International Journal of Sociotechnology and Knowledge Development
Volume 16 • Issue 1 • January-December 2024

A New Encryption-Based Algorithm for Embedded Image Steganography

Ali Mohammed Abed
Université de Sfax, Tunisia

Houcemeddine Hermassi
ENI Carthage, Tunisia

Walid Barhoumi
https://orcid.org/0000-0003-2123-4992
Institut Supérieur d'Informatique, Tunisia

ABSTRACT

This journal paper deals with Steganography technique which is a method for hiding secret communications inside a cover object during sender-receiver communication. From ancient times to the present, the security of secret information has been a key concern. It has long been an area of interest for researchers to create mechanisms for sending data without disclosing it to anybody other than the intended receiver. To facilitate the safe transport of data, researchers have periodically created a variety of approaches, including steganography. Using the synergies that may be obtained by combining cryptography with steganography. This paper's work seeks to improve an innovative approach for hiding a hidden message inside an image. This study developed a new encryption-based method for embedded image steganography, LSB with the RSA algorithm, to upsurge data security. These depicted results were subjected to the comparative analysis of the existing previous predictive models with the present proposed work which is superior to them.

KEYWORDS

Steganography, Encryption-Based Method, Secret Communications, Hiding Image

INTRODUCTION

It is evident that technology has influenced our lives and is indispensable to our daily existence. Regular advancements in technology are being made thanks to the continuous scientific contributions made by the research community. The progression of technology is now used as a proxy for evaluating other elements of a society's overall social growth and progress.

Researchers have been developing standards and innovative methods to strengthen cybersecurity policy, enhancing the security of critical infrastructures, and implementing national defensive countermeasures. Effective frameworks are required to facilitate the use of data analytics to anticipate attacks, identify optimal countermeasures to respond to attacks, and optimize the allocation of resources after an attack.

Cyberattacks are classified based on a range of actions. Some attacks involve data and information theft. Others shut down entire systems. Attacks may be motivated by political unrest or social or economic problems (Khater., 2023).

DOI: 10.4018/IJSKD.349224

Many organizations are driven by technology. If you consider the nature of workforce shortages and recruiting challenges in areas like artificial intelligence and cybersecurity, it is important to understand how organizations need to recruit diverse technology-savvy talent including those from diverse cultures, backgrounds, and religions. There have been several incidents in the United States that point to significant problems with religious incivility in the workplace (Burrell, 2021).

In particular, the media has seen a dramatic shift from printed newspapers to video hosting websites. People have shifted their major mode of communication to that of the media. People are now able to exchange photos, movies, & audio with one another across social networking platforms. It has assisted in reducing the effect that physical distance has on communication, also it has enabled the sharing of digital media. Not only are media platforms used for social communication, but they are also utilized for marketing by firms, evaluating customer service, influencers for generating material on social alertness, distributing news digitally by newspapers, etc. Email is now the primary means of communication, both formally and informally, surpassing even the use of social media as the dominant platform. The public has access to a wide variety of video-hosting websites, some of which include YouTube & TikTok, amongst others. On the one hand, technology empowers us and enriches our lives; on the other hand, privacy & security are jeopardized. Digital media is sent across untrusted communication channels; therefore, it is susceptible to tampering and may be utilized by terrorists, hackers, & others with ill intent to reveal locations of covert meetings. On the other hand, it is vital for government officials, police officers, as well as security personnel to effectively convey classified information and corporate secrets in a way that cannot be interrupted & altered. Methods of information security are required not only for the safe flow of data but also for the intercepting and decoding of any illegal or secret communications that may be taking place.

The concept of "information hiding" refers to the practice of concealing sensitive data from prying eyes, such as those of potential attackers or other interested parties. The most common methods for hiding sensitive information are steganography, cryptography, & watermarking (Singh et al., 2020), (Pathak et al., 2018). The goal of cryptography is to transform readable plaintext into unintelligible form called ciphertext. Encryption and decryption are the two algorithms that make up the field of cryptography. Encryption algorithm is utilized to create ciphertext from plain text at sending end of the process. When the message is received at its destination, the technique for decryption is used to separate the plain text from ciphertext (Abood & Guirguis, 2018).

The technique of incorporating confidential material into any type of digital media is referred to as watermarking. Embedding may take the form of a symbol or emblem that serves the purpose of establishing ownership and protecting copyrights (Kumar et al., 2018), (Boenisch, 2020). Steganography refers to the method of concealing sensitive or private information inside digital media while leaving it accessible to the user. The fact that the concealed message is inaccessible to the human sight makes it resistant to attack (Wang et al., 2019).

Data security from unauthorized users or hackers and the provision of a high level of security to prevent data alteration are the two primary components of data security. Because of the dramatic rise in the amount of data that may be sent via the internet in recent years, this aspect of data security has received lots of attention in recent times. Numerous methods, such as cryptography, steganography, and digital watermarking, have been developed in current years with the purpose of making data transfers carried out through the internet more resistant to unauthorized access. While Cryptography is technique for concealing information by encoding it into "cipher text" & transferring it to intended recipient using unknown key, Steganography adds layer of protection by concealing the cipher text inside an image or other format that seems to be invisible (Nehra, 2015).

Both steganography & cryptography are well-known & commonly utilized methods that change information (messages) to cypher them or disguise the fact that they exist. These approaches have several applications in computer science and other related domains, including the protection of e-mails, credit card information, business data, etc. To be more exact, steganography refers to both the art & science of communicating in manner that conceals fact that communication is taking place. To prevent