

SECURE DATA TRANSFER OVER INTERNET USING IMAGE STEGANOGRAPHY.

Summary research paper's:

1. Secure data transfer through internet using cryptography and image steganography

Nunna and Krishna [1] presents a hybrid system that combines cryptography and image steganography to enhance the security of data transfer over the internet. The authors use the XOR operation for encrypting the data, which is then pseudo-randomly embedded into the image using a user-defined key. This method provides two layers of security by first encrypting the message and then hiding it within the image, making it more resistant to unauthorized access and detection. XOR is not best used as part of a larger encryption scheme, as relying solely on XOR may not be sufficient under advanced attacks. The study did not discuss any of the criteria for testing , such as: Peak Signal-to-Noise Ratio (PSNR) and Mean Squared Error (MSE) metrics to measure the quality of the stego-image compared to the original image.

2. Enhanced Data Security of Communication System Using Combined Encryption and Steganography

The authors propose [2] a novel method that combines encryption and steganography to protect sensitive information during transmission. Their methodology involves three main components: Image Analysis Using Discrete Wavelet Transform (DWT): The methodology begins by analyzing both the host image and the secret image using DWT, which decomposes the images into various frequency components. This allows for efficient manipulation and embedding of

the secret image within the host image. 2. Embedding Process: The primary image intended for protection is embedded into the host image through a zeroing technique. Specific coefficients of the host image are set to zero to create space for the secret image components. The authors then modulate the values of these coefficients using the values from the secret image, ensuring that the hidden image is not easily detectable. 3. Encryption: Following the embedding, the combined image undergoes encryption using an exponential mathematical function. This process transforms the modulated image into an encrypted form, enhancing security and making it difficult for unauthorized users to retrieve the hidden information. Limitations of the Methodology : 1. Computational Complexity: The use of Discrete Wavelet Transform (DWT) and complex mathematical functions for embedding and encryption may result in increased computational requirements. 2. Image Quality Degradation: While the method aims to conceal the secret image effectively, the process of modifying pixel values and embedding can lead to visible artifacts or degradation in the quality of the host image, especially if not properly managed.

3. A Novel Image Steganography Method for Industrial Internet of Things Security

Hassaballah et al. [3] proposed a novel image steganography method named HHO-IWT aimed at enhancing security in the Industrial Internet of Things (IIoT). The method utilizes Harris hawk's optimization (HHO) combined with integer wavelet transform (IWT) to embed secret data in cover images. Their approach focuses on optimizing pixel selection for embedding, which improves payload capacity while maintaining high visual quality and security against steganalysis attacks. The study discussed the stealth method in the Industrial Internet of Things only, which makes it limited to this technology only, without referring to the effectiveness of its use in other uses.

4. Hybrid Secure Data Transfer Scheme Using Cryptography and Steganography

Shree and Swami [4] proposed a hybrid secure data transfer scheme that utilizes both cryptographic techniques and image steganography. Their method first encrypts plaintext into a ciphertext image, which is then concealed within a cover image to create a stego-image. The study did not specify the encryption algorithm used, so the level of security depends on the quality of the encryption algorithm used. Furthermore, the study did not detail the methodology used in the steganography process. so, providing precise details about this would be useful to evaluate the effectiveness of the proposed system.

5. Securing Data via Cryptography and Arabic Text Steganography

Alkhudaydi and Gutub [5] , presents a dual-layer security system that combines lightweight cryptography (LWC) with Arabic text steganography. The methodology consists of two main stages: 1. Light-Weighted Cryptography (LWC), where sensitive text is first encrypted using lightweight encryption algorithms such as AES, DES, or IDEA to convert it into an unreadable format. 2. Arabic Text Hiding: The encrypted data is not embedded in an image or media as is customary, but rather embedded within the Arabic text's diacritical marks. In other words, the Arabic text with diacritical marks is the encrypted text. Although the methodology aims to make hidden information difficult to detect, the cover text, when it appears with diacritics that do not conform to Arabic grammar rules, may raise suspicions among attackers that hidden data is present. Furthermore, the encryption algorithms used in the study (AES, DES, IDEA) still require computational costs.

Critical Analysis

The combination of encryption and steganography has emerged as a promising approach to securing data transmission, especially in environments with stringent security requirements. The reviewed studies highlight various methodologies that enhance data

protection through innovative techniques. For example, the hybrid systems proposed by Nona and Krishna, as well as Shree and Swami, emphasize the importance of two-layer security. However, these studies often lacked sufficient details regarding the encryption algorithms used.

Moreover, although the use of lightweight encryption is beneficial for resource-constrained devices, as demonstrated in the work of Al-Khadji and Ghotab, it poses challenges related to computational costs and potential vulnerabilities. The reliance on XOR operations in some studies highlights a common weakness: XOR alone may not withstand sophisticated attacks, requiring more robust encryption techniques.

Furthermore, embedding data within images or text often weakens the quality of the host medium, making it vulnerable to attackers. Notable limitations of the discussed methodologies such as the lack of performance metrics like PSNR and MSE reveal the need for a more comprehensive evaluation framework to assess the effectiveness of these systems. Overall, while the combination of encryption and concealment offers an innovative path forward, ongoing research must address these gaps to ensure reliable and secure data transmission.

Connection:

1. Hybrid Systems:

A prevailing trend is the development of hybrid systems that combine encryption and steganography to enhance data security. Systems that rely solely on stealth technology are more vulnerable to hacking.

2. Dual-Layer Security:

Studies emphasize the importance of a dual-layer security approach, where data is first encrypted using encryption algorithms and then hidden within a storage

medium using stealth techniques. This makes data more resistant to unauthorized access and disclosure.

Conflicts between the findings:

1. Effectiveness of Encryption Algorithms:

Some studies, such as those by Shree and Swami, do not specify the encryption algorithms used, leading to uncertainty about the achieved level of security. In contrast, other studies emphasize the importance of using strong algorithms such as AES, noting that relying on unspecified methods can expose systems to risks, as in the study by Nunna and Krishna, which used the XOR algorithm to encrypt data.

2. Quality vs. Security Trade-off:

While many studies aim to enhance security, they often point to a trade-off related to the quality of the host medium. For example, embedding techniques that manipulate the host's diacritical values can lead to significant flaws, as demonstrated in the work by Alkhudaydi and Gutub, where Arabic text appears with random diacritical marks that do not conform to Arabic diacritical rules.

3. Computational Complexity vs. Simple Solutions

Approaches that advocate simple encryption, as in the Nunna and Krishna study, may conflict with those that require more computationally intensive techniques, such as the discrete wavelet transform (DWT). While simple solutions aim for efficiency, they may not provide the same level of security as heavier algorithms, creating a conflict in application suitability.

References

- [1] K. C. Nunna and R. Marapareddy, "Secure data transfer through internet using cryptography and image steganography," *Conf. Proc. - IEEE SOUTHEASTCON*, vol. 2, 2020, doi: 10.1109/SoutheastCon44009.2020.9368301.
- [2] H. T. S. Alrikabi and H. T. Hazim, "Enhanced Data Security of Communication System Using Combined Encryption and Steganography," *Int. J. Interact. Mob. Technol.*, vol. 15, no. 16, pp. 144–157, 2021, doi: 10.3991/ijim.v15i16.24557.
- [3] M. Hassaballah, M. A. Hameed, A. I. Awad, and K. Muhammad, "A Novel Image Steganography Method for Industrial Internet of Things Security," *IEEE Trans. Ind. Informatics*, vol. 17, no. 11, pp. 7743–7751, 2021, doi: 10.1109/TII.2021.3053595.
- [4] R. Shree and D. Swami, "Hybrid Secure Data Transfer Scheme Using Cryptography and Steganography," *Lect. Notes Networks Syst.*, vol. 166, pp. 577–583, 2021, doi: 10.1007/978-981-15-9689-6_62.
- [5] M. Alkhudaydi and A. Gutub, "Securing Data via Cryptography and Arabic Text Steganography," *SN Comput. Sci.*, vol. 2, no. 1, 2021, doi: 10.1007/s42979-020-00438-y.