Cuttlefish(A Prototype Encryption Algorithm with Steganography)

A Thesis

Presented to the Faculty of

Information and Communications Technology Program

STI College Bacoor

In Partial Fulfilment

of the Requirements for the Degree

Bachelor of Science in Computer Science

Gian Daniel C. Buenaventura

Marjorie Mae F. De Leon

Johnivan B. De Mesa

Bernabe S. Posadas Jr.

<Date Approved>

ENDORSEMENT FORM FOR ORAL DEFENSE

TITLE OF RESEARCH: Cuttlefish(A Prototype Encryption Algorithm with Steganography)

NAME OF PROPONENTS: Gian Daniel C. Buenaventura

Marjorie Mae F. De Leon

Johnivan B. De Mesa

Bernabe S. Posadas Jr.

In Partial Fulfilment of the Requirements

for the degree Bachelor of Science in Computer Science

has been examined and is recommended for Oral Defense.

ENDORSED BY:

Roland S. Doctolero

Thesis Adviser

APPROVED FOR PROPOSAL DEFENSE:

Jeanny O. Garcia

Thesis Coordinator

NOTED BY:

Jeanny O. Garcia

Program Head

<Date of Oral Defense>

# APPROVAL SHEET

This thesis titled: Cuttlefish (A Prototype Encryption Algorithm) prepared and submitted by Gian Daniel C. Buenaventura; Marjorie Mae F. De Leon ; Johnivan B. De Mesa; and Bernabe S. Posadas Jr., in partial fulfilment of the requirements for the degree of Bachelor of Science in Computer Science, has been examined and is recommended for acceptance an approval.

Roland S. Doctolero

Thesis Adviser

Accepted and approved by the Thesis Review Panel

in partial fulfilment of the requirements for the degree of

Bachelor of Science in Computer Science

|  |  |
| --- | --- |
| Prof. Jeanny O. Garcia | Prof. Emilyn A. Donor |
| Panel Member | Panel Member |

Mr.Jason Sespeñe

Lead Panelist

APPROVED:

|  |  |
| --- | --- |
| Jeanny O. Garcia | Jeanny O. Garcia |
| Thesis Coordinator | Program Head |

<Date of Proposal Defense>

# Acknowledgements

First and foremost, the proponents praises and thanks to the God, the Almighty, for His showers of blessings throughout their research work to complete the research successfully, the proponents thank for the strength that keep them standing and for the hope that keep us believing that this affiliation would be possible and more interesting.

The proponents wish to thank their thesis coordinator and review panel for their efforts to give suggestions and evaluation on the proposed system.

The proponents also wish to thank their thesis advisory, Mr. Angelo Maderal and Mr. Ronald S. Doctolero for their patience and skills to in helping us to structure and write this thesis. For this the proponents are sincerely grateful and thankful on their efforts through reading of this thesis and for their helpful comments.

The proponents also wanted to thank their family who inspired, encouraged and fully supported us for every trial that comes our way. This journey would not have been possible without them. They were especially grateful to their parents, who supported them emotionally and financially.

The proponents are immensely grateful to all involved in this project as without their inspiration and valuable suggestion it would not have been possible to develop the project within the prescribed time.

# Abstract

Title of research**: Cuttlefish (A Prototype Encryption Algorithm with Steganography)**

Researchers: Gian Daniel C. Buenaventura

Marjorie Mae F. De Leon

Johnivan B. De Mesa

Bernabe S. Posadas

Degree: Bachelor of Science in Computer Science

Date of Completion: <Month year of graduation>

Key words: Steganography, Cryptography, LSB based Steganography

Steganography is the art of hiding information and an effort to conceal the existence of the embedded information. Steganography is often confused with cryptography because the both are used for used to protect important information. It serves as a better way of securing message than cryptography which only conceals the content of the message not the existence of the message. In Steganography original message is being hidden within a carrier such that the changes so occurred in the carrier are not observable. On the other hand Cryptography basically means art of protecting information by converting it into unreadable format. Cryptography and Steganography are present in different domains of network security and often used as separate techniques to provide confidentiality and security of data. In this research the proponents conducted, a new encryption algorithm for encoding data files. This development of new encryption algorithm will help the entire sector to secure their data files. This encryption algorithm uses 16-bit or 128-bit as a key to encrypt the data. CBC block cipher is used in 16-bit encryption algorithm to avoid pattern on identical blocks the plaintext will be XORed to the recent cipher block if any present while a modified CBC block cipher algorithm is used in 128-bit encryption algorithm to also avoid pattern on identical blocks but before the plaintext will be XOR to the recent cipher block, the encryption key will undergo a key scrambling algorithm to avoid repletion of using the same key in each block improving resistance against cryptanalysis. Key scrambling algorithm used are similar they created 128-bit encryption algorithm data scrambling methods. To protect encoded data from any potential circumstance other users of the system from extraction of the secret data. The system can use password as a layer to protect the data and to hide encoded data on a video cover, the proposed system used LSB algorithm that will hide data on last 2 bits of the every color information stored in a pixel.

# Table of Contents

|  |  |  |
| --- | --- | --- |
|  | | Page |
| Title Page | | I |
| Endorsement Form for Proposal Defense | | ii |
| Approval Sheet | | Iii |
| Acknowledgements | | Iv |
| Abstract | | V |
| Table of Contents | | Vi |
| List of Tables | | Vii |
| List of Figures | | Viii |
| List of Appendices | | Ix |
| Introduction | | 1 |
|  | Background of the problem | 1 |
|  | Overview of the current state of technology | 2 |
|  | Objectives of the study | 3 |
|  | Scope and limitations of the study | 3 |
| Literature Review | | 5 |
|  | Review of related literature, studies or systems | 5 |
|  | Synthesis | 32 |
| Cuttlefish (A Prototype Encryption Algorithm with Steganography) | | 33 |
| Results and Discussions | | 40 |
| Conclusions and Recommendations | | 78 |
| References | | 79 |
| Appendices | | 83 |

# List of Tables

|  |  |  |
| --- | --- | --- |
| Table |  | Page |
| 1 | test data table | 40 |
| 2 | Video Cover 1 information | 40 |
| 3 | Video Cover 2 information | 40 |
| 4 | Test Results for “ACCOMPLISHMENT AND COSULTAION FORM.docx” using different key size. | 41 |
| 5 | PSNR results of test 1 | 41 |
| 6 | PSNR results of test 2 | 41 |
| 7 | Test Results for Attachment B\_OJT Training Plan Template.xls using different key size. | 42 |
| 8 | PSNR results of test 3 | 42 |
| 9 | PSNR results of test 4 | 42 |
| 10 | Test Results for Attachment G\_Daily Time Record.pdf using different key size. | 43 |
| 11 | PSNR results of test 5 | 43 |
| 12 | PSNR results of test 6 | 43 |
| 13 | Test Results for Chrysanthemum.jpg using different key size. | 44 |
| 14 | PSNR results of test 7 | 45 |
| 15 | PSNR results of test 8 | 45 |
| 16 | Test Results for exorciser.jar using different key size | 46 |
| 17 | PSNR results of test 9 | 47 |
| 18 | PSNR results of test 10 | 49 |
| 19 | Test Results for my night.mp3 using different key size | 49 |
| 20 | PSNR results of test 11 | 57 |
| 21 | PSNR results of test 12 | 57 |
| 22 | Test Results for OJT-Copy-for-students.zip using different key size | 58 |
| 23 | PSNR results of test 13 | 58 |
| 24 | PSNR results of test 14 | 58 |
| 25 | Test Results No. 2 for “ACCOMPLISHMENT AND COSULTAION FORM.docx” using different key size. | 59 |
| 26 | PSNR results of test 15 | 59 |
| 27 | PSNR results of test 16 | 59 |
| 28 | Test Results No. 2 for Attachment B\_OJT Training Plan Template.xls using different key size. | 60 |
| 29 | PSNR results of test 17 | 60 |
| 30 | PSNR results of test 18 | 60 |
| 31 | Test Results No. 2 for Attachment G\_Daily Time Record.pdf using different key size. | 61 |
| 32 | PSNR results of test 19 | 61 |
| 33 | PSNR results of test 20 | 61 |
| 34 | Test Results No. 2 for Chrysanthemum.jpg using different key size. | 62 |
| 35 | PSNR results of test 21 | 62 |
| 36 | PSNR results of test 22 | 62 |
| 37 | Test Results No. 2 for exorciser.jar using different key size | 63 |
| 38 | PSNR results of test 23 | 63 |
| 39 | PSNR results of test 24 | 63 |
| 40 | Test Results No. 2 for my night.mp3 using different key size | 64 |
| 41 | PSNR results of test 25 | 64 |
| 42 | PSNR results of test 26 | 64 |
| 43 | Test Results for OJT-Copy-for-students.zip using different key size | 65 |
| 44 | PSNR results of test 27 | 65 |
| 44  45  46  47  48  49  50 | PSNR results of test 28  Test Results for No Game No Life Opening Full.flac using different key size  PSNR results of test 29  PSNR results of test 30  Test Results for Watch No Game No Life Episode 1 English Sub.mp4 using different key size  PSNR result of test 31  PSNR result of test 32 | 65  66  69  71  72  75  77 |

# List of Figures

|  |  |  |
| --- | --- | --- |
| Figure |  | Page |
| 1 | “Standard AVI RIFF form” | 24 |
| 2 | “RIFF AVI form using OpenDML” | 25 |
| 3 | “Prototype model” | 34 |
| 4 | “The Proposed System Flowchart” | 36 |
| 5 | “gear like shift” | 37 |
| 6 | “changes on color green when modifying its LSB” | 39 |
|  |  |  |

# List of Appendices

|  |  |  |
| --- | --- | --- |
| Appendix |  | Page |
|  | A. Gantt chart of activities | 84 |
|  | B. Actual Thesis Expenses | 86 |
|  | C. User’s Manual | 89 |
|  | D. Curriculum Vitae of Researchers | 110 |
|  |  |  |
|  |  |  |

# Introduction

This research aims to create a prototype Encryption Algorithm and create a stegosystem that uses LSB algorithm to store encrypted information coming from the created prototype algorithm to hide it on a cover .AVI format video. This chapter defines the proponent’s motivation for researching about cryptography, video based steganography and LSB insertion algorithm. This research outlines the main objective and attempts to propose a solution to challenge the start of the art.

## Background of the problem

The continued growth of information communication technologies makes any kinds of information accessible to anyone using the system. From homes to companies, the data they send to cyberspace is stored, processed, retrieved and transmitted electronically. The ease of sending information through this system is convenient and fast. Banks, companies, and even government agencies now implementing this system to take advantage to its speed and convenience for their clients. Slowly in our country the Philippines is implementing this system to serve its people better and even have its own department purposed for information technology innovation the Department of Information Communication Technology (DICT). Government Agencies started to develop online transaction and automated elections, Banks implemented online banking for their clients to bank online, and Companies use online shopping to sell their products online. As the data is stored electronically, this poses a threat to data breach where unwanted individuals able to get information without consent of the individual own that information.

To overcome this problem, the proponents strive to make a prototype encryption with steganography to hide sensitive information.

## Overview of the current state of the technology

## Throughout the world, information communication technology is used to store, process, retrieve and transmit data. Currently many encryption algorithms are created to address data breach problem. By encrypting information, if in any case the information has somehow been breached by an unwanted individual, it requires research about the algorithm used to break the encryption. Steganography is more concern about how to conceal data without any noticeable changes to a cover object. During the past, steganography helped in wars and prevent other parties to intercept messages by concealing the existence of the messages.

According to Mohammad Suleman in his article “5 Free Video Steganography Software to Hide Files in Videos” Hiding messages and documents in videos could be a great trick to share secret messages over the internet. The best part is that the secret message that you embed in videos can only be decrypted by the same software which you used for hiding your file. There is much Steganography software available, but very few support video files as carriers.

OpenPuff and DeEgger are one of the examples of video steganography software, they use different approach of hiding the data like masking, file injection, etc. these software however has its limitation like OpenPuff can only embed up to 256 MB and DeEgger combines the payload and the cover video file size that leads to noticeable file size changes.

By using uncompressed video RGB 24bit AVI file, storing the metadata of the embedded file to the unused chunk of the cover video and using LSB algorithm to embed the payload file, the proposed prototype can achieve little to no changes to the file size of the cover video and a dedicated prototype encryption so that only the proposed prototype can extract the embedded file.

## Objectives of the study

## The general objective of this study is to create an encryption algorithm with steganography. During the study, the proponents have a general idea on what the current problem is and attempts to address those problem. After the study, the proponent will then conclude if they were able to solve the problem and pass down the concept to the future researchers for the improvement of this concept.

Specific Objectives of the study

1. To identify the current problem of Information Communication Technology related data communication and address it by applying cryptography and steganography technology.
2. Study about Cryptography and Steganography
3. Make a new encryption algorithm to be used in encoding data
4. Implement an existing steganography scheme.
5. Help contribute to computer information security by making a prototype application that uses encryption algorithm with combination of steganography.

## Scope and limitations of the study

The proposed system will have the following features:

* **Data embedding** – with the use of algorithm which is Least Significant Bit(LSB) algorithm, an algorithm that exploits the human visual system by hiding the message on the LSB of every color attribute of a single pixel. The system will embed encrypted information to the video cover stated by the user
* **Data Extraction –**the system can extract embedded data from a cover video if an embed file is found and decrypt it with the use of the prototype encryption algorithm then save it on the computer file path given by the user.
* **Validation -** The system will validate if the necessary requirements are met before embedding or extracting process begins. The system will pop out a message to the user to tell what requirements are not met for them to comply.
* **Settings –** The module contains various useful settings, settings like single or multiple files selection as payload, an option to delete a source file after embedding, an option to protect embedded data with a password and key size selection for better security.
* **Key Size –** the proposed system can use between fast 16 bit key or slower but more secured 128 bit key stated by the user via Settings.

Limitations

The proposed system is designed to encrypt file data stored in the computer and hides the information in a cover video having an extension file of AVI (.avi) with no compression codecs applied.

Specifically, the proposed system limitations are:

* The proposed system cannot use AVI file with compression codecs applied like Theora, XVID, Cinepak and h.264 as cover video due to data loss from its compression algorithm that uses lossy compression techniques to achieve smaller size. In case of lossless compression like huffyuv, using LSB approach will result to unstable changes to video file size.
* The system will not be able to embed payload capacity of 2GB(2,147,483,648 bytes) or if the size of the payload is greater than the video cover can hold.
* Multiple files will be compressed and extracted as a zip file to achieve a smaller metadata.
* Other Video Containers like QuickTime and MP4 as the system can only decode AVI files.

# Literature Review

## Review of related literature, studies or systems

This chapter shows a list of related studies and literature that served as basis to the proponents to pursue their topic with the title of “Cuttlefish (A Prototype Encryption Algorithm with Steganography)”. The proponents do not own any of the studies listed and the researchers will not copy any of this works.

## ICT (information and communications technology - or technologies)

ICT (information and communications technology - or technologies) is an umbrella term that includes any communication device or application, encompassing: radio, cellphones, computer and network hardware and software, satellite systems and so on, as well as the various services and applications associated with them, such as videoconferencing and distance learning. ICTs are mostly told in a particular context, such as ICTs in education, health care, or libraries.

ICT, or information and communications technology is the infrastructure and components that enable modern computing.

It is generally accepted to mean all devices, networking components, applications and systems that combined allow people and organizations to interact in the digital world.

## Components of an ICT system

ICT encompasses both the internet-enabled sphere as well as the mobile one powered by wireless networks. It also includes antiquated technologies, such as landline telephones, radio and television broadcast all of which are still used today alongside cutting-edge ICT pieces such as artificial intelligence and robotics.

ICT is sometimes used synonymously with IT; however ICT is generally used to represent a broader, more comprehensive list of all components related to computer and digital technologies than IT.

The list of ICT components is considerate, and it keeps growing. Some components, like computers and telephones, have existed for decades. Others, such as smartphones, or robots, are more recent entries.

ICT commonly means more than its list of components, though. It also encompasses the application of all those various components. It's here that the real potential, power and danger of ICT can be found.

## ICT's societal and economic impact

ICT is leveraged for economic, societal and interpersonal transactions and interactions. ICT has drastically changed how people work, communicate, learn and live. Moreover, ICT continues to revolutionize all parts of the human experience as first computers and now robots do many of the tasks once handled by humans.

ICT's importance to economic development and business growth has been so monumental, in fact, that it's credited with ushering in what many have labeled the Fourth Industrial Revolution.

ICT also underpins broad shifts in society, as individuals are moving from personal interactions to ones in the digital space. This new era is frequently termed the Digital Age

These various institutions assert that those without ICT capabilities are left out of the multiple opportunities and benefits that ICT creates and will therefore fall further behind in socio-economic terms.

Within the ICT market, the advancement of ICT capabilities has made the development and delivery of various technologies cheaper for ICT vendors and their customers while also providing new market opportunities. Consumers now enjoy more choices in delivery and price points as a result.

## The significance of ICT in enterprises

For businesses, advances within ICT have brought a slew of cost savings, opportunities and conveniences. They range from highly automated businesses processes that have cut costs, to the big data revolution where organizations are turning the vast trove of data generated by ICT into insights that drive new products and services, to ICT-enabled transactions such as internet shopping and telemedicine and social media that give customers more choices in how they shop communicate and interact.

But ICT has also created problems and challenges to organizations and individuals alike -- as well as to society as a whole. The digitization of data, the expanding use of high-speed internet and the growing global network together have led to new levels of crime, where so-called bad actors can hatch electronically enabled schemes or illegally gain access to systems to steal money, intellectual property or private information or to disrupt systems that control critical infrastructure. ICT has also brought automation and robots that displace workers who are unable to transfer their skills to new positions. And ICT has allowed more and more people to limit their interactions with others.

## ICT HISTORY

IT defines as **Information Technology**, consists of study, design, advance development, accomplishment, support or administration of computer foundation information system, mostly software application and computer hardware. Information technology works with the use of electronic computers and computer software to renovate, defend, develop, broadcast and assorted types of information. Information technology has overstuffed to cover many features of computing and technology, and this word is more familiar than ever before. Information technology subject can be quite large, encompassing many fields. IT professionals perform different types of responsibilities that range from installing applications to designing complex computer networks.

IT professional's responsibilities are data management, networking, database, software design, computer hardware, management and administration of whole system. IT (Information Technology) is combined word of computer and communications or "InfoTech". Information Technology illustrates any technology which helps to manufacture, manipulate, accumulate, communicate or broadcast information.

The term "information technology" evolved in the 1970s. Its basic concept, however, can be traced to the World War II alliance of the military and industry in the development of electronics, computers, and information theory. After the 1940s, the military remained the major source of research and development funding for the expansion of automation to replace manpower with machine power. Since the 1950s, four generations of computers have evolved. Each generation reflected a change to hardware of decreased size but increased capabilities to control computer operations. The first generation used vacuum tubes, the second used transistors, the third used integrated circuits, and the fourth used integrated circuits on a single computer chip. Advances in artificial intelligence that will minimize the need for complex programming characterize the fifth generation of computers, still in the experimental stage.

The first commercial computer was the UNIVAC I, developed by John Eckert and John W. Mauchly in 1951. It was used by the Census Bureau to predict the outcome of the 1952 presidential election. For the next twenty-five years, mainframe computers were used in large corporations to do calculations and manipulate large amounts of information stored in databases. Supercomputers were used in science and engineering, for designing aircraft and nuclear reactors, and for predicting worldwide weather patterns. Minicomputers came on to the scene in the early 1980s in small businesses, manufacturing plants, and factories.

In 1975, the Massachusetts Institute of Technology developed microcomputers. In 1976, Tandy Corporation's first Radio Shack microcomputer followed; the Apple microcomputer was introduced in 1977. The market for microcomputers increased dramatically when IBM introduced the first personal computer in the fall of 1981. Because of dramatic improvements in computer components and manufacturing, personal computers today do more than the largest computers of the mid-1960s at about a thousandth of the cost. Computers today are divided into four categories by size, cost, and processing ability. They are supercomputer, mainframe, minicomputer, and microcomputer, more commonly known as a personal computer. Personal computer categories include desktop, network, laptop, and handheld.

We are currently living an unprecedented moment of technological progress. In the history of humanity we have never observed such acceleration of scientific and technological knowledge as the one we are currently living. This growing phenomenon studied and called Technological Singularity.

One of the most relevant elements of this phenomenon is related to its global nature, since technological progress is not only limited to countries traditionally prone to innovation, but is now also being extended to emerging countries.

In this framework, we have been able to identify relevant innovative experiences that suppose the utilization of Information and Communication Technology (ICT) to solve social problems/needs from low-income populations. Technologies can have a capital role to reach the Sustainable Development Goals and to enhance the quality of life of most disadvantaged people.

Another important factor which has allowed reaching this level of innovation is the global growth of the so-called open knowledge.

## Data Breach

A data breach is an incident involving someone hacking an individual’s data without authorization; they may be after personal info, property data, health records and other sensitive files and topics.

Common data breach exposures include personal information, such as credit card numbers, Social Security numbers and healthcare histories, as well as corporate information, such as customer lists, manufacturing processes and software source code. If anyone who is not specifically authorized to do so view such data, the organization charged with protecting that information is said to have suffered a data breach. Data breach is a major violation in network law

## Data breach causes

A familiar example of a data breach is an attacker hacking into a corporate website and stealing sensitive data out of a database. However, not all breaches are so dramatic. Data breaches can be brought about by weak passwords, missing software patches that are exploited or lost or stolen laptop computers and mobile devices. Users connecting to rogue wireless networks that capture login credentials or other sensitive information in transit can also lead to unauthorized exposures. Social engineering -- especially attacks carried out via email phishing -- can lead to users providing their login credentials directly to attackers or through subsequent malware infections. Criminals can then use the credentials they obtained to gain entry to sensitive systems and records, access which often goes undetected for months. Threat actors can also target third-party business partners in order to gain access to large organizations; such incidents typically involve hackers compromising less secure businesses to obtain access to the primary target.

While hackers and cybercriminals often cause data breaches, there are also incidents where enterprises or government agencies inadvertently expose sensitive or confidential data on the internet. These incidents are typically known as accidental data breaches, and they usually involve organizations misconfiguring cloud services or failing to implement the proper access controls, such as password requirements for public-facing web services or applications.

Ways to protect information

Data at rest and data in transit are two basic types of data encryption designed to protect, if a computer, hard drive or database is hacked, encryption makes data unreadable.

Encrypting data is mainly achieved through Full disk encryption (FDE), File encryption; End to end (E2E) encryption, Encrypted web connections, Encrypted email servers, and Pre-encrypting data that’s not synced with the cloud.

Encryption can be simple or incredibly complex depending on the algorithm and the length of the key. The longer the key, the more protection, but also the more processing power required to handle both the encrypting and decrypting process

According to Lipinski, Michael. (2011)- Protecting information against today's sophisticated, real-time threats in today's mobile environment is a challenge that keeps a lot of IT security professionals up at night. What is our defense against a breach that exposes a user's file system? How do we protect sensitive data that walks out of the enterprise every day on laptops, mobile devices and removable media? We could say that we've established policies to prevent that from happening. That is a viable mitigation tactic.

According to Choi Seung et al.*–* Construction departs from the oft-used paradigm of re-encrypting the same message with different keys and then proving consistency of encryption. Instead, it encrypt an encoding of the message; the encoding is based on an error-correcting code with certain properties of reconstruction and secrecy from partial views, satisfied, e.g., by a Reed–Solomon code.

Based on Information hiding terminology (1996) - Hiding Information terminologies:

## A. The process of hiding the embedded message is called embedding.

## B. Getting the embedded message out of the stego-message again is called extracting.

## C. The party from whom the embedded message is hidden is called the stego-analyst.

## D. The key has to be generated, often depending on one or more security parameters (e.g.one for the cryptographic security of a pseudorandom sequence and another for the collusion size). The standard case where the same key is used in embedding and extracting is called symmetric.

## E. An entity or person that embeds and extracts is called an embedded or an extractor,

Cryptography

According to Pope, M. et al. (2012) - Steganography is the art and science of hiding information. In the digital realm, steganography (which literally means "covered writing"), involves hiding data or messages in digital files and other digital structures. The carriers holding the hidden content may appear to be innocuous, and would be ignored by a casual observer. The field of digital information hiding has grown significantly since the 1990s. Evidence of this growth can be seen at workshops on information hiding and in occasional reports of use by criminals and terrorists as reported in the popular press. In contrast to cryptography where the message is encoded, the purpose of steganography is to hide the fact that a message is being sent. Once encoded, a cryptographically altered message typically appears unrecognizable and would raise suspicions. The primary advantage of steganography over cryptography is that the carriers do not attract attention to themselves, to messengers, or to recipients. Modern information technology enables novice computer users to create steganographic messages, transmit, and unhide them without special expertise.

Cryptography involves creating written or generated codes that allows information to remain a secret, cryptography converts data into an unreadable format for an unauthorized user, allowing it to be transmitted without unauthorized entities decoding it back to its readable format

Information security uses cryptography on several levels, the information can’t be read without a key to decrypt it, and the information maintains its integrity during transit while being stored. Cryptography also helps in nonrepudiation which means that the sender and the delivery of a message can be verified.

According to Joachim. von zur Gathen (2015)*-* Cryptography is a key technology in electronic key systems. It is used to keep data secret, digitally sign documents, access control, etc. Therefore, users should not only know how its techniques work, but they must also be able to estimate their efficiency and security.

In cryptography there are several main Encryption methods

Full disk encryption (FDE) is the primary way to protect computer hard drives and the at-rest data on them, any files saved on the disk are automatically encrypted.

File Encryption is a way to encrypt at-rest data on a file-by-file basis so it can’t be read if it’s intercepted, however this isn’t automatic but it is beneficial because data will stay encrypted after it’s where it was originally from.

End to End (E2E) Encryption obscures any content of message so only the senders and receivers can read it, the function about E2E encryption is that it tackles all the vulnerabilities on the communication chain which is the middle and both ends.

Block Cipher

A block cipher is a symmetric cryptographic algorithm that operates on a fixed-size block of data using a shared, secret key. Plaintext is used during the encryption, and the resulting encrypted text is called a ciphertext. The same key is used for both the encryption of the plaintext and the decryption of the ciphertext.

Based on Techopedia - Block cipher encrypts/decrypts its input one block at a time instead of one bit at a time using a shared, secret key. The block is fixed in size; otherwise, padding is necessary. This algorithm is symmetric. During encryption, it uses the shared key to transform its plaintext input into a cyphertext (encrypted text). During decryption, it uses the same key to transform the cyphertext back to the original plaintext. The length of the output is the same as the input.

Well-known implementations of the block cipher algorithm are the Data Encryption Standard (DES), TripleDES and the Advanced Encryption standard (AES).

The counterpart of block cypher is the stream cypher, which operates on its input one bit at a time, also using a shared key.

An alternative to the block cipher algorithm is public-key cryptography or asymmetric cryptography. This algorithm uses a public key to encrypt plaintext and a private key to decrypt the resulting ciphertext.

Encrypted web connections via HHTPS, these connections use a Secure Sockets Layer or transport layer security protocols, these are used to have better protected communications on the web, HTTPS uses SSL and TLS as encryption keys to authorize access encrypted data that’s passed between them.

Encrypted email servers is a public key encryption essentially gives SMTP email servers to send and receive encrypted messages.

Pre-encrypting data that’s synced with the cloud many software’s are available that can pre-encrypt data before it is sent to cloud, making it unreadable by the cloud or anyone who hacks in to it. However files still stored on the local machine has not been encrypted and are still vulnerable.

According to Delov, D., and Dwork C., (2000)- The notion of cryptography, an extension of semantically secure cryptography, is defined. Informally, in the context of encryption the additional requirement is that given the ciphertext it is impossible to generate a ciphertext so that the respective plaintexts are related. The same concept makes sense in the contexts of string commitment and zero-knowledge proofs of possession of knowledge. Non-malleable schemes for each of these three problems are presented. The schemes do not assume a trusted center; a user need not know anything about the number or identity of other system users. Cryptosystem is the first proven to be secure against a strong type of chosen ciphertext attack, in which the attacker knows the ciphertext she wishes to break and can query the decryption oracle on any ciphertext other than the target.

According to Daniel Lloyd Calloway (2008)- without having near-flawless strong cryptographic security built into them would be vulnerable to would-be hackers, organized crime, terrorist or enemy government.

QuickCrypto - allows to hide one or more files in a folder. this is not simple 'hidden attribute' file hiding but physically moves the file and keeps it associated to its original folder for recovery.

Based on A research paper on cryptography encryption and compression techniques (2017) - By using cryptography many goals can be achieved, These goals can be either all achieved at the same time in one application, or only one of them.

These goals are:

1. Confidentiality: it is the most important goal, that ensures that nobody can understand the received message except the one who has the decipher key.
2. Authentication: it is the process of proving the identity that assures the communicating entity is the one that it claimed to be. This means that the user or the system can prove their own identities to other parties who don’t have personalknowledge of their identities.
3. Data Integrity: it ensures that the received message has not been changed in any way from its original form. The data may get modified by an unauthorized entity intentionally or accidently. Integrity service confirms that whether data is intact or not since it was last created, transmitted, or stored by an authorized user. This can be achieved by using hashing at both sides the sender and the recipient in order to create a unique message digest and compare it with the one that received.
4. Non-Repudiation: it is mechanism used to prove that the sender really sent this message, and the message was received by the specified party, so the recipient cannot claim that the message was not sent. For example, once an order is placed electronically, a purchaser cannot deny the purchase order, if non-repudiation service was enabled in this transaction.
5. Access Control: it is the process of preventing an unauthorized use of resources. This goal controls who can have access to the resources, If one can access, under which restrictions and conditions the access can be occurred, and what is the permission level of a given access.

Steganalysis- The process of detecting, presence of secret data in cover media.

Based on data security using compression and cryptography technique (2017) - Data is any type of stored digital information. Security is about the protection of assets. Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites. Cryptography is evergreen and developments. Cryptography protects users by providing functionality for the encryption of data and authentication of other users.

Based on Simple Substitution Ciphers - substitution cipher is a method of concealment that replaces each letter of a plaintext message with another letter. The key gives the correspondence between a plaintext letter and its replacement cipher text letter.

based on The DES Algorithm Illustrated - encryption (otherwise known as scrambling, enciphering or privacy transformation) represents the only means of protecting such data during transmission and a useful means of protecting the content of data stored on various media, providing encryption of adequate strength can be devised and validated and is inherently integral into system architecture.

Based on Cryptography Enabled Security Guarantees for over the Top Networks Using GSM Short Messaging Service -By defining a protocol for low-cost, pervasive, secure and reliable data communications, the scope and reach of M2M applications can be increased.

DEPARTMENT 301 BACHELOR OF SCIENCE IN ELECTRONICS AND COMMUNICATIONS ENGINEERING of lyceum - Files are treated as a valuable belonging of an individual so its security and safety is a must. Data encryption is another way of protecting data and it's already stepping through its way in the industry.

RIALTHO: Application of 512 Bit Block Size Using Encryption/Description Algorithm- This study adopts a symmetric-key cryptography that operates in block ciphers. The researchers of the study the block ciphers are slower if they contain big block size. The idea is to make a cryptographic algorithm that is time efficient while being big in terms of its block size.

Randomly Encryption Using Genetic Algorithm - a genetic algorithm utilized to establish an approach for random key to each letter in text massage encoding/ decoding. The test results indicated that using this approach achieved good performance to hide text massage that because choosing random key by genetic algorithm gives the approach difficulties that cannot easily discover or break the key.

Steganography

Steganography is the art of hiding information from sight by embedding it in a file such as a picture, steganography is data hidden within data and an encryption technique that can be used together with cryptography to protect data, both steganography and cryptography has a different approach. The goal of cryptography is to make data unreadable by a third party, steganography is concerned with hiding data from third parties. Steganography techniques are often used with images, video files, and audio files.

Based on Neural Information Processing Systems, NIPS (2017)- Steganography is the practice of concealing a secret message within another ordinary, message. Commonly steganography is used to unobtrusively hide a small message within the noisy regions of a larger image.

According to Kumar, A. And Pooja, K. (2010) *-* Steganography is the art of hiding information and an effort to conceal the existence of the embedded information. It serves as a better way of securing message than cryptography which only conceals the content of the message not the existence of the message. Original message is being hidden within a carrier such that the changes so occurred in the carrier are not observable.

According to Merill, K., Ernest, B., and Mark B. S.(2008) *-* Steganography has long been regarded as a tool used for illicit and destructive purposes such as crime and warfare. Currently, digital tools are widely available to ordinary computer users also. Steganography software allows both illicit and legitimate users to hide messages so that they will not be detected in transit. This article provides a brief history of steganography, discusses the current status in the computer age, and relates this to forensic, security, and legal issues. The paper concludes with recommendations for digital forensics investigators, IT staff, individual users, and other stakeholders.

Based On The Limits of Steganography (1998) - Classical steganography concerns itself with ways of embedding a secret message in a cover message.

Edge-based image steganography (2014) - uses edges in the cover image to embed messages. Amount of data to be embedded plays an important role on selecting edges

Based on Digital Image Steganography Survey and Analysis of Current Methods (2016) – there are two kinds of image steganographic domains, Spatial and Frequency domains. Spatial domain embedding is based on physic allocation of pixels in an image. Here the LSB’s if the cover medium is replaced by secret bits. It is a simple method for data embedding but cannot withstand or resist attacks like transforms or compression but their payload is high. Conversely in transform domain method, the medium is manipulated indirectly and the image is transformed into its frequency domain.

Based on Comparison of LSB Steganography in GIF and BMP Images (2013) - They are Advantages of using LSB,

1. Major advantage of the LSB algorithm is it is quick and easy.
2. There has also been steganography software developed which work around LSB color alterations via palette manipulation.
3. LSB insertion also works well with gray-scale images.

Based on An Overview on Audio Steganography Techniques (2012) - Audio Least Significant Bit (LSB) steganography takes advantage of the quantization error that usually derives from the task of digitizing the audio signal. As the name states, the information is encoded into the right most bits per samples or least significant bits from audio data. Ideally, the embedding capacity of an audio file with this method is 1 kbps per 1 kHz of sampled data. That is, if a file is sampled at 44 kHz then it is possible to embed 44 kilobits on each second of audio.

Based on A Study on Video Steganographic Techniques (2015) - there are various steganography techniques using video

A. LSB (Least Significant Bit) method LSB Is said to be the best method for data protection because of its simplicity and commonly used approach. It is the most easiest and effective way of embedding data. In LSB, the cover video’s pixel values are extracted which are in bytes, then its LSB are substituted by the bits of the secret message. Now since changing only the LSB bits of the host video, it doesn’t get distorted and almost looks alike as the original video.

B. Non-uniform rectangular partition

This method is for uncompressed videos. In non-uniform rectangular partition, data hiding is done by hiding an uncompressed secret video file in the host video stream. But we have to make sure that both the secret as well as the cover file should be of almost the same size. Each of the frames of both the secret as well as cover videos is applied with image steganography with some technique. The secret video file will be hidden in the leftmost four least significant bits of the frames of the host video.

C. Compressed video steganography

This method is done entirely on the compressed domain. Data can be embedded in the block of I frame with maximum scene change and in P and B block with maximum magnitude of motion vectors. The AVC encoding technique yields the maximum compressing efficiency.

D. Anti-forensics technique

Anti-forensic techniques are actions taken to destroy, hide and/or manipulate the data to attack the computer forensics. Anti-forensic provides security by preventing unauthorized access, but can also be used for criminal use also. Steganography is a kind of anti- forensic where we try to hide data under some host file. Steganography along with anti- forensics makes the system more secure.

E. Masking and filtering

Masking and filtering are used on 24 bits/pixel -images and are applicable for both colored and gray scale images. It is like watermarking over an image and doesn’t affect the quality of that image. Unlike other steganography techniques, in data masking the secret message is so processed such that it appears similar to a multimedia file. Data masking cannot easily be detected by traditional steganalysis.

Based on a secure data hiding technique using video steganography - the common term which is necessary to understand any steganography system.

Cover Media- It is the medium in which secret information is embedded in such a way that it is difficult to detect the presence of data.

Stego- Media- It is medium obtained after embedding the secret information.

Secret data- The data or information to be hidden in cover media.

Digital signal encoding and decoding apparatus - Digital data is conveyed along with the analog signal by selectively quantizing the analog signal in response to the level of each of the digital bits to be sent. By determining which quantization function was used, a decoder may recover the embedded digital data.

Based on Embedded data glyph technology for hardcopy digital documents (1994) - Bitmap printing from digital sources is commonly termed "digital printing"; however, machine retrieval of information content from printed images is typically inaccurate and unreliable in terms of digital information systems standards. For example, good optical character recognition systems provide error rates on the order of 1%. In another example, digital color copying, the loss of information compared to the original digital print file is much higher. Fundamentally, hardcopy printed for the needs of human readers does not provide a reliable digital data channel. In this sense these hardcopies are analog rather than digital documents. Embedded data technologies provide the means for encoding and retrieving digital information marked on hardcopy documents; they enable reliable information exchange between paper and electronic domains.

Chameleon (2003) - Chameleon uses an adaptive encoding technique based on the concept presented by Yeuan-Kwen Lee and Ling-Hwei Chen in the paper "High Capacity Image Steganographic Model".

ADAPTIVE DIGITAL STEGANOGRAPHY FOR TRUE-COLOR BITMAPS - a new image steganography software was presented to answer the need for a software that makes optimum use of hiding space in an image without creating any visible distortions. Along with a highly secure method for randomized encoding, techniques for adaptive encoding were incorporated with the design of the software. These techniques include capacity evaluation minimum-error replacement and error diffusion

BRIEF HISTORY OF STEGANOGRAPHY

Ancient Greece and Rome

Steganography has a long history, going back to the ancient Greek and Roman civilizations. Herodotus, the Greek historian, reports how king Darius shaved the head of a prisoner and wrote a secret message on his scalp. After the hair grew back, the prisoner was sent to the king’s son-in-law Aristogoras in Miletus and effectively delivering the message undetected by the enemy. A less time- consuming method of delivering secret messages was used by a soldier named Demeratus who needed to send a message to Sparta that king Xerxes planned to invade Greece. Demeratus removed the wax from a writing tablet, wrote the message on the underlying wood, and re-applied the wax. Both examples explain why the word steganography is based on the Greek word for “covered writing” (steganos = unseen or hidden; graphia = writing): protection of the message is assured not through making the message undecipherable, but by hiding the existence of the message altogether. Sending undecipherable messages is the technique of cryptography (kryptos = hidden or secret), and both techniques are often used in conjunction. The Romans accomplished the goal of sending messages undetected by writing between the lines of innocuous documents with invisible ink made from fluids like milk, urine and fruit juices. When the document was heated, the invisible ink would darken and become visible.

Middle Ages

At the end of the Middle Ages, two authors produced seminal works on steganography. Johannes Trithemius (1462-1526) wrote the three volumes of Steganographia (ca. 1499) which superficially describe black magic, specifically using spirits to communicate over long distances. However, by deciphering the text with a simple substitution method, one can read treatises on both cryptography and steganography. More than a century later, Gaspari Schotti picked up where Trithemius left off and published Steganographia (1665), which focuses on techniques with text, invisible inks, and incorporating hidden messages in music.

More Recent History

In the mid-19th century, a global technology revolution dramatically altered information transmission speed so that what took days or weeks to convey (at the speed of ships and horses) could be achieved in minutes with the new telegraph. Almost immediately, businesses and individuals sought to conceal their true message from telegraph operators, especially when the messages might be sensitive or might convey strategic business information. Some messages were simply enciphered, but others were creatively disguised using various steganographic schemes to prevent telegraph operators from becoming suspicious. (Standage, 1999)

In the late 19th century, Lord Baden-Powell was employed as a scout by the British army. To hide his drawings of positions of Boer artillery bases, he hid maps in drawings of butterflies. Certain markings on the wings of the butterflies were actually enemy installation positions. Thus, he would not be suspected even if he were caught. Hiding messages was further perfected by the German invention of the microdot, where photographs the size of printed periods contain images of standard size pages. FBI Director J. Edgar Hoover labelled this as “the enemy’s masterpiece of espionage.” Other advancements during World War I included the advent of null ciphers, where unencrypted messages about ordinary events contain hidden messages. For instance, the following message sent by the German embassy in Washington, DC, to their headquarters in Berlin “Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suet’s and vegetable oils” can be decoded by taking the second letter of each word, and results in “Pershing sails from NY June 1”. (Kahn, 1996) As evidenced by comparing the message sizes, this technique was relatively inefficient. Additionally, some of these messages are nonsensical, and therefore may raise suspicions.

Computer Age

The advent of the digital computer has introduced new opportunities for hiding messages, but also new challenges for forensic investigation. International workshops on information hiding and steganography have been held regularly since 1996 (Moulin and O’Sullivan, 2003), however, the majority of development and use of computerized steganography has occurred since 2000 (Cole, 2003). The use of steganography is now well within the reach of an average person with a computer and an Internet connection (Bartlett, 2003), and the most recent development is the potential use of steganography in Internet Telephony systems such as Skype (Mazurczyk and Szczypiorski, 2008).

## AVI and its File Structure

The AVI is a media file format created by Microsoft built to play video files, used to format of video distribution, AVI files includes video and audio data from its container and support audio-video synchronization, The AVI container formats derives from RIFF, RIFF stands for Resource interchange file format. The RIFF was created to store multimedia, unlike MOV and MPEG, AVI is less compressed with larger file size.

The AVI file format can be encoded with different types of codecs like the DivX and

XviD to achieve high quality of audio and video with satisfying compression so that it

can make promos, short videos and many others.

FOURCC

The Four-character codes or FOURCC is a set of codes that are four characters in length hence the name, it was introduced by Microsoft to identify video data stream formats, data chunks, index entries and other information more clearly, the unique FOURCC value assigned to every compression format and pixel layout allows video frames to be passed between file and codec by ensuring the FOURCC of the source frame matches a FOURCC supported by the codec, FOURCCs describe the software technology that was used to produce multimedia data.

AVI RIFF File Structure

One of Microsoft’s AVI file format, the RIFF is a file specification used with applications that can capture, edit and play back audio-video sequences. To put it simply, AVI files contain multiple streams from different types of data. Most of AVI’s sequences use both audio and video streams; some variations of an AVI sequence can use video data without an audio stream.

RIFF chunk format

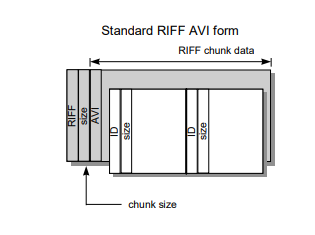


Figure 1 “Standard AVI RIFF form”

An AVI file begins as a standard RIFF chunk, there is only one RIFF chunk per file, RIFF sub chunks may be either LIST chunks or regular sub-chunks. LIST chunks obey the same structure and may have regular or LIST sub-chunks, any other RIFF sub-chunks only have an ID identifier and a size; however these regular sub-chunks may not have sub-chunks.

RIFF file format implies a maximum chunk size of 4 GB due to the size being stored as a 32-bit value, however limitations to the RIFF parser code and MCIAVI limits the file to only 1 GB, At data rates of 10 MB/s, a 1 GB file will last less than 2 minutes.

An AVI file can be extended beyond 1 GB by adding more than one RIFF chunk at the same file, each chunk can have a maximum size of 1 GB, Standard AVI apps will see the first RIFF chunk as a standard AVI file, this chunk must be complete, Information that the file is extended over 1 GB should be placed in the Extended AVI header. All other AVI information should be stored in the first chunk so that may be accessible to all other applications

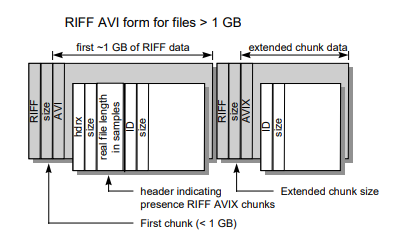


Figure 2 “RIFF AVI form using OpenDML”

AVI standard index chunk

The AVI standard index chunk contains information that indexes AVI frames

A single standard index chunk can only index data within a 4 GB region, the dwoffset field points to the start of the data itself, and not to the start of the RIFF chunk for that field.

AVI Field Index chunk

The AVI field index Chunk is the same as the standard index chunk except that it contains the locations of each field in the same frame

## OpenDML

OpenDML is a more advanced AVI file format which supports AVI files larger then 2GB, it is used to specify multiple RIFF chunks that bring the capacity to whatever level, The file system supports one that STFS can carry AVI files that reach 32 Terabytes added RIFF chunks are tagged as AVIX

## Video Codecs

In Video Computing, The file extension of a video file only defines what container is used to hold the media information of a certain video including the video and audio streams. Codecs are used to encode the video stream. It can either be uncompressed or compressed. There are various codecs used in an AVI file. They can be lossless h.264, Cinepak, XVID, Theora, or a raw RGB or YUV video codecs.

## Raw Video

Raw video codecs encodes the video with no compression applied. Video containers using this codec will have a large storage space occupied due to it encodes all video information signals from the camera. The information can be encoded as raw RGB or YUV colour space.

## RGB VS YUV

RGB color is a color encoder using red, green and blue as values. These values correspond directly to portions of the visible spectrum. The three values form a mathematical coordinate system called a color space, the red component defines an axis of the system; blue is second and green is third, any valid RGB color falls somewhere within its color space. RGB is the common represent color, however other coordinate systems are possible, the YUV refers to a family of color spaces, it encodes brightness information separately from the color information. YUV uses three values to represent color same way as RGB, The Y component is called Luma, it represents the brightness value of the color, YUV color spaces always use luma, Luma is derived from an RGB color by taking a weighted average of red, green and blue components. The U and V components are called chroma values or color difference values, derived by subtracting the Y value from the red and blue components of the original RGB color.

H.264/MPEG-4 part 10

This codec has high improvement and coding efficiency and error robustness besides the previous version of the codecs, it’s originally designed with video conferences and different old type of videos

It has built in high definition video rendering, however it can also format low quality videos for smaller devices making it able to be compatible for single standard codecs.

This codec is by far the most used throughout the world ranging all across the net and other sources.

Cinepak

Cinepak is one of the first video compression to allow full motion video on CD-ROMS, Cinepak uses 320x240 resolution video at 1x CD-ROM transfer rates, It’s one of the codecs that has been used to port CD-ROM’s for most game consoles, It was the main video codec for the early versions of Quicktime and Microsoft video for windows, however it was suspended by other codecs MPEG-4 was more viable, Cinepak may still be playable by most media players, it is based on vector quantization

XVID

Xvid is an open source video codec based on MPEG-4 for both Xvid and DivX, it was created to offer free alternative to the other video codecs, both DivX and Xvid was distributed differently, the Xvid codec may not be a video formatted but it’s a program used to compress and decompress videos to MPEG-4 as a compression standard to save on a disk space and file transfer speeds, Xvid supports new DVD players, it is possible to compress a full length DVD quality type of video or movie to fit on a single CD which sometimes require 2 CDs while still maintaining the original quality despite that it can offer higher quality videos at a smaller file size which take less time to encode than MPEG-2 Unlike any other codec Xvid is a free software available to anyone and is the most popular video codecs online, however it isn’t as used as DivX codecs.

Theora

Theora is a free lossy video compression format, developed by the Xiph.org foundation distributed alongside other free and open media projects, including the Vorbis audio format and the Ogg container

It is broadly comparable in design and bitrate efficiency to MPEG-4, earlier versions of Windows media video and Realvideo while lacking some of the features present in some of these codecs, it is comparable in open standards philosophy to the BBC’s Dirac codec. Theora functions like most other codecs like distributing film and videos online and on discs; this codec is in the same class as MPEG-4/DIVX.

Based on Steganography of Audio Files- With the fast paced development of the internet, exchanging or hiding of private data has become a serious concern. There are a number of solutions to counter this problem like cryptology and steganography. Steganography is the practice of hiding private or sensitive information within something that appears to be nothing out of the usual. The advantage of using steganography over cryptography is that in steganography the person looking at the object wherein information is hidden won’t be able to notice the information stashed there, therefore would not attempt to decrypt it.

TYPES OF IMAGE COMPRESSION

An image is a 2-D signal that is processed by human visual systems. These signals that are representing an image are commonly in the form of analog. Although for the storage, processing and the transmission through the computer applications, these signals needed to be converted from the analog form to their digital form. An image or a digital image is usually a 2-Dimensional array of the pixels. In the raw form, the images may cover a huge amount of the memory in the RAM and in the storage, both. Image compression is for reducing the redundancy and irrelevance of image/data to allow them to either store or transmit the data in a better way

Image compression can be further classified or divided in two separate types such as lossy compression and losslesscompression. In the lossy compression as its name indicated that it results in the loss of little information. In this technique the compressed image is same as to actual/original uncompressed image yet not exact to the previous one as within the compression process littler information related to the image has been lost. So they are normally applied for the photographs. The very natural example of the lossy compression is a JPEG. Where are in Lossless compression, it compresses an image by encoding it’s all information from the actual file, so in case if the image is get decompressed again, then it will be the exactly same as the actual image. For examples of the lossless technique of image compression are PNG and GIF i.e., GIF only provides 8-bit images. At the time of using a specific format of image compression that basically based on what is being get compressed.

LOSSLESS

Lossless In the technique of Lossless compression with the compressing of data that is when gets decompressed will be the same replica of actual data. In this case, when the binary data like the documents, executable etc. are get compressed. This required to be reproduced exactly when get decompressed again. On the contrary, the images and the music also required not to be generated 'exactly'. A resemblance of the actual image is sufficient for the most objective, as far as the error or problems between the actual and compressed image is avoidable or tolerable. These types of compression are also known as noiseless as they never add noise to signal or image. It is also termed as the entropy coding as it uses the techniques of decomposition/statistics to remove/reduce the redundancy. It is also used only for the some specific applications along with the rigid needs like a medical-imaging.

Below mentioned techniques consists in the lossless compression:

1. Huffman encoding
2. Run length encoding
3. Arithmetic coding
4. Dictionary Techniques

LOSSY

In the technique of Lossy compression, it decreases the bits by recognizing the not required information and by eliminating it.The system of decreasing the size of the file of data is commonly termed as the data-compression, though its formal name is the source-coding that is coding get done at source of data before it gets stored or sent. In these methods few loss of the information is acceptable. Dropping non-essential information from the source of data can save the storage area. The Lossy data-compression methods are aware by the researches on how the people anticipate data in the question. As an example, the human eye is very sensitive to slight variations in the luminance as compare that there are so many variations in the color. The Lossy image compression technique is used in the digital cameras, to raise the storage ability with the minimal decline of the quality of picture. Similarly in the DVDs which uses the lossy MPEG-2 Video codec technique for the compression of the video. In the lossy audio compression, the techniques of psycho acoustics have been used to eliminate the non-audible or less audible components of signal.

**According to Pope, M. et al.(2012)** *-* This article presents an overview of steganography's history and the categories of steganography methods, followed by a discussion of the application areas for steganography. It also present some technical details of the techniques and software for applying steganography, including some security-related attack issues.

Based on various image compressions - Image compression can be further classified or divided in two separate types such as lossy compression and lossless compression. In the lossy compression as its name indicated that it results in the loss of little information. In this technique the compressed image is same as to actual/original uncompressed image yet not exact to the previous one as within the compression process littler information related to the image has been lost. So they are normally applied for the photographs. The very natural example of the lossy compression is a JPEG. Where are in Lossless compression, it compresses an image by encoding it’s all information from the actual file, so in case if the image is get decompressed again, then it will be the exactly same as the actual image. For examples of the lossless technique of image compression are PNG and GIF i.e., GIF only provides 8-bit images. At the time of using a specific format of image compression that basically based on what is being get compressed. (Compression Article needed)

Image Steganography of Multiple File Types with Encryption and Compression Algorithms -accepts secret file and compress it using ZLIB algorithm then encrypt it using DES algorithm and then embed it to an cover image using LSB algorithm

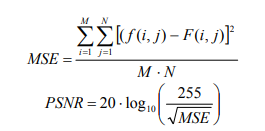
Software Dependent Image Data Compression using Multiple Encryption -An easy way to make the file smaller is to use data compression software that is both near-lossless and can provide a compression algorithm that can rival that of conventional compression algorithms like PNG and BMP. This will be done by compressing the picture based on its characteristic color.

PSNR

According to Yubing Wang in his “Survey of Objective Video Quality Measurements”

PSNR is derived by setting the mean squared error (MSE) in relation to the maximum

possible value of the luminance (for a typical 8-bit value this is -1 = 255) as

follows:

Where *f(i,j)* is the original signal at pixel *(i, j), F(i, j)* is the reconstructed signal, and

M x N is the picture size. The result is a single number in decibels, ranging from 30 to

40 for medium to high quality images.

He also states that despite several objective video quality models have been developed in the past two decades, PSNR continues to be the most popular evaluation of the quality difference among pictures.

PSNR is the most commonly used in image comparison due to its accessible to everyone and fast computation. It is express in decibels from 0dB(max difference) to infinitive(no difference).The higher the value of dB means the closer it gets to the reference input. Acceptable PSNR values for lossy compression in images and video frames are between 30 to 50dB.

Synthesis

It was stated that Cryptography’s only concern is hiding the contents of the file while steganography is concerned only of concealing the existence of secret message. This led the proponent’s development of a system with the combination of the two technologies to make a much better security. Like Chameleon and Image Steganography of Multiple File Types with Encryption and Compression Algorithms, it uses LSB algorithm to replace the LSB of the RGB values of the pixels inside the video frames to conceal the encrypted data of the user.

For the encryption, the proponents made a prototype encryption algorithm that uses arithmetic operation and logical operations to encode the data and theoretically prevent other LSB based steganography application from extracting the data.

# cuttlefish (A Prototype encryption algorithm with steganography)

## Overview of the project

The proponents researched about on how they can help the world of ICT in terms of data privacy. The proponents came up with this project because they saw that through this system, they can give user the privacy they want by hiding their confidential data on an innocent looking AVI video file. This is can be a major help contributing to confidential communication by sending innocent file to the receiver without anyone giving suspicion to the file. In respect to data policy act, the proponents do not encouraged user to use the system on illegal means.

The proposed system uses a created encryption algorithm as an encoder and decoder of embedded file. In this way, only the proposed system can only decode the embedded file back to its original form if the same system is used to embed the data from the cover video. The system also uses LSB algorithm for embedding the encoded file in RGB 24-bit AVI video file.

## System design specification

Methodology

Prototype model is commonly used in projects that aim to refine the existing system. In this model, the proponents build new system based on the existing one then let the user test and evaluate it. After evaluation, if the prototype is acceptable then it undergoes refinement for polishing and make the final product else rework until an acceptable model is finally achieves.

The perceived advantage of prototyping is refinement that allows improvements of the existing system.

The proponents choose this methodology simply because of its refinement capability to the existing system and user’s involvement. The proponents make sure that it satisfies the user and noticeable improvement versus the existing system.

Final Product

Refinement

Quick Design

Requirements gathering

User Evaluation

Building the Prototype

Figure 3 “Prototype model”

Quick Design

The proponents will design prototype model based one the information they gather from the first phase

Building the Prototype

The Proponents will construct the first prototype based from the design they made during the design phase

User Evaluation

The user now tests the model for errors, bugs, ease of use and overall performance. User will grade the system based on either their own checklist or the master checklist the proponents provided. Depending on the results, the model will undergo refinement to fix unnecessary behaviors.

Refinement

The prototype model will now undergo refinement. In this phase, the proponent will fix unnecessary behaviors and go back the design phase if necessary.

Final Product

The final system is now a finished product and is ready for use by the targeted customers.

Hardware/Software Requirements

This software can run in a common low-end computer with windows operating system. The ideal Requirements for this software as follows:

Hardware:

* Intel i3 2nd gen or higher processor
* 2 GB of RAM as minimum. 4 GB of RAM is recommended
* At least 20MB of memory space for the executable file.

Software

* Microsoft .Net Framework 4.5 or above
* Windows 7 or above

System flowchart

This show how the system operates using a representation on how the system interact with each variables and processes using a flowchart

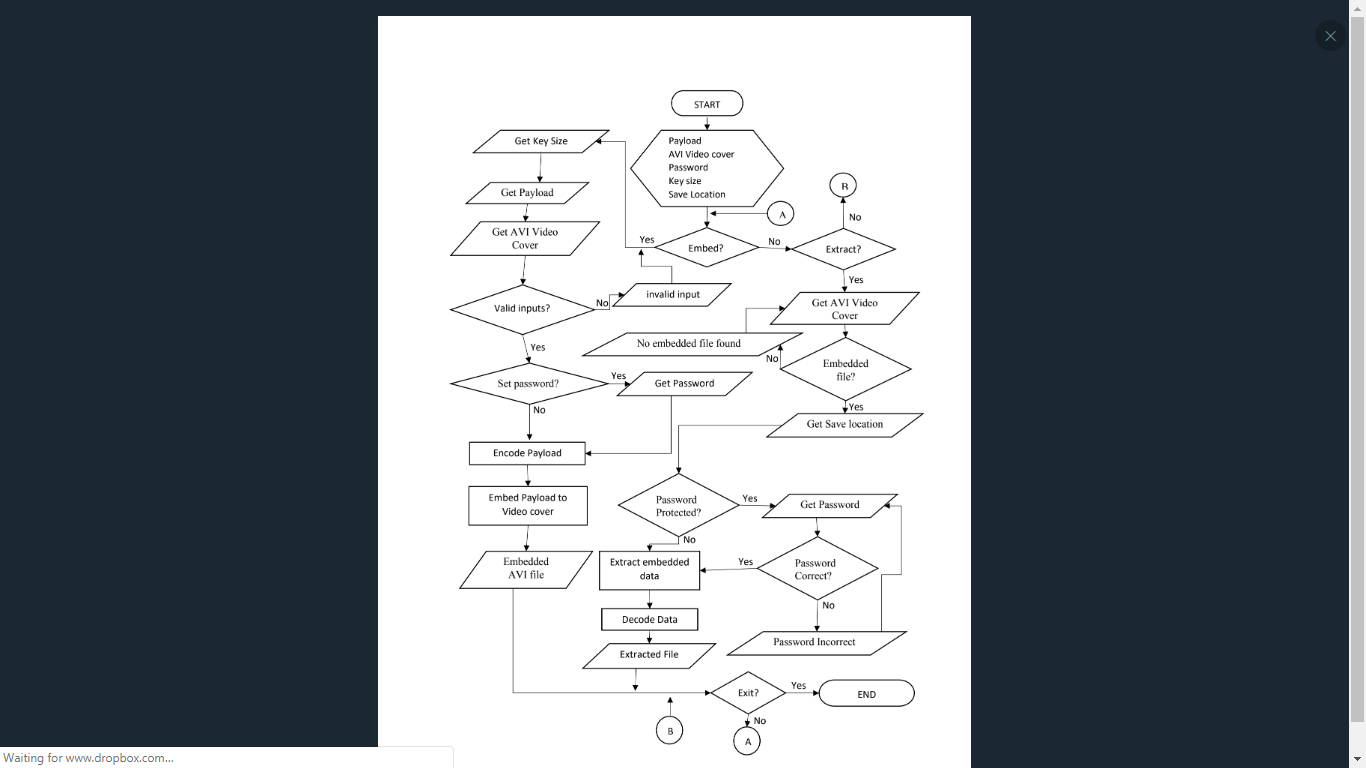


Figure 4 “The Proposed System Flowchart”

Method used in Cuttlefish

Encryption

Encryption is vital in the proposed system. It encodes data into unreadable cipher text that will be the embedded in the cover video. It uses 16-bit or 128-bit as a key to encrypt the data.

Algorithm for 16-bit encryption

Here are the steps on how the proposed system encrypts data using 16-bit encryption

1. Generate 16 bit key and max repeat count
2. If the size of plaintext is odd then add one byte to the end of the plaintext
3. Divide plaintext into 1x2 blocks
4. Swap each data of each block
5. Subtract key to each block
6. Check how many times repeated
7. If repeat count is even then each byte of the block is equal to itself XOR to the XOR of first byte of the key plus repeat count and second byte of the key minus repeat count. If repeat count is odd then each byte of the block is equal to itself XOR to the XOR of first byte of the key minus repeat count and second byte of the key plus repeat count.
8. Repeat if repeat count is not equal to max repeat count
9. To decrypt, reverse the process.

Algorithm for 128-bit key encryption

1. Generate 128 bit key
2. Divide plaintext into 4x4 blocks if some parts cannot be converted to 4x4 then convert it to linear array instead.
3. If the next block is a linear array, proceed to step 8

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. Do a gear like shift by moving the data from outer circle counter clockwise and inner circle clockwise

Figure 5 “gear like shift”

1. Send the first row to the last row of the block
2. Send the first column to the last column of the block
3. Subtract and XOR the block to the key.
4. If the block is a linear array, Send the first byte of the linear array to its last part. Else proceed to step 10.
5. Subtract and XOR the array to the key
6. Proceed to the next block and go back to step 2 until no blocks is left.
7. To decrypt, reverse the process.

CBC block cipher algorithm.

We only use on 16-bit encryption algorithm. To avoid patterns on identical blocks, the proposed system uses CBC block cipher algorithm without the presence of initializing vector (IV) in addition to encryption algorithm. The plaintext will be XORed to the recent cipher block if any present

Modified CBC block cipher algorithm.

We only use on 128-bit encryption algorithm. To avoid patterns on identical blocks, the proposed system uses a modified CBC block cipher algorithm without the presence of initializing vector (IV) in addition to encryption algorithm. Before the plaintext will be XOR to the recent cipher block, the encryption key will undergo a key scrambling algorithm to avoid repetition of using the same key to each block improving resistance against cryptanalysis.

Key scrambling algorithm

The key will undergo scrambling algorithm. the sequence of scrambling is like in the scrambling used on the 128-bit encryption algorithm namely gear like shift, send the first row to last row, and send the first column to last column except instead of doing it all at once it does one each on each block it passes.

Password Protection

To protect encoded data from any potential other users of the system from extraction of the secret data. The system can use password as a layer to protect the data. The password set by the user will be included in the final step of the encryption algorithm by simply XORing the every byte of the password to each block

LSB algorithm.

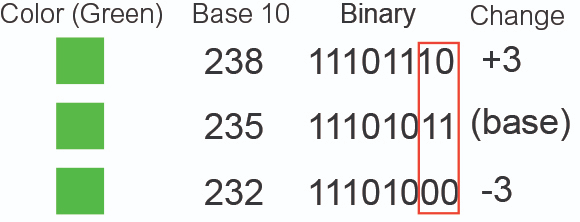
To hide encoded data on a video cover, the proposed system will hide data on last 2 bits of every color information’s stored in a pixel.

Figure 6 “changes on color green when modifying its LSB”

# Results and Discussions

This research presents the experiment conducted by the proponents. Experiment is the testing of an idea with the goal to verify, falsify, or establish its validity using a series of inputs and outputs. In this study, the proposed system developed by the proponents is evaluated.

The proponents prepared nine different file types to be used in the proposed system. These files will served as payload data for the system to be embed in the video cover and extract it after.

Data File Used as Payload Data

|  |  |
| --- | --- |
| ACCOMPLISH AND CONSULTATION FORM.docx | 15.33 KB |
| Attachments B\_OJT Training Plan Template.xls | 50.00 KB |
| Attachments G\_Daily Time Record.pdf | 88.59 KB |
| Chrysanthemum.jpg | 858.78 KB |
| Exorciser.jar | 2.46 KB |
| My night.mp3 | 6.64 KB |
| OJT-Copy-for-students.zip | 237.93 KB |
| Watch No Game No Life Episode 1 English Sub.mp4 | 50.59 KB |
| No Game No Life Opening Full.flac | 51.21 KB |

Table 1 - test data table

The proponents then prepared two different AVI files with different frame dimension to be used as video cover.

AVI File Used as Video Cover for Test Result 1.

|  |  |
| --- | --- |
| Video Cover : | 1080p(8 sec).avi |
| Capacity: | 123.99 MB |
| Codec: | RGB 24 bit |

|  |  |
| --- | --- |
| Video Cover : | 360p (7 sec).avi |
| Capacity: | 9.60 MB |
| Codec: | RGB 24 bit |

Table 2 - Video Cover 1 information Table 3 – Video Cover 2 information

Table Legend

IDENTICAL – Extracted File is identical to source payload file

CORRUPTED - Extracted File is not identical to source file or unreadable.

Test Results for “ACCOMPLISHMENT AND COSULTAION FORM.docx” using Video Cover 1 and different key size.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Test # | Filename | Key Size | Time Elapsed | | Extracted File Condition |
| Embedding | Extracting |
| 1 | ACCOMPLISHMENT AND COSULTAION FORM.docx | 16 bit | 00:00:00:1872 | 00:00:00:4427 | IDENTICAL |
| 2 | ACCOMPLISHMENT AND COSULTAION FORM.docx | 128 bit | 00:00:00:1827 | 00:00:00:4539 | IDENTICAL |

Table 4 – Test results for ACCOMPLISHMENT AND CONSULTATION FORM.docx

PSNR Results of all frames using different key sizes

|  |  |  |  |
| --- | --- | --- | --- |
| FRAME | PSNR R | PSNR G | PSNR B |
| 1 | 48.73 | 48.66 | 48.61 |
| 2 - 233 | INF | INF | INF |

|  |  |  |  |
| --- | --- | --- | --- |
| frame | PSNR R | PSNR G | PSNR B |
| 1 | 48.68 | 48.64 | 48.67 |
| 2 -233 | INF | INF | INF |

# 

Table 5 – PSNR results of test 1 Table 6 – PSNR results of test 2

Test Results for “Attachment B\_OJT Training Plan Template.xls” using video cover 1 and different key size.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Test # | Filename | Key Size | Time Elapsed | | Extracted File Condition |
| Embedding | Extracting |
| 3 | Attachment B\_OJT Training Plan Template.xls | 16 bit | 00:00:00:3074 | 00:00:00:6638 | IDENTICAL |
| 4 | Attachment B\_OJT Training Plan Template.xls | 128 bit | 00:00:00:3421 | 00:00:00:6639 | IDENTICAL |

Table 7 – Test results for Attachment B\_OJT Training Plan Template.xls

PSNR Results of all frames using different key sizes

|  |  |  |  |
| --- | --- | --- | --- |
| FRAME | PSNR R | PSNR G | PSNR B |
| 1 | 44.19 | 44.19 | 44.19 |
| 2 | 51.48 | 51.50 | 51.39 |
| 3 - 233 | INF | INF | INF |

|  |  |  |  |
| --- | --- | --- | --- |
| FRAME | PSNR R | PSNR G | PSNR B |
| 1-233 | INF | INF | INF |

|  |  |
| --- | --- |
| Table 8 – PSNR result of test 3. | Table 9 – PSNR result of test 4. |

Test Results for “Attachment G\_Daily Time Record.pdf” video cover using different key size.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Test # | Filename | Key Size | Time Elapsed | | Extracted File Condition |
| Embedding | Extracting |
| 5 | Attachment G\_Daily Time Record.pdf | 16 bit | 00:00:00:4100 | 00:00:00:7790 | IDENTICAL |
| 6 | Attachment G\_Daily Time Record.pdf | 128 bit | 00:00:00:4000 | 00:00:00:7979 | IDENTICAL |

Table 10 – Test results for Attachment G\_Daily Time Record.pdf

PSNR Results of all frames using different key sizes

|  |  |  |  |
| --- | --- | --- | --- |
| FRAME | PSNR R | PSNR G | PSNR B |
| 1 | 44.17 | 44.17 | 44.19 |
| 2 | 44.11 | 44.15 | 44.10 |
| 3 | 54.21 | 54.12 | 54.26 |
| 4 – 233 | INF | INF | INF |

|  |  |  |  |
| --- | --- | --- | --- |
| FRAME | PSNR R | PSNR G | PSNR B |
| 1 | 44.17 | 44.19 | 44.17 |
| 2 | 44.13 | 44.14 | 44.13 |
| 3 | 54.10 | 54.09 | 54.11 |
| 4 - 233 | INF | INF | INF |

|  |  |
| --- | --- |
| Table 11 – PSNR result of test 5. | Table 12 – PSNR result of test 6. |

Test Results for “Chrysanthemum.jpg” using video cover and different key size.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Test # | Filename | Key Size | Time Elapsed | | Extracted File Condition |
| Embedding | Extracting |
| 7 | Chrysanthemum.jpg | 16 bit | 00:00:02:8425 | 00:00:03:2099 | IDENTICAL |
| 8 | Chrysanthemum.jpg | 128 bit | 00:00:02:9827 | 00:00:03:3741 | IDENTICAL |

Table 13 – Test results for Attachment G\_Daily Time Record.pdf

PSNR Results of all frames using different key sizes.

|  |  |  |  |
| --- | --- | --- | --- |
| Frame | PSNR R | PSNR G | PSNR B |
| 1 | 44.19 | 44.19 | 44.19 |
| 2 | 44.15 | 44.16 | 44.14 |
| 3 | 44.18 | 44.17 | 44.18 |
| 4 | 44.14 | 44.13 | 44.13 |
| 5 | 44.17 | 44.12 | 44.13 |
| 6 | 44.16 | 44.15 | 44.16 |
| 7 | 44.14 | 44.16 | 44.12 |
| 8 | 44.11 | 44.15 | 44.10 |
| 9 | 44.13 | 44.12 | 44.11 |
| 10 | 44.15 | 44.15 | 44.13 |
| 11 | 44.16 | 44.16 | 44.15 |
| 12 | 44.17 | 44.15 | 44.17 |
| 13 | 44.16 | 44.18 | 44.15 |
| 14 | 44.13 | 44.19 | 44.11 |
| 15 | 44.12 | 44.18 | 44.11 |
| 16 | 44.15 | 44.15 | 44.19 |
| 17 | 44.11 | 44.17 | 44.15 |
| 18 | 44.16 | 44.15 | 44.14 |
| 19 | 44.18 | 44.15 | 44.16 |
| 20 | 44.12 | 44.17 | 44.13 |
| 21 | 48.70 | 48.58 | 48.67 |
| 22-233 | Inf | Inf | Inf |

|  |  |  |  |
| --- | --- | --- | --- |
| Frame | PSNR R | PSNR G | PSNR B |
| 1 | 44.18 | 44.19 | 44.19 |
| 2 | 44.16 | 44.11 | 44.14 |
| 3 | 44.15 | 44.13 | 44.14 |
| 4 | 44.14 | 44.15 | 44.14 |
| 5 | 44.14 | 44.14 | 44.14 |
| 6 | 44.19 | 44.12 | 44.19 |
| 7 | 44.09 | 44.13 | 44.13 |
| 8 | 44.17 | 44.12 | 44.12 |
| 9 | 44.16 | 44.13 | 44.16 |
| 10 | 44.14 | 44.16 | 44.10 |
| 11 | 44.19 | 44.16 | 44.14 |
| 12 | 44.16 | 44.17 | 44.18 |
| 13 | 44.13 | 44.13 | 44.18 |
| 14 | 44.17 | 44.14 | 44.14 |
| 15 | 44.14 | 44.12 | 44.15 |
| 16 | 44.15 | 44.14 | 44.18 |
| 17 | 44.11 | 44.13 | 44.15 |
| 18 | 44.16 | 44.13 | 44.13 |
| 19 | 44.16 | 44.16 | 44.14 |
| 20 | 44.16 | 44.17 | 44.15 |
| 21 | 48.62 | 48.56 | 48.67 |
| 22-233 | inf | Inf | Inf |

# 

# 

Table 14 – PSNR result of test 7. Table 15 – PSNR result of test 8.

Test Results for “exorciser.jar” using video cover and different key size.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Test # | Filename | Key Size | Time Elapsed | | Extracted File Condition |
| Embedding | Extracting |
| 9 | exorciser.jar | 16 bit | 00:00:08:0699 | 00:00:08:4670 | IDENTICAL |
| 10 | exorciser.jar | 128 bit | 00:00:08:3402 | 00:00:08:9670 | IDENTICAL |

Table 16 – Test results for exorciser.jar

PSNR Results of all frames using different key sizes

| Frame | PSNR R | PSNR G | PSNR B |
| --- | --- | --- | --- |
| 1 | 44.18 | 44.17 | 44.20 |
| 2 | 44.10 | 44.14 | 44.12 |
| 3 | 44.15 | 44.16 | 44.18 |
| 4 | 44.16 | 44.15 | 44.12 |
| 5 | 44.14 | 44.13 | 44.14 |
| 6 | 44.15 | 44.12 | 44.15 |
| 7 | 44.12 | 44.14 | 44.14 |
| 8 | 44.14 | 44.18 | 44.13 |
| 9 | 44.11 | 44.18 | 44.13 |
| 10 | 44.11 | 44.14 | 44.11 |
| 11 | 44.19 | 44.19 | 44.16 |
| 12 | 44.15 | 44.18 | 44.18 |
| 13 | 44.16 | 44.15 | 44.13 |
| 14 | 44.13 | 44.11 | 44.14 |
| 15 | 44.17 | 44.15 | 44.19 |
| 16 | 44.18 | 44.14 | 44.15 |
| 17 | 44.14 | 44.14 | 44.14 |
| 18 | 44.15 | 44.14 | 44.15 |
| 19 | 44.16 | 44.17 | 44.15 |
| 20 | 44.16 | 44.14 | 44.13 |
| 21 | 44.14 | 44.14 | 44.17 |
| 22 | 44.15 | 44.15 | 44.17 |
| 23 | 44.14 | 44.16 | 44.12 |
| 24 | 44.14 | 44.12 | 44.13 |
| 25 | 44.15 | 44.16 | 44.13 |
| 26 | 44.17 | 44.12 | 44.15 |
| 27 | 44.15 | 44.13 | 44.15 |
| 28 | 44.11 | 44.15 | 44.15 |
| 29 | 44.14 | 44.13 | 44.15 |
| 30 | 44.14 | 44.14 | 44.11 |
| 31 | 44.16 | 44.12 | 44.17 |
| 32 | 44.13 | 44.14 | 44.15 |
| 33 | 44.11 | 44.13 | 44.17 |
| 34 | 44.14 | 44.15 | 44.14 |
| 35 | 44.17 | 44.16 | 44.14 |
| 36 | 44.15 | 44.16 | 44.16 |
| 37 | 44.16 | 44.17 | 44.19 |
| 38 | 44.15 | 44.10 | 44.13 |
| 39 | 44.12 | 44.16 | 44.15 |
| 40 | 44.12 | 44.17 | 44.14 |
| 41 | 44.12 | 44.15 | 44.16 |
| 42 | 44.15 | 44.14 | 44.14 |
| 43 | 44.14 | 44.17 | 44.22 |
| 44 | 44.16 | 44.17 | 44.16 |
| 45 | 44.15 | 44.14 | 44.15 |
| 46 | 44.16 | 44.17 | 44.16 |
| 47 | 44.13 | 44.15 | 44.13 |
| 48 | 44.10 | 44.15 | 44.12 |
| 49 | 44.15 | 44.13 | 44.14 |
| 50 | 44.14 | 44.14 | 44.12 |
| 51 | 44.12 | 44.17 | 44.17 |
| 52 | 44.15 | 44.14 | 44.17 |
| 53 | 44.20 | 44.16 | 44.16 |
| 54 | 44.15 | 44.14 | 44.12 |
| 55 | 44.14 | 44.16 | 44.18 |
| 56 | 44.15 | 44.14 | 44.11 |
| 57 | 44.14 | 44.12 | 44.12 |
| 58 | 44.11 | 44.13 | 44.17 |
| 59 | 44.96 | 44.01 | 43.99 |
| 60 | 45.98 | 45.86 | 45.89 |
| 61-233 | inf | inf | inf |

Table 17 – PSNR result of test 9

|  |
| --- |
|  |

| Frame | PSNR R | PSNR G | PSNR B |
| --- | --- | --- | --- |
| 1 | 44.20 | 44.17 | 44.21 |
| 2 | 44.14 | 44.15 | 44.13 |
| 3 | 44.14 | 44.18 | 44.17 |
| 4 | 44.16 | 44.16 | 44.17 |
| 5 | 44.14 | 44.18 | 44.16 |
| 6 | 44.17 | 44.15 | 44.13 |
| 7 | 44.13 | 44.12 | 44.14 |
| 8 | 44.12 | 44.16 | 44.12 |
| 9 | 44.17 | 44.13 | 44.13 |
| 10 | 44.12 | 44.13 | 44.12 |
| 11 | 44.12 | 44.15 | 44.16 |
| 12 | 44.19 | 44.20 | 44.17 |
| 13 | 44.15 | 44.13 | 44.15 |
| 14 | 44.13 | 44.13 | 44.17 |
| 15 | 44.14 | 44.12 | 44.15 |
| 16 | 44.17 | 44.15 | 44.14 |
| 17 | 44.12 | 44.16 | 44.14 |
| 18 | 44.14 | 44.13 | 44.19 |
| 19 | 44.15 | 44.12 | 44.16 |
| 20 | 44.13 | 44.12 | 44.17 |
| 21 | 44.13 | 44.14 | 44.15 |
| 22 | 44.15 | 44.12 | 44.17 |
| 23 | 44.19 | 44.16 | 44.15 |
| 24 | 44.16 | 44.15 | 44.22 |
| 25 | 44.18 | 44.19 | 44.19 |
| 26 | 44.15 | 44.17 | 44.16 |
| 27 | 44.18 | 44.13 | 44.17 |
| 28 | 44.18 | 44.13 | 44.13 |
| 29 | 44.17 | 44.18 | 44.12 |
| 30 | 44.17 | 44.17 | 44.17 |
| 31 | 44.14 | 44.16 | 44.15 |
| 32 | 44.10 | 44.18 | 44.13 |
| 33 | 44.17 | 44.10 | 44.16 |
| 34 | 44.16 | 44.19 | 44.14 |
| 35 | 44.18 | 44.19 | 44.16 |
| 36 | 44.16 | 44.17 | 44.15 |
| 37 | 44.16 | 44.15 | 44.16 |
| 38 | 44.16 | 44.17 | 44.13 |
| 39 | 44.13 | 44.13 | 44.16 |
| 40 | 44.17 | 44.19 | 44.12 |
| 41 | 44.16 | 44.18 | 44.18 |
| 42 | 44.15 | 44.12 | 44.16 |
| 43 | 44.16 | 44.16 | 44.17 |
| 44 | 44.19 | 44.17 | 44.16 |
| 45 | 44.16 | 44.17 | 44.18 |
| 46 | 44.14 | 44.17 | 44.16 |
| 47 | 44.15 | 44.14 | 44.15 |
| 48 | 44.12 | 44.15 | 44.16 |
| 49 | 44.15 | 44.17 | 44.16 |
| 50 | 44.15 | 44.12 | 44.15 |
| 51 | 44.15 | 44.14 | 44.12 |
| 52 | 44.12 | 44.13 | 44.16 |
| 53 | 44.15 | 44.19 | 44.13 |
| 54 | 44.14 | 44.18 | 44.13 |
| 55 | 44.15 | 44.13 | 44.13 |
| 56 | 44.14 | 44.15 | 44.16 |
| 57 | 44.12 | 44.13 | 44.12 |
| 58 | 44.15 | 44.14 | 44.12 |
| 59 | 43.96 | 44.00 | 43.96 |
| 60 | 45.90 | 45.91 | 45.91 |
| 61-233 | inf | inf | inf |

Table 18 – PSNR result of test 10.

Table 18 – PSNR result of test 10

Test Results for “my night.mp3” using video cover 1 and different key size.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Test # | Filename | Key Size | Time Elapsed | | Extracted File Condition |
| Embedding | Extracting |
| 11 | my night.mp3 | 16 bit | 00:00:21:5132 | 00:00:22:3965 | IDENTICAL |
| 12 | my night.mp3 | 128 bit | 00:00:22:1992 | 00:00:23:5961 | IDENTICAL |

Table 19 – Test results for my night.mp3

PSNR Results of all frames using different key sizes.

| Frame | PSNR R | PSNR G | PSNR B |
| --- | --- | --- | --- |
| 1 | 44.22 | 44.18 | 44.19 |
| 2 | 44.13 | 44.11 | 44.12 |
| 3 | 44.14 | 44.13 | 44.12 |
| 4 | 44.11 | 44.14 | 44.16 |
| 5 | 44.14 | 44.12 | 44.19 |
| 6 | 44.13 | 44.15 | 44.20 |
| 7 | 44.11 | 44.15 | 44.13 |
| 8 | 44.16 | 44.13 | 44.15 |
| 9 | 44.17 | 44.17 | 44.15 |
| 10 | 44.12 | 44.09 | 44.14 |
| 11 | 44.14 | 44.16 | 44.12 |
| 12 | 44.12 | 44.16 | 44.12 |
| 13 | 44.14 | 44.16 | 44.19 |
| 14 | 44.12 | 44.16 | 44.14 |
| 15 | 44.18 | 44.15 | 44.13 |
| 16 | 44.16 | 44.15 | 44.19 |
| 17 | 44.13 | 44.17 | 44.13 |
| 18 | 44.13 | 44.13 | 44.12 |
| 19 | 44.13 | 44.13 | 44.16 |
| 20 | 44.13 | 44.15 | 44.12 |
| 21 | 44.14 | 44.14 | 44.19 |
| 22 | 44.17 | 44.14 | 44.15 |
| 23 | 44.19 | 44.17 | 44.12 |
| 24 | 44.14 | 44.14 | 44.13 |
| 25 | 44.17 | 44.17 | 44.16 |
| 26 | 44.14 | 44.13 | 44.14 |
| 27 | 44.18 | 44.18 | 44.13 |
| 28 | 44.11 | 44.14 | 44.12 |
| 29 | 44.15 | 44.18 | 44.17 |
| 30 | 44.14 | 44.15 | 44.15 |
| 31 | 44.16 | 44.15 | 44.17 |
| 32 | 44.14 | 44.15 | 44.15 |
| 33 | 44.10 | 44.14 | 44.13 |
| 34 | 44.13 | 44.15 | 44.13 |
| 35 | 44.18 | 44.16 | 44.17 |
| 36 | 44.17 | 44.18 | 44.16 |
| 37 | 44.16 | 44.15 | 44.15 |
| 38 | 44.16 | 44.15 | 44.14 |
| 39 | 44.17 | 44.17 | 44.18 |
| 40 | 44.15 | 44.16 | 44.14 |
| 41 | 44.14 | 44.14 | 44.09 |
| 42 | 44.16 | 44.17 | 44.14 |
| 43 | 44.13 | 44.18 | 44.14 |
| 44 | 44.16 | 44.20 | 44.14 |
| 45 | 44.16 | 44.16 | 44.17 |
| 46 | 44.16 | 44.16 | 44.18 |
| 47 | 44.15 | 44.15 | 44.10 |
| 48 | 44.14 | 44.15 | 44.16 |
| 49 | 44.15 | 44.13 | 44.14 |
| 50 | 44.14 | 44.13 | 44.19 |
| 51 | 44.15 | 44.18 | 44.16 |
| 52 | 44.12 | 44.17 | 44.15 |
| 53 | 44.15 | 44.18 | 44.14 |
| 54 | 44.14 | 44.18 | 44.14 |
| 55 | 44.14 | 44.16 | 44.15 |
| 56 | 44.12 | 44.14 | 44.18 |
| 57 | 44.13 | 44.09 | 44.14 |
| 58 | 44.14 | 44.11 | 44.12 |
| 59 | 43.97 | 43.99 | 43.98 |
| 60 | 43.86 | 44.01 | 45.95 |
| 61 | 44.10 | 44.45 | 44.21 |
| 62 | 44.14 | 44.40 | 44.23 |
| 63 | 44.13 | 44.44 | 44.22 |
| 64 | 44.09 | 44.44 | 44.23 |
| 65 | 44.06 | 44.44 | 44.25 |
| 66 | 44.04 | 44.51 | 44.26 |
| 67 | 44.09 | 44.43 | 44.23 |
| 68 | 44.10 | 44.39 | 44.25 |
| 69 | 44.14 | 44.39 | 44.28 |
| 70 | 44.14 | 44.33 | 44.25 |
| 71 | 44.13 | 44.38 | 44.24 |
| 72 | 44.07 | 44.38 | 44.29 |
| 73 | 44.12 | 44.38 | 44.22 |
| 74 | 44.13 | 44.36 | 44.24 |
| 75 | 44.11 | 44.35 | 44.21 |
| 76 | 44.10 | 44.36 | 44.22 |
| 77 | 44.06 | 44.32 | 44.24 |
| 78 | 44.13 | 44.32 | 44.26 |
| 79 | 44.14 | 44.34 | 44.20 |
| 80 | 44.12 | 44.47 | 44.24 |
| 81 | 44.07 | 44.48 | 44.22 |
| 82 | 44.13 | 44.46 | 44.20 |
| 83 | 44.04 | 44.46 | 44.28 |
| 84 | 44.05 | 44.47 | 44.29 |
| 85 | 44.18 | 44.45 | 44.29 |
| 86 | 44.14 | 44.45 | 44.25 |
| 87 | 44.10 | 44.44 | 44.24 |
| 88 | 44.16 | 44.40 | 44.15 |
| 89 | 44.16 | 44.35 | 44.20 |
| 90 | 44.17 | 44.44 | 44.18 |
| 91 | 44.19 | 44.43 | 44.24 |
| 92 | 44.15 | 44.40 | 44.25 |
| 93 | 44.16 | 44.37 | 44.18 |
| 94 | 44.15 | 44.37 | 44.13 |
| 95 | 44.17 | 44.33 | 44.13 |
| 96 | 44.16 | 44.35 | 44.13 |
| 97 | 44.21 | 44.37 | 44.12 |
| 98 | 44.15 | 44.37 | 44.11 |
| 99 | 44.12 | 44.35 | 44.18 |
| 100 | 44.15 | 44.32 | 44.13 |
| 101 | 44.20 | 44.32 | 44.17 |
| 102 | 44.15 | 44.35 | 44.14 |
| 103 | 44.14 | 44.35 | 44.18 |
| 104 | 44.09 | 44.29 | 44.15 |
| 105 | 44.13 | 44.24 | 44.01 |
| 106 | 44.15 | 44.26 | 44.03 |
| 107 | 44.15 | 44.35 | 44.18 |
| 108 | 44.17 | 44.27 | 44.18 |
| 109 | 44.16 | 44.31 | 44.11 |
| 110 | 44.10 | 44.30 | 44.16 |
| 111 | 44.11 | 44.34 | 44.15 |
| 112 | 44.14 | 44.35 | 44.13 |
| 113 | 44.15 | 44.33 | 44.14 |
| 114 | 44.14 | 44.38 | 44.17 |
| 115 | 44.10 | 44.36 | 44.20 |
| 116 | 44.13 | 44.37 | 44.18 |
| 117 | 44.12 | 44.35 | 44.21 |
| 118 | 44.13 | 44.34 | 44.11 |
| 119 | 44.11 | 44.32 | 44.17 |
| 120 | 44.12 | 44.39 | 44.17 |
| 121 | 44.10 | 44.41 | 44.19 |
| 122 | 44.05 | 44.37 | 44.16 |
| 123 | 44.07 | 44.45 | 44.12 |
| 124 | 44.12 | 44.46 | 44.09 |
| 125 | 44.08 | 44.46 | 44.08 |
| 126 | 44.10 | 44.44 | 44.12 |
| 127 | 44.00 | 44.39 | 44.17 |
| 128 | 44.12 | 44.43 | 44.05 |
| 129 | 44.17 | 44.46 | 44.12 |
| 130 | 44.15 | 44.49 | 44.05 |
| 131 | 44.14 | 44.49 | 44.15 |
| 132 | 44.13 | 44.42 | 44.11 |
| 133 | 44.13 | 44.48 | 44.07 |
| 134 | 44.14 | 44.42 | 44.04 |
| 135 | 44.16 | 44.53 | 44.12 |
| 136 | 44.19 | 44.55 | 44.10 |
| 137 | 44.24 | 44.61 | 44.13 |
| 138 | 44.28 | 44.60 | 44.12 |
| 139 | 44.31 | 44.70 | 44.08 |
| 140 | 44.28 | 44.69 | 44.07 |
| 141 | 44.25 | 44.72 | 44.09 |
| 142 | 44.21 | 44.62 | 44.09 |
| 143 | 44.21 | 44.54 | 44.09 |
| 144 | 44.22 | 44.54 | 44.16 |
| 145 | 44.23 | 44.63 | 44.05 |
| 146 | 44.24 | 44.66 | 44.15 |
| 147 | 44.33 | 44.76 | 44.09 |
| 148 | 44.36 | 44.76 | 44.08 |
| 149 | 44.30 | 44.75 | 44.12 |
| 150 | 44.23 | 44.84 | 44.14 |
| 151 | 44.23 | 44.81 | 44.14 |
| 152 | 44.24 | 44.71 | 44.16 |
| 153 | 44.27 | 44.72 | 44.09 |
| 154 | 44.33 | 44.72 | 44.15 |
| 155 | 44.24 | 44.86 | 44.16 |
| 156 | 44.22 | 44.87 | 44.18 |
| 157 | 44.23 | 44.90 | 44.15 |
| 158 | 44.25 | 44.91 | 44.10 |
| 159 | 44.25 | 44.97 | 44.15 |
| 160 | 44.27 | 44.02 | 44.13 |
| 161 | 44.25 | 44.98 | 44.17 |
| 162 | 50.29 | 51.00 | 50.29 |
| 163-233 | INF | INF | INF |

|  |
| --- |
| Table 20 – PSNR result of test 11. |

| Frame | PSNR R | PSNR G | PSNR B |
| --- | --- | --- | --- |
| 1 | 44.18 | 44.20 | 44.16 |
| 2 | 44.14 | 44.15 | 44.13 |
| 3 | 44.16 | 44.15 | 44.14 |
| 4 | 44.12 | 44.14 | 44.14 |
| 5 | 44.15 | 44.16 | 44.14 |
| 6 | 44.18 | 44.16 | 44.17 |
| 7 | 44.16 | 44.11 | 44.12 |
| 8 | 44.16 | 44.12 | 44.12 |
| 9 | 44.16 | 44.14 | 44.16 |
| 10 | 44.08 | 44.10 | 44.15 |
| 11 | 44.13 | 44.18 | 44.16 |
| 12 | 44.16 | 44.16 | 44.16 |
| 13 | 44.16 | 44.15 | 44.19 |
| 14 | 44.16 | 44.15 | 44.17 |
| 15 | 44.15 | 44.13 | 44.15 |
| 16 | 44.18 | 44.16 | 44.17 |
| 17 | 44.14 | 44.16 | 44.17 |
| 18 | 44.11 | 44.16 | 44.15 |
| 19 | 44.17 | 44.14 | 44.11 |
| 20 | 44.16 | 44.13 | 44.12 |
| 21 | 44.14 | 44.13 | 44.17 |
| 22 | 44.16 | 44.13 | 44.17 |
| 23 | 44.16 | 44.14 | 44.14 |
| 24 | 44.16 | 44.19 | 44.13 |
| 25 | 44.15 | 44.15 | 44.12 |
| 26 | 44.14 | 44.19 | 44.11 |
| 27 | 44.17 | 44.12 | 44.16 |
| 28 | 44.14 | 44.17 | 44.17 |
| 29 | 44.14 | 44.19 | 44.15 |
| 30 | 44.17 | 44.14 | 44.11 |
| 31 | 44.16 | 44.12 | 44.16 |
| 32 | 44.12 | 44.16 | 44.12 |
| 33 | 44.15 | 44.09 | 44.15 |
| 34 | 44.15 | 44.15 | 44.19 |
| 35 | 44.14 | 44.18 | 44.10 |
| 36 | 44.17 | 44.14 | 44.17 |
| 37 | 44.17 | 44.15 | 44.13 |
| 38 | 44.16 | 44.20 | 44.18 |
| 39 | 44.14 | 44.18 | 44.17 |
| 40 | 44.13 | 44.19 | 44.20 |
| 41 | 44.15 | 44.17 | 44.14 |
| 42 | 44.13 | 44.16 | 44.17 |
| 43 | 44.17 | 44.18 | 44.20 |
| 44 | 44.16 | 44.17 | 44.16 |
| 45 | 44.19 | 44.16 | 44.19 |
| 46 | 44.18 | 44.11 | 44.13 |
| 47 | 44.13 | 44.14 | 44.11 |
| 48 | 44.14 | 44.10 | 44.14 |
| 49 | 44.15 | 44.14 | 44.11 |
| 50 | 44.11 | 44.13 | 44.17 |
| 51 | 44.17 | 44.19 | 44.13 |
| 52 | 44.14 | 44.13 | 44.15 |
| 53 | 44.14 | 44.13 | 44.15 |
| 54 | 44.14 | 44.16 | 44.14 |
| 55 | 44.15 | 44.16 | 44.17 |
| 56 | 44.14 | 44.14 | 44.08 |
| 57 | 44.16 | 44.10 | 44.17 |
| 58 | 44.16 | 44.13 | 44.15 |
| 59 | 43.97 | 44.00 | 44.99 |
| 60 | 44.87 | 44.04 | 43.94 |
| 61 | 44.10 | 44.49 | 44.22 |
| 62 | 44.10 | 44.46 | 44.23 |
| 63 | 44.09 | 44.48 | 44.20 |
| 64 | 44.14 | 44.45 | 44.24 |
| 65 | 44.05 | 44.44 | 44.24 |
| 66 | 44.04 | 44.44 | 44.24 |
| 67 | 44.09 | 44.46 | 44.22 |
| 68 | 44.13 | 44.38 | 44.27 |
| 69 | 44.13 | 44.40 | 44.26 |
| 70 | 44.11 | 44.32 | 44.26 |
| 71 | 44.10 | 44.37 | 44.24 |
| 72 | 44.06 | 44.38 | 44.31 |
| 73 | 44.10 | 44.43 | 44.26 |
| 74 | 44.07 | 44.36 | 44.27 |
| 75 | 44.10 | 44.30 | 44.20 |
| 76 | 44.10 | 44.34 | 44.23 |
| 77 | 44.07 | 44.33 | 44.29 |
| 78 | 44.14 | 44.46 | 44.21 |
| 79 | 44.13 | 44.45 | 44.21 |
| 80 | 44.13 | 44.46 | 44.24 |
| 81 | 44.09 | 44.45 | 44.25 |
| 82 | 44.09 | 44.46 | 44.26 |
| 83 | 44.07 | 44.45 | 44.28 |
| 84 | 44.07 | 44.51 | 44.33 |
| 85 | 44.13 | 44.46 | 44.32 |
| 86 | 44.09 | 44.42 | 44.25 |
| 87 | 44.09 | 44.45 | 44.28 |
| 88 | 44.20 | 44.36 | 44.15 |
| 89 | 44.15 | 44.36 | 44.21 |
| 90 | 44.13 | 44.38 | 44.18 |
| 91 | 44.15 | 44.42 | 44.24 |
| 92 | 44.14 | 44.39 | 44.24 |
| 93 | 44.18 | 44.36 | 44.20 |
| 94 | 44.18 | 44.35 | 44.18 |
| 95 | 44.17 | 44.35 | 44.13 |
| 96 | 44.21 | 44.30 | 44.12 |
| 97 | 44.18 | 44.34 | 44.12 |
| 98 | 44.13 | 44.33 | 44.14 |
| 99 | 44.13 | 44.37 | 44.11 |
| 100 | 44.16 | 44.37 | 44.16 |
| 101 | 44.15 | 44.27 | 44.16 |
| 102 | 44.15 | 44.31 | 44.18 |
| 103 | 44.15 | 44.34 | 44.22 |
| 104 | 44.15 | 44.31 | 44.11 |
| 105 | 44.13 | 44.27 | 44.04 |
| 106 | 44.09 | 44.28 | 44.01 |
| 107 | 44.17 | 44.35 | 44.19 |
| 108 | 44.17 | 44.27 | 44.17 |
| 109 | 44.17 | 44.31 | 44.13 |
| 110 | 44.12 | 44.31 | 44.11 |
| 111 | 44.12 | 44.33 | 44.13 |
| 112 | 44.09 | 44.37 | 44.14 |
| 113 | 44.12 | 44.33 | 44.12 |
| 114 | 44.12 | 44.39 | 44.21 |
| 115 | 44.09 | 44.38 | 44.22 |
| 116 | 44.13 | 44.38 | 44.20 |
| 117 | 44.12 | 44.38 | 44.17 |
| 118 | 44.12 | 44.38 | 44.15 |
| 119 | 44.14 | 44.28 | 43.18 |
| 120 | 44.09 | 45.39 | 45.18 |
| 121 | 44.11 | 44.37 | 44.20 |
| 122 | 44.07 | 44.40 | 44.16 |
| 123 | 44.06 | 44.47 | 44.15 |
| 124 | 44.12 | 44.47 | 44.05 |
| 125 | 44.09 | 44.43 | 44.08 |
| 126 | 44.08 | 44.49 | 44.06 |
| 127 | 44.06 | 44.46 | 44.16 |
| 128 | 44.10 | 44.46 | 44.14 |
| 129 | 44.16 | 44.42 | 44.17 |
| 130 | 44.11 | 44.47 | 44.11 |
| 131 | 44.14 | 44.47 | 44.13 |
| 132 | 44.14 | 44.42 | 44.07 |
| 133 | 44.12 | 44.46 | 44.08 |
| 134 | 44.14 | 44.43 | 44.00 |
| 135 | 44.20 | 44.55 | 44.13 |
| 136 | 44.21 | 44.52 | 44.08 |
| 137 | 44.29 | 44.63 | 44.07 |
| 138 | 44.26 | 44.63 | 44.09 |
| 139 | 44.26 | 44.69 | 44.08 |
| 140 | 44.29 | 44.71 | 44.06 |
| 141 | 44.24 | 44.67 | 44.08 |
| 142 | 44.22 | 44.59 | 44.10 |
| 143 | 44.21 | 44.54 | 44.10 |
| 144 | 44.28 | 44.53 | 44.10 |
| 145 | 44.23 | 44.63 | 44.11 |
| 146 | 44.22 | 44.62 | 44.12 |
| 147 | 44.35 | 44.77 | 44.05 |
| 148 | 44.37 | 44.75 | 44.09 |
| 149 | 44.32 | 44.76 | 44.13 |
| 150 | 44.23 | 44.79 | 44.17 |
| 151 | 44.22 | 44.79 | 44.12 |
| 152 | 44.22 | 44.73 | 44.14 |
| 153 | 44.31 | 44.70 | 44.07 |
| 154 | 44.33 | 44.75 | 44.11 |
| 155 | 44.26 | 44.86 | 44.13 |
| 156 | 44.23 | 44.87 | 44.15 |
| 157 | 44.24 | 44.89 | 44.13 |
| 158 | 44.26 | 44.89 | 44.13 |
| 159 | 44.24 | 44.97 | 44.16 |
| 160 | 44.27 | 44.97 | 44.18 |
| 161 | 44.26 | 44.99 | 44.14 |
| 162 | 50.25 | 50.96 | 50.30 |
| 163-233 | inf | inf | inf |

|  |
| --- |
| Table 21 – PSNR result of test 12. |

Test Results for “OJT-Copy-for-students.zip” using video cover and different key size.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Test # | Filename | Key Size | Time Elapsed | | Extracted File Condition |
| Embedding | Extracting |
| 13 | OJT-Copy-for-students.zip | 16 bit | 00:00:08:0699 | 00:00:08:4670 | IDENTICAL |
| 14 | OJT-Copy-for-students.zip | 128 bit | 00:00:08:3402 | 00:00:08:9670 | IDENTICAL |

Table 22 – Test results for OJT-Copy-for-students.zip

PSNR Results of all frames using different key sizes

|  |  |  |  |
| --- | --- | --- | --- |
| FRAME | PSNR R | PSNR G | PSNR B |
| 1 | 44.20 | 44.16 | 44.20 |
| 2 | 44.15 | 44.16 | 44.15 |
| 3 | 44.15 | 44.14 | 44.13 |
| 4 | 44.14 | 44.13 | 44.13 |
| 5 | 44.14 | 44.14 | 44.14 |
| 6 | 46.12 | 46.09 | 46.14 |
| 7 - 233 | INF | INF | INF |

|  |  |  |  |
| --- | --- | --- | --- |
| FRAME | PSNR R | PSNR G | PSNR B |
| 1 | 44.15 | 44.15 | 44.17 |
| 2 | 44.15 | 44.16 | 44.14 |
| 3 | 44.14 | 44.16 | 44.14 |
| 4 | 44.11 | 44.15 | 44.16 |
| 5 | 44.14 | 44.16 | 44.17 |
| 6 | 46.08 | 46.03 | 46.09 |
| 7 - 233 | INF | INF | INF |

|  |  |
| --- | --- |
| Table 23 – PSNR result of test 13. | Table 24 – PSNR result of test 14. |

TEST TABLE 2 RESULTS For Video Cover.

Test Results for “ACCOMPLISHMENT AND COSULTAION FORM.docx” using Video Cover 2 and different key size.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Test # | Filename | Key Size | Time Elapsed | | Extracted File Condition |
| Embedding | Extracting |
| 15 | ACCOMPLISHMENT AND COSULTAION FORM.docx | 16 bit | 00:00:00:1430 | 00:00:00:5624 | IDENTICAL |
| 16 | ACCOMPLISHMENT AND COSULTAION FORM.docx | 128 bit | 00:00:00:1386 | 00:00:00:5651 | IDENTICAL |

Table 25 – Test results No. 2 for ACCOMPLISHMENT AND CONSULTATION FORM.docx

PSNR Results of all frames using different key sizes

|  |  |  |  |
| --- | --- | --- | --- |
| frame | PSNR R | PSNR G | PSNR B |
| 1 | 59.14 | 59.02 | 59.00 |
| 2 -264 | INF | INF | INF |

# 

|  |  |  |  |
| --- | --- | --- | --- |
| FRAME | PSNR R | PSNR G | PSNR B |
| 1 | 59.15 | 59.03 | 59.08 |
| 2 – 264 | INF | INF | INF |

Table 26 – PSNR results of test 15 Table 27 – PSNR results of test 16

Test Results for “Attachment B\_OJT Training Plan Template.xls” using Video Cover 2 and different key size.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Test # | Filename | Key Size | Time Elapsed | | Extracted File Condition |
| Embedding | Extracting |
| 17 | Attachment B\_OJT Training Plan Template.xls | 16 bit | 00:00:00:2315 | 00:00:00:5628 | IDENTICAL |
| 18 | Attachment B\_OJT Training Plan Template.xls | 128 bit | 00:00:00:2395 | 00:00:00:5631 | IDENTICAL |

Table 28 – Test results No. 2 for Attachment B\_OJT Training Plan Template.xls

PSNR Results of all frames using different key sizes

|  |  |  |  |
| --- | --- | --- | --- |
| FRAME | PSNR R | PSNR G | PSNR B |
| 1 | 54.12 | 53.79 | 54.06 |
| 2 – 264 | INF | INF | INF |

|  |  |  |  |
| --- | --- | --- | --- |
| FRAME | PSNR R | PSNR G | PSNR B |
| 1 | 54.12 | 53.80 | 54.04 |
| 2 – 264 | INF | INF | INF |

|  |  |
| --- | --- |
| Table 29 – PSNR result of test 17. | Table 30 – PSNR result of test 18. |

Test Table Results 2 for “Attachment G\_Daily Time Record.pdf” Video Cover using different key size.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Test # | Filename | Key Size | Time Elapsed | | Extracted File Condition |
| Embedding | Extracting |
| 19 | Attachment G\_Daily Time Record.pdf | 16 bit | 00:00:00:3264 | 00:00:00:5572 | IDENTICAL |
| 20 | Attachment G\_Daily Time Record.pdf | 128 bit | 00:00:00:3370 | 00:00:00:5749 | IDENTICAL |

Table 31 – Test results No. 2 for Attachment G\_Daily Time Record.pdf

PSNR Results of all frames using different key sizes

|  |  |  |  |
| --- | --- | --- | --- |
| FRAME | PSNR R | PSNR G | PSNR B |
| 1 | 51.72 | 51.16 | 51.75 |
| 2 – 264 | INF | INF | INF |

|  |  |  |  |
| --- | --- | --- | --- |
| FRAME | PSNR R | PSNR G | PSNR B |
| 1 | 51.74 | 51.13 | 51.76 |
| 2 - 264 | INF | INF | INF |

|  |  |
| --- | --- |
| Table 32 – PSNR result of test 19. | Table 33 – PSNR result of test 20. |

Test Results 2 for “Chrysanthemum.jpg” using Video Cover and different key size.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Test # | Filename | Key Size | Time Elapsed | | Extracted File Condition |
| Embedding | Extracting |
| 21 | Chrysanthemum.jpg | 16 bit | 00:00:02:2386 | 00:00:03:8770 | IDENTICAL |
| 22 | Chrysanthemum.jpg | 128 bit | 00:00:02:3681 | 00:00:01:0685 | IDENTICAL |

Table 34 – Test results 2 for Chrysanthemum.jpg

PSNR Results of all frames using different key sizes

|  |  |  |  |
| --- | --- | --- | --- |
| FRAME | PSNR R | PSNR G | PSNR B |
| 1 | 44.21 | 44.04 | 44.23 |
| 2 | 45.26 | 45.04 | 45.30 |
| 3-264 | inf | inf | inf |

|  |  |  |  |
| --- | --- | --- | --- |
| FRAME | PSNR R | PSNR G | PSNR B |
| 1 | 44.20 | 44.03 | 44.24 |
| 2 | 45.27 | 45.04 | 45.30 |
| 3-264 | inf | inf | inf |

|  |  |
| --- | --- |
| Table 35 – PSNR result of test 21. | Table 36 – PSNR result of test 22. |

# 

Test Results 2 for “exorciser.jar” using Video Cover and different key size.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Test # | Filename | Key Size | Time Elapsed | | Extracted File Condition |
| Embedding | Extracting |
| 23 | exorciser.jar | 16 bit | 00:00:16:8669 | 00:00:01:7552 | IDENTICAL |
| 24 | exorciser.jar | 128 bit | 00:00:06:3644 | 00:00:02:1048 | IDENTICAL |

Table 37 – Test results No. 2 for exorciser.jar

PSNR Results of all frames using different key sizes

|  |  |  |  |
| --- | --- | --- | --- |
| FRAME | PSNR R | PSNR G | PSNR B |
| 1 | 44.20 | 44.03 | 44.23 |
| 2 | 44.20 | 44.04 | 44.24 |
| 3 | 44.21 | 44.02 | 44.27 |
| 4 | 44.21 | 44.02 | 44.28 |
| 5 | 44.21 | 44.03 | 44.27 |
| 6 | 50.70 | 50.12 | 51.03 |
| 7-264 | inf | inf | inf |

|  |  |  |  |
| --- | --- | --- | --- |
| FRAME | PSNR R | PSNR G | PSNR B |
| 1 | 44.20 | 44.03 | 44.24 |
| 2 | 44.20 | 44.02 | 44.25 |
| 3 | 44.22 | 44.02 | 44.28 |
| 4 | 44.21 | 44.02 | 44.27 |
| 5 | 44.20 | 44.04 | 44.27 |
| 6 | 50.70 | 50.13 | 51.01 |
| 7-264 | inf | inf | inf |

|  |  |
| --- | --- |
| Table 38 – PSNR result of test 23. | Table 39 – PSNR result of test 24. |

Test Results 2 for “my night.mp3” using Video Cover and different key size.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Test # | Filename | Key Size | Time Elapsed | | Extracted File Condition |
| Embedding | Extracting |
| 25 | my night.mp3 | 16 bit | 00:00: 21:5132 | 00:00: 3:5480 | IDENTICAL |
| 26 | my night.mp3 | 128 bit | 00:00:17:6295 | 00:00:04:7610 | IDENTICAL |

Table 40 – Test results 2 for my night.mp3

PSNR Results of all frames using different key sizes.

|  |  |  |  |
| --- | --- | --- | --- |
| Frame | PSNR R | PSNR G | PSNR B |
| 1 | 44.20 | 44.02 | 44.24 |
| 2 | 44.19 | 44.02 | 44.24 |
| 3 | 44.22 | 44.03 | 44.28 |
| 4 | 44.21 | 44.02 | 44.27 |
| 5 | 44.21 | 44.03 | 44.27 |
| 6 | 44.20 | 44.03 | 44.26 |
| 7 | 44.22 | 44.04 | 44.18 |
| 8 | 44.23 | 44.05 | 44.20 |
| 9 | 44.22 | 44.04 | 44.18 |
| 10 | 44.22 | 44.04 | 44.19 |
| 11 | 44.24 | 44.04 | 44.19 |
| 12 | 44.23 | 44.04 | 44.19 |
| 13 | 44.24 | 44.02 | 44.19 |
| 14 | 44.25 | 44.03 | 44.20 |
| 15 | 52.83 | 52.36 | 52.93 |
| 16-264 | INF | INF | INF |

|  |  |  |  |
| --- | --- | --- | --- |
| Frame | PSNR R | PSNR G | PSNR B |
| 1 | 44.20 | 44.02 | 44.24 |
| 2 | 44.20 | 44.02 | 44.24 |
| 3 | 44.21 | 44.02 | 44.28 |
| 4 | 44.21 | 44.03 | 44.27 |
| 5 | 44.20 | 44.03 | 44.27 |
| 6 | 44.21 | 44.03 | 44.27 |
| 7 | 44.22 | 44.03 | 44.19 |
| 8 | 44.22 | 44.05 | 44.20 |
| 9 | 44.22 | 44.05 | 44.19 |
| 10 | 44.21 | 44.05 | 44.19 |
| 11 | 44.24 | 44.03 | 44.18 |
| 12 | 44.24 | 44.03 | 44.20 |
| 13 | 44.23 | 44.05 | 44.19 |
| 14 | 44.24 | 44.04 | 44.20 |
| 15 | 52.80 | 52.34 | 52.96 |
| 16-264 | INF | INF | INF |

|  |
| --- |
| Table 41 – PSNR result of test 25 |

|  |
| --- |
| Table 42 – PSNR result of test 26 |

Test Results No.2 for “OJT-Copy-for-students.zip” using Video Cover 2 and different key size.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Test # | Filename | Key Size | Time Elapsed | | Extracted File Condition |
| Embedding | Extracting |
| 27 | OJT-Copy-for-students.zip | 16 bit | 00:00:08:0699 | 00:00:08:4670 | IDENTICAL |
| 28 | OJT-Copy-for-students.zip | 128 bit | 00:00:08:3402 | 00:00:08:9670 | IDENTICAL |

Table 43 – Test results 2 for OJT-Copy-for-students.zip

PSNR Results of all frames using different key sizes

|  |  |  |  |
| --- | --- | --- | --- |
| FRAME | PSNR R | PSNR G | PSNR B |
| 1 | 47.31 | 46.97 | 47.39 |
| 2-264 | inf | inf | inf |

|  |  |  |  |
| --- | --- | --- | --- |
| FRAME | PSNR R | PSNR G | PSNR B |
| 1 | 47.31 | 46.96 | 47.40 |
| 2-264 | inf | inf | inf |

|  |  |
| --- | --- |
| Table 44 – PSNR result of test 27 | Table 45 – PSNR result of test 28 |

Test Results 2 for “OJT-Copy-for-students.zip” using Video Cover and different key size.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Test # | Filename | Key Size | Time Elapsed | | Extracted File Condition |
| Embedding | Extracting |
| 29 | No Game No Life Opening Full.flac | 16 bit | 00:02:24:5958 | 00:00:23:0895 | IDENTICAL |
| 30 | No Game No Life Opening Full.flac | 128 bit | 00:02:30:1593 | 00:00:32:5169 | IDENTICAL |

Table 46 – Test results No. 2 for No Game No Life Opening Full.flac

PSNR Results of all frames using different key sizes

| Frame | PSNR R | PSNR G | PSNR B |
| --- | --- | --- | --- |
| 1 | 44.21 | 44.03 | 44.24 |
| 2 | 44.21 | 44.02 | 44.25 |
| 3 | 44.22 | 44.02 | 44.27 |
| 4 | 44.22 | 44.03 | 44.26 |
| 5 | 44.20 | 44.04 | 44.28 |
| 6 | 44.20 | 44.02 | 44.26 |
| 7 | 44.22 | 44.04 | 44.19 |
| 8 | 44.21 | 44.04 | 44.20 |
| 9 | 44.22 | 44.05 | 44.17 |
| 10 | 44.21 | 44.05 | 44.19 |
| 11 | 44.23 | 44.03 | 44.18 |
| 12 | 44.24 | 44.04 | 44.19 |
| 13 | 44.23 | 44.02 | 44.19 |
| 14 | 44.23 | 44.04 | 44.19 |
| 15 | 44.23 | 44.03 | 44.17 |
| 16 | 44.22 | 44.03 | 44.19 |
| 17 | 44.23 | 44.02 | 44.18 |
| 18 | 44.23 | 44.03 | 44.18 |
| 19 | 44.24 | 44.03 | 44.16 |
| 20 | 44.22 | 44.03 | 44.19 |
| 21 | 44.22 | 44.01 | 44.19 |
| 22 | 44.23 | 44.02 | 44.19 |
| 23 | 44.22 | 44.01 | 44.18 |
| 24 | 44.23 | 44.02 | 44.21 |
| 25 | 44.22 | 44.02 | 44.19 |
| 26 | 44.21 | 44.03 | 44.19 |
| 27 | 44.23 | 44.02 | 44.18 |
| 28 | 44.22 | 44.03 | 44.20 |
| 29 | 44.22 | 44.03 | 44.20 |
| 30 | 44.22 | 44.04 | 44.20 |
| 31 | 44.22 | 44.05 | 44.17 |
| 32 | 44.21 | 44.04 | 44.18 |
| 33 | 44.22 | 44.05 | 44.17 |
| 34 | 44.21 | 44.04 | 44.19 |
| 35 | 44.21 | 44.04 | 44.17 |
| 36 | 44.21 | 44.03 | 44.19 |
| 37 | 44.21 | 44.02 | 44.20 |
| 38 | 44.20 | 44.02 | 44.20 |
| 39 | 44.22 | 44.03 | 44.17 |
| 40 | 44.21 | 44.03 | 44.19 |
| 41 | 44.20 | 44.03 | 44.18 |
| 42 | 44.21 | 44.02 | 44.19 |
| 43 | 44.21 | 44.03 | 44.19 |
| 44 | 44.22 | 44.02 | 44.23 |
| 45 | 44.20 | 44.03 | 44.24 |
| 46 | 44.21 | 44.03 | 44.24 |
| 47 | 44.21 | 44.03 | 44.22 |
| 48 | 44.22 | 44.03 | 44.23 |
| 49 | 44.20 | 44.03 | 44.22 |
| 50 | 44.19 | 44.03 | 44.25 |
| 51 | 44.21 | 44.03 | 44.18 |
| 52 | 44.20 | 44.02 | 44.22 |
| 53 | 44.20 | 44.03 | 44.20 |
| 54 | 44.21 | 44.03 | 44.19 |
| 55 | 44.22 | 44.03 | 44.19 |
| 56 | 44.20 | 44.02 | 44.20 |
| 57 | 44.20 | 44.03 | 44.20 |
| 58 | 44.20 | 44.03 | 44.19 |
| 59 | 43.20 | 44.02 | 44.20 |
| 60 | 44.21 | 44.02 | 44.25 |
| 61 | 44.21 | 44.01 | 44.22 |
| 62 | 44.20 | 44.02 | 44.23 |
| 63 | 44.22 | 44.03 | 44.21 |
| 64 | 44.21 | 44.02 | 44.22 |
| 65 | 44.19 | 44.02 | 44.22 |
| 66 | 44.20 | 44.03 | 44.21 |
| 67 | 44.21 | 44.03 | 44.20 |
| 68 | 44.21 | 44.03 | 44.21 |
| 69 | 44.22 | 44.03 | 44.20 |
| 70 | 44.21 | 44.03 | 44.21 |
| 71 | 44.23 | 44.03 | 44.19 |
| 72 | 44.20 | 44.04 | 44.21 |
| 73 | 44.21 | 44.03 | 44.22 |
| 74 | 44.21 | 44.02 | 44.21 |
| 75 | 44.21 | 44.02 | 44.20 |
| 76 | 44.23 | 44.04 | 44.22 |
| 77 | 44.21 | 44.02 | 44.22 |
| 78 | 44.21 | 44.04 | 44.23 |
| 79 | 44.22 | 44.03 | 44.23 |
| 80 | 44.20 | 44.02 | 44.22 |
| 81 | 44.21 | 44.04 | 44.22 |
| 82 | 44.21 | 44.03 | 44.23 |
| 83 | 44.21 | 44.03 | 44.21 |
| 84 | 44.22 | 44.01 | 44.22 |
| 85 | 44.21 | 44.03 | 44.23 |
| 86 | 44.21 | 44.03 | 44.22 |
| 87 | 44.22 | 44.02 | 44.22 |
| 88 | 44.22 | 44.03 | 44.20 |
| 89 | 44.21 | 44.03 | 44.23 |
| 90 | 44.21 | 44.02 | 44.21 |
| 91 | 44.22 | 44.02 | 44.20 |
| 92 | 44.23 | 44.02 | 44.20 |
| 93 | 44.23 | 44.03 | 44.20 |
| 94 | 44.22 | 44.02 | 44.20 |
| 95 | 44.22 | 44.03 | 44.20 |
| 96 | 44.21 | 44.02 | 44.20 |
| 97 | 44.22 | 44.03 | 44.19 |
| 98 | 44.21 | 44.02 | 44.21 |
| 99 | 44.21 | 44.02 | 44.20 |
| 100 | 44.17 | 44.04 | 44.24 |
| 101 | 44.18 | 44.03 | 44.23 |
| 102 | 44.70 | 44.90 | 44.36 |
| 103 | 44.70 | 44.90 | 44.37 |
| 104 | 44.75 | 44.17 | 44.76 |
| 105 | 44.74 | 44.15 | 44.75 |
| 106 | 44.73 | 44.18 | 44.75 |
| 107 | 44.75 | 44.17 | 44.75 |
| 108 | 44.75 | 44.16 | 44.75 |
| 109 | 44.75 | 44.16 | 44.75 |
| 110 | 51.81 | 54.49 | 51.79 |
| 111- 264 | INF | INF | INF |

Table 47 – PSNR result of test 29

| Frame | PSNR R | PSNR G | PSNR B |
| --- | --- | --- | --- |
| 1 | 44.21 | 44.02 | 44.25 |
| 2 | 44.20 | 44.02 | 44.24 |
| 3 | 44.22 | 44.03 | 44.27 |
| 4 | 44.21 | 44.03 | 44.26 |
| 5 | 44.21 | 44.02 | 44.27 |
| 6 | 44.20 | 44.03 | 44.26 |
| 7 | 44.22 | 44.04 | 44.19 |
| 8 | 44.21 | 44.04 | 44.20 |
| 9 | 44.23 | 44.05 | 44.19 |
| 10 | 44.21 | 44.04 | 44.19 |
| 11 | 44.24 | 44.04 | 44.18 |
| 12 | 44.23 | 44.04 | 44.20 |
| 13 | 44.24 | 44.04 | 44.19 |
| 14 | 44.23 | 44.04 | 44.20 |
| 15 | 44.24 | 44.02 | 44.18 |
| 16 | 44.22 | 44.01 | 44.18 |
| 17 | 44.23 | 44.02 | 44.18 |
| 18 | 44.23 | 44.01 | 44.18 |
| 19 | 44.23 | 44.03 | 44.16 |
| 20 | 44.23 | 44.02 | 44.19 |
| 21 | 44.22 | 44.02 | 44.19 |
| 22 | 44.22 | 44.02 | 44.19 |
| 23 | 44.23 | 44.02 | 44.18 |
| 24 | 44.24 | 44.02 | 44.20 |
| 25 | 44.23 | 44.01 | 44.19 |
| 26 | 44.22 | 44.03 | 44.20 |
| 27 | 44.22 | 44.01 | 44.19 |
| 28 | 44.22 | 44.04 | 44.21 |
| 29 | 44.23 | 44.05 | 44.20 |
| 30 | 44.22 | 44.03 | 44.19 |
| 31 | 44.23 | 44.04 | 44.17 |
| 32 | 44.22 | 44.04 | 44.18 |
| 33 | 44.21 | 44.04 | 44.18 |
| 34 | 44.22 | 44.04 | 44.18 |
| 35 | 44.23 | 44.03 | 44.17 |
| 36 | 44.22 | 44.02 | 44.19 |
| 37 | 44.22 | 44.02 | 44.20 |
| 38 | 44.21 | 44.03 | 44.20 |
| 39 | 44.21 | 44.03 | 44.18 |
| 40 | 44.21 | 44.03 | 44.19 |
| 41 | 44.21 | 44.03 | 44.18 |
| 42 | 44.21 | 44.03 | 44.18 |
| 43 | 44.21 | 44.05 | 44.19 |
| 44 | 44.22 | 44.01 | 44.23 |
| 45 | 44.21 | 44.02 | 44.23 |
| 46 | 44.20 | 44.03 | 44.24 |
| 47 | 44.22 | 44.01 | 44.23 |
| 48 | 44.20 | 44.03 | 44.23 |
| 49 | 44.20 | 44.02 | 44.23 |
| 50 | 44.20 | 44.03 | 44.23 |
| 51 | 44.20 | 44.02 | 44.19 |
| 52 | 44.20 | 44.03 | 44.22 |
| 53 | 44.19 | 44.02 | 44.20 |
| 54 | 44.21 | 44.02 | 44.19 |
| 55 | 44.20 | 44.02 | 44.21 |
| 56 | 44.19 | 44.03 | 44.19 |
| 57 | 44.19 | 44.02 | 44.20 |
| 58 | 44.19 | 44.03 | 44.20 |
| 59 | 43.19 | 44.02 | 44.20 |
| 60 | 44.21 | 44.01 | 44.24 |
| 61 | 44.22 | 44.03 | 44.22 |
| 62 | 44.22 | 44.02 | 44.23 |
| 63 | 44.21 | 44.04 | 44.22 |
| 64 | 44.21 | 44.03 | 44.23 |
| 65 | 44.20 | 44.04 | 44.22 |
| 66 | 44.21 | 44.03 | 44.22 |
| 67 | 44.21 | 44.04 | 44.20 |
| 68 | 44.22 | 44.01 | 44.21 |
| 69 | 44.22 | 44.02 | 44.20 |
| 70 | 44.22 | 44.02 | 44.21 |
| 71 | 44.22 | 44.03 | 44.19 |
| 72 | 44.20 | 44.04 | 44.21 |
| 73 | 44.22 | 44.02 | 44.22 |
| 74 | 44.21 | 44.02 | 44.22 |
| 75 | 44.21 | 44.04 | 44.22 |
| 76 | 44.22 | 44.03 | 44.23 |
| 77 | 44.23 | 44.02 | 44.23 |
| 78 | 44.22 | 44.04 | 44.24 |
| 79 | 44.23 | 44.03 | 44.23 |
| 80 | 44.20 | 44.02 | 44.22 |
| 81 | 44.21 | 44.02 | 44.22 |
| 82 | 44.21 | 44.03 | 44.22 |
| 83 | 44.21 | 44.04 | 44.21 |
| 84 | 44.21 | 44.02 | 44.22 |
| 85 | 44.20 | 44.02 | 44.21 |
| 86 | 44.21 | 44.02 | 44.21 |
| 87 | 44.21 | 44.03 | 44.21 |
| 88 | 44.21 | 44.04 | 44.23 |
| 89 | 44.22 | 44.03 | 44.22 |
| 90 | 44.21 | 44.03 | 44.23 |
| 91 | 44.23 | 44.03 | 44.21 |
| 92 | 44.22 | 44.02 | 44.20 |
| 93 | 44.22 | 44.02 | 44.20 |
| 94 | 44.22 | 44.02 | 44.19 |
| 95 | 44.22 | 44.03 | 44.19 |
| 96 | 44.21 | 44.02 | 44.21 |
| 97 | 44.20 | 44.03 | 44.20 |
| 98 | 44.20 | 44.02 | 44.21 |
| 99 | 44.20 | 44.02 | 44.19 |
| 100 | 44.17 | 44.05 | 44.24 |
| 101 | 44.19 | 44.03 | 44.22 |
| 102 | 44.71 | 44.90 | 44.37 |
| 103 | 44.70 | 44.91 | 44.37 |
| 104 | 44.75 | 44.16 | 44.76 |
| 105 | 44.74 | 44.16 | 44.76 |
| 106 | 44.74 | 44.16 | 44.75 |
| 107 | 44.75 | 44.16 | 44.75 |
| 108 | 44.74 | 44.16 | 44.76 |
| 109 | 44.76 | 44.16 | 44.75 |
| 110 | 51.81 | 54.48 | 51.80 |
| 111- 264 | INF | INF | INF |

Table 48 – PSNR result of test 30

Test Results 2 for “Watch No Game No Life Episode 1 English Sub.mp4” using Video Cover and different key size.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Test # | Filename | Key Size | Time Elapsed | | Extracted File Condition |
| Embedding | Extracting |
| 31 | Watch No Game No Life Episode 1 English Sub.mp4 | 16 bit | 00:02:21:8734 | 00:00:22:2940 | IDENTICAL |
| 32 | Watch No Game No Life Episode 1 English Sub.mp4 | 128 bit | 00:02:46:1740 | 00:00:34:8811 | IDENTICAL |

Table 46 – Test results 2 for Watch No Game No Life Episode 1 English Sub.mp4

PSNR Results of all frames using different key sizes

| Frame | PSNR R | PSNR G | PSNR B |
| --- | --- | --- | --- |
| 1 | 44.20 | 44.03 | 44.22 |
| 2 | 44.20 | 44.03 | 44.24 |
| 3 | 44.21 | 44.03 | 44.27 |
| 4 | 44.21 | 44.03 | 44.27 |
| 5 | 44.21 | 44.04 | 44.26 |
| 6 | 44.21 | 44.03 | 44.27 |
| 7 | 44.22 | 44.03 | 44.20 |
| 8 | 44.21 | 44.04 | 44.20 |
| 9 | 44.21 | 44.04 | 44.19 |
| 10 | 44.21 | 44.03 | 44.19 |
| 11 | 44.23 | 44.03 | 44.18 |
| 12 | 44.23 | 44.02 | 44.19 |
| 13 | 44.23 | 44.03 | 44.20 |
| 14 | 44.24 | 44.04 | 44.20 |
| 15 | 44.24 | 44.03 | 44.17 |
| 16 | 44.23 | 44.03 | 44.19 |
| 17 | 44.22 | 44.02 | 44.18 |
| 18 | 44.22 | 44.02 | 44.18 |
| 19 | 44.24 | 44.04 | 44.16 |
| 20 | 44.22 | 44.02 | 44.18 |
| 21 | 44.22 | 44.01 | 44.19 |
| 22 | 44.22 | 44.01 | 44.19 |
| 23 | 44.23 | 44.02 | 44.17 |
| 24 | 44.23 | 44.02 | 44.20 |
| 25 | 44.22 | 44.02 | 44.20 |
| 26 | 44.22 | 44.02 | 44.20 |
| 27 | 44.22 | 44.03 | 44.18 |
| 28 | 44.22 | 44.03 | 44.21 |
| 29 | 44.21 | 44.04 | 44.20 |
| 30 | 44.22 | 44.03 | 44.20 |
| 31 | 44.22 | 44.05 | 44.18 |
| 32 | 44.23 | 44.05 | 44.19 |
| 33 | 44.22 | 44.04 | 44.19 |
| 34 | 44.23 | 44.04 | 44.18 |
| 35 | 44.24 | 44.04 | 44.17 |
| 36 | 44.21 | 44.01 | 44.19 |
| 37 | 44.22 | 44.03 | 44.20 |
| 38 | 44.22 | 44.02 | 44.20 |
| 39 | 44.21 | 44.04 | 44.19 |
| 40 | 44.21 | 44.02 | 44.19 |
| 41 | 44.20 | 44.03 | 44.19 |
| 42 | 44.20 | 44.02 | 44.19 |
| 43 | 44.21 | 44.03 | 44.19 |
| 44 | 44.20 | 44.03 | 44.23 |
| 45 | 44.20 | 44.02 | 44.24 |
| 46 | 44.20 | 44.02 | 44.24 |
| 47 | 44.21 | 44.02 | 44.23 |
| 48 | 44.20 | 44.04 | 44.23 |
| 49 | 44.19 | 44.02 | 44.23 |
| 50 | 44.20 | 44.04 | 44.23 |
| 51 | 44.21 | 44.03 | 44.18 |
| 52 | 44.21 | 44.03 | 44.23 |
| 53 | 44.19 | 44.02 | 44.20 |
| 54 | 44.21 | 44.02 | 44.20 |
| 55 | 44.20 | 44.03 | 44.18 |
| 56 | 44.19 | 44.02 | 44.20 |
| 57 | 44.20 | 44.04 | 44.20 |
| 58 | 44.19 | 44.02 | 44.20 |
| 59 | 44.19 | 44.02 | 44.21 |
| 60 | 44.21 | 44.02 | 44.24 |
| 61 | 44.22 | 44.03 | 44.24 |
| 62 | 44.21 | 44.01 | 44.24 |
| 63 | 44.21 | 44.03 | 44.21 |
| 64 | 44.20 | 44.03 | 44.22 |
| 65 | 44.20 | 44.04 | 44.22 |
| 66 | 44.19 | 44.03 | 44.22 |
| 67 | 44.20 | 44.03 | 44.19 |
| 68 | 44.20 | 44.03 | 44.21 |
| 69 | 44.21 | 44.02 | 44.20 |
| 70 | 44.22 | 44.02 | 44.21 |
| 71 | 44.22 | 44.03 | 44.20 |
| 72 | 44.21 | 44.02 | 44.22 |
| 73 | 44.20 | 44.03 | 44.22 |
| 74 | 44.21 | 44.03 | 44.22 |
| 75 | 44.21 | 44.04 | 44.21 |
| 76 | 44.22 | 44.04 | 44.24 |
| 77 | 44.22 | 44.03 | 44.22 |
| 78 | 44.22 | 44.03 | 44.23 |
| 79 | 44.22 | 44.04 | 44.22 |
| 80 | 44.20 | 44.04 | 44.24 |
| 81 | 44.21 | 44.03 | 44.22 |
| 82 | 44.20 | 44.03 | 44.23 |
| 83 | 44.21 | 44.02 | 44.22 |
| 84 | 44.19 | 44.01 | 44.22 |
| 85 | 44.20 | 44.02 | 44.22 |
| 86 | 44.20 | 44.02 | 44.21 |
| 87 | 44.21 | 44.03 | 44.21 |
| 88 | 44.21 | 44.02 | 44.22 |
| 89 | 44.21 | 44.03 | 44.22 |
| 90 | 44.21 | 44.02 | 44.22 |
| 91 | 44.22 | 44.02 | 44.20 |
| 92 | 44.23 | 44.02 | 44.20 |
| 93 | 44.22 | 44.02 | 44.20 |
| 94 | 44.23 | 44.03 | 44.20 |
| 95 | 44.21 | 44.03 | 44.20 |
| 96 | 44.21 | 44.03 | 44.20 |
| 97 | 44.22 | 44.02 | 44.18 |
| 98 | 44.20 | 44.03 | 44.20 |
| 99 | 44.20 | 44.03 | 44.20 |
| 100 | 44.16 | 44.04 | 44.24 |
| 101 | 44.19 | 44.03 | 44.22 |
| 102 | 43.71 | 43.90 | 43.37 |
| 103 | 43.70 | 43.91 | 43.37 |
| 104 | 42.75 | 46.16 | 42.75 |
| 105 | 42.75 | 46.16 | 42.75 |
| 106 | 42.75 | 46.16 | 42.76 |
| 107 | 42.75 | 46.16 | 42.76 |
| 108 | 44.24 | 47.62 | 44.24 |
| 109- 264 | INF | INF | INF |

Table 49 – PSNR result of test 31

| Frame | PSNR R | PSNR G | PSNR B |
| --- | --- | --- | --- |
| 1 | 44.20 | 44.03 | 44.24 |
| 2 | 44.20 | 44.03 | 44.25 |
| 3 | 44.22 | 44.03 | 44.27 |
| 4 | 44.21 | 44.03 | 44.27 |
| 5 | 44.21 | 44.04 | 44.27 |
| 6 | 44.20 | 44.03 | 44.26 |
| 7 | 44.22 | 44.03 | 44.19 |
| 8 | 44.22 | 44.04 | 44.19 |
| 9 | 44.23 | 44.04 | 44.19 |
| 10 | 44.22 | 44.03 | 44.19 |
| 11 | 44.24 | 44.03 | 44.18 |
| 12 | 44.24 | 44.02 | 44.19 |
| 13 | 44.25 | 44.03 | 44.18 |
| 14 | 44.24 | 44.04 | 44.21 |
| 15 | 44.24 | 44.03 | 44.17 |
| 16 | 44.22 | 44.03 | 44.19 |
| 17 | 44.23 | 44.02 | 44.18 |
| 18 | 44.23 | 44.02 | 44.18 |
| 19 | 44.23 | 44.04 | 44.17 |
| 20 | 44.21 | 44.02 | 44.19 |
| 21 | 44.22 | 44.01 | 44.19 |
| 22 | 44.22 | 44.01 | 44.19 |
| 23 | 44.22 | 44.02 | 44.17 |
| 24 | 44.22 | 44.02 | 44.20 |
| 25 | 44.22 | 44.02 | 44.19 |
| 26 | 44.23 | 44.02 | 44.20 |
| 27 | 44.22 | 44.03 | 44.19 |
| 28 | 44.23 | 44.03 | 44.20 |
| 29 | 44.23 | 44.04 | 44.19 |
| 30 | 44.22 | 44.03 | 44.19 |
| 31 | 44.23 | 44.05 | 44.17 |
| 32 | 44.22 | 44.05 | 44.18 |
| 33 | 44.22 | 44.04 | 44.18 |
| 34 | 44.23 | 44.04 | 44.18 |
| 35 | 44.24 | 44.04 | 44.17 |
| 36 | 44.22 | 44.01 | 44.19 |
| 37 | 44.22 | 44.03 | 44.19 |
| 38 | 44.21 | 44.02 | 44.20 |
| 39 | 44.21 | 44.04 | 44.19 |
| 40 | 44.22 | 44.02 | 44.19 |
| 41 | 44.22 | 44.03 | 44.19 |
| 42 | 44.22 | 44.02 | 44.18 |
| 43 | 44.21 | 44.03 | 44.19 |
| 44 | 44.20 | 44.03 | 44.24 |
| 45 | 44.20 | 44.02 | 44.25 |
| 46 | 44.21 | 44.02 | 44.24 |
| 47 | 44.20 | 44.02 | 44.23 |
| 48 | 44.20 | 44.04 | 44.23 |
| 49 | 44.19 | 44.02 | 44.23 |
| 50 | 44.20 | 44.04 | 44.23 |
| 51 | 44.20 | 44.03 | 44.19 |
| 52 | 44.20 | 44.03 | 44.21 |
| 53 | 44.19 | 44.02 | 44.19 |
| 54 | 44.21 | 44.02 | 44.20 |
| 55 | 44.20 | 44.03 | 44.19 |
| 56 | 44.20 | 44.02 | 44.20 |
| 57 | 44.21 | 44.04 | 44.19 |
| 58 | 44.18 | 44.02 | 44.21 |
| 59 | 44.21 | 44.02 | 44.20 |
| 60 | 44.20 | 44.02 | 44.24 |
| 61 | 44.20 | 44.03 | 44.24 |
| 62 | 44.22 | 44.01 | 44.23 |
| 63 | 44.22 | 44.03 | 44.21 |
| 64 | 44.19 | 44.03 | 44.22 |
| 65 | 44.20 | 44.04 | 44.22 |
| 66 | 44.20 | 44.03 | 44.22 |
| 67 | 44.21 | 44.03 | 44.20 |
| 68 | 44.21 | 44.03 | 44.20 |
| 69 | 44.21 | 44.02 | 44.21 |
| 70 | 44.22 | 44.02 | 44.21 |
| 71 | 44.22 | 44.03 | 44.19 |
| 72 | 44.20 | 44.02 | 44.21 |
| 73 | 44.21 | 44.03 | 44.22 |
| 74 | 44.20 | 44.03 | 44.22 |
| 75 | 44.22 | 44.04 | 44.21 |
| 76 | 44.21 | 44.04 | 44.23 |
| 77 | 44.23 | 44.03 | 44.22 |
| 78 | 44.22 | 44.03 | 44.23 |
| 79 | 44.22 | 44.04 | 44.23 |
| 80 | 44.20 | 44.04 | 44.23 |
| 81 | 44.21 | 44.03 | 44.23 |
| 82 | 44.21 | 44.03 | 44.23 |
| 83 | 44.21 | 44.02 | 44.21 |
| 84 | 44.20 | 44.01 | 44.22 |
| 85 | 44.20 | 44.02 | 44.22 |
| 86 | 44.21 | 44.02 | 44.22 |
| 87 | 44.22 | 44.03 | 44.21 |
| 88 | 44.22 | 44.02 | 44.22 |
| 89 | 44.20 | 44.03 | 44.22 |
| 90 | 44.21 | 44.02 | 44.22 |
| 91 | 44.23 | 44.02 | 44.21 |
| 92 | 44.22 | 44.02 | 44.20 |
| 93 | 44.22 | 44.02 | 44.20 |
| 94 | 44.22 | 44.03 | 44.20 |
| 95 | 44.22 | 44.03 | 44.18 |
| 96 | 44.21 | 44.03 | 44.20 |
| 97 | 44.22 | 44.02 | 44.20 |
| 98 | 44.21 | 44.03 | 44.22 |
| 99 | 44.20 | 44.03 | 44.20 |
| 100 | 44.16 | 44.04 | 44.22 |
| 101 | 44.19 | 44.03 | 44.23 |
| 102 | 44.70 | 44.90 | 43.37 |
| 103 | 43.70 | 44.91 | 43.36 |
| 104 | 42.75 | 46.16 | 42.75 |
| 105 | 42.75 | 46.16 | 42.75 |
| 106 | 42.76 | 46.16 | 42.75 |
| 107 | 42.75 | 46.16 | 42.75 |
| 108 | 44.25 | 47.62 | 44.24 |
| 109- 264 | INF | INF | INF |

Table 50 – PSNR result of test 32

After the first phase of this chapter, the proponents gathered results of the accuracy and speed of the algorithm in embedding and extracting a file. The tests produced positive extracted file condition results comparing the different key size and video cover.

# Conclusions and Recommendations

As the proponent study the current ICT and its problems, the proponents found out that data breach is a one of causes of data theft. Data breach happen on unsecured transmission or storage of confidential data. To address the problem, the proponent introduced a project that utilizes cryptography and steganography to securely hide data storage on a computer. The proposed project uses their own created encryption algorithm to encode payload data to an uncompressed AVI file. Their own created encryption algorithm derived from their findings on different existing algorithms and different practices on block cipher encryption. As they study steganography, They picked LSB algorithm to store the encoded data on an AVI video cover, due to its simplicity and causes no changes on files size of the video. To store information of the embedded data and key used in encoding to be used in encoding to be used on extraction without changing the file size of video cover, they found out that using LSB algorithm and it achieve an average PSNR rating of 42-44dB on every color attribute of a pixel given if all pixels are modified.

Based on their studies and results they therefore conclude that data breach is one of the main concerns of secure communication. The proponents also conclude that cryptography and steganography can be a solution to address data breach. By combining both encryption and steganography, it can achieve a better security than using just one of the two. By using a very own created encryption algorithm to encode data, it can achieve a state where only proposed system can decode the embedded data. By using 2-bit LSB algorithm, it can achieve a video frame output few but unnoticeable video degradation based on visual representation and PSNR result. Based on test results, storing the information of embedded data on unused chuck of the cover and using LSB for embedding achieved no changes to file size of the cover video.

The proponents can recommend to further enhance this concept are creating better non existing encryption to give uniqueness in encoding data than other existing system, securing the key used in encoding to avoid reverse engineering of the encryption algorithm and enhancement of LSB algorithm to improve video cover quality.

# References

Book

* Choi Seung et al. A Black-Box Construction of Non-malleable Encryption from Semantically Secure Encryption; Journal of Cryptology, 2018, Vol.31(1), pp.172-201
* Information hiding terminology. In: Anderson R. (eds) Information Hiding. IH 1996. Lecture Notes in Computer Science, vol 1174. Springer, Berlin, Heidelberg
* Lipinski, Michael. Encryption; SC Magazine, Oct 2011, Vol.22(10), p.38
* Pope, M. et al. Digital Steganography - An Introduction to Techniques and Tools; Communications of the Association for Information Systems, 2012, Vol.30, p.347

Article

* David L. Hecht, David L. Hecht, } "Embedded data glyph technology for hardcopy digital documents", Proc. SPIE 2171, Color Hard Copy and Graphic Arts III, (9 May 1994); doi: 10.1117/12.175304; https://doi.org/10.1117/12.175304
* Microsoft (2017) AVI RIFF file reference. Retrieve from https://docs.microsoft.com/en-us/windows/desktop/directshow/avi-riff-file-reference
* Pope, M., Warkentin, M., Bekkering, E., & Schmidt, M. (2012). Digital Steganography - An Introduction to Techniques and Tools. Communications of the Association for Information Systems, 30, 347.
* Various Image Compression Techniques: Lossy and Lossless. Available from: https://www.researchgate.net/publication/303319054\_Various\_Image\_Compression\_Techniques\_Lossy\_and\_Lossless [accessed Oct 27 2018].

URL’s

* Carey Wodehouse (2017) Encryption, Introduction to protect your data Retrieve From: https://www.upwork.com/hiring/development/introduction-to-encryption-data-security/
* Chris Pete (2016) : What is Steganography ( All types of Technique and Tools) Retrieve From: https://kifanga.com/what-is-steganography
* Daniel L Calloway: LITERATURE REVIEW OF CRYPTOGRAPHY & NETWORK SECURITY Retrieved From: http://www.academia.edu/662784/Literature\_Review\_on\_Cryptography\_and\_Network\_Security
* Joachim. von zur GathenJonathan Cummins, Patrick Diskin, Samuel Lau and Robert Parlett (2004): Steganography And Digital Watermarking Retrieve From: https://purdue-primo-prod.hosted.exlibrisgroup.com
* Margaret Rouse and Mary K. Pratti (2017) : ICT( Information and Communications Technology or Technologies) Retrieve From: https://www.linkedin.com/pulse/ict-information-communications-technology-definition-mohamed-taher
* Mark David Gan: Chameleon Retrieved in http://chameleon-stego.tripod.com/downloads/Chameleon\_Technical\_Paper.pdf
* Steganography Software. Retrieve in http://quickcrypto.com/steganography-software.html
* Yang Li, Yu Sasaki, Kazuo Sakiyama ; Security of Block Ciphers Retrieve From:https://www.oreilly.com/library/view/security-of block/9781118660010/c01.xhtml

Journal

* Delov, D., and Dwork C., Nonmalleable Cryptography; SIAM Journal on Computing, 2000, Vol.30(2), pp.391-437
* Kumar, A. And Pooja, K. Steganography- A Data Hiding Technique; International Journal of Computer Applications, 2010, Vol.9(7)
* Merill, K., Ernest, B., and Mark B. S. Steganography: Forensic, Security, and Legal Issues; Journal of Digital Forensics, 01 June 2008, Vol.3(2), pp.17-34
* Saiful Islam, Mangat R Modi, Phalguni Gupta (2014) Edge-based image steganography Retrieved From: https://link.springer.com/article/10.1186/1687-417X-2014-8

PDF’s

* Chris Christensen (2015) Simple Substitution Ciphers (Page No. 33) Retrieved From: https://www.nku.edu/~christensen/1402%20Simple%20substitution%20and%20Caesar%20cipher.pdf
* Dworkin, M., NIST Special Publication 800-38A, 2001 Edition: Recommendation for Block Cipher Modes of Operation, Methods and Techniques, December 2001, Natl. Inst. Stand. Technol. [Web page], http://www.csrc.nist.gov/publications/ nistpubs/800-38a/sp800-38a.pdf.
* Eltyeb E. A bed Elgabar (2013) Comparison of LSB Steganography in BMP and JPEG Images (Volume-3, Issue-5) International Journal of Soft Computing and Engineering (IJSCE) Retrieved From: https://pdfs.semanticscholar.org/ea32/dbcb2a1027af4c9c0676d08ee6d470aa6a2d.pdf
* J. OrlinGrabbe: The DES Algorithm Illustrated (Vol 2, No. 28.) Laissez Faire City Times, Retrieved From: http://www.citethisforme.com/guides/apa-annotated-bibliography/how-to-cite-a-ebook
* Jasmendez: THESIS IT - LYCEUM OF THE PHILIPPINES UNIVERSITY CAVITE Retrieved From: https://www.coursehero.com/file/17205794/THESIS-IT/
* MazdakZamani, AzizahBt Abdul Manaf, Shahidan M. Abdullah (2012). An Overview on Audio Steganography Techniques (vol6.issue13.13) International Journal of Digital Content Technology and its Applications(JDCTA) Retrieved From: http://www.globalcis.org/jdcta/ppl/JDCTA%20Vol6%20No13%20Binder1\_part13.pdf
* Kumari, Sarita (2017). A research Paper on Cryptography Encryption and Compression Techniques (Volume 6 Issue, Page No. 20915-20919) Retrieved From: file:///D:/INSTALLLER/3630-Article%20Text-6635-1-10-20180104.pdf
* Louis Anthony T. Flores (2012). RIALTHO: Application of 512 Bit Block Size Using Encryption/Description Algorithm Retrieved From: https://etd.ohiolink.edu/rws\_etd/document/get/toledo1341524458/inline
* Ross J. Anderson, Fabien A.P. Petitcolas (1998). On The Limits of Steganography (16(4):474-481) IEEE Journal of Selected Areas in Communications Retrieved From: https://www.cl.cam.ac.uk/~rja14/Papers/jsac98-limsteg.pdf
* Ruchita Sharma, Swarnalata Bollavarapu (2015). Data QuickCrypto Compression and Cryptography Techniques (Volume 117 – No.14) Retrieved From: https://research.ijcaonline.org/volume117/number14/pxc3903342.pdf
* SyedaMusfiaNasreen , Gaurav Jalewal, Saurabh Sutradhar (2015). A Study on Video Steganographic Techniques (Volume, 05 Issue, 10) International Journal of Computational Engineering Research (IJCER) Retrieved From: http://www.ijceronline.com/papers/Vol5\_issue10/E0510030034.pdf
* Sakshi Jindal, Navdeep Kaur (2016). DIGITAL IMAGE STEGANOGRAPHY SURVEY AND ANALYSIS OF CURRENT METHODS (Vol.6, No3). IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) Retrieved From: https://ijcsits.org/papers/vol6no32016/3vol6no3.pdf

Appendices

Appendix A. Gantt Chart

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| MONTH | JUNE | | | | JULY | | | | AUGUST | | | | SEPTEMBER | | | | OCTOBER | | | | NOVEMBER | | | | DECEMBER | | | | JANUARY | | | | FEBRUARY | | | | MARCH | | | |
| ACTIVITY |
| Requirements Gathering |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Research |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Quick Design & Building  Prototype |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Making Flow Chart |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Coding |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| User Evaluation |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Testing |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Evaluation |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Refinement |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

Appendix B. Actual Thesis Expenses

THESIS EXPENSES

|  |  |  |  |
| --- | --- | --- | --- |
| Quantity | Specifics | Approximate Cost | Actual Cost |
| 41 | Mobile data connection expenses per week used for research. | PHP 3,690 | PHP 3,690 |
| 33 | PC Rental | PHP 1,650 | PHP 1,650 |
|  | Printing and Xerox | PHP 1,000 |  |
| 4 person | Foods and Drinks | PHP 2,500 | PHP |
| 1 | Project Documentation Peripherals | PHP 500 | PHP 500 |
| 4 person | Fare | PHP 650 | PHP 640 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Prepared by:

Gian Daniel C. Buenaventura Marjorie Mae F. De Leon

Johnivan B. De Mesa Bernabe S. Posada Jr.

Noted by:

Ma. Guia C. Buenaventura Michelle F. De Leon

Ma. Corazon De Mesa Emelita V. Sy

Approved by:

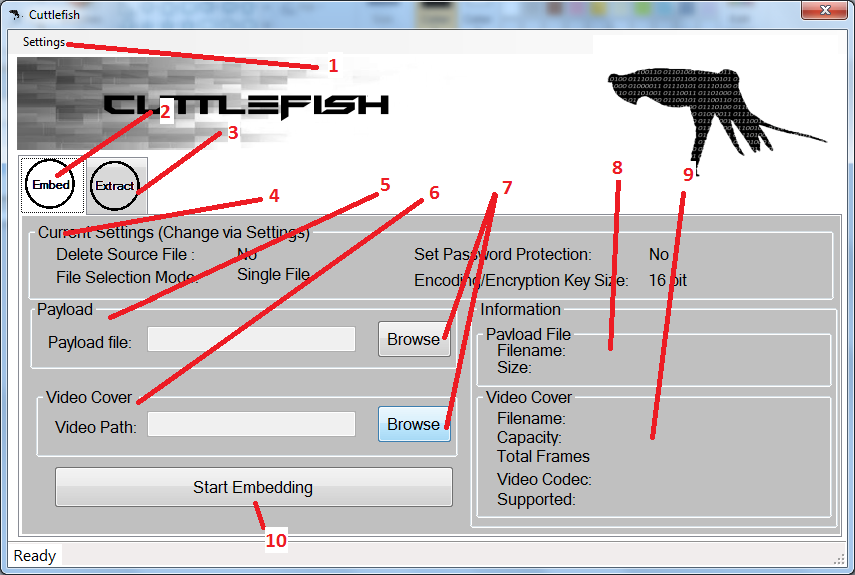
Engr. Ronaldo Doctolero Jeanny o. Garcia

Appendix C.USER’s MANUAL

Appendix C. User’s Manual

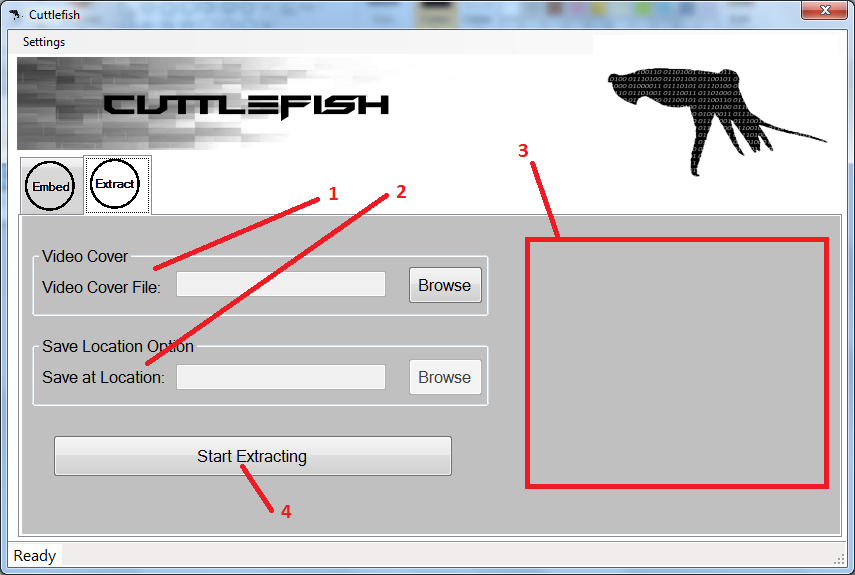
System Window Overview

Embed Tab



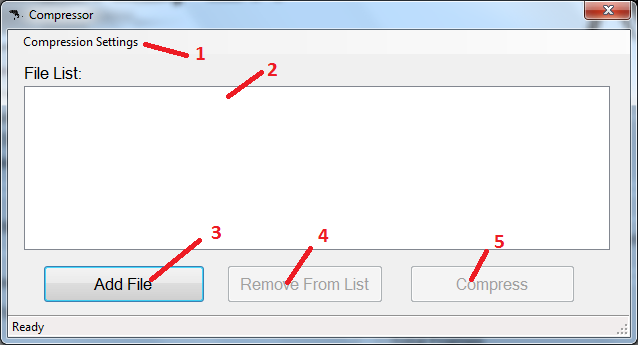
1. Settings
2. Embed Tab
3. Extract Tab
4. Current Settings Label Group box
5. Payload Input Group box
6. Video Cover Input Group
7. Browse Button
8. Payload Information Label Group box
9. Video Cover Information Label Group box
10. Embed Button

Extract Tab



1. Video Cover Group box
2. Save Location Option Group box
3. Embedded File Information Field
4. Start Extracting button

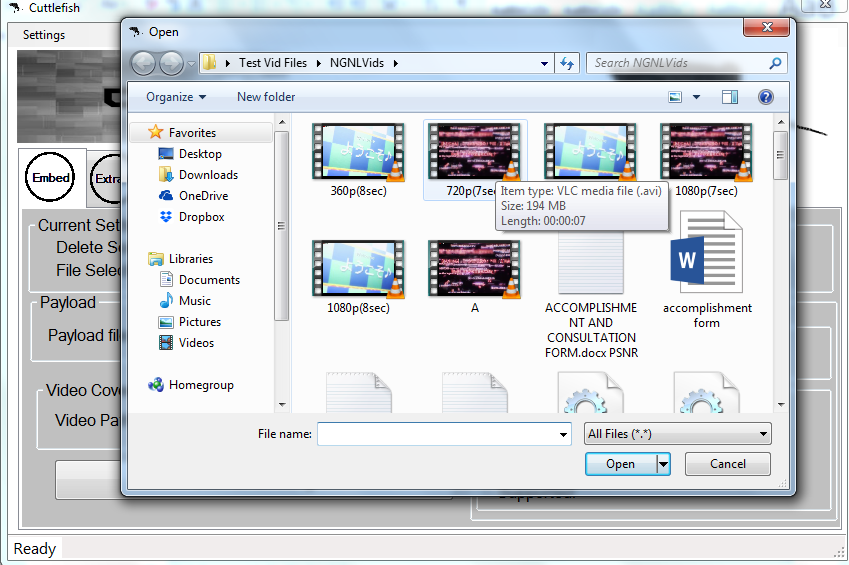
Compressor Window



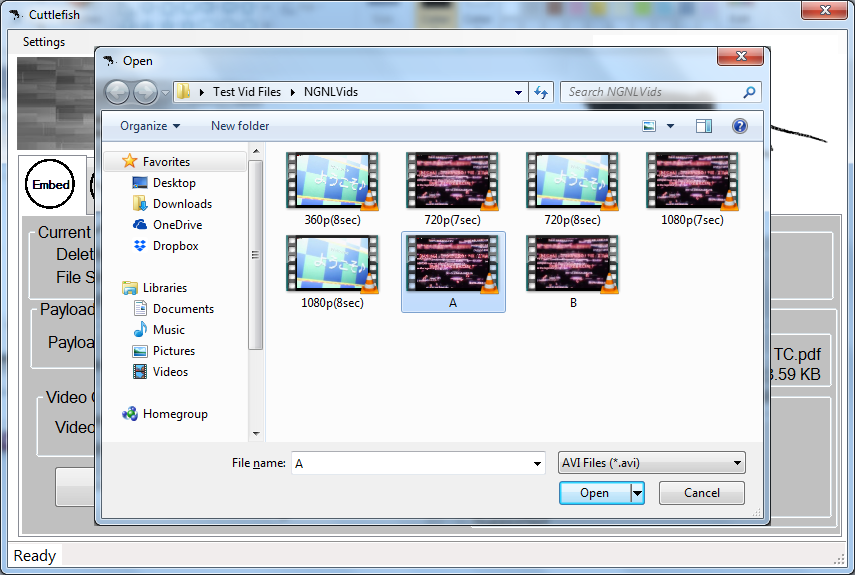
1. Compression Settings
2. File List
3. Add File button
4. Remove From List button
5. Compress button

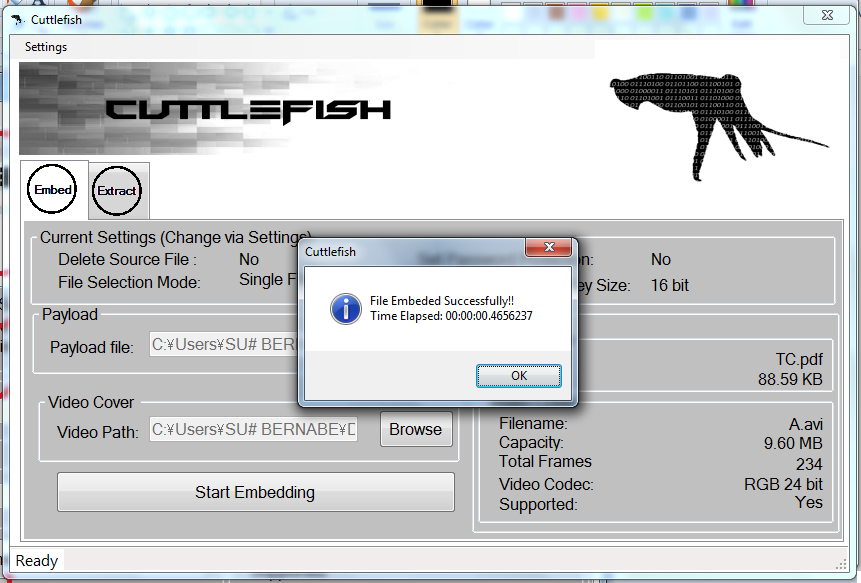
How to Embed a file

1. Open the program and select Embed Tab
2. Click Browse under Payload Input Group box then choose the file you want to embed then click Open



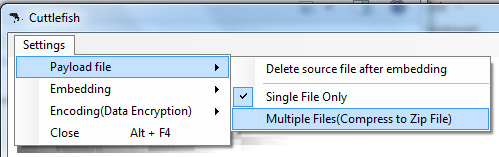
1. After you click Open the program will load the file’s information and display it on Payload Information Label Group box
2. Now Click Browse under Video Cover Input Group box then choose a suitable AVI video cover then click Open



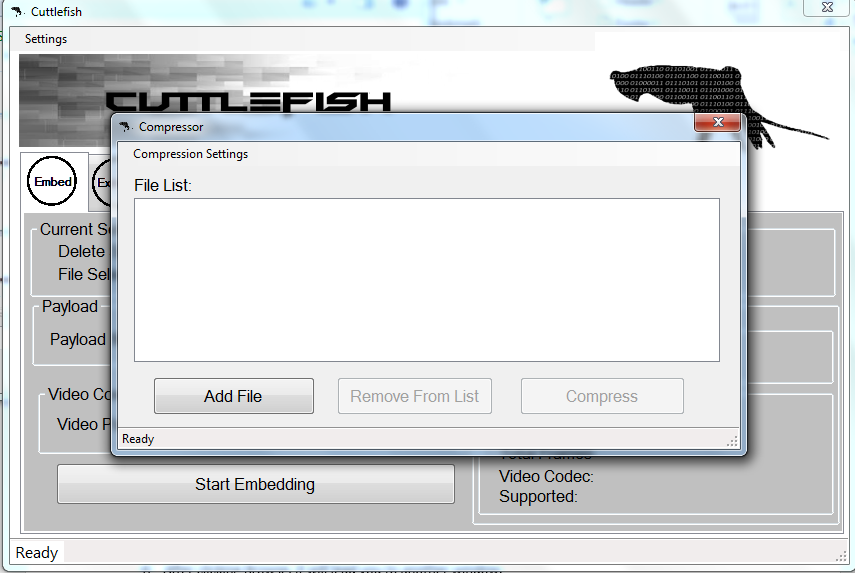
1. After you click Open the system will load and display the Video Cover Information on Video Cover Information Group box
2. Click Start Embedding to begin embedding the file.
3. After the program finishes embedding the file, a message box will appear to the screen to inform that the program finishes its task 
4. The Video Cover is now embedded with a file awaiting its extraction.

How to Embed Multiple Files

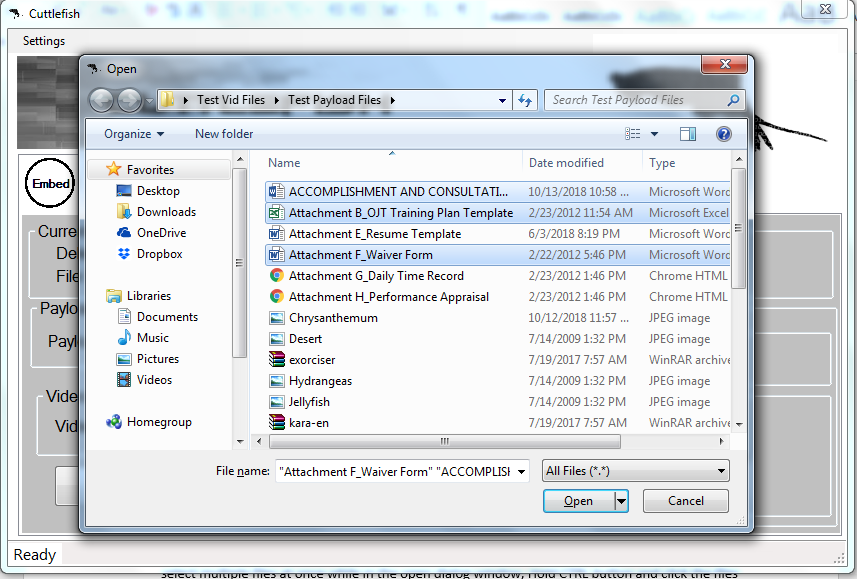
1. To embed multiple files, Select Multiple Files(Compress to Zip File) under Settings > Payload File



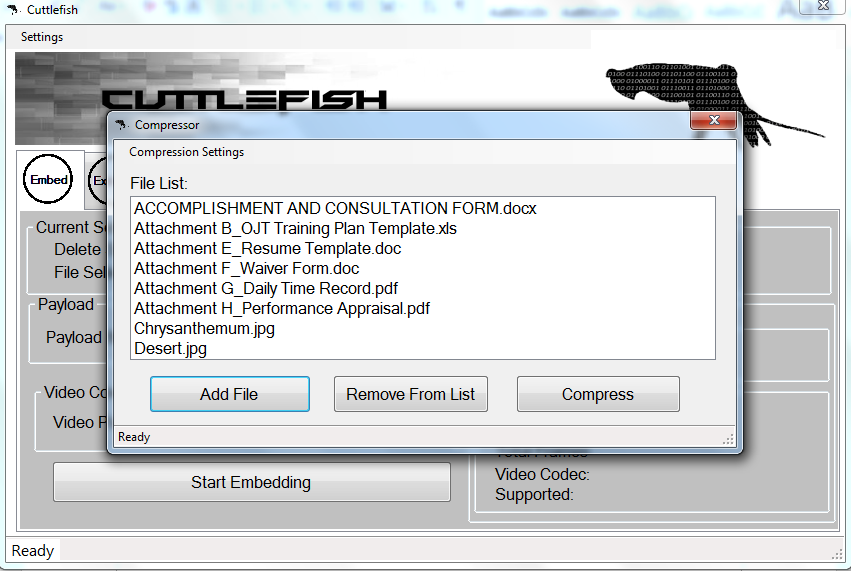
1. After selecting, the program updates Current Settings Group box to reflect changes to settings.
2. Click Browse under Payload Input Group box.
3. After clicking Browse, it will lead you to another window.



1. To add files to the list, Click Add File. Choose the file you wish to add then Click Open. NOTE: to select multiple files at once while in the open dialog window, Hold CTRL button and click the files you wish to add.

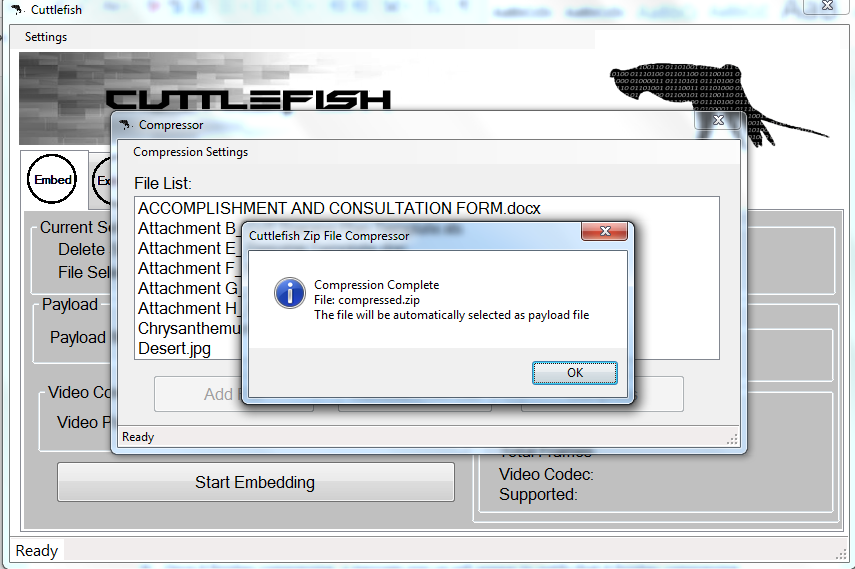


1. After you clicked Open, the file will be added to the list.

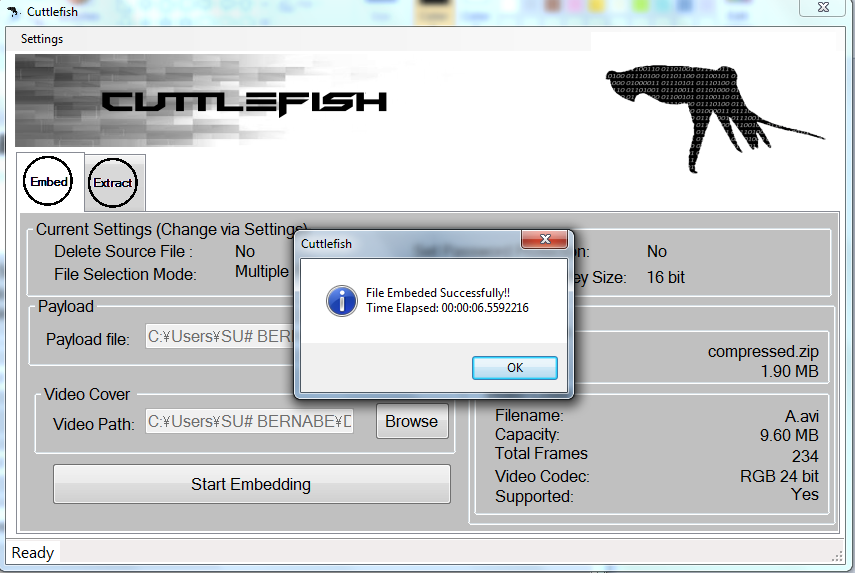


1. If you want to remove some files on the list, select the filename then click Remove From List.
2. Once you are done, click Compress and wait for the program to finish compressing.

1. Once it finishes compressing, a message pop up will appear to notify that it finishes compressing the file and automatically closes the window and choose the compressed file as payload.



1. To embed the compressed file, refer to step 4 to 8 of “How to embed a file” included in this manual.

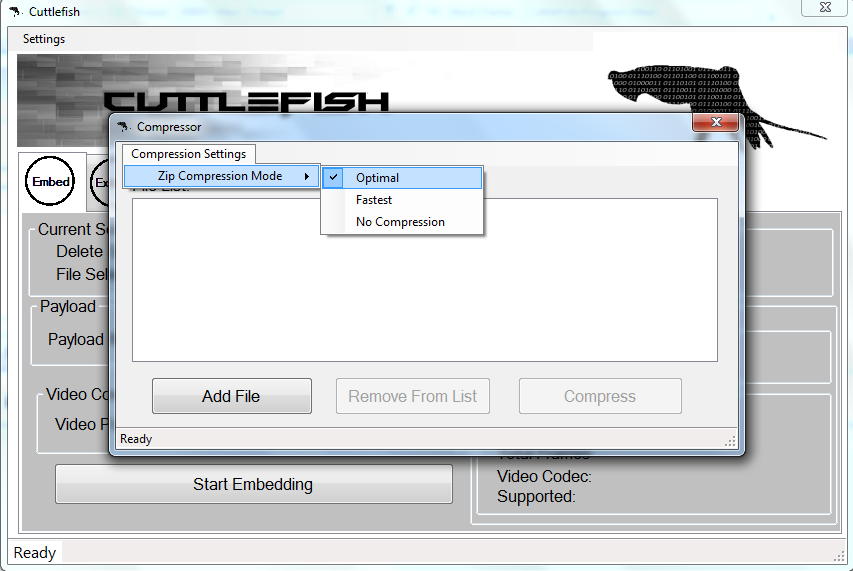


1. To switch back on selecting only a single file, go to Settings > Payload File again and

click Single File Only.

Checking and Changing mode of the Program’s Compressor module.

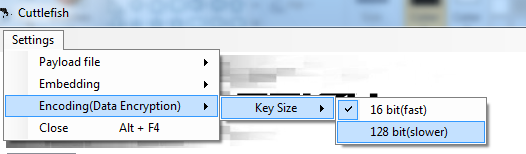
1. The program compress multiple files to zip files in order to fit it on a single video cover. Currently its supports 3 modes of compression, Optimal, Fastest, and No Compression. To check the mode being used, go to Compression settings > Zip Compression Mode



1. Each Modes yields different compressed file size from no compression(just combine files to one and may bigger than the size of the files combined),Fastest(fast compression but bigger file size) to optimal(smallest file size but slower).To change the mode to be use , click on desired mode.

Changing how the system encodes payload data to video cover

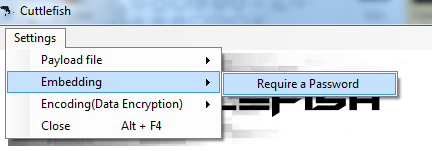
1. The program uses its own dedicated encryption algorithm to encode data. This to ensure that only the system can extract the embedded file. It can use a quick 16 bit key or a slower 128 bit key for encryption to encode the data. To change the key size used, go to Settings > Encoding(Data Encryption) > Key Size.



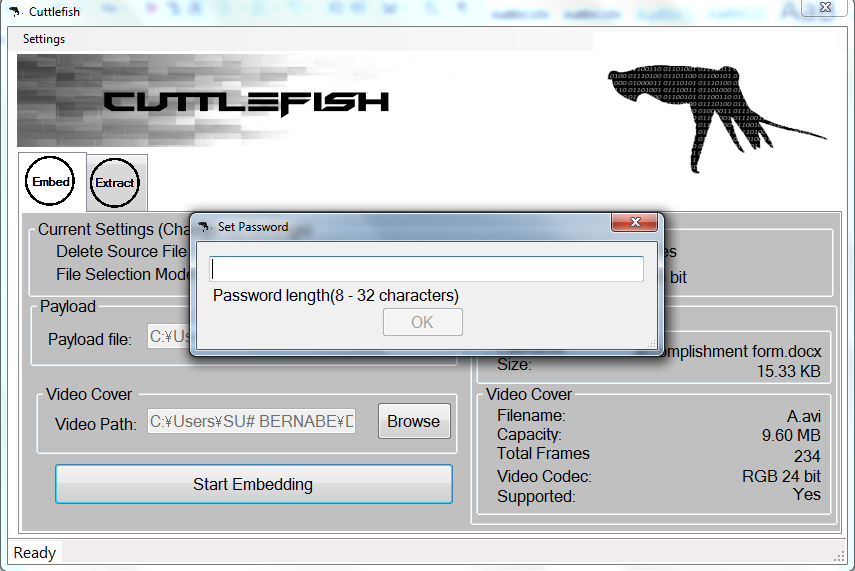
1. Click on Desired Key Size.
2. After clicking, the system will now use the selected key size on next embedding.

Protecting embedded data with password

1. To set a password whenever one tries to extract your embedded file, go to Settings > Embedding > and click Require a Password



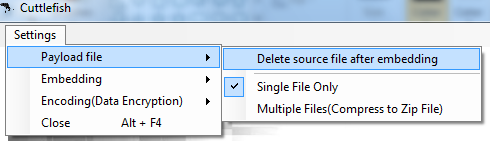
1. After clicking Require a Password, it will now require you to set a password whenever you embed. It will show a pop up window for you to set a password when you click Start Embedding



1. Enter your desired password and click OK
2. After clicking OK, whenever someone tries to extract the embedded data it will need to enter a password to extract the data.
3. To turn off Password Protection on your next embedding, go to Settings, Embedding again and click Require a Password.

Deleting Payload File after Embedding

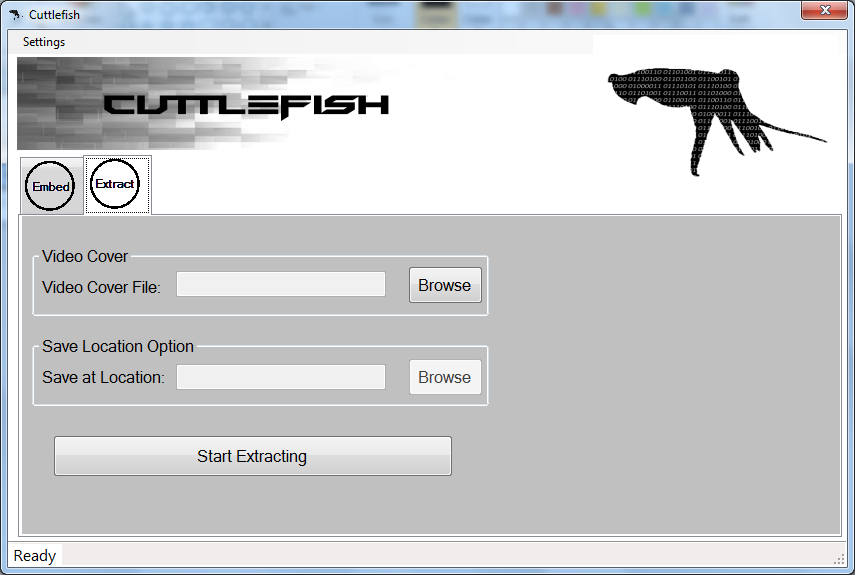
1. If you wish to delete the source payload file after embedding it to a video cover, go to Settings > Payload file and click Delete source file after embedding



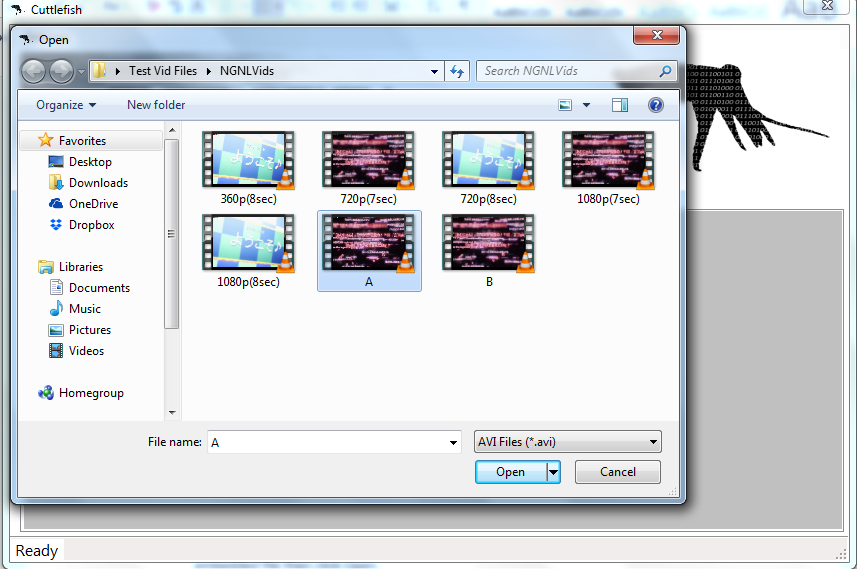
1. The program will now automatically delete the file after embedding it on a video cover.
2. To turn off automatic deletion of payload file, go to Settings > Payload file again and click Delete source file after embedding

How to Extract data from a Video File

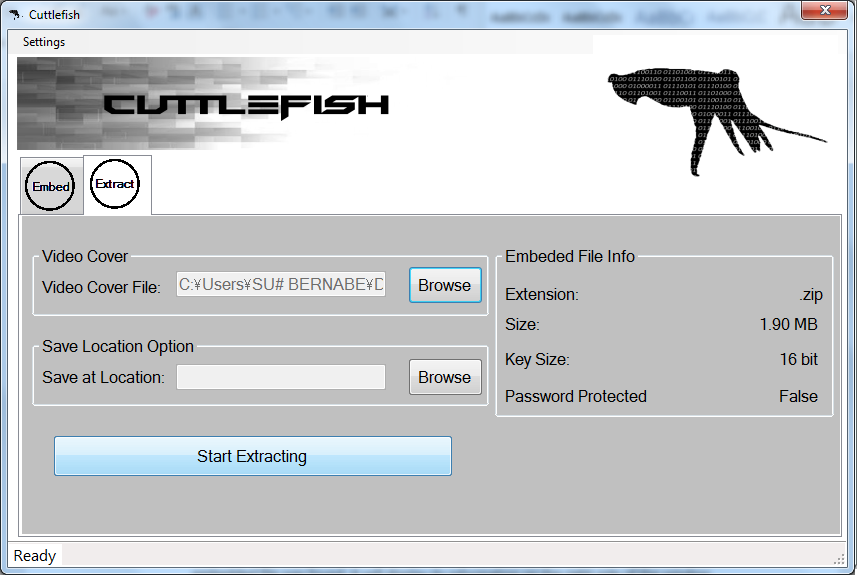
1. From Embed Tab, Click Extract Tab to switch to extract module.



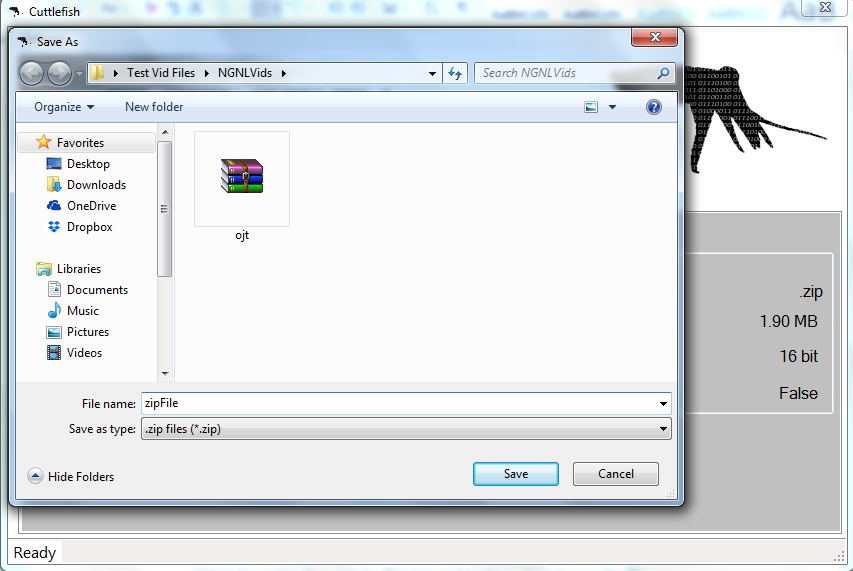
1. Under Video Cover Group box, Click Browse then choose a video cover carrying an embedded file then click Open.



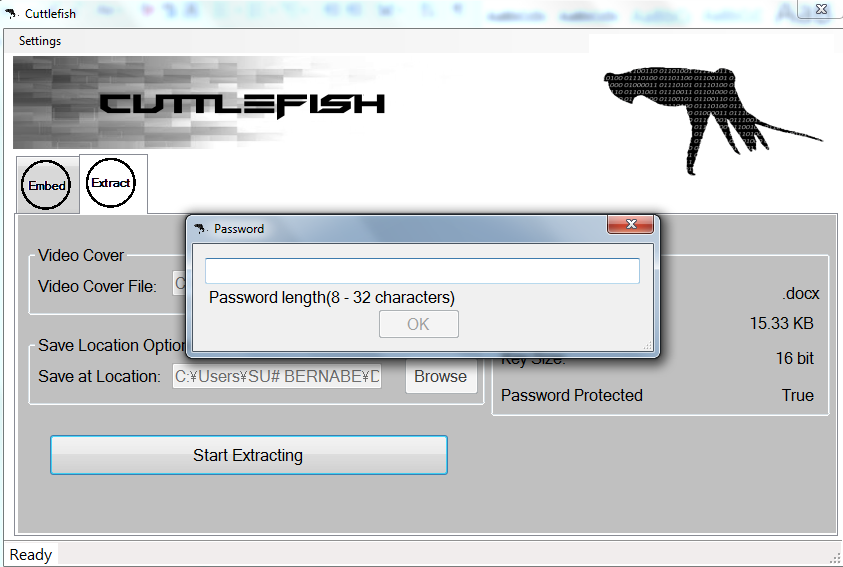
1. After clicking Open, the program will search the video cover for embedded data. If an embedded file was found, it will display its information on the right side of the window



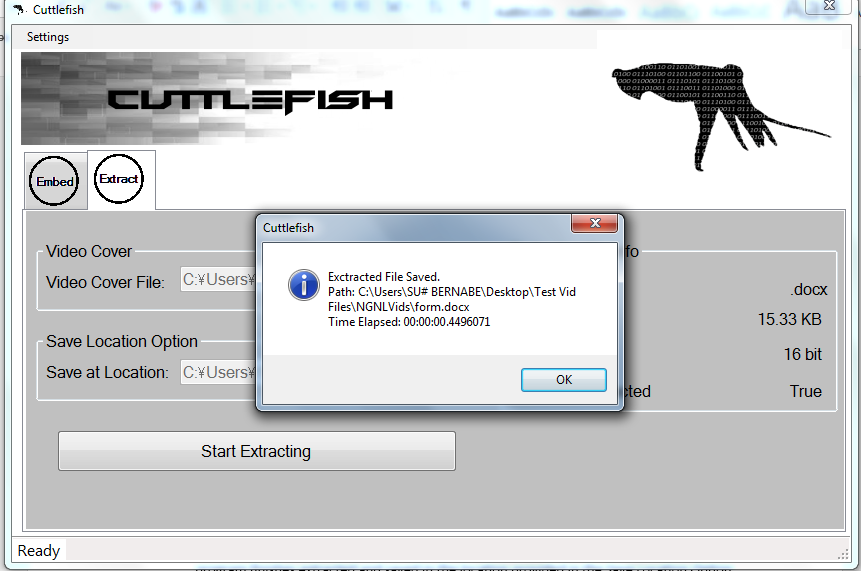
1. To provide a save location for the embedded file, click on Browse under Save Location Option Group box then give it a filename and location where to save the file then click Save.



1. After clicking Save, click Start Extracting.
2. A popup window will appear requiring you to enter a password if a password was set during embedding the file. Enter the right password and click OK to extract the file. If no password was set, it will proceed to extraction.



1. After the program finishes extracting the file, a pop up window will appear informing the program finishes extracted and saved in the location provided in the Save Location Option Group box.



Appendix D. Curriculum Vitae of Researchers

Curriculum Vitae of

GIAN DANIEL C. BUENAVENTURA

31-A First Reyville Subdivision, Habay II, Bacoor City 4102

Gian2099@gmail.com

#09258085666

EDUCATIONAL BACKGROUND

|  |  |  |
| --- | --- | --- |
| Level | Inclusive Dates | Name of school/ Institution |
| Tertiary | June 2015 ~ present | STI Collage Bacoor , Cavite |
| Tertiary | June 2013 ~ March 2015 | Mapúa Institute of Technology , Manila |
| High School | June 2009 ~ March 2013 | St. Rose of Lima School, Las Pinas |
| Elementary | June 2002 ~ March 2008 | Benedictine Institute of Learning, Imus |

PROFESSIONAL OR VOLUNTEER EXPERIENCE

|  |  |  |  |
| --- | --- | --- | --- |
| Inclusive Dates | Nature of Experience/  Job Title | Name and Address of Company or Organization |  |
|  |  |  |  |
| n/a |  |  |  |
|  |  |  |  |

AFFILIATIONS

|  |  |  |
| --- | --- | --- |
| Inclusive Dates | Name of Organization | Position |
| January 2017 ~ present | Cavite Real Bikers | Member |
| June 2016 ~ present | Cavite Ghost Bikers | Member |
| November 2015 ~ present | Vigintillion Society | Vice President |
|  |  |  |

SKILLS

|  |  |  |
| --- | --- | --- |
| SKILLS | Level of Competency | Date Acquired |
| Web Programming | Beginner | November 2017 |
| C# Programming | Average | June 2016 |
| C++ Programming | Average | March 2014 |
| Java Programming | Average | June 2015 |

TRAININGS, SEMINARS OR WORKSHOP ATTENDED

|  |  |
| --- | --- |
| Inclusive Dates | Title of Training, Seminar or Workshop |
| January 21, 2018 | Leadership Workshop |
| February 7, 2017 | Embracing the Grind. Facing the Giants of Life. |
| December 14, 2016 | Student Convention |
| July 19, 2015 | Student Development Seminar: Self-Development |

Curriculum Vitae of

MARJORIE MAE F. DE LEON

209 B int. Tramo St. Tabon III Kawit, Cavite

Marjdeleon0799@yahoo.com

#09064403055

EDUCATIONAL BACKGROUND

|  |  |  |
| --- | --- | --- |
| Level | Inclusive Dates | Name of school/ Institution |
| Tertiary | 2015-Present | STI college Bacoor |
| High School | 2011-2015 | Emiliano TriaTirona Memorial National High School |
| Elementary | 2005-2011 | Aguinaldo Elementary School |

PROFESSIONAL OR VOLUNTEER EXPERIENCE

|  |  |  |
| --- | --- | --- |
| Inclusive Dates | Nature of Experience/  Job Title | Name and Address of Company or Organization |
|  |  |  |
| n/a |  |  |
|  |  |  |
|  |  |  |

AFFILIATIONS

|  |  |  |
| --- | --- | --- |
| Inclusive Dates | Name of Organization | Position |
| June 2016 ~ present | Vigintillion Society | Secretary |
|  |  |  |
|  |  |  |
|  |  |  |

SKILLS

|  |  |  |
| --- | --- | --- |
| SKILLS | Level of Competency | Date Acquired |
| Web Programming | Beginner | November 2017 |
| C# Programming | Average | June 2016 |
| C++ Programming | Average | March 2014 |
| Java Programming | Average | June 2015 |

TRAININGS, SEMINARS OR WORKSHOP ATTENDED

|  |  |
| --- | --- |
| Inclusive Dates | Title of Training, Seminar or Workshop |
| February 7, 2017 | Embracing the Grind. Facing the Giants of Life. |
| December 14, 2016 | Student Convention |
| July 19, 2015 | Student Development Seminar: Self-Development |
|  |  |

Curriculum Vitae of

JOHNIVAN B. DE MESA

Block 13 Lot 6 Montefaro west bucandala Imus Cavite

Ivanstorm117@gmail.com

#09065567770

EDUCATIONAL BACKGROUND

|  |  |  |
| --- | --- | --- |
| Level | Inclusive Dates | Name of school/ Institution |
| Tertiary | 2014-Present | STI college Bacoor |
| High School | 2009-2014 | Imus institute |
| Elementary | 2005-2011 | MCA Montessori school |

PROFESSIONAL OR VOLUNTEER EXPERIENCE

|  |  |  |
| --- | --- | --- |
| Inclusive Dates | Nature of Experience/  Job Title | Name and Address of Company or Organization |
|  |  |  |
| n/a |  |  |
|  |  |  |
|  |  |  |

AFFILIATIONS

|  |  |  |
| --- | --- | --- |
| Inclusive Dates | Name of Organization | Position |
|  |  |  |
| n/a |  |  |
|  |  |  |
|  |  |  |

SKILLS

|  |  |  |
| --- | --- | --- |
| SKILLS | Level of Competency | Date Acquired |
| English Fluency | Expert | 1999 |
| C# Programming | Beginner | 2016 |
| Java Programming | Beginner | 2015 |

TRAININGS, SEMINARS OR WORKSHOP ATTENDED

|  |  |
| --- | --- |
| Inclusive Dates | Title of Training, Seminar or Workshop |
| February 7, 2017 | Embracing the Grind. Facing the Giants of Life. |
| December 14, 2016 | Student Convention |
| July 19, 2015 | Student Development Seminar: Self-Development |

Curriculum Vitae of

BERNABE S. POSADAS JR.

Blk 8 Lot 9 Terrassa ph2, Imus Cavite

bernabe\_posadas@yahoo.com

#09453540754

EDUCATIONAL BACKGROUND

|  |  |  |
| --- | --- | --- |
| Level | Inclusive Dates | Name of school/ Institution |
| Tertiary | 2015-Present | STI college Bacoor |
| High School | 2011-2015 | Gen. Emilio Agunaldo National High School |
| Elementary | 2004-2011 | BuhaynaTubig Elementary School |

PROFESSIONAL OR VOLUNTEER EXPERIENCE

|  |  |  |
| --- | --- | --- |
| Inclusive Dates | Nature of Experience/  Job Title | Name and Address of Company or Organization |
|  |  |  |
| 2018 – 2019 | Student Assistant | STI College Bacoor |
|  |  |  |
|  |  |  |

AFFILIATIONS

|  |  |  |
| --- | --- | --- |
| Inclusive Dates | Name of Organization | Position |
|  |  |  |
| n/a |  |  |
|  |  |  |
|  |  |  |

SKILLS

|  |  |  |
| --- | --- | --- |
| SKILLS  Phyton Programming | Level of Competency  Beginner | Date Acquired  2018 |
| C# Programming | Average | 2016 |
| Java Programming | Beginner | 2015 |
| Web Programming | Beginner | 2015 |

TRAININGS, SEMINARS OR WORKSHOP ATTENDED

|  |  |
| --- | --- |
| Inclusive Dates | Title of Training, Seminar or Workshop |
| February 7, 2017 | Embracing the Grind. Facing the Giants of Life. |
| December 14, 2016 | Student Convention |
| July 19, 2015 | Student Development Seminar: Self-Development |