CHAPTER 6

CONCLUSION AND FUTURE WORK

6.1 Research Objective (RO) Achieved

This section revisits the research objectives stated in Section 1.5 to ensure their fulfilment, which will lead to achieving the main goal.

6.1.1 RO#1: Design the solution for audio steganography.

In this research, the design process begins with a literature review on the LSB audio steganography technique and an evaluation on 30 cover selection methods articles to identify research issues. The primary research problem identified is that audio steganography often generates subpar stego-files due to improper cover audio selection. After conducting several critical analyses in Section 2.6, a literature classification is produced that provides a better ability to recognize the strengths and weaknesses of the current method. An examination of the existing literature reveals a limited number of approaches discussed, without any cover selection classification criteria being present. Nonetheless, upon a thorough analysis of the literature, two theoretical frameworks were identified to enhance the stego-file characteristic performance outlined in Section 2.7. This could be achieved through the development of an audio steganography algorithm and careful manipulation of various inputs, including the secret message, cover file, and steganographic keys. As a result, a new design was proposed in Section 3.3.

This section explains how the proposed solution works by discussing the elements and formulations used to enhance the dynamic security characteristic and selecting a suitable cover audio with respect to the trade-off in audio steganography characteristics. To enhance the dynamic security feature, the following elements were used: 1) chaotic block, and 2) rounding mechanism. For selecting a good cover audio based on the audio steganography characteristics trade-off, the elements used were: 1) a set of evaluation metrics for imperceptibility, dynamic security and robustness; and 2) trade-off consideration rules. Finally, the flow and logical design were presented and analysed to ensure a clear implementation process.

6.1.2 RO#2: Implementation of the solution for audio steganography.

The proposed solution was implemented in Matlab and is comprised of three distinct algorithms which are BCM-LSB (LSB embedding level), MCAS (cover selection level) and CAS (audio steganography model level). The implementation of the solution is reported in Chapter 4.

6.1.2.1 BCM-LSB Algorithm

The BCM-LSB has solved the dynamic security problem by introducing an amended block-based embedding technique that implements both sequential and selective embedding. This sequential embedding is done per block rather than the entire audio, which has significantly improved the dynamic security aspect. Furthermore, the selective initial embedding place introduces randomness into the method, which increases its resistance against secret message direct retrieval attacks.

The parameters that influence the dynamic security performance of BCM-LSB are:

1. Length of secret message

2. Length of cover audio
3. Set of keys: *x*, *r* and *n*
4. Bit embed per sample (*bps*)

Next, BCM-LSB is combined with the MCAS technique.

6.1.2.2 MCAS Algorithm

When selecting cover audio for audio steganography, there are three main issues to consider: 1) the limited selection method, 2) the lack of consideration for the trade-off between steganography characteristics, and 3) the inaccurate dynamic security metric. To address these issues, the MCAS proposes cover audio selection method that considers the trade-offs and uses more refined dynamic security metrics. The MCAS helps user selects an audio file in .wav format as covers from a database of random audio files that includes speech and music-based audio. During the evaluation of the cover audio file, the trade-offs between imperceptibility, robustness and dynamic security are considered to ensure it suggests the set of well-rounded and balanced cover audio files. The trade-off consideration involves finding another solution that produces higher values of two other characteristics at the same value of a specific characteristic. Lastly, a dynamic security metric was introduced to fix the issue of inaccurate metric. This metric considers the distribution level of the secret message across the cover audio and the difference between the modified segments. The MCAS utilizes three metrics to evaluate performance characteristics, including:

1. SNR – to evaluate the imperceptibility characteristic.
2. BER from AWGN attack – to evaluate the robustness characteristic.
3. Seg-SNR – to evaluate the dynamic security characteristic.

6.1.2.3 CAS Algorithm

A full solution of CAS algorithm which combines BCM-LSB and MCAS was then presented. The parameters used for the cover selection process are:

1. Cover audio index in the database.
2. Set of keys: *x, r* and *n.*
3. Bit embed per sample (*bps*).

Once MCAS successfully discovered a set of solutions, one cover audio was chosen to be utilized for the BCM-LSB. The selection process involved evaluating imperceptibility, robustness, and dynamic security values, which were then normalized and added to determine the most optimal solution. The solution with the highest normalized value was selected to generate a stego-file.

6.1.3 RO#3: Evaluation of the solution performance

The results of evaluations and comparisons are presented in Chapter 5. The evaluations are divided into two parts which are performance evaluations on the parameters used by proposed solutions. A detailed discussion of the evaluations carried out on the BCM-LSB algorithm was provided in Section 5.1.1. During these evaluations, two parameters, namely *bps* and set key *x, r* and *n,* were assessed to determine the optimal values that would produce the best imperceptibility, capacity, robustness and dynamic security performance. Additionally, Section 5.1.2 delves further into the evaluations of the MCAS. In these evaluations, three parameters were evaluated, namely the number of generations, size of population and removal duplicated solution algorithm, to determine the best values that would ensure the accuracy and optimal performance of all selected covers.

The comparisons are divided into three parts which are LSB embedding level, cover selection level, and audio steganography model level. The comparisons made at LSB embedding level are on the BCM-LSB against existing LSB embedding algorithm are discussed in Section 5.2.1. The comparisons cover all characteristics performance such as imperceptibility, capacity, robustness and dynamic security. Next, the comparisons made at cover selection level are on the MCAS algorithm against existing cover selection algorithm are discussed in Section 5.2.2. These comparisons assessed both the quality and quantity of the selected cover. Lastly, the comparison made at audio steganography model level is on the CAS algorithm against existing audio steganography model that require human input to select the cover audio for the algorithm, as presented in Section 5.2.3. This comparison evaluated the quality and quantity of the selected solution.

6.2 Research Contributions

The contributions in this research are divided into two sections: the fundamental and technical contributions. The fundamental contributions focus on how this research adds to the body of knowledge in cover audio selection and LSB audio steganography. The technical contributions relate to the practical and empirical aspects of the research.

1. Fundamental Contributions:
    - The proposed classification: The classification improves the definition of behaviours in cover selection, leading to better mapping of cover selection methods. Furthermore, the review analysis offers an improved depiction of the methods and a broader opportunity to identify the strength and weaknesses of each method. The review focuses on 18 articles that thoroughly inspect and evaluate cover selection methods,

rendering a valuable point of reference for both established and emerging researchers in the domain.

- The BCM-LSB Concept: Although the concept is based on the idea of selective least significant bit embedding, but there are significant differences. For example, BCM-LSB uses random embedding based on smaller segments instead of embedding based on the whole audio. Additionally, the proposed method includes a rounding mechanism that preserves the capacity of basic least significant bit embedding, which is higher compared to selective least significant bit embedding.
- The MCAS Concept: To the best of the author's knowledge, this is the first cover audio selection method proposed. It is also the first cover selection that considers the selection criteria based on different characteristics simultaneously. Additionally, a dynamic security formulation has been proposed to improve the selection criteria. The existing dynamic security metric is too broad and does not accurately rank the covers according to their dynamic security value.

2. Technical Contributions:
    - The Empirical MCAS method: The MCAS has been implemented empirically, using a combination of parameter settings and sub-techniques to enhance the performance of any method for selecting cover audio. This is an important development, as it provides a wealth of technical information and implementation background.
    - The Empirical BCM-LSB method: An empirical implementation of the BCM-LSB which includes a combination of parameters setting and sub-techniques to improve the performance of the LSB method. This is

significant because it provides high-level technical details and implementation background.

- A new record of dynamic security in LSB: The existing record in LSB managed to distribute the error throughout the audio; however, the error differences between segments are sometimes high due to the different encoding levels. The proposed method achieved a stable distribution of errors in the audio while maintaining consistency between segments.
- A better cover suggestion based on multiple characteristics aiming to be at least as good as the existing method's suggestion was proposed.

6.3 Research Limitations

It is important to note that this research work has several limitations:

1. Audio steganography pre-processing step is excluded.

   The process of embedding secret messages does not include pre-processing steps like compression or encryption. However, implementing these steps can affect the capacity, imperceptibility, dynamic security, and robustness performance. This is because the secret message's length changes depending on whether encryption or compression is used, and this can vary depending on whether the message is longer or shorter.

2. Key exchange protocol is not applied.

   The audio steganography algorithm BCM-LSB does not utilize a key exchange protocol, which may compromise its security performance even when steganographic keys are implemented.

3. Self-collected dataset is used.

This work did not use a standardized audio dataset but instead utilized a personally collected dataset from free audio websites. Additionally, utilizing various audio sample rates, stereo settings, and different bit per sample can result in different capacities, imperceptibility, dynamic security, and robustness performance.

6.4 Future Works

The potential future directions of this research are outlined as follows:

1. In this research, an amended audio steganography algorithm that combines cover selection and audio steganography embedding method was proposed. The algorithm can be further enhanced by selecting other audio steganography methods or cover selection methods which give the best results.
2. In MCAS, evaluation metrics focus on imperceptibility, robustness and dynamic security. Future work may include new security characteristic metric to address additional security issues in audio steganography.
3. This research implements a heuristic search to find suitable cover selection. Future work may involve fine-tuning the parameters to accelerate and improve the accuracy of the selected solutions.
4. A machine learning algorithm can enhance the cover selection process by analysing different parameters extracted from audio files, and consequently reducing the selection time. Additionally, the implementation of the algorithm in real-time can be achieved through the utilization of machine learning.
5. The proposed algorithm can be implemented for other types of media, such as audio formats or images.

6. A time complexity analysis can evaluate the algorithm's performance based on the parameters used in the cover selection method.
7. A video cover selection algorithm based on the CAS model can be implemented using a performance characteristic evaluation metric.

In conclusion, this research was conducted to address and aid the lack of awareness about audio steganography among computer and mobile users where information security is crucial. The enormous amount of data exchanged over wired and wireless communication channels. To ensure confidentiality and data security, various techniques are available for hiding information within common music files and audio streams. It is crucial for individuals, organizations, enterprises, and governments to comprehend the intricacies, aspects, and advantages of audio steganography to ensure the safety of their private information that is regularly exchanged and transmitted.

List of Publications

1. Muhammad Harith Noor Azam, Farida Ridzuan, M. Norazizi Sham Mohd Sayuti, and Ahmed Alsabhany. A.Balancing the Trade-Off between Capacity and Imperceptibility for Least Significant Bit Audio Steganography Method: A New Parameter. 2019 IEEE Conference on Application, Information and Network Security, AINS 2019. Pp 48-53.
2. Muhammad Harith Noor Azam, Farida Ridzuan, and M. Norazizi Sham Mohd Sayuti (2022). A New Method to Estimate Peak Signal to Noise Ratio for Least Significant Bit Modification Audio Steganography. Pertanika Journal of Science & Technology, 30(1).
3. Muhammad Harith Noor Azam, Farida Ridzuan, and M. Norazizi Sham Mohd Sayuti (2023). Optimized Cover Selection for Audio Steganography Using Multi-Objective Evolutionary Algorithm. Journal of Information and Communication Technology, 22(2), 255-282.