CHAPTER I

INTRODUCTION

1.1 Background

Digital transformation has fundamentally changed the way organizations store, manage, and distribute information. Confidential documents, including financial reports, business strategies, and other sensitive data, are now stored in digital formats that are increasingly vulnerable to cyberattacks (Admass et al., 2024).

To address these security risks, various conventional techniques have been developed to protect digital documents. Symmetric encryption algorithms such as AES (Advanced Encryption Standard) and asymmetric algorithms like RSA (Rivest–Shamir–Adleman) are commonly employed to ensure confidentiality and secure communication (Yudistira, 2024). Digital signatures play a significant role in ensuring the authenticity and integrity of digital documents by allowing recipients to verify document origin and detect unauthorized modifications through public key cryptography (Yudistira, 2024). In addition, watermarking techniques embed imperceptible ownership or authenticity markers within digital content, which can later be used for verification or tamper detection (Jalil & Mirza, 2009).

Although traditional encryption such as AES and RSA can effectively secure digital documents, it has a notable limitation. When decryption is attempted using an incorrect key, the result is often an error or unreadable output. This clear feedback can be exploited by attackers through brute-force attacks.

Another technique that addresses the limitations of encryption alone is steganography. This method conceals the presence of sensitive data by embedding it into cover media such as digital images. The Least Significant Bit (LSB) approach is one of the most widely used steganographic methods due to its simplicity and efficiency. However, LSB-based steganography faces limitations in embedding capacity and vulnerability to detection through statistical steganalysis (Luo et al., 2024). Recent studies suggest that choosing appropriate file formats such as PNG can improve the balance between imperceptibility and payload capacity, making LSB embedding more practical in security applications (Sahu & Swain, 2020).

Gharbi and Nori (2022) describe honey encryption (HE) as a method that protects data by producing decoy outputs when decryption is attempted with an incorrect key. Unlike conventional encryption, which typically fails or returns unreadable results when the wrong key is used, HE returns outputs that appear valid. This behavior misleads attackers and makes it difficult to determine whether a guessed key is correct or not. As emphasized by Gharbi and Nori, this characteristic complicates brute-force attacks by eliminating clear indicators of decryption success or failure.

Beyond technical vulnerabilities, the broader context of digital transformation also contributes to increased exposure to threats. Saeed et al. (2023) point out that although digital systems offer high operational efficiency, their integration also introduces new and complex attack surfaces. Consequently, the implementation of comprehensive and layered security strategies is essential to ensure the confidentiality, integrity, and availability of sensitive information.

By integrating steganography and honey encryption, a more robust multi-layered protection scheme can be achieved. In this combined approach, ciphertext is first protected using honey encryption and then hidden inside a cover image using LSB steganography. This not only conceals the presence of encrypted content but also ensures that attackers who attempt to break the encryption without the correct key receive misleading outputs, thereby strengthening the overall security posture.

This research aims to evaluate the effectiveness of integrating honey encryption and steganography in enhancing the security of confidential documents against combined attacks, specifically brute-force attacks on encrypted data and steganalysis on cover media. The evaluation focuses on the validity of decoy outputs, the time efficiency of encryption and decryption processes, and the visual quality impact caused by embedding ciphertext into the cover media. Through this evaluative approach, the study aims to contribute to the development of more robust and adaptive data protection solutions in the digital era.

1.2 Problem Identification

1. Limitations of Traditional Encryption:

   Ciphertext generated by standard encryption techniques often displays detectable patterns, making them vulnerable to brute-force attacks (Admass et al., 2024). However, the ability to mislead attackers when the key is incorrect remains limited.

2. Limitations of Steganography Techniques:

   Common LSB-based steganographic methods have restricted embedding capacity and are prone to detection through statistical steganalysis (Luo et

al., 2024). This raises concerns about their robustness when used in high-risk environments.

3. Challenges in Decoy Output Generation:

   While honey encryption can produce misleading decoy outputs, maintaining output consistency and realistic formatting under incorrect keys remains technically challenging (Gharbi & Nori, 2022).

1.3 Research Questions

1. How to design and implement a PDF document security system by combining honey encryption and LSB-based steganography techniques?
2. How can the system produce output in the form of a decoy document when the decryption process is carried out with an inappropriate key?
3. What is the visual quality of the cover image after inserting the ciphertext, and how likely is the insertion to be detected through steganalysis techniques?

1.4 Research Limitations

1. This research only examines the protection of documents in PDF format.
2. The generated ciphertext will be embedded into PNG digital images.
3. All experiments are conducted in a controlled laboratory environment using dummy documents.

1.5 Research Objectives

1. Design and implement a PDF document security system using a combination of honey encryption and LSB-based steganography techniques.

2. Test the system's ability to produce output in the form of decoy documents when the decryption process is carried out with the wrong key as a form of simulation of brute-force attacks.
3. Evaluate the quality of stego media generated from the ciphertext insertion process through measuring the level of visual distortion and testing the detection by steganalysis tools.

1.6 Research Significances

1.6.1 Theoretical Significances

1. Development of Data Security Literature :

   This research will enrich the literature in the field of data security by integrating two techniques that have previously been studied separately, namely honey encryption and steganography. This is expected to produce a new conceptual model for multi-layered security systems.
2. Identification of Gaps and Challenges :

   This research helps identify the shortcomings of conventional methods in terms of encryption and steganography, while also providing a foundation for the development of more robust integration strategies to protect confidential documents.

1.6.2 Practical Significances

1. Enhancement of Confidential Document Security :

   The research findings are expected to provide recommendations for organizations in implementing effective multi-layered security systems, thereby minimizing the risk of data theft or leakage.

2. Applications Across Various Sectors :

   The findings of this research have the potential for application in sectors that heavily rely on the protection of sensitive data, such as banking, healthcare, and government, thus enhancing stakeholder trust in information system