CHAPTER 1
INTRODUCTION

1.1 Background

Communication is the process of exchanging messages or information from one place to another. The rapid development of digital communication at this era allows information to be addressed easily and quickly. This situation encourages the need for message security, especially confidential messages, so that it can safely arrive at its destination. The message or information can be in the form of text, images, sound, or video. This need is increasing due to the COVID-19 pandemic, which encourages changes in people's lifestyles to shift their daily activity to become more digital-based. This increasing need also moves linearly with user concerns about the security of a message or data — the most fundamental and crucial factor in digital communication, especially in critical data such as control data. There have been many cases of digital leaks. Recorded by the National Cyber Security Operations Center, the number of cyber-attacks in Indonesia increased 4 times during the COVID-19 pandemic, reaching 189,937,542 cases as of 2020 from 39,330,231 cases as of 2019. In an effort to anticipate, there are several techniques in securing a data or message, one of which is steganography. Steganography is the technique of inserting a data or message into a media cover (text, images, sound, and video) with the aim of disguising the message so that the intruder cannot see the hidden message without degrading the quality of the media cover [4, 5]. According to [4, 6], there are other methods for sending information, such as cryptography and watermarking. Table 1.1 shows the distinctions between cryptography, steganography, and watermarking methods. The table depicts how steganography has a higher level of security than the other two methods, and how the embedded message is always invisible.

Table 1.1. Comparison of Information Security Types

Qualification	Cryphtography	Steganography	Watermarking
Carrier Object	text files or image	Any media file	Digital image/Audio
Secret Information	Text	Any type of file	Watermark
Secret Key	Neccessary	Optional	Optional
Visibility	Yes	Never	May or may not be
Objective	Protection	Secret communication	Copyright protection
Security	High	Very High	High
Capacity	High	High	Low

Video steganography is a steganography technique by inserting confidential data in a video cover. Videosteganography can be classified into two domains, the spatial domain, and the transform domain [4]. Transform Domain is a technique for converting from the time domain to the frequency domain. This technique (transformation domain) is commonly used in video steganography in Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) [1, 4, 6, 7]. In DWT, there are three frequency levels: High, Middle, and Low. [7] compares DCT and DWT, with DWT outperforming DCT in terms of embedding capacity and security for video steganography at high level sub-band frequencies. Unlike in [1], the researcher used DWT at the Middle and High frequency levels for each YUV component, compared it to the LSB method, and obtained more stable robustness results. Then, according to [4], DWT from image steganography has the advantage of improving stego image quality, security, and durability, with coefficients indicating spatial and frequency features.

The secret data/messages that have been inserted into a video are called stego-videos. Stego-video, which will be transmitted to a network, has a risk that will cause damage to the receiving side. This damage can be caused by a packet loss [8].Based on the previous research [1, 7], this thesis proposes a fault tolerance scheme in streaming video steganography using repetition code to ensure the reception of hidden information in noisy channels; such as lowering ad packs in video streaming.

The robustness of information hidden in a video can be calculated using PSNR to see that the quality of the stego video has the same quality as the cover video (original video). The higher the PSNR value, the higher the quality of the reconstruction. The use of the DWT method which offers high resolution at low frequencies gives a PSNR value of 131.49 dB using the H.265 codec. The high PSNR value in this study was influenced by the choice of codec. The comparison between the H264 and

H265 codecs can be seen from the large block size used, H265 tends to have a larger block size than H264 and only requires half the bandwidth of the H.264 codec, and the H.264 codec is a lossy compression format which means some image quality which is lost during compression. [9, 10].

1.2 Problem Identification

Digital communication requires a high security level when transmitting data or information, especially confidential data, as in data control or autonomous vehicles. Due to these circumstances, there is a demand for a technique that allows recipients to safely receive their message. Based on that demand, steganography could be seen as an effective solution for safeguarding sensitive information or messages, by inserting a message into a media cover to disguise messages from unknown intruders. Through this research, we will observe how an image (hidden message) is inserted into a video (cover media). Video is a data delivery medium that uses the User Datagram Protocol (UDP) in transmitting its data. This protocol is connectionless, which means that UDP is a protocol that prioritizes delivery time (speed) and ignores lost packets (packet loss). As a result, a method for ensuring fault tolerance is required. However, the term "fault tolerant" here, referred to the influence that comes from packet loss. Based on the arguments above, the problem formulation in this study will focused on:

- How does packet loss affect messages that were inserted into a video cover?
- How does packet loss affect codec selection?
- How does packet loss affect the number of n in the use of repetition code?
- How does packet loss affect the user experience?

1.3 Objective

The main purpose of this study is to observe the impact on the process of sending data or messages (images) sent to a network, after being inserted into the cover video, by proposing a fault tolerance scheme in streaming video steganography using repetition codes to ensure the receipt of hidden information in noisy channels such as dropping of advertising packets in video streaming.

1.4 Scope of Work

Limitation of the problem in this study is divided into several factors such as:

1. Testing the fault tolerant scheme is only limited to using the packet drop scheme by setting the packet drop percentage value.
2. The video streaming process in this thesis utilizes VLC Media Player, which functions as both a VLC server and a VLC client.
3. Video streaming is only limited to video media and does not include audio.
4. The types of video codecs used in this thesis are the H.264 and H.265 codecs.
5. The streaming protocol used in this study is Real Time Streaming Protocol (RTSP).
6. The video steganography method used is limited to Discrete Cosine Transform (DCT).
7. The type of data information security used is only limited to steganography, especially video steganography.
8. The video steganography method used is limited to discrete wavelet transform (DWT).
9. The secret data that was inserted in the video cover, will be in a shape of image.
10. The secret data is inserted in the ”Y” component.
11. Confidential data will be inserted in each odd frame(1,3,5,7,..853) and frame multiplier of 3 (3,6,9,12,...853)
12. The code repetition process will be carried out on frame n=(1,3,5,7,..853) and n=(3,6,9,12,...853)

1.5 Research Methodology

This thesis is divided into 3 parts to obtain high-quality results:

- Literature Study This thesis investigates the fundamental theories of Steganography, particularly the use of media covers in the form of video, Discrete Wavelet Transform (DWT), Codec, Video Streaming, and Fault Tolerant. The

purpose of this literature review is to explain basic concepts and theories that will be used to support system models, proposed schemes, and outcome analysis.

- Fault tolerant design uses packet drop scheme to get the minimum tolerance possible This thesis designed fault tolerant using a packet drop scheme to get the tolerance to a minimum by turning the percentage of packet drop using clumsy software when streaming video continues through VLC. The streaming video contains stego video designed using the MATLAB simulator.
- Proof of fault tolerant scheme This thesis proves a fault tolerant scheme by setting the percentage of packet drops during video streaming and seeing the effect of packet drop on the user experience by paying attention to the selection of codecs and the use of steganography.