

IMAGE STEGANOGRAPHY USING HASH
FUNCTION AND COMPRESSION

AHMAD SULAIMAN BIN ZURKIFLI

Bachelor of Computer Science (Network
Engineering) with Honours

UNIVERSITI MALAYSIA PAHANG

UNIVERSITI MALAYSIA PAHANG

DECLARATION OF THESIS AND COPYRIGHT

Author's Full Name : Ahmad Sulaiman Bin Zurkifli

Date of Birth :

Title : Image Steganography using Hash Function and Compression

Academic Session : Sem 1 2022/2023

I declare that this thesis is classified as:

- CONFIDENTIAL (Contains confidential information under the Official Secret Act 1997)*
- RESTRICTED (Contains restricted information as specified by the organization where research was done)*
- OPEN ACCESS I agree that my thesis to be published as online open access (Full Text)

I acknowledge that Universiti Malaysia Pahang reserves the following rights:

1. The Thesis is the Property of Universiti Malaysia Pahang
2. The Library of Universiti Malaysia Pahang has the right to make copies of the thesis for the purpose of research only.
3. The Library has the right to make copies of the thesis for academic exchange.

Certified by:

(Student's Signature)

(Supervisor's Signature)

New IC/Passport Number:
001024-11-0437
Date: 28/07/2023

Name of Supervisor:
Ts. Dr. Liew Siau Chuin
Date: 28/07/2023

NOTE : * If the thesis is CONFIDENTIAL or RESTRICTED, please attach a thesis declaration letter.



SUPERVISOR'S DECLARATION

I/We* hereby declare that I/We* have checked this thesis/project* and in my/our* opinion, this thesis/project* is adequate in terms of scope and quality for the award of the degree of *Doctor of Philosophy/ Master of Engineering/ Master of Science in

(Supervisor's Signature)

Full Name : Liew Siau Chuin
Position : SENIOR LECTURER
FACULTY OF COMPUTING
COLLEGE OF COMPUTING & APPLIED SCIENCE
UNIVERSITI MALAYSIA PAHANG
Date : 26600 PEKAN, PAHANG DARUL MAKMUR
TEL : 09-424 4645 FAX : 09-424 4666
28/07/2023



STUDENT'S DECLARATION

I hereby declare that the work in this thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at Universiti Malaysia Pahang or any other institutions.

(Student's Signature)

Full Name : AHMAD SULAIMAN BIN ZURKIFLI

ID Number : CA20158

Date : 28/07/2023

IMAGE STEGANOGRAPHY USING HASH FUNCTION AND COMPRESSION

AHMAD SULAIMAN BIN ZURKIFLI

Thesis submitted in fulfillment of the requirements
for the award of the degree of
Doctor of Philosophy/Master of Science/Master of Engineering

Faculty of Computing
UNIVERSITI MALAYSIA PAHANG

JANUARY 2023

ACKNOWLEDGEMENTS

I want to start by expressing my gratitude to Ts. Dr. Liew Siau Chuin, who oversaw my final year project. He has been incredibly supportive of my studies and is always eager to respond to my inquiries. My supervisor helped me with my research throughout this time by applying her knowledge and experience. He always makes the opportunity to check on me, let me know how I'm doing, and give me tips on how to create a high-calibre report for my senior project.

Next, I want to express my gratitude to UMP for giving the resources I needed to conclude my research. I also value the help and support that was given. I was able to use the UMP features to access journal services using the EZPROXY UMP for searching prior research and journals associated with the title of my research, including the library explorer, IEEE explorer, and sciencedirect.com.

Finally, I would want to express my gratitude to my family for their unwavering support and assistance throughout this difficult time in my studies. Then, I must also express my gratitude to my friends, who constantly provide me advice and assist me in finishing the research.

ABSTRAK

Steganografi imej ialah kaedah untuk menyembunyikan sebarang data atau mesej rahsia dalam fail imej. Dalam kajian ini, steganografi imej, yang menggunakan kunci rahsia untuk meningkatkan keselamatan maklumat tersembunyi sambil meningkatkan pendekatan LSB, diperkenalkan. Sebelum dibenamkan ke dalam imej muka depan, imej mesej akan dimampatkan menggunakan algoritma mampatan lossy untuk mengurangkan saiz imej. Sebelum dan selepas pembedaan imej mesej, imej muka depan dicincang menggunakan fungsi cincang. Fungsi cincang akan digunakan dalam imej stego, dan hasilnya akan disimpan dalam imej hos untuk pengesahan tambahan sepanjang proses pengekstrakan. Teknik yang dicadangkan menggunakan fungsi cincang dan pemampatan lossless untuk menggambarkan steganografi imej

ABSTRACT

An image steganography is a method for concealing any data or secret messages within an image file. In this study, image steganography, which uses a secret key to improve hidden information security while enhancing the LSB approach, is introduced. Before being embedded into a cover image, the message image will be compressed using lossy compression algorithms to reduce the size of the image. Prior to and following the embedding of a message image, the cover image is hashed using the hash function. The hash function will be used in the stego image, and the result will be kept in the host image for additional verification throughout the extraction process. The suggested technique uses hash function and lossless compression to illustrate image steganography.

TABLE OF CONTENTS

CHAPTER 1	1
1.1 Introduction	1
1.2 Background of the problem	3
1.3 Objective	3
1.4 Scope	4
1.5 Thesis Organization	5
CHAPTER 2	6
2.1 Introduction	6
2.2 Three Related Work	6
2.3 Comparative Analysis	8
2.4 Chapter Summary	9
CHAPTER 3	10
3.1 Introduction	10
3.2 Research Management Framework/Methodology	10
3.2.1 Planning & Definition	11
3.2.2 Data Collection and analysis	11
3.2.3 Topic Summary	11
3.3 Project Requirement	12
3.3.1 Input and Output	12
3.3.2 Process Description	12
3.4 Propose Design	15
3.4.1 Full Flowchart of embedding process	15

3.4.2	Testing plan for embedding process	16
3.4.3	Full flowchart of extracting process	17
3.4.4	Testing plan for extracting process	18
3.4.5	Overall flowchart	19
3.5	Data Design	20
3.5.1	Cover Image and Message Image	20
3.5.2	Secret Key Preparation	23
3.5.3	Hash Function and Compression	24
3.6	Tools	25
3.7	Potential use of proposed solution	26
CHAPTER 4		27
4.1	Introduction	27
4.2	Implementations	27
4.2.1	Input	28
4.2.2	Output	29
4.2.3	Process Description	29
4.2.4	Case Study	30
4.3	Result	31
4.3.1	Embedding	31
4.3.2	Extracting	36
4.4	Analysis of the Result	39
CHAPTER 5		40
5.1	Introduction	40
5.2	Objective Revisited	40

5.3	Limitation	41
5.4	Conclusion and Future Work	42

LIST OF TABLES

Table 1: Comparative Analysis	8
Table 2: Preparation of secret key	23
Table 3: Embedding result for Lena.png	31
Table 4: Embedding result for Baboon.png	32
Table 5: Embedding result for Pepper.png	33
Table 6: Embedding result for Baboon2.png	34
Table 7: Embedding result for Cat.png	35
Table 8: Extracting process for different stego image and same message image	39

LIST OF FIGURES

Figure 1: Embedding Process	13
Figure 2: Extraction Process	14
Figure 3: Full flowchart of embedding process	15
Figure 4: Full flowchart of extracting process	17
Figure 5: Overall Flowchart	19
Figure 6: lena.png	21
Figure 7: Pepper.png	21
Figure 8: Baboon.png	21
Figure 9: Example of message image	22
Figure 10: Example of information message image	22
Figure 11: MatLab Logo	25
Figure 12: Sample image	28
Figure 13: Ghant Chart	45

LIST OF ABBREVIATIONS

LSB	Least Significant Bit
SHA	Secure Hash Algorithm
PSNR	Peak Signal-to-Noise Ratio
MSE	Mean Squared Error
1D	1 Dimensional

CHAPTER 1

INTRODUCTION

1.1 Introduction

The process of hiding text, audio, image, or information in another text, audio, or image is called steganography(*What Is Steganography? - Definition from SearchSecurity*, n.d.). To avoid being discovered, it involves hiding sensitive data inside of an ordinary, message or non-secret file. The information that was hidden in the steganography will subsequently be removed from the regular file or communication to prevent discovery. When used with encryption, steganography is a further step that can be used to hide or safeguard data. The word steganography is from two keywords that have been combined that are “steganos” which means concealed or covered and “graphein” which means writing(*What Is Steganography? - Definition from SearchSecurity*, n.d.). Several types of steganography are video steganography, audio steganography, image steganography, and text steganography. The process of steganography can be divided into two which is embedding function and decoding function.

There are two types of image compression in image steganography which is lossless compression and lossy compression (*(PDF) Colour Image Steganography Using SHA-512 and Lossless Compression*, n.d.). Lossless compression ensures that image quality is maintained even when the file size is lowered. The file can also be decompressed to get it back to how it was before. Lossy compression raises the potential that the messages that have been embedded can be partially lossy but the advantage of the lossy compression is size smaller. So, if any image wants to be compressed before be embedded to image steganography, lossy compression is much preferable since it can make the image smaller. In image steganography which is to hide data or information in an image, compression is much preferable to did before embedded in the cover image to prevent from the bad result and quality of image steganography.

LSB or Least Significant Bit is a binary number's lowest bits (Raggo & Hosmer, 2013). For example, "0" at the right most is the least significant bit in "10010010" binary number. The usage of LSB in image steganography is it replace least significant bit of image with the bits of message to be hidden(Raggo & Hosmer, 2013). Any image format is a fantastic option for LSB steganography. Since the LSB operates in the spatial domain, it is crucial that no error of any kind be introduced. By using this technique, part of the LSB in the cover picture are switched out for the secret data bits of the hidden message. Although LSB offers simple computations, its capacity is constrained. Due to how simple it is to obtain the secret message by obtaining the LSB, the simple LSB technique is likewise not reliable. Since the LSB inversion method improves the stego image quality, it is preferred. This method inverts the LSB of each pixel's cover based on secret data values rather than replacing them(Raggo & Hosmer, 2013).

Any function that converts data of any size into fixed-size values is called hash function. Hash values, digests, hash codes, or just hashes are the names given to the results of a hash function. The values are typically used to index a hash table, a fixed-size table. Scatter storage addressing or hashing referred for a hash function that is used to index a hash table. For covers hash function, MD5, SHA-1, SHA-256, and whirlpool are the most popular and likely to be used. The Security Hash Algorithm (SHA), used in the Digital Signature Standard (DSS), was authorised in 1993. The initial iteration of SHA, known as SHA-0, is utilised in the literature on cryptography (Mironov, 2005). Because SHA-1 features an additional instruction that is significant from a cryptanalytic standpoint, it different from SHA-0. As a result, SHA-1 take the place of SHA-0, and the SHA family keeps developing, leading to SHA-224, 256, 384, 512 and the whirlpool hash function.

1.2 Background of the problem

In the age of technology, the use of steganography in an organization is very important in order to protect the important information of an organization from being stolen by the wrong person such as hackers. There are many organizations that have important information that they want to hide from outsiders but do not know the best way to hide it. This is because, in today's technological age, experts in the field of IT security such as hackers can detect and obtain information that they want from any organization easily in various ways. Therefore, the use of steganography is one of the solutions for this problem. If important information can be stolen by outsiders, most likely, a person or an organization may spend a lot of money to recover the information. If the information has been hidden such as using image steganography, it is most likely that the information cannot be known by outsiders because it has been hidden in the cover image. Although the hackers can steal the steganography image that has information hidden in it, it is most likely that the hackers do not know that there is information in the image. Although some of organization can produce image steganography easily, but the quality of the image steganography may not be guaranteed. Because of that, this propose research is important in order to know whether image steganography can be a high quality or not by implementing hash function and compression.

1.3 Objective

There are three objectives that are:

- 1.) To study image steganography using hash function and compression
- 2.) To develop image steganography using lossless compression and SHA-512
- 3.) To evaluate the proposed algorithm

1.4 Scope

Target User:

Authorities or governments who want to keep sensitive data hidden, especially information on their users or clients, are doing so for security reasons. Any message or piece of information can be concealed using image steganography, and only certain recipients will be able to see it. It is done to prevent the effortless theft of any essential information by undesirable or other people. In other words, using image steganography, information or a message in an image can be safely concealed. For this, primarily any authorities, organisations, or governments that must safeguard consume information at all times.

Image format: Portable Network Graphics (PNG)

Software:

- MatLab
- Microsoft Office Word

1.5 Thesis Organization

Chapter 1 explains about the propose research which is image steganography using hash function and compression by describing the concepts, technique and theory of steganography. This chapter also provides background of the problem that the suggested study is intended to address. This chapter also provided and expounded on other examples of the problem. The following three research objective are also covered in this chapter. The research scope is also briefly explained in this chapter to wrap things up.

Chapter 2 is the component of this thesis devoted to literature review. Three works that are linked to this research are examined in this chapter. This chapter also provides explanation for all three linked works, including the methodology used in each work and how they were used. The three linked works were then subjected to a comparison examination, and this chapter also evaluated each work's benefits and drawbacks.

Chapter 3 is the part of this thesis devoted to methodology. This chapter includes the introduction, which explains what was accomplished in chapter 3, This chapter also covered the project requirements, such as the flowchart of the process, and the framework or technique for research management. Next, this chapter also provided the proposed design of the study, proof of initial concept, and lastly, the Gantt chart. All of these things are explained in the chapter 3.

Chapter 4 covered the discussion and outcomes of this thesis. The results or outcomes of the suggested research are presented in this chapter in terms of PSNR value obtained. To assess if the outcome seems to be of high quality or not, a brief explanation is provided along with each PSNR number. Finally, this chapter also includes the study's functional test results.

Chapter 5 is the chapter that concludes this thesis. The goals of the suggested research are reviewed in this chapter. Other than that, this chapter also discusses the constraints or limitations of the suggested research. Lastly, some recommendations for the research's future work are also provided.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

There are three works related to this research will be explored in this chapter. The explanation about the related works will be given such as the methods that these works use and how it was deployed. Other than that, this chapter also will show the comparatively analysis of these three works and the advantage and disadvantage of it.

2.2 Three Related Work

There are three related work or method that will be explained in this chapter that are Dedi and Akmal's method, Cheng method, and Marghny and Loay method. Dedi and Akmal's method(Darwis et al., 2021) introduces a novel approach named Center Embedded Pixel Positioning (CEPP) to address the cropping problem in steganography. CEPP utilizes Least Significant Bit (LSB) Matching and centers the secret image within the cover image. The experiment's evaluation revealed that the secret image can be recovered through sequential cropping of up to 40% on any side (left, right, up, or bottom) of the cover image. The secret image can also be retrieved when a total asymmetric cropping area covers 25% on two sides (either left-right, left-up, or right-up). Moreover, if the total asymmetric cropping area includes the bottom part, the secret image can still be recovered with up to 70% cropping. However, if three sides are included in the asymmetric cropping area, the algorithm fails to retrieve the secret image. When cropping specifically at the bottom, the secret image can be extracted up to 70%.

Besides, for Osama and Aziza method (AbdelWahab et al., 2019), it described about image steganography techniques with compression algorithm. In this method, there is a comparison of the two technique. Least Significant Bit (LSB) was utilized in the initial technique, which lacked both encryption and compression (AbdelWahab et al., 2019). In the second technique, LSB is used after the secret message has been encrypted. Additionally, the image is transformed into the frequency domain using the discrete cosine transform (DCT). The DCT algorithm is implemented in frequency domain, where the stego-image is transformed from spatial domain to frequency domain and the payload bits are inserted into the frequency components of the cover image. Spatial domain mean that it works with image as they are while for frequency domain, it works with the rate of change of the spatial domain pixel values. The LSB algorithm is implemented in spatial domain, where the packet bits are embedded into the least significant bits of the cover image to develop the stego-image. Results from this method clearly show we are able to hide the required information in messages while reducing their size, allowing us to send the data more safely with a lower total capacity impact than with other algorithms. The effectiveness of these two approaches is assessed based on the variables MSE and PSNR.

Next, for Zahid and Hamid method (Nezami et al., 2022), it suggest a method that uses as many as four least significant bits (LSB) and a hash function to encrypt plain text as ciphertext and encode it as an image which is a stego-image (Nezami et al., 2022). Hash functions are mathematical techniques that give any entity a special identification. The message was secured using this method's use of the hash function. The hash function uses a key value and a pixel number as input and outputs a number. The sender and receiver have already exchanged the key value. A substitution cypher is used in the Caesar cypher, a type of symmetric-key cryptography. To make a text message difficult to decipher, it works by replacing the letters with random letters. This technique involves shifting each letter of a message to specific locations in the alphabet. To replace text, the LSBs of the image's pixel value are employed. Since just the LSBs are changed, human eyes are unable to predict the difference between the original image and the final image. The findings show that the suggested technique performs better than the current technique in terms of security and effectiveness with acceptable MSE and PSNR.

2.3 Comparative Analysis

Steganography Methods	Dedi and Akmal's method	Osama and Aziza 's method	Zahid and Hamid's method
Method Used	<ul style="list-style-type: none"> - Applied LSB substitution technique for the process of image steganography. - Use Center Embedded Pixel Positioning (CEPP). 	<ul style="list-style-type: none"> - Use Discrete Cosine Transform (DCT) technique to transform the image from spatial domain to frequency domain. - Applied LSB substitution technique for the process of image steganography. - Use lossy compression to compress each block after DCT was applied. 	<ul style="list-style-type: none"> - Uses as many as four least significant bits (LSB) for the process of image steganography - Uses a hash function to encrypt plain text as ciphertext and encode it as an image which is a stego-image.
Cover Image used	Baboon.png	Baboon.png	Baboon.png
PSNR value of steganography image (in dB)	50.09	51.12	43.89

Table 1: Comparative Analysis

2.4 Chapter Summary

In summary, the three works that are related to the propose research have been covered in this chapter by providing the explanation of each works including the method and difference of those works. Other than that, this chapter also have explained the comparative analysis about those works which is the method used, cover image used, and PSNR value of steganography image (in dB). From the comparison, the advantage and disadvantage each related works can been known. Based on this related works, it can be reference and guide for the propose research which is image steganography using hash function and compression.

CHAPTER 3

METHODOLOGY

3.1 Introduction

This chapter discuss about the overall approach or framework that has been used in this research. It has covered method or technique or approach to be used whereas will be discuss the methodology in details to accomplish the research. The content for this chapter contains project management framework or methodology, project requirement, propose design, data design, proof of initial concept, testing or validation plan, potential use of proposed solution, and lastly, the Gantt Chart are all included in this chapter's material. All of these topics will be discussed in this chapter.

3.2 Research Management Framework/Methodology

A framework in research can offer a structure for planning and carrying out the study, as well as help the researcher identify and solve the main problems and concerns surrounding the subject. This may entail laying out the precise methods or processes that must be followed as well as offering a theoretical or conceptual framework for the study. The research in this instance has a framework with a theatrical base, indicating that the research may be centred on a subject relating to performance. Planning and definition, data collecting and analysis, and other steps or processes are typical stages in the research process and can assist guarantee that the research is thorough and quite well. It's important to remember that a framework aids in keeping the research focused and concentrated on the study's specific goals. It also aids in providing a brief and logical flowchart for conducting the research. This is particularly helpful in complex research projects since it helps the researcher stay on track and make sure all-important areas of the subject are covered. It's also essential to keep in mind that the framework could change if new knowledge and insights are discovered during the course of the investigation. As a result, the research can be modified to better address important issues or questions and to make

sure that it is as detailed and educational as possible. A research framework can offer an organized way to conducting research. It can be particularly helpful in complex research projects by offering a clear and logical sequence of procedures for carrying out the research and maintaining the researcher's focus.

3.2.1 Planning & Definition

Planning and definition of the research have been sought in this phase in order to develop a solid plan prior to doing the research. First, for planning definition procedure is the knowledgeable about how to properly arrange the flow of the research in order to avoid any problems, was where it all began. The next step is research subject selection, which entails concentrating on the chosen topic and looking for the related literature. Last but not least, be aware of the method selection to provide a smooth study flow.

3.2.2 Data Collection and analysis

It was necessary to gather research data for this phase and conduct an analysis of it. Evidence gathering, data collecting tools, data collection, interview transcription, and data analysis are the five components of this phase. All of those factors are crucial in obtaining high-quality research data that can be used to inform decision-making. If the evidence collection is inadequate, the process must be restarted at the planning and definition stage to obtain an adequate evidence collection.

3.2.3 Topic Summary

In conclusion, the framework or the procedure that have been explained above will be applied in this research which is planning and definition phase and data collection and analysis phase. It is because if a research can be doing by a good planning and got a various data collection and analysis, it can give more understanding to the people about the research that has been done. It is same with this research where this section will explain about the platform and tools that will be used, the preparation of the things needed, and the overall flow of the process as a guideline.

3.3 Project Requirement

3.3.1 Input and Output

For Embedding process, the cover image and the message image are utilised as inputs for this study before being included in the final product or the output which is the stego image. The research's cover image used is lena.bmp, is displayed in figure xx. Before becoming the output, which is the stego image, the cover image and message image must undergo a number of steps or process. To assess or test the created stego image's quality, a PSNR value will be obtained from the stego image. While for extraction process, the stego image is defined as the inputs and the message image that gets after extraction process is called output.

3.3.2 Process Description

The process of image steganography, which involves concealing any information within an image, normally involves two crucial steps: embedding and extraction. The embedding is procedure in which the message is hidden within the cover image. Many approaches, including least significant bit (LSB) insertion, masking and filtering, and transform domain methods, can be used to do this. The objective of the embedding procedure is to produce a stego image that resembles the original cover image as closely as possible while yet hiding the concealed content inside. It is then transmitted to the selected recipient after the stego image has been made. The extraction procedure is then carried out by the recipient of the stego image in order to get the message that was hidden within the cover image. Numerous methods, including feature-based methods, statistical methods, and LSB extraction, can be used to do this. It is important to remember that in this situation, the security of the secret message is essential. It is because the information hidden in the cover image is probably private and only meant for certain people. Due to their high level of security and ability to survive image processing and compression, reliable and secure embedding algorithms are used. In summary, the process of image steganography involves hiding any information within an image, and normally involves two important steps: the embedding process and the extraction process.

3.3.2.1 Embedding process

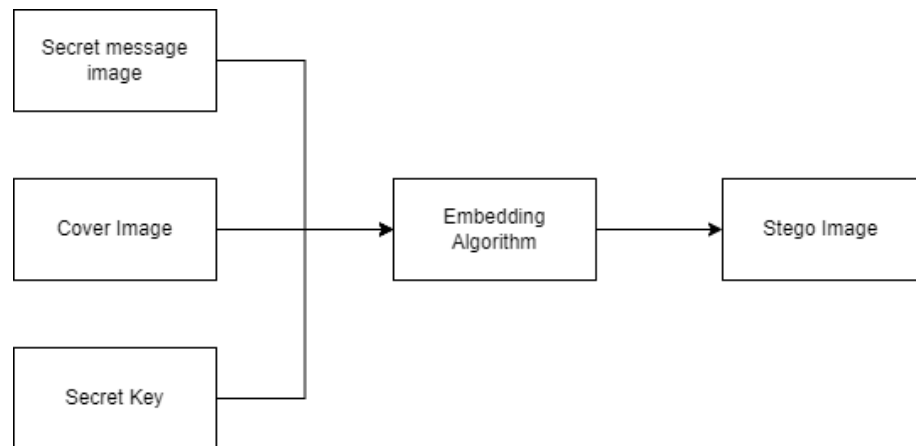


Figure 1: Embedding Process

Figure 7 shows the flow of embedding process. There are three things that need to be found before going through the phase embedding algorithm, namely secret message image, cover image, and secret key. Secret message image is an image that contains text that want to hide in the cover image. Cover image is the image used to hide the secret message image, which is the one used in this research is lena.bmp. The location of the bits that must be substituted in image steganography will be determined by the secret key, which is a text message. Embedding algorithm is the algorithm used to embedded all those three things to be a stego image. In other terms, in order to create the stego image during the process of embedding the secret message, the cover image, secret key and message image are required. The cover image will have the message image embedded in it. Calculating the PSNR values ensures that the image quality s high.

3.3.2.2 Extraction process

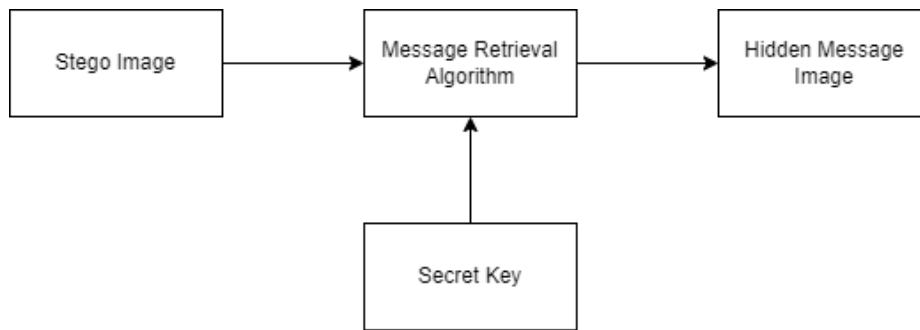


Figure 2: Extraction Process

Figure 9 shows the extraction process. The stego image is an image that have hidden message image in it that will go through the phase of message retrieval algorithm in order to produce the hidden message image. Retrieval information is required where and how to obtain the secret message from the stego image during the extraction procedure. The key, also known as the secret key created from a text message in this study, is the retry information. The proper message image will be retrieved if the key provided is identical, indicating that the location of extracting the embedded message is right, otherwise, the incorrect message will be retrieved.

3.4 Propose Design

3.4.1 Full Flowchart of embedding process

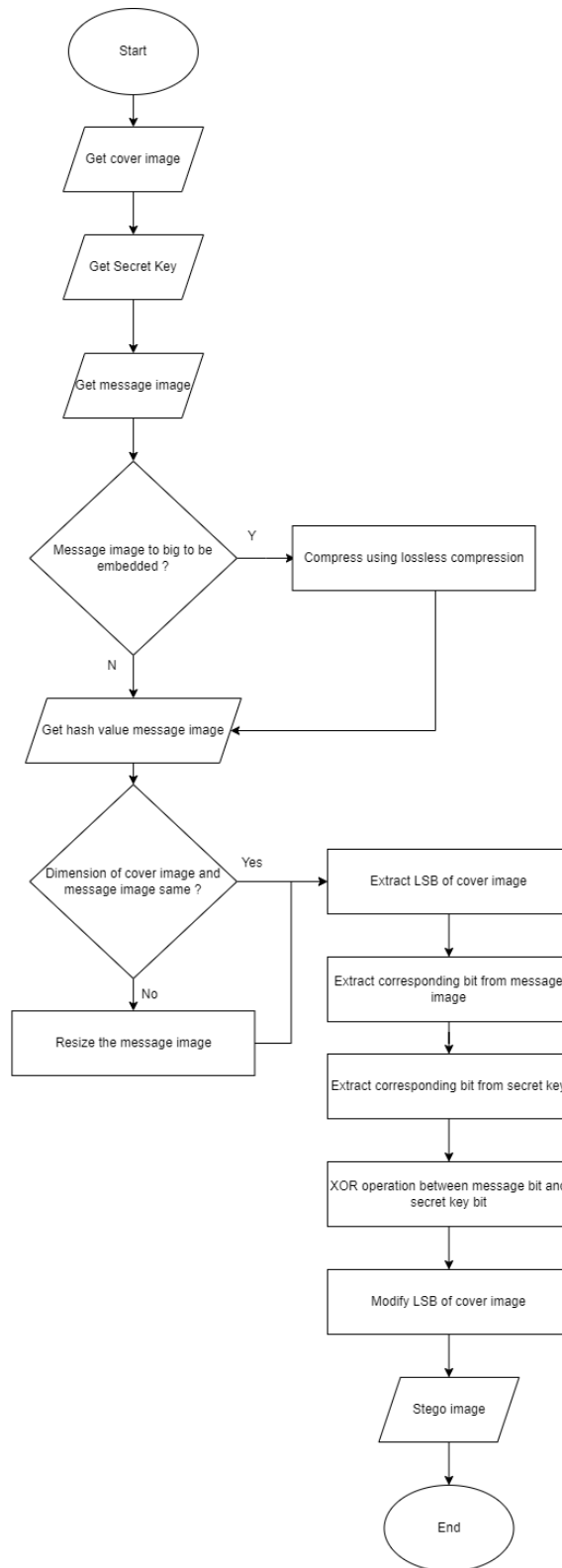


Figure 3: Full flowchart of embedding process

3.4.2 Testing plan for embedding process

1. Get the cover image. Choose cover image that want to use.
2. Get Secret Key. Determine secret key that want to use.
3. Get message image. Message image can be any image that have any information that want to be hide.
4. Get hash value for message image. Get hash value using SHA-512 hash function.
5. Determine whether dimension of message image is same as cover image or not. If not, resize the message image as the cover image.
6. Extract the LSB of the cover image pixel for the current color channel (red, green, and blue).
7. Extract the corresponding bit from the message image for the same color channel.
8. Extract the corresponding bit from the secret key based on the current position
9. Perform a bitwise XOR operation between the message bit and the key bit.
10. Modify the LSB of the cover image pixel for the current color channel using the embedded bit.
11. Get the stego image. The stego image has been created.

3.4.3 Full flowchart of extracting process

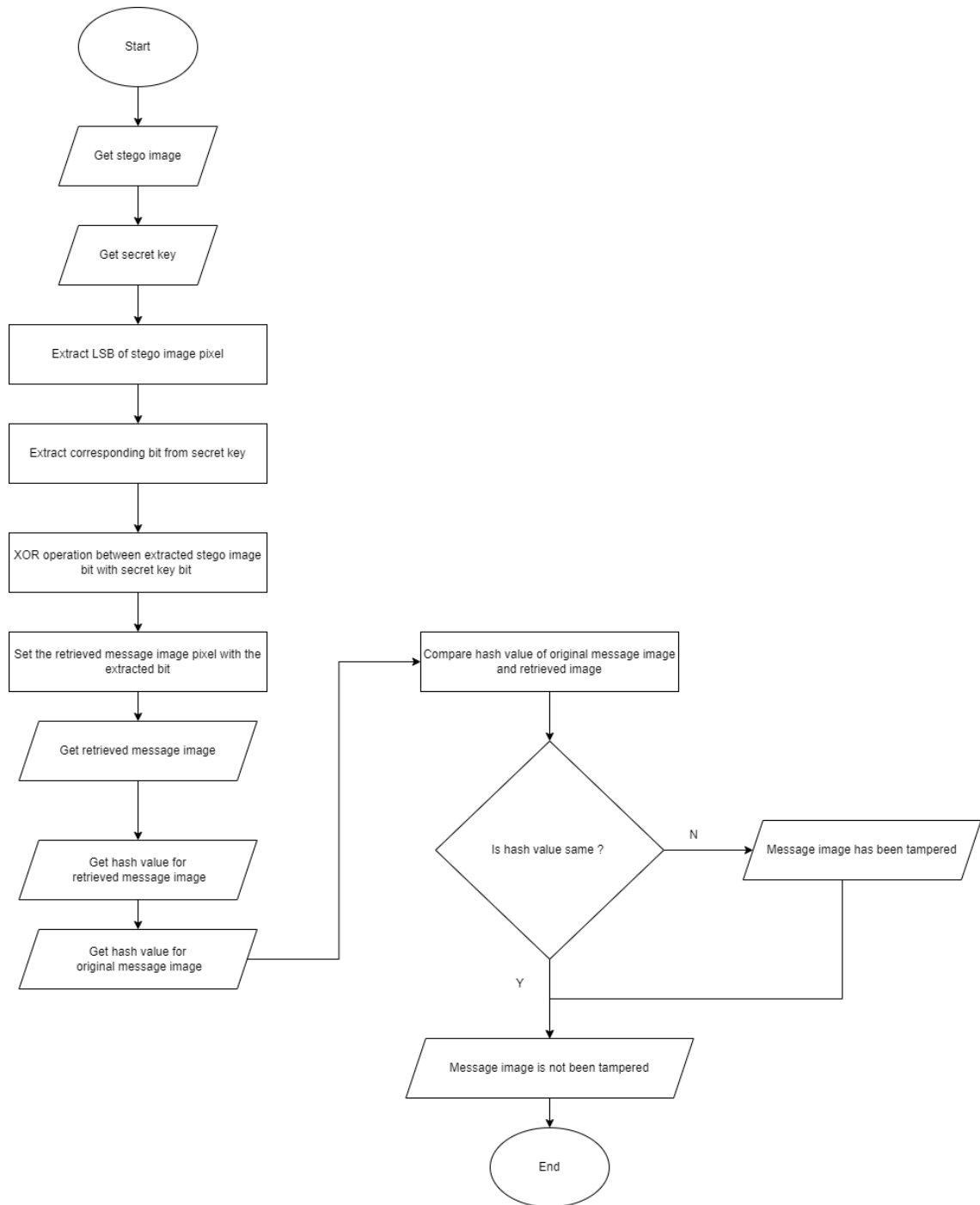


Figure 4: Full flowchart of extracting process

3.4.4 Testing plan for extracting process

1. Get stego image. The stego image that send from sender.
2. Get secret key. Get the secret key from the sender.
3. Extract the least significant bit (LSB) of the stego image pixel: The LSB of the current stego image pixel in the corresponding color channel is extracted using the bitget function.
4. Extract the corresponding bit from the secret key for retrieval: The corresponding bit from the secret key for retrieval is extracted using the same formula as during embedding.
5. Perform bitwise XOR operation to retrieve the message bit: The extracted bit from the stego image and the corresponding bit from the secret key for retrieval are XORed to retrieve the original message bit.
6. Set the retrieved message image pixel with the extracted bit: The retrieved message image pixel in the corresponding color channel is modified by setting the LSB to the extracted message bit.
7. Get retrieved message image.
8. Get hash value for retrieved message image.
9. Get hash value for original message image. Get the hash value from the sender.
10. Compare the hash value of retrieved message image with original message image.
11. If the hash value is not same, means that the message image hidden in the cover image has been tampered, while if same, means that the retrieved message image is same as the original message image that hidden in the cover image before.

3.4.5 Overall flowchart

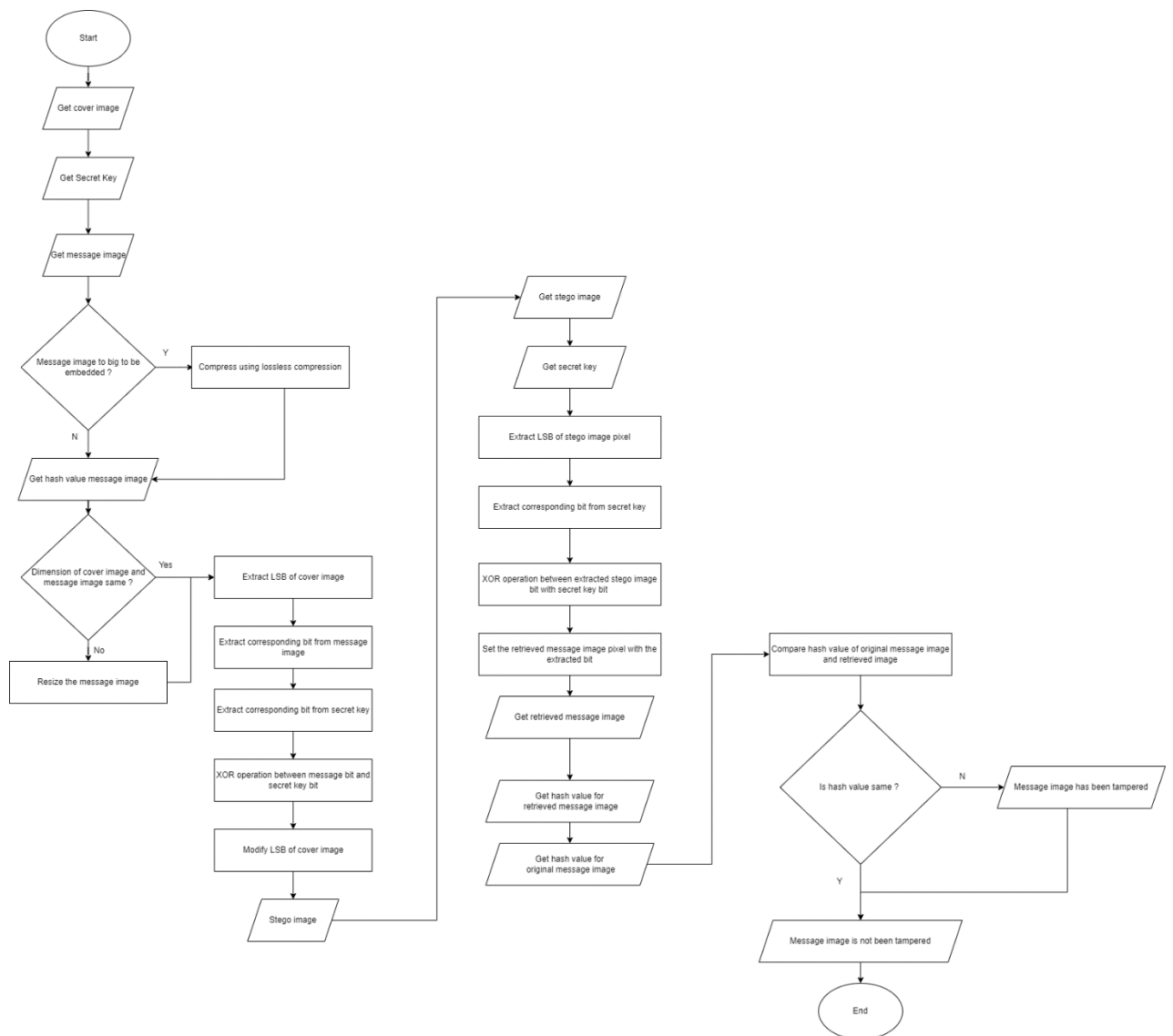


Figure 5: Overall Flowchart

3.5 Data Design

3.5.1 Cover Image and Message Image

In this study, data is encrypted and concealed within images using the image steganography technique. Lena.bmp, Peppers.bmp, and Mandrill.bmp 24-bit 512 by 512-pixel versions are the cover images utilized in this study. The cover image is the picture in which the host picture will be included (Tom et al., 2018). Figure 5, 6, and 7 below shows the example of cover image which is lena.bmp, pepper.bmp and mandrill.bmp. Because they are recognized and contain unique features, these images are frequently used in steganography research. Message image is the image that used to be hidden in the cover image. Normally, the message image contains the secret message or information that want to be hidden to make just certain people only can see it.

3.5.1.1 Cover Image

The specific format image that will be used as the cover image in this study is png. The format is chosen because it has a good balance of texture and smooth areas, making it a suitable cover image for hiding data. The data to be encrypted will be embedded in the least significant bits of the pixels in the image, which is a common method of hiding data in image steganography. It is significant to remember that an image's ability to hide data depends on its size, resolution, and type of the image. Since a wider image will contain more pixels, it might hide more information than a smaller one. Additionally, the cover image should be carefully picked because it will make it harder to find data manipulation if it does not. The encrypted data will be concealed within this image, which makes it difficult for anyone to find the concealed data without being aware of the steganography technique utilized. This method can be used to send data securely over the internet or to conceal sensitive information in an otherwise attractive image.

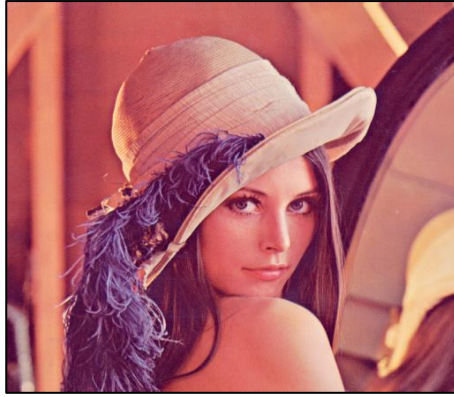


Figure 6: lena.png



Figure 7: Pepper.png

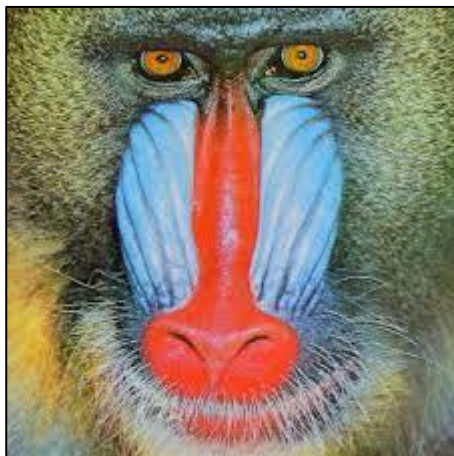


Figure 8: Baboon.png

3.5.1.2 Message Image

The message image is the image that is contained within the cover image (*Hiding Secret Messages in Images with Steganography and Metadata*, n.d.). The user may choose any image for this purpose, although it is usually chosen to be visually unnoticeable in order to avoid drawing attention to the fact that the cover image contains a concealed message. Figure 9 shows the example of message image, the Lena.bmp image, which is frequently used as an illustration of a message image, is a common test image in the field of image processing and compression research. The picture is a picture of a young woman, and the name "Lena" comes from the Playboy centrefold from which it was taken. Since it's straightforward and has a good combination of detail, textures, and smooth sections, it's frequently used as a sample image and is perfect for taken a different approach image processing technique. Figure 10 shows the example of information message image.

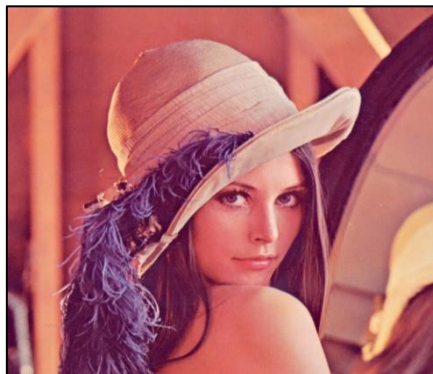


Figure 9: Example of message image

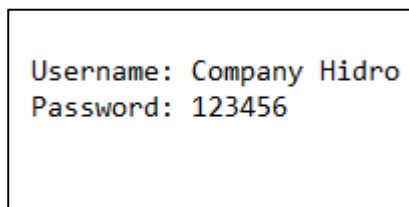



Figure 10: Example of information message image

3.5.2 Secret Key Preparation

The position of the bits to be substituted in image steganography will be determined in this study using a text message that serves as a secret key. When a message is encrypted and decrypted using symmetric encryption, a secret key is the piece of data or parameter that is required (*What Is a Secret Key? - Definition from Techopedia*, n.d.). As a result, the text message's decimal value will be changed to a binary value, and the binary value will then be transformed into a one-dimensional (1D) array bit stream as part of the steganography process. Figure 6 below is an illustration of a secret key:

Text Message Used (secret)	Text Message in Decimal	Text Message in Binary
S	115	01110011
E	101	01100101
C	99	01100011
R	114	01110010
E	101	01100101
T	116	01110100



011100110110010101100011011100100110010101110100

Table 2: Preparation of secret key

3.5.3 Hash Function and Compression

A hash function in steganography is a mathematical operation that accepts an input or message and outputs a fixed-length string of characters, often a digest specific to the input. (*What Is Hash Function? - Definition from Techopedia*, n.d.) The hash value represents a description of the prior string of characters, even if it is often smaller than the original. As for the hash function, SHA-512 has been chosen to hash the cover image before making the embedding process. SHA-512, or Secure Hash Algorithm 512 is one of the hash functions. It is a hashing method that transforms text into a fixed-size string, regardless of its length. Each output generates a length of SHA-512 of bits which is 64 bytes. The chosen of SHA-512 is preferable for image steganography as it is less vulnerable to attacks and more secure. The 512-bit hash values will be compared to guarantee that the retrieved message is accurate and similar to the embedded message. The user may determine whether the message image that has been recovered is the correct one, which strengthens the security of image steganography. As for the compression, the proposed research will use lossy compression which means, before embedding the message image into the cover image, the message image will be compressed using lossy compression in order to make the image smaller than before. It is important in order to get the better image steganography quality.

3.6 Tools

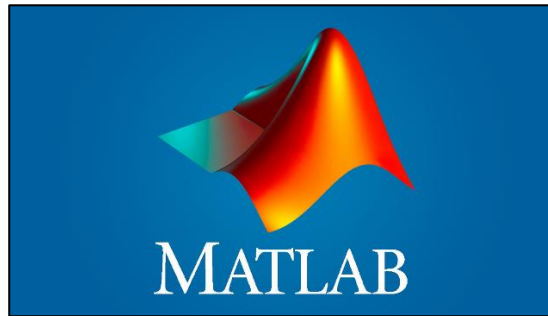


Figure 11: MatLab Logo

Figure 10 shows MatLab logo. MatLab is the software that will be used for the research. MatLab is a computer programming framework created especially for scientists and engineers to evaluate and create products and systems that change the world(*What Is MATLAB? - MATLAB & Simulink*, n.d.). The MATLAB language, a matrix-based syntax that enables the most natural expression of computer mathematics, is the core of MATLAB. In the domains of engineering, economics, and science, MATLAB is a highly regarded high-level software tool and programming language. The acronym MATLAB, which refers to "Matrix Laboratory," conveys that the software is made to work with matrices and data arrays. The ability to execute matrix and array operations is one of MATLAB's distinctive features, which makes it ideal for operations like signal processing, image processing, and linear algebra. Additionally, it has a number of built-in tools and routines for carrying out typical tasks including solving differential equations, designing optimal systems, and conducting statistical analysis.

The MATLAB programming language is user-friendly and has a syntax that is comparable to those of other well-known programming languages like C, C++, and Python. Additionally, it has a user-friendly design that allows interaction with data and calculation through a graphical interface, making it usable by individuals who might not have a significant experience in programming. MATLAB offers a framework for building and exchanging unique tools and applications in addition to its strong computational capabilities. Through MATLAB's File Exchange, users can build their own algorithms and implementations to carry out particular tasks and distribute them to others. Users can benefit from others' labour and give back to the community in this way.

3.7 Potential use of proposed solution

This proposed solution has the potential to be used by various organizations due to the security of the information that is hidden through the steganography process. As the main purpose of the steganography process, which is to hide information among other information, this proposed method provides a solution to hide information in the form of images among other images, making the hidden information more secure. The hidden information is also not easily obtained by other people or unwanted people to get the information because the recipient of the information needs a secret key to get the hidden information, and only the sender knows the secret key used. It is mean that whether the hacker get the stego image, they hardly to get the message image because they do not know the secret key. Therefore, this proposed solution has great potential to be used by any organization or scope that has been explained.

CHAPTER 4

IMPLEMENTATION, RESULT AND DISCUSSION

4.1 Introduction

The chapter will explain the implementation, result and discussion about the development research. Chapter 4 covered the implementation, discussion and outcomes of this thesis. The results or outcomes of the suggested research are presented in this chapter in terms of the PSNR value obtained. To assess whether the outcome seems high quality, a brief explanation is provided along with each PSNR number. This chapter also includes the study's functional test results. Finally, this chapter also includes input, output, process description, flowchart, algorithm, and result and discussion.

4.2 Implementations

The implementation of the method to generate results will be the main topic of this sub-topic. The implementation process includes numerous steps, involving embedding, extraction, hashing, and compression. Additionally, it gives a brief description of each phase as well as the tools and methods used to carry out the implementation, as well as the parameters utilized, and the reasoning around them whenever needed.

4.2.1 Input



Baboon.png



Pepper.png



Baboon2.png



Cat.png



Lena.png

Figure 12: Sample image

Figure 12 shows the sample of image that will be used as the cover image and also the message image in this study. The format of all of those images is in png format. Input for the embedding process is the cover image and message image while input for the extracting process is the stego image. Stego image means that the image that have message image hidden in it.

4.2.2 Output

The primary outcomes of this study or experiment consist of steganography images, wherein a color message image is embedded within a color cover image. Furthermore, the hash values of the original message image and the retrieved image are compared to verify the authenticity of the hidden message. The integrity of the stego image is also confirmed by hashing the tampered image. Additionally, several metrics, including Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR), are utilized to assess the quality of the stego images.

4.2.3 Process Description

This process description outlines the steps of a steganography algorithm using LSB embedding. Firstly, the original color PNG image (CoverImage.png) is loaded and compressed using PNG lossless compression, saved as CompressedImage.png. The cover image and message image (CMessageImage.png) are then loaded. If their dimensions different, the message image is resized to match the cover image. LSB embedding is performed by iterating over each pixel of the cover image. For each RGB color channel, the least significant bit (LSB) of the cover image pixel, message image, and secret key are extracted.

The message bit and key bit are XORed, modifying the LSB of the cover image pixel. This process is repeated for all pixels, resulting in the stego image (StegoImage.png). The original and reconstructed images are loaded and converted to double precision. The mean squared error (MSE) and peak signal-to-noise ratio (PSNR) are calculated based on the comparison. The PSNR value and sizes of the cover and stego images (in KB) are displayed. For retrieval, the user enters a secret key. If it matches the original, the message image is retrieved from the stego image by reversing the LSB embedding process.

The retrieved message image is saved as RetrievedMessageImage.png. To verify integrity, the SHA-512 hash values of the original and retrieved message images are calculated and compared. If they match, the integrity is confirmed, and the retrieved message image is displayed. If the retrieval key doesn't match the original secret key, an error message is shown. Lastly, there is a function called calcSHA512Hash that calculates the SHA-512 hash value for an image by converting it to a byte array and using the SHA-512 algorithm from the java.security library.

4.2.4 Case Study

In today's digital era, the need for secure and confidential communication has become paramount. Steganography, a technique that involves hiding data within innocuous carrier files, offers a powerful solution for covert communication. Sarah and John, two colleagues working on a highly confidential project, leverage steganography to exchange sensitive information securely. By hiding their messages within innocent-looking image files, they add an extra layer of security to their communication, making it more difficult for unauthorized individuals to intercept or decipher the hidden information. Steganography allows them to communicate covertly, avoiding raising suspicion and maintaining the confidentiality of their information. In conclusion, steganography proves to be a valuable tool for secure communication. The practical application of steganography in such scenarios offers enhanced privacy, security, and integrity in digital communication.

4.3 Result

4.3.1 Embedding



Cover Image	Stego Image	Message Image	Cover Image Size (KB)	Stego Image Size (KB)	PSNR value (dB)	MSE value
 Lena.png		Lena.png	134.19	91.70	49.8918	0.000010
		Baboon.png	134.19	91.81	51.1127	0.000008
		Pepper.png	134.19	91.75	51.1566	0.000008
		Baboon2.png	134.19	86.96	51.1334	0.000008
		Cat.png	134.19	91.65	51.1167	0.000008

Table 3: Embedding result for Lena.png



Cover Image	Stego Image	Message Image	Cover Image Size (KB)	Stego Image Size (KB)	PSNR value (dB)	MSE value
 Baboon.png		Lena.png	742.70	613.51	51.1446	0.000008
		Baboon.png	742.70	613.58	49.8917	0.000010
		Pepper.png	742.70	613.47	51.1382	0.000008
		Baboon2.png	742.70	613.41	51.1404	0.000008
		Cat.png	742.70	613.50	51.1461	0.000008

Table 4: Embedding result for Baboon.png



Cover Image	Stego Image	Message Image	Cover Image Size (KB)	Stego Image Size (KB)	PSNR value (dB)	MSE value
 Pepper.png		Lena.png	4746.00	3256.84	51.1413	0.000008
		Baboon.png	4746.00	3267.12	51.1397	0.000008
		Pepper.png	4746.00	3155.07	49.8917	0.000010
		Baboon2.png	4746.00	3131.62	51.1521	0.000008
		Cat.png	4746.00	3248.28	51.1398	0.000008

Table 5: Embedding result for Pepper.png



Cover Image	Stego Image	Message Image	Cover Image Size (KB)	Stego Image Size (KB)	PSNR value (dB)	MSE value
 Baboon2.png		Lena.png	83.58	83.55	51.1495	0.000008
		Baboon.png	83.58	83.76	51.1441	0.000008
		Pepper.png	83.58	83.85	51.1615	0.000008
		Baboon2.png	83.58	70.64	49.8917	0.000010
		Cat.png	83.58	83.72	51.1538	0.000008

Table 6: Embedding result for Baboon2.png






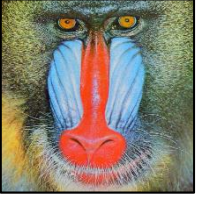








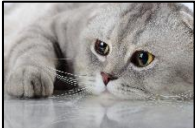


Cover Image	Stego Image	Message Image	Cover Image Size (KB)	Stego Image Size (KB)	PSNR value (dB)	MSE value
 Cat.png		Lena.png	4107.80	3842.37	51.142	0.000008
		Baboon.png	4107.80	3866.16	51.1424	0.000008
		Pepper.png	4107.80	3859.93	51.1412	0.000008
		Baboon2.png	4107.80	3651.19	51.1413	0.000008
		Cat.png	4107.80	3621.29	49.8917	0.000010

Table 7: Embedding result for Cat.png

4.3.2 Extracting

Stego Image	Message Image (Compressed Image)	Retrieved image	Hash function original message image	Hash function retrieved image	Original and retrieved image match (Y/N)
Lena.png 			CA7940 5BF152 63BF08 6FF3D5 E8C958 DBD245 A5E20B C2A43D 1D36A2 51B69D 6FFFDE 70C981 D4F0B2 B03B67 44AA23 B48BE8 0D06EE A6EE38 0FD7A4 B5ADA4 F117A9 C6	CA7940 5BF152 63BF08 6FF3D5 E8C958 DBD245 A5E20B C2A43D 1D36A2 51B69D 6FFFDE 70C981 D4F0B2 B03B67 44AA23 B48BE8 0D06EE A6EE38 0FD7A4 B5ADA4 F117A9 C6	Y
Baboon.png			7A8BE8 3E4419 EABB90 6D019E DE6996	7A8BE8 3E4419 EABB90 6D019E DE6996	Y

			CC7FFF 7EAED9 83E40A 1D3B6B 947C24 DF06C9 3F1C3F E13A48 A17570 724654 3CCDB0 D98610 BFEBE0 AC5469 ACE6E1 35099C 9B	CC7FFF 7EAED9 83E40A 1D3B6B 947C24 DF06C9 3F1C3F E13A48 A17570 724654 3CCDB0 D98610 BFEBE0 AC5469 ACE6E1 35099C 9B	
Pepper.png 			028CAF 1ABDCE 969E72 061069 E7988A 2D7C59 EC5642 422DE4 BB6CBB 0B8030 F29788 276658 E27FD6 264DAB 5B160A F75FD7 B7E7BE 7C2BFC 40F81C	028CAF 1ABDCE 969E72 061069 E7988A 2D7C59 EC5642 422DE4 BB6CBB 0B8030 F29788 276658 E27FD6 264DAB 5B160A F75FD7 B7E7BE 7C2BFC 40F81C	Y

			896E43 685B19 45	896E43 685B19 45	
Baboon2.png 			B61C9A 5F0724 83869B B47C1A 03FC05 4A8CAB 5BAF06 CE7DD9 913104 A4CC55 90765C BB6278 A505B8 3FA441 CA4B61 028BC1 8CE573 FAE34E 692C5E D5EB9A 552246 19	B61C9A 5F0724 83869B B47C1A 03FC05 4A8CAB 5BAF06 CE7DD9 913104 A4CC55 90765C BB6278 A505B8 3FA441 CA4B61 028BC1 8CE573 FAE34E 692C5E D5EB9A 552246 19	Y
Cat.png 			1515635 6636CF0 9262F15 FB5D2C8 D86B5F9 7E0F1E3 40CA536 0ECB75C 7AD4A3 D 934DB97	1515635 6636CF0 9262F15 FB5D2C8 D86B5F9 7E0F1E3 40CA536 0ECB75C 7AD4A3 D 934DB97	Y

			974E40A	974E40A	
			39F14E8	39F14E8	
			28753B4	28753B4	
			E288CF3	E288CF3	
			2BDE59E	2BDE59E	
			85C794F	85C794F	
			3E201D8	3E201D8	
			775D787	775D787	
			6E	6E	

Table 8: Extracting process for different stego image and same message image

4.4 Analysis of the Result

Based on the embedding result, it is evident that the range of the Peak Signal-to-Noise Ratio (PSNR) value falls between 49 and 53. This range indicates that the message image has been successfully embedded into the cover image, resulting in a stego image of high quality. Furthermore, the PSNR value achieved using this method surpasses that of the technique discussed in chapter 2, indicating an improvement in image quality. In addition to the PSNR, the Mean Squared Error (MSE) value is also noteworthy, as it falls within the range of 0.000008 to 0.000010. This range signifies that the distortion between the embedded message image and the original cover image is minimal, further corroborating the effectiveness of the steganography technique employed.

Moving on to the extraction process, the hash value for the retrieved message image matches that of the original message image. This outcome demonstrates that the hidden message image has been successfully extracted from the cover image without any tampering or alteration, thereby ensuring the integrity of the embedded information. To enhance the security of the image steganography, a secret key with the text "secret" was utilized in both the embedding and extracting processes. This key serves as an additional layer of protection, safeguarding the hidden message against unauthorized access. Furthermore, various other functions such as hash function, Least Significant Bit (LSB) technique, and compression have been successfully employed. The strength that got during the development is the ability to solve the error while the weakness is to understand whether the development is in correct way or not. The challenge is to find the resources or reference to create the propose method.

CHAPTER 5

CONCLUSION

5.1 Introduction

Chapter 5 serves as the concluding section of this thesis, providing a comprehensive overview of the entire research journey. It begins by revisiting and reviewing the goals that were set for the research, allowing for an assessment of their accomplishment and highlighting the contributions made. Furthermore, this chapter delves into an examination of the constraints and limitations that were encountered during the research process, shedding light on the challenges faced and their implications on the outcomes. It acknowledges factors such as time constraints, resource limitations, and potential biases, offering transparency and contextualizing the findings. Lastly, this chapter offers valuable recommendations for future research, suggesting potential avenues for further exploration, areas of improvement, and opportunities to expand the scope of the study. These recommendations provide valuable guidance for researchers and pave the way for continued advancements in the field.

5.2 Objective Revisited

In revisiting the objectives set forth in this research, the first objective was to study image steganography using hash function and compression. This objective has been successfully achieved through a comprehensive investigation of the integration of hash functions and compression techniques in image steganography. The research explored a hash functions which is SHA-512 and examined its effectiveness in concealing and extracting hidden information within images. Additionally, the compression algorithms which is lossless compression were analysed and its impact on the steganographic process was evaluated. The successful completion of this objective has contributed to an enhanced understanding of the role of hash functions and compression in image steganography.

The second objective aimed to develop image steganography using lossless compression and SHA-512. This objective has also been successfully accomplished by devising a novel approach that combines lossless compression techniques with the robust SHA-512 algorithm for image steganography. The research involved designing and implementing an efficient framework that leverages lossless compression to reduce the size of message images while ensuring the integrity of the hidden information. The utilization of SHA-512, a secure hashing algorithm, further enhanced the security and reliability of the steganographic process. The successful achievement of this objective has led to the development of an advanced image steganography technique that offers both effective compression and robust data protection.

The third objective focused on evaluating the proposed algorithm. This objective has been met through a rigorous evaluation process that involved extensive testing and analysis. The performance of the developed algorithm was assessed using various metrics, such as embedding capacity, image quality, and security. The evaluation included comparative studies with existing steganography techniques to validate the superiority and effectiveness of the proposed algorithm. The favourable results obtained during the evaluation phase confirm the successful achievement of this objective. The algorithm demonstrated satisfactory embedding capacity, preserved image quality, and ensured the security and integrity of the hidden information.

5.3 Limitation

The first limitation of the method is its restriction to working exclusively with PNG format images. This means that the method cannot be directly applied to other commonly used image formats such as JPEG, BMP, or TIFF. If the cover image or the message image is in a different format, it would require additional steps to convert them into PNG format before the steganography process can be applied. This limitation may introduce extra complexity and may not be ideal in situations where PNG format is not readily available or preferred.

Another limitation of the method is the approach used for embedding the secret key. In this method, the secret key is not embedded directly into the cover image, rather, it is solely used to determine the locations where the LSB (Least Significant Bit) of the cover image is modified. While this approach provides a means of selecting specific locations for embedding the hidden message, it also means that the secret key itself is not

concealed within the stego image. This limitation may pose a security risk as the absence of a hidden secret key could potentially make it easier for unauthorized individuals to tamper with or access the hidden message.

The use of the LSB technique for embedding the hidden message introduces another limitation. LSB embedding involves modifying the least significant bit of the cover image to store the hidden information. However, this technique is vulnerable to detection by advanced steganalysis algorithms. The presence of LSB changes in the cover image can potentially be identified through statistical analysis or visual inspection, which compromises the method's robustness against detection. This limitation may impact the effectiveness and security of the steganographic process, particularly in scenarios where strong resistance against detection is required.

5.4 Conclusion and Future Work

In conclusion, the developed method of image steganography utilizing hash function and compression has successfully achieved the objective requirements. The implementation incorporated four key techniques, namely lossless compression, LSB technique, secret key usage, and SHA-512 as the hash function. The process involved embedding and extracting hidden information within the cover image. Through this method, the objective of secure and covert communication was achieved as can be seen the result in the chapter 4. The PSNR and MSE value has been calculated to determine the quality of the image steganography.

Moving forward, there are several areas that offer opportunities for future work in the field of image steganography using hash function and compression. Firstly, enhanced embedding techniques can be explored to improve the capacity and robustness of the steganographic algorithm. Investigating alternative embedding domains or advanced LSB methods could potentially enhance the overall performance and security of the technique. Additionally, it is essential to evaluate the method's robustness against compression attacks. Further research can focus on analyzing the impact of lossless compression on the hidden data and developing strategies to mitigate the distortion introduced by compression. By enhancing the algorithm's resilience to compression attacks, the overall quality and integrity of the hidden information can be maintained.

Furthermore, conducting a comprehensive security analysis of the steganographic algorithm is crucial. This includes vulnerability assessments, statistical analysis, and evaluation against known attacks. By identifying potential weaknesses and improving the security measures, the method can be made more resistant to unauthorized detection and extraction. By addressing these future work directions, the image steganography technique utilizing hash function and compression can be further improved and developed to meet evolving security requirements and challenges in the field.

REFERENCES

- (PDF) *Colour Image Steganography Using SHA-512 and Lossless Compression*. (n.d.). Retrieved January 17, 2023, from https://www.researchgate.net/publication/322331105_Colour_Image_Steganography_Using_SHA-512_and_Lossless_Compression
- AbdelWahab, O. F., Hussein, A. I., Hamed, H. F. A., Kelash, H. M., Khalaf, A. A. M., & Ali, H. M. (2019). Hiding data in images using steganography techniques with compression algorithms. *Telkomnika (Telecommunication Computing Electronics and Control)*, 17(3), 1168–1175. <https://doi.org/10.12928/TELKOMNIKA.V17I3.12230>
- Darwis, D., Junaidi, A., Shofiana, D. A., & Wamiliana. (2021). A New Digital Image Steganography Based on Center Embedded Pixel Positioning. *Cybernetics and Information Technologies*, 21(2), 89–104. <https://doi.org/10.2478/cait-2021-0021>
- Hiding secret messages in images with steganography and metadata*. (n.d.). Retrieved January 22, 2023, from <https://www.drchaos.com/post/hiding-secret-messages-in-images-with-steganography-and-metadata>
- Nezami, Z. I., Ali, H., Asif, M., Aljuaid, H., Hamid, I., & Ali, Z. (2022). An efficient and secure technique for image steganography using a hash function. *PeerJ Computer Science*, 8, e1157. <https://doi.org/10.7717/PEERJ-CS.1157>
- Raggo, M., & Hosmer, C. (2013). Multimedia Data Hiding. *Data Hiding*, 69–90. <https://doi.org/10.1016/B978-1-59-749743-5.00004-3>
- Tom, A., Thomas, A. V, Jose, J., Jose, M., Darsana, P., & Scholar, U. G. (2018). Hiding Host Image using a Cover Image. *International Journal of Engineering Research & Technology*, 3(5). <https://doi.org/10.17577/IJERTCONV3IS05038>
- What is a Secret Key? - Definition from Techopedia*. (n.d.). Retrieved January 17, 2023, from <https://www.techopedia.com/definition/24865/secret-key>
- What is Hash Function? - Definition from Techopedia*. (n.d.). Retrieved January 17, 2023, from <https://www.techopedia.com/definition/19744/hash-function>
- What Is MATLAB? - MATLAB & Simulink*. (n.d.). Retrieved January 22, 2023, from <https://www.mathworks.com/discovery/what-is-matlab.html>
- What is Steganography? - Definition from SearchSecurity*. (n.d.). Retrieved December 4, 2022, from <https://www.techtarget.com/searchsecurity/definition/steganography>

APPENDIX

No	Activity	Month Week	October				November				December				January				February			
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Planning Phase																						
2	Finding supervisor and suggest a title	2																				
3	Meeting supervisor	1																				
4	Determine title, requirement, and problem statement	2																				
5	Determine objectives and scope	1																				
6	Meeting supervisor	1																				
7	Determine methodology	2																				
8	Review the past studies' publications.	2																				
9	Consult with supervisor	1																				
10	Submit report for first evaluation	1																				
11	Do corrections and add new contents	2																				
Design Phase																						
12	Design suggested methodology	4																				
13	Collected dataset	1																				
14	Determine diagram, and flowcharts	3																				
15	Consult with supervisor	1																				
16	Make corrections	2																				
17	Prepare slides, video, and required documents	1																				
18	Submit for evaluators evaluation	1																				
19	Presentations to the evaluators	1																				
20	Make corrections for the last submission	2																				
21	Submit the finalized report to supervisor for final evaluations	1																				

Figure 13: Ghant Chart