International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 13, Issue 7, July 2024)

Review of Image Steganography Method for Domestic Internet of Things

Himanshu Jharaniya[1], Nitin Choudhary[2], Dr. Gourav Shrivastava[3]
[1]Research Scholar, Big Data and Cloud Computing, Sage University Bhopal
[2]Assistant Professor, School of Advanced Computing, Sage University Bhopal
[3]Associate Professor, (Head of Department),School of Advance Computing, Sage University, Bhopal
himanshujharaniya1995@gmail.com, nitin.c@sageuniversity.edu.in, gourav.s@sageuniversity.edu.in

Abstract— **Image steganography, the art of hiding information within digital images, has emerged as a critical technique for ensuring data privacy and security in the rapidly expanding domain of the Internet of Things (IoT). This review delves into the various image steganography methods specifically tailored for domestic IoT environments, where the seamless and secure exchange of data between household devices is paramount. We analyze the strengths and weaknesses of existing techniques, including spatial domain methods, frequency domain methods, and adaptive steganography, with a focus on their applicability to IoT systems.**

Keywords— Image Steganography, IOT, Security, Information, Artificial Intelligence.

I. INTRODUCTION

The Internet of Things (IoT) has revolutionized the way we interact with our environment, particularly within domestic settings. Smart homes equipped with interconnected devices, ranging from security cameras to home appliances, offer unprecedented convenience and functionality. However, this connectivity also presents significant security challenges. As more personal data is transmitted and stored within these systems, ensuring its privacy and security becomes increasingly critical. Image steganography, the practice of concealing information within images, has emerged as a promising solution to these challenges.

Steganography, derived from the Greek words "steganos" (hidden) and "graphein" (writing), is a technique that enables the covert embedding of data into various forms of media, such as text, audio, video, and images. Among these, image steganography is particularly advantageous due to the widespread use and large data capacity of digital images. By embedding sensitive information within images, it becomes possible to protect data from unauthorized access while maintaining the perceptual quality of the carrier image. This dual requirement of security and imperceptibility is crucial in domestic IoT environments, where the seamless integration of security measures into everyday devices is essential.

Traditional image steganography techniques can be broadly classified into spatial domain methods and frequency domain methods. Spatial domain methods, such as Least Significant Bit (LSB) substitution, directly modify the pixel values of the carrier image to embed the secret data. These methods are relatively simple and computationally efficient, making them suitable for real-time applications in IoT devices. However, they are often susceptible to various forms of attacks, such as noise addition and image compression. On the other hand, frequency domain methods, such as Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT), embed data by altering the frequency coefficients of the image. These methods typically offer greater robustness against attacks but are computationally more intensive.

In recent years, the integration of machine learning and artificial intelligence into image steganography has garnered significant attention. Advanced techniques, such as deep learning-based steganography, leverage neural networks to optimize the embedding process, enhancing both the security and imperceptibility of the hidden data. These methods have shown promising results, particularly in adapting to the dynamic and diverse nature of domestic IoT environments.

Despite the advancements, several challenges remain in the application of image steganography to domestic IoT systems. The heterogeneous nature of IoT devices, varying in computational power and storage capacity, necessitates the development of flexible and scalable steganographic methods. Additionally, the dynamic and often unpredictable nature of domestic IoT networks requires robust techniques capable of maintaining data integrity and security under varying conditions.

This review aims to provide a comprehensive overview of the current state of image steganography methods tailored for domestic IoT environments. We will examine traditional techniques, recent advancements, and emerging trends, with a focus on their applicability and effectiveness in securing IoT systems. By highlighting the strengths and limitations of existing methods, we aim to identify potential areas for future research and development, ultimately contributing to the advancement of secure and efficient data protection strategies in the realm of domestic IoT.

II. LITERATURE SURVEY

M. Kashif et al [1] presented a technique based on digital picture steganography termed Harris hawks optimization-integer wavelet transform (HHO-IWT) for secure communication and data in the IIoT context. The approach uses a metaheuristic optimization algorithm known as HHO to effectively choose picture pixels that may be utilised to conceal bits of secret data inside integer wavelet transformations, so embedding the data in the cover images.

T. S. Deepak, et al.[2] Information is crucial to the success of every business in the modern day. In most companies, data is increasingly being generated by workers and other end-users. In this situation, data protection is an issue for every firm. Many problems, such as data loss, confidentiality, integrity, and availability, might arise, for instance, while storing information on the cloud. Solutions to these problems may be found in the many data security methods now available. Cryptography and steganography are the two most common methods. With the aid of these methods, a fresh strategy for bolstering safety measures and maximising data storage capacity has been offered in this study. It all starts with locking down that cover photo.

A. Sharma et al.[3] Communication speed is essential in today's fast-paced world. It has been shown to be a simple and effective method of global communication. However, the risks of espionage during data transmission seem to have grown in tandem with technological development. There is still a significant and precise need in Network Security to safeguard information at every stage of its journey. Cryptography is a way for securing data transmissions using codes and other forms of encryption. This ensures that the informed recipient can properly recognise, use, operate, and store the data for their own needs.

J. Barker et al,[4] Innovating new ways to sense and control the physical world, the Internet of Things (IoT) is reshaping the most cutting-edge technology. Through the IoT, disparate smart devices may work together to collect and analyse data from their immediate surroundings. Recent years have seen a proliferation of sensor devices that have made it possible to use a wide spectrum of IoT technologies in the real world. Possessing such qualities paves the way for significant obstacles. Internet of Things (IoT) networks confront a huge problem in the form of security. Smart and strong adversaries are impossible to defend against using just conventional methods.

S. G., C. Ashwin, et al.[5] Data transmission occurs constantly in the ever-changing realm of Internet of Things. Data transmission network security has traditionally relied on either steganography or cryptography alone, but recently, a number of hybrid systems that use both have been presented. Cryptography is useful because if an attacker can guess the secret key, they can readily decode the data and see it in plaintext. Conversely, if the altered content of a picture can be discerned, the culprit might use steganography to decipher the original message. As a result, this study introduces a brand-new technique for secure and efficient data transfer. Both cryptographic and steganographic approaches are included into the plan to provide the highest degree of safety for the concealed information.

S. Chen, , et al [6] The widespread implementation of the Internet of Things depends on people feeling safe and confident in its reliability (IoT). Using steganographic secret sharing, this research presents a secure message authentication technique for the Internet of Things. In our approach, the dealer divides the message and gives each half to a different participant; the message is only decoded when both authorised parties provide their permission. Neither party may share the communication without the other's permission. Each message sent via IoT connections is encrypted using a generative adversarial network and disguised as a picture of a human face (the "shadow image") to protect against malicious intrusions (GAN). Each user's shadow picture is produced using the user's private key, and a convolutional neural network (CNN) is trained to decode the user's message share from that image. It's possible that the shadow pictures will be distorted or altered in some way while being sent from the dealer to the participant.

Masoud M. Z. et al. [7] The age of the Internet of Things (IoT) has resulted in the worldwide proliferation of devices that produce and transmit data. Achieving analysis, analytics, and visualisation need this data to reach end devices. Smartphones are a part of the Internet of Things age, and as such, they may create and alter data. However, the computing power and storage capacity of such devices is inadequate to permit significant reductions in device size or power consumption. The information produced by these gadgets must be encrypted before being sent to another location. To that end, this paper presents HidSave, a novel approach to steganography for concealing picture data.

S. Dhawan et al.,[8] The Internet of Things (IoT) is a space where massive amounts of data are being sent at all times. While ensuring the safety of these records is no easy feat, encryption and steganography provide promising solutions. In matters of user authentication and data privacy, these methods are crucial. As part of this study, we present a method that combines IoT protocol with steganography to provide a very high level of security. In this paper, we present a mechanism for picture steganography that makes use of a variety of methods to strengthen the secret data's protection using a Binary bit-plane decomposition (BBPD) based image encryption method. To further improve payload capacity, we next propose an adaptive embedding procedure based on the Salp Swarm Optimization Algorithm (SSOA) to adjust the parameters of the steganographic embedding function for edge and smooth blocks.

Nicolai Mohamed et al. [9] Image-based software is quite common nowadays. Steganography refers to a class of data-hiding techniques used to conceal the existence of a private conversation between two parties. This is accomplished by embedding the steganographic medium within a cover medium, so delivering a stego medium that is ideally undetectable by an outside observer. Image steganalysis, the polar opposite of steganography, is concerned with discovering hidden pictures. There is a steady increase in the safety of image steganography methods. Criminals on the Internet may use these methods to have an anonymous conversation that has malevolent intent.

Kabulov, A., et al.,[10] Using digital sensor data synthesis to solve the issue of secure transmission based on steganographic replacement is becoming more relevant in the Internet of Things. The degree of blacking out of the grayscale message is an important consideration here. When it comes to the security of data in IoT systems, several approaches are taken, and many issues are resolved. In this article, we suggest a technique and algorithm for a grayscale computer picture, where the value of each pixel is a single sample expressing the quantity of light and conveying just that information.

III. CHALLENGES

While image steganography presents a promising approach to enhancing security in domestic IoT environments, several significant challenges need to be addressed to ensure its effective implementation. These challenges encompass various aspects, including technical limitations, computational constraints, security vulnerabilities, and the dynamic nature of IoT networks. Understanding and addressing these challenges is crucial for the development of robust and practical steganographic solutions.

Limited Processing Power: Many IoT devices, particularly those used in domestic settings, have limited processing power and memory. Implementing sophisticated steganographic algorithms that require significant computational resources can be challenging on such devices.

Real-time Processing: The need for real-time data processing and communication in IoT environments imposes constraints on the complexity of steganographic methods. Ensuring that these methods can operate efficiently without causing delays is essential.

Data Capacity: The capacity of images to hold hidden data is limited. Balancing the amount of embedded information with the need to maintain the perceptual quality of the image is a delicate task, particularly when dealing with high-resolution images or video streams in IoT systems.

Noise and Compression: IoT devices often compress data to save bandwidth, and the transmission of data can introduce noise. Traditional steganographic methods, especially those in the spatial domain, may not be robust against such alterations, leading to the loss of hidden information.

Steganalysis: Advanced steganalysis techniques are continually being developed to detect hidden data. Ensuring that steganographic methods remain imperceptible and secure against these detection techniques is an ongoing challenge.

Heterogeneity of Devices: Domestic IoT networks consist of a wide variety of devices with different capabilities and communication protocols. Developing steganographic methods that are flexible and can operate seamlessly across diverse devices is complex.

Network Variability: The dynamic nature of IoT networks, characterized by varying connectivity and network conditions, requires robust steganographic techniques that can maintain data integrity and security under fluctuating circumstances.

Scalable Solutions: As the number of IoT devices in domestic environments continues to grow, scalable steganographic methods that can efficiently handle large-scale deployments are necessary. Ensuring that these methods can adapt to increasing data loads and network sizes is crucial.

Data Privacy: While steganography aims to enhance data privacy, the use of hidden information can raise ethical concerns, particularly regarding consent and transparency. Ensuring that steganographic practices comply with privacy regulations and ethical standards is important.

Malicious Use: The potential for steganography to be used for malicious purposes, such as hiding malware or unauthorized data, poses a significant challenge. Developing mechanisms to detect and prevent such misuse is essential.

Standardization: The lack of standardized protocols for implementing steganography in IoT environments can hinder interoperability between devices from different manufacturers. Establishing common standards and frameworks is necessary to facilitate seamless integration.

Power Efficiency: Many IoT devices operate on limited power sources, such as batteries. Implementing energy-efficient steganographic algorithms that do not significantly drain the device's power supply is crucial for the longevity and sustainability of IoT networks.

Addressing these challenges requires a multidisciplinary approach, involving advancements in algorithm design, computational optimization, security protocols, and regulatory frameworks. By tackling these issues, researchers and practitioners can develop more robust, efficient, and secure image steganography methods tailored for domestic IoT environments, ultimately enhancing the overall security and privacy of smart homes.

IV. CONCLUSION

The integration of image steganography into domestic Internet of Things (IoT) environments offers a promising avenue for enhancing data privacy and security. As smart homes become increasingly prevalent, the need to safeguard sensitive information transmitted between interconnected devices is paramount. This review has provided a comprehensive overview of various image steganography methods, highlighting their applicability, strengths, and limitations within domestic IoT settings. Image steganography holds substantial potential for enhancing the security and privacy of domestic IoT systems. This review has highlighted the current state of the field, identified key challenges, and pointed to potential future research directions. By continuing to innovate and address these challenges, researchers and practitioners can contribute to the creation of secure and efficient data protection strategies, ultimately fostering the growth and adoption of smart home technologies.

References

1. M. Kashif, I. Shakeel, S. Ahmad and S. Mehfuz, "Enhanced Pixel Privacy: Leveraging Deep Learning for Advanced Image Steganography," 2023 7th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Kirtipur, Nepal, 2023, pp. 535-541, doi: 10.1109/I-SMAC58438.2023.10290153.
2. T. S. Deepak and V. Enireddy, "High Payload Capacity using Steganography Combined with Cryptography," 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2021, pp. 1448-1453, doi: 10.1109/I-SMAC52330.2021.9640859.
3. A. Sharma, A. Batta and V. K. Sharma, "A Review on Image Steganography and its Applications," 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2021, pp. 1466-1473, doi: 10.1109/I-SMAC52330.2021.9640838.
4. J. Barker, A. Hamada and M. Azab, "Lightweight Proactive Moving-target Defense for Secure Data Exchange in IoT Networks," 2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2021, pp. 0317-0322, doi: 10.1109/IEMCON53756.2021.9623218.
5. G. G, C. Ashwin, B. V. P, A. A and A. Hiremath, "Enhanced Data Encryption in IOT using ECC Cryptography and LSB Steganography," 2021 International Conference on Design Innovations for 3Cs Compute Communicate Control (ICDI3C), 2021, pp. 173-177, doi: 10.1109/ICDI3C53598.2021.00043.
6. S. Chen, C. -C. Chang and I. Echizen, "Steganographic Secret Sharing With GAN-Based Face Synthesis and Morphing for Trustworthy Authentication in IoT," in IEEE Access, vol. 9, pp. 116427-116439, 2021, doi: 10.1109/ACCESS.2021.3105590.
7. M. Z. Masoud, Y. Jaradat, A. Manasrah, I. Jannoud and A. Zerek, "HidSave: An Image Steganography Technique based on SudoKu Method for Smartphones," 2021 IEEE 1st International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering MI-STA, 2021, pp. 887-890, doi: 10.1109/MI-STA52233.2021.9464512.
8. S. Dhawan, C. Chakraborty, J. Frnda, R. Gupta, A. K. Rana and S. K. Pani, "SSII: Secured and High-Quality Steganography Using Intelligent Hybrid Optimization Algorithms for IoT," in IEEE Access, vol. 9, pp. 87563-87578, 2021, doi: 10.1109/ACCESS.2021.3089357.
9. N. Mohamed, T. Rabie, I. Kamel and K. Alnajjar, "Detecting Secret Messages in Images Using Neural Networks," 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2021, pp. 1-6, doi: 10.1109/IEMTRONICS52119.2021.9422500.
10. A. Kabulov, I. Saymanov, I. Yarashov and F. Muxammadiev, "Algorithmic method of security of the Internet of Things based on steganographic coding," 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2021, pp. 1-5, doi: 10.1109/IEMTRONICS52119.2021.9422588.