1	frame no	before	after
23	21	55.99	51.23
24	22	55.56	51.15
25	23	56.46	50.87
26	24	55.49	50.6
27	25	56.46	51.45
28	26	56.16	51.31
29	27	55.8	50.35
30	28	55.51	50.22
31	29	55.15	50.1
32	30	55	50.91
33	31	54.55	49.6
34	32	54.55	49.6
35	33	54.36	49.34
36	34	54.14	49.05
37	35	53.92	48.68
38	36	53.91	48.6
39	37	53.68	48.36
40	38	53.62	48.3
41	39	53.53	47.6
42	40	53.52	47.2
43	41	53.44	47.31



	A	B	C
1	frame no	before	after
44	42	53.21	47.25
45	43	53.09	47.2
46	44	53.94	47.15
47	45	53.12	47.07
48	46	53.23	47.03
49	47	53.3	47
50	48	52.76	46.65
51	49	52.41	46.5
52	50	52.42	46.35
53	51	52.93	46.23
54	52	52.42	46.15
55	53	52.42	46.1
56	54	52.72	46.05
57	55	53.28	47.35
58	56	53.22	47.15
59	57	53.11	47.08
60	58	52.95	46.88
61	59	53.06	46.62
62	60	53.21	46.15
63	61	53.45	46.28
64	62	53.51	48.65



	A	B	C
1	frame no	before	after
65	63	53.56	48.68
66	64	53.62	48.95
67	65	53.72	48.75
68	66	53.96	48.93
69	67	53.98	48.95
70	68	54.15	48.6
71	69	54.37	48.52
72	70	54.58	48.65
73	71	54.55	47.13
74	72	54.95	47.55
75	73	55.14	48.26
76	74	55.5	48
77	75	55.85	48.63
78	76	56.19	49.36
79	77	56.43	49.5
80	78	56.52	49.69
81	79	56.47	49.75
82	80	56.53	49.8
83	81	56.04	49.52
84	82	55.73	49.69
85	83	55.58	49.04



	A	B	C
1	frame no	before	after
86	84	55.54	48.63
87	85	55.45	48.15
88	86	55.49	48.24
89	87	55.48	48.63
90	88	55.46	48.61
91	89	55.39	48.49
92	90	54.43	48.52
93	91	54.2	48.44
94	92	54.54	48.36
95	93	54.63	48.32
96	94	54.51	48.68
97	95	54.8	48.96
98	96	54.36	48.55
99	97	54.14	48.4
100	98	54.26	48.37
101	99	54.05	48.17
102	100	53.79	47.85
103	101	53.13	47.6
104	Avg	54.76	49.17