Al-Salam Journal for Engineering and Technology
Journal Homepage: http://journal.alsalam.edu.iq/index.php/ajest
e-ISSN: 2790-4822 p-ISSN: 2958-0862

Lightweight Steganography Technique in The Internet of Things: A survey

Hiba Adnan Qasim[1]*, Rana Saad Mohammed[1]

[1] Department of Computer Science, Collage of Education, Mustansiriyah University, Baghdad, IRAQ.

*Corresponding Author: Hiba Adnan Qasim

DOI: https://doi.org/10.55145/ajest.2024.03.01.008
Received August 2023; Accepted October 2023; Available online November 2023

ABSTRACT: In the context of the Internet of Things (IoT), lightweight steganography provides a revolutionary combination of technology and security, where data concealment meets the efficiency requirements of IoT devices. Lightweight steganography, as opposed to conventional steganographic methods, focuses on concealing information inside digital content while using the least amount of computer resources and energy. Secure data transfer is essential in the IoT world because linked devices may communicate with one another without interruption. IoT devices may communicate private data discreetly while conserving system resources, thanks to the elegant approach offered by lightweight steganography. This novel method makes use of complex algorithms that gently change data packets, turning them into bearers of hidden information without raising any red flags. The secrecy of IoT ecosystems is strengthened by lightweight steganography's easy integration of covert communication channels. In addition to improving data security, this technology also optimizes bandwidth usage and increases device battery life. A future when linked devices may transmit information safely, effectively, and surreptitiously is predicted as the IoT environment develops. This would usher in a period of unmatched data security and resource optimization.

Keywords: lightweight, steganography, internet of things

1. INTRODUCTION

The integration of intelligent technology with information technology is rapidly advancing, and remote monitoring and control through the internet is possible, but this convenience comes with potential security threats if proper measures are not taken [1][2]. Smart devices like cameras must wirelessly transmit data to central servers due to limited energy and computing power [3]. Encryption techniques provide security for the content of information, but they do not conceal the presence of secret information [1]. Steganography is employed to hide information and establish a covert communication channel for secret messages that only the intended recipient is aware of [4]. Steganography can take various forms, such as image, text, audio, and video steganography [5], and can be categorized based on the method employed [6]. Steganography is an intelligent data-hiding technology in which the secret data is placed in a cover media so that the media carrying the secret message are imperceptible to the intruder or attacker [7]. A network of actual items is known as the "internet of things" (IOT). The internet has developed into a network of devices of all types and sizes, including cars, smart phones, home appliances, toys, cameras, medical equipment, industrial systems, animals, people, and buildings. These devices are all connected, communicating, and sharing information in accordance with predetermined protocols in order to achieve smart reorganizations, positioning, tracing, safety and control, and even real-time online monitoring and online upgrades for individual users [8]. Steganography and cryptography are two examples of existing data protection techniques that are not suitable for direct adaptation due to their computational complexity, application-specificity, and rigidity. The IoT ecosystem is also portrayed as having a wide range of heterogeneous devices, high data rate traffic, and restricted device capability. Given the aforementioned constraints, simple steganography algorithms can be used to solve IoT cybersecurity problems [9]. IoT lightweight steganography can enhance communication security, prevent unwanted access to devices and systems, safeguard the intellectual property of devices and apps, and safeguard sensitive data from theft and manipulation. Lightweight steganography

*Corresponding author: hibaadnan96@uomustansiriyah.edu.iq

assists in protecting sensitive information and preventing rivals from stealing by concealing authentication credentials, security information, proprietary software, and algorithms. Additionally, it makes wireless networks used by IoT devices more secure[10]. This paper survey for study last lightweight steganography techniques in the context of the Internet of Things and make comparison between them to know direction of modern techniques.

2. RELATED WORKS

Chen et al. The authors suggest a brand-new steganography system that can conceal a secret picture under a cover image while maintaining the cover image's aesthetic quality. Their method involves combining convolutional neural networks (CNNs), attention mechanisms, and non-activated feature fusion (NAFF) to create a high-quality concealed picture that is undetectable to human observers by learning a mapping between the cover and secret images. The results of the comprehensive trials the authors did to establish the efficacy and efficiency of their suggested approach reveal that it performs better than existing methods in terms of visual quality and security. However, their technique is restricted to image-based data transfer or storage, and it could not be **relevant to other types of data**. Furthermore, the authors did not investigate how various cover pictures or hidden images affected the functionality of their network [1].

Chai et al. an end-to-end video steganography network that inserts hidden data into video frames using a coding unit mask-based method. The authors compare their suggested network to three other networks and discover that it has a lower PSNR value but a larger embedding capacity and better visual quality. The suggested network has a high computational complexity, which the authors also mention as a potential drawback for real-time applications. Overall, the article offers hope for enhancing video steganography, but further investigation is required to maximize its effectiveness and overcome its drawbacks. [11].

Subramaniyan et al. The method entails creating a compact model termed GANash utilizing latent space-compressed generative adversarial networks (GANs). The major goal of this effort was to accelerate performance, which is crucial for deployment, in terms of how long it takes to encode and decode data. The model was created to be affordable and suitable for computer engines with modest specifications. The findings demonstrated that GANash outperformed SteganoGAN in terms of mean squared error, PSNR, and time to encode and decode [6].

Rostam et al. The suggested techniques involve encoding secret data and picture data into DNA sequences and disguising randomly chosen secret data genomes in each block pixel except the block's core pixel. The secret key of the chaos function is created using the block's center pixels, which are then utilized to generate a random selection of blocks and secret data. In order to maximize privacy preservation, the article offers three layers of protection in the information concealment procedure. The outcomes of the suggested techniques demonstrate that the security and privacy of the smart city system may be increased by using DNA in picture steganography. The research includes simulation results that show the viability of the suggested techniques in terms of grayscale image PSNR, SSIM, MSE, and BER metrics. The research lacks comprehensive examination of suggested approaches' limits, effectiveness in smart city systems, and their impact on image quality and information-hiding time, necessitating further research to ensure their applicability and efficacy [12].

Alarood et al. In order to protect privacy and authenticity in IoT networks, the article suggests a steganography technique dubbed IoTSteg. In their strategy, suitable pixels in the cover picture are selected using weighted pixel classification, and the secret data is concealed using traditional LSB embedding. PSNR, CDTO, and SSIM are a few examples of the metrics used to evaluate the method.

The findings demonstrate that the suggested strategy achieves great competence in the embedding process while preserving the cover pictures' imperceptibility. The PSNR score of 66.61 achieved for a test utilizing 8000 bits and 4 cover images of 512 pixels indicates good stereo picture quality. The plan is evaluated in relation to other plans and judged to be workable and competitive. Simulating outcomes requires a time-consuming system. Additionally, it can have trouble processing noisy photos. Future research is recommended by the authors to overcome these issues and advance the system's real-time capabilities and noise reduction strategies.

IoT networks can benefit from the proposed IoTSteg scheme, which offers a viable solution for privacy and authenticity. Although it provides good embedding and picture-quality outcomes, more advancements are required to tackle real-time difficulties and noisy images [13].

3. STEGANOGRAPHY

Steganography has a long history of being used to covertly transmit data through physical means, with examples dating back to before the computer age [14]. Today, steganography has significantly advanced with the aid of computers, hardware, and software, allowing for digital steganography using various media types [15]. Examples of historical steganography techniques include Histaiacus shaving a messenger's head and writing a secret message on the bald scalp, which was retrieved by shaving the messenger's hair again [14].

4. TECHNIQUES FOR STEGANOGRAPHY

a- Image steganography involves hiding secret data within an image, which serves as a cover object. Images are often used as cover sources due to the large number of bits in their digital representation, and various steganography techniques have been developed for different image formats [16].

1- Least Significant Bits (LSB) are a straightforward method for embedding data in cover images. The simplest steganography methods directly embed the message bits into the cover image's least significant bit plane. Predictable progression. There is no human-perceivable effect when modulating the least significant bit since the There is little variation in magnitude. A suitable cover picture is required to conceal a hidden message inside an image. A lossless compression format must be used since this approach uses bits from each pixel in the image; otherwise, the concealed information would be lost during the transformations of a lossy compression algorithm. A bit of each of the red, green, and blue color components may be utilized in a 24-bit color picture, allowing for a total of 3 bits to be recorded in each pixel [17]. As an illustration, the grid below, which uses 9 bytes of memory, may be thought of as 3 pixels of a 24-bit color image:

(00100111 11101001 11001000) (00100111 11001000 11101001) (11001000 00100111 11101001)

The following grid is produced when the character A, whose binary value is 10000001, is inserted:

(0010011**1** 1110100**0** 1100100**0**) (0010011**0** 1100100**0** 1110100**0**) (1100100**0** 0010011**1** 11101001)

In this instance, the character might be correctly inserted by changing just three bits. When selecting the maximum cover size, just half of the bits in a picture will often need to be changed in order to conceal a hidden message. The message is successfully concealed as a result of the least significant bit shifts, which are too minute to be detected by the human visual system (HVS) [18].

It also has certain restrictions, though:

Low embedding capacity: Only a modest amount of data—typically 1 or 2 bits—can be embedded per pixel using LSB insertion. This is so because altering even the smallest portion within a pixel has a negligible effect on how the image looks as a whole.

Lack of robustness: straightforward image processing techniques like compression, noise filtering, and cropping make it straightforward to find and remove LSB encoded data.

Security flaws: There are a variety of tools available for identifying and deleting LSB embedded data, and LSB insertion methods are well-known for their use [19]-[20].

2- Masking and filtering to conceal a message, masking and filtering techniques, which are often limited to 24 bits or grayscale pictures, adopt a different strategy. These techniques produce markings in an image that are practically identical to paper watermarks. For example, changing the brightness of specific areas of the picture can do this. While masking does alter an image's obvious characteristics, it may also be done in a way that makes the changes invisible to the human eye. Masking is more resilient than LSB modification in terms of compression, cropping, and other types of image processing since it makes use of the visible portions of the picture. It is more suitable than other options since the information is not lost at the "noise" level but rather is present in the viewable section of the image If a lossy compression method like JPEG is being employed, LSB adjustments should be made [18].

One of the primary drawbacks of masking is that, especially in complicated or noisy images, it can be challenging to precisely choose the region of interest. Masking can also bring artifacts into the image, including halo effects or sharp edges. The difficulty in selecting the best filter for the task at hand is one of the key drawbacks of filtering. Additionally, filtering can generate distortions like blurring or ringing in the image [21]-[22]-[23].

b- Text files can be used for steganography using tools like StegParty, which utilizes rules based on the flexible nature of the English language to conceal small amounts of data, appearing as minor typos or grammatical errors [24]. Although the amount of data that can be hidden using this method is limited, it can be used with files such as Word documents and HTML files [15].

1-Line-Shift Coding This is a technique for changing a document to make it more distinctive by vertically moving the positions of text lines. This encoding can be applied to a page image's bitmap or to the format file. The format file or bitmap may be used to extract the embedded code word. Since the original picture is known to have consistent line spacing between subsequent lines inside a paragraph, in some circumstances, this decoding may be done without the original image [17].

the following LSC restrictions:

Low embedding capacity: LSC can only embed a modest amount of data—typically 1 or 2 bits—per line of text. This is due to the fact that changing a line of text by more than a few characters will cause the change to be obvious to the unaided eye.

Poor robustness: LSC implanted data may be readily found and removed, especially with the use of basic text-processing functions like line breaks, justification, and word wrapping.

Security flaws: There are a variety of tools available for identifying and deleting LSC embedded data, and LSC algorithms are well-known [25].

2-Feature Coding This coding technique can be used to encode a format file or a document's bitmap picture. Depending on the code word, specific text properties are inspected in the image and either changed or left alone. The original image, or more particularly, a description of the change in pixels at a feature, is needed for decoding. There are several options for text characteristics; in this case, we decide to change the upward, vertical end lines, or the tops of letters like b, d, and h. These end lines are modified by lengthening or shortening them by one (or more) pixels, but the end line characteristic is left unchanged [26]. It is crucial to be aware of its drawbacks, including the difficulties of embedding substantial volumes of data, its linguistic sensitivity, and its security weaknesses[27].

c- Audio signals can be used to hide secret data by modifying the binary sequence of the audio file. Several methods for audio steganography exist, including least significant bit encoding, parity encoding, phase coding, and spread spectrum [16].

1- LSB Coding Analog audio signals are converted to digital binary sequences using the sampling technique and quantization. This method replaces the low-order bit (LSB) of each sample's binary sequence in a digital audio file with the binary equivalent of a secret message[17].

It also has certain restrictions, though:

Poor robustness: LSB encoded data is quickly identifiable and erasable, particularly by basic audio processing operations like compression, noise filtering, and cropping.

Security flaws: There are a variety of tools available for identifying and deleting LSB embedded data, and LSB algorithms are well-known for having security issues[28].

2- Phase Coding Phase changes in audio signals are harder for the human auditory system (HAS) to detect than noise. The phase coding approach makes use of this reality. This method achieves an inaudible encoding in terms of signal-to-noise ratio by encoding the secret message bits as phase changes in a digital signal's phase spectrum[17].

incorporating the following phase coding restrictions:

-LSB coding and other digital audio steganography methods are less computationally difficult than phase coding.

-Data that uses phase coding is susceptible to phase shifts in the audio signal.

-Phase coding can cause the audio quality to suffer, especially when there is a lot of embedded data.

-In comparison to low-frequency audio, high-frequency audio has a lesser embedding capacity for phase coding [28].

d- Video steganography involves hiding any type of data within digital video, allowing for the concealment of a large amount of data in a video file. Two primary approaches for performing video steganography are embedding data in uncompressed raw video and then compressing the data, or embedding data directly into a compressed data stream [16].

1- Least significant bit (LSB) The most popular video steganography technique is this one. The secret message is inserted into the video pixels' LSBs. Although LSB steganography is very simple to see, it may be made more secure by employing methods like bit diffusion and encryption [29].

The LSB approach has a weakness in that it is not very secure. Anyone who knows that the LSB approach is being used may readily retrieve the secret message by just glancing at the least important bits of the video. The LSB method is further susceptible to steganalysis assaults, which are methods for identifying the existence of concealed data in a movie. The video quality of the LSB approach may suffer as a result, which is another drawback. The video may become noisy or distorted if there is too much data packed in it. The LSB approach may also increase the likelihood of compression problems in the video[30].

2- Spatial domain video steganography The hidden message is included into the video frames' raw pixel values in this kind of video steganography. LSB substitution, which entails embedding the secret message in the least significant bits of the pixel values, is a popular method of spatial domain video steganography [31].

The study discusses the following limitations of spatial domain video steganography:

Lack of security: Due to how simple it is to identify and extract the concealed data, spatial domain video steganography is not very safe.

Reduced video quality: Using spatial domain video steganography, excessive data embedding might reduce video quality.

Sensitivity to noise and compression: The hidden data in spatial domain video steganography is vulnerable to noise and compression[30].

e- Secret communication across networks can be achieved by exploiting protocols in the network itself, such as TCP/IP, creating covert channels to transmit messages secretly between hosts [15].

1- TCP header steganography The secret message is concealed in the TCP header of the packets using this kind of packet steganography. The sequence number, acknowledgement number, and other details are included in the TCP header. Although TCP header steganography is more challenging to implement than IP header steganography, it is also harder to detect [32].

2- Covert timing channel steganography with this kind of packet steganography, the timing of the packets contains the hidden message. The hidden message could be included, for instance, in the intervals between packets or the intervals between the fields of a packet header. Both detecting and using covert timing channel steganography are exceedingly challenging tasks[33].

f- A DNA-based method for hiding data in a video file was developed, involving converting the video into image frames and using the least significant bit (LSB) substitution approach to embed data in randomly selected frames at random positions. However, the resulting steganography video file had low data hiding capacity and non-zero payload, even though the degradation was minimal [34].

1-Direct Encoding with this technique, the secret message is directly encoded by substituting certain nucleotides in the DNA sequence with other nucleotides. Although this technique is really straightforward to use, it is also rather simple to spot [35].

However, it has a few drawbacks, such as:

expensive cost: The price of synthesizing and sequencing DNA is still rather expensive.

Low data capacity: The length of the DNA sequence determines how much information can be stored there.

Error-prone procedures include the sequencing and synthesis of DNA. This implies that while encoding or decoding, the secret data may get distorted.

Detectability: A number of methods, including statistical analysis and anomaly detection, can be used to identify direct encoding in DNA steganography[36].

4.1 Lightweight IN IOT SYSTEMS

The Internet of Things (IoT) is an emerging technology that enables machine-to-machine communication and allows people to control their household appliances through smart devices [14]. Wireless Sensor Networks (WSNs) are also widely used in various fields to collect physical or environmental data, with decision-making often decentralized [15]. However, the security of IoT devices, which are limited by their energy, properties, and power, has not received much attention [16]. To address these limitations, cloud computing and IoT devices need to be physically or virtually connected to fully utilize cloud computing services [17]. The objective of IoT is to establish a secure and reliable infrastructure for exchanging data among connected devices [16]. Using in smart city and smart home et, limited resource restrictions on resources similar to Power for many devices with limited resources, like wearables, sensors, and Internet of Things (IoT) devices, power consumption is a significant limitation. Since these devices frequently run on batteries, it's critical to reduce their power usage to increase battery life. Bandwidth Another significant limitation for devices with limited resources is bandwidth. These gadgets frequently communicate over constrained-bandwidth, low-power wireless networks. The quantity of data that these devices broadcast and receive must thus be kept to a minimum. Other restrictions Other resource limitations that may encourage the use of lightweight approaches are: Memory Keeping Cost of processing power [37].

5. SECURITY CHALLENGES IN IOT

Interoperability and scalability are crucial in IoT networks, as they must support a broad range of devices with heterogeneous capabilities and accommodate the large number of devices deployed [18]. However, addressing the security of such devices requires simple and low-complexity schemes, capable of handling high payloads for transmitting secured data [18]. While the collective volume of data generated by a large number of devices is significant, current classical steganographic techniques might be impractical, complex, unsalable, and non-resilient to noise to be directly adaptable in IoT environments [16]. Therefore, implementing lightweight steganography in IoT presents challenges such as scalability, noise resilience, and practicality [16].

Table 1. - comparison between previous study

Author	A problem	Solve	Measures	Data hide	Data set	Future work	Advantage	Disadvantage
Ambika et al [4]	Two security concerns need to be taken into account: the possibility of GAN decoding model leakage and the danger of sensitive information loss in the presence of transmission noise..	using Generative Adversarial Networks (GAN)	RS-BPP stands for Rate-Stego-Bits-Per-Pixel. It is a measure of the efficiency of a steganography algorithm. It is calculated by dividing the number of bits used to hide the secret message by the number of pixels in the cover image. WPSNR stands for Weighted Peak Signal-to-Noise Ratio. It is a variation of PSNR that takes into account the human visual system's sensitivity to different frequencies. It is calculated in a similar way to PSNR, but the weights are adjusted to reflect the human visual system's sensitivity. PSNR, SSIM	Text in image	Div2K COCO Pascal VOC	surpasses existing works with an embedding capacity exceeding them by at least 3.5%. However, the efficiency of the discriminator is hindered by the limitations of GAN training, indicating the need to explore alternative machine learning models. The next step is to rigorously test the solution's performance against various steganalysis attacks to evaluate its effectiveness.	In wireless sensor networks, steganography using GANs produces many "natural" carrier images, improving steganography performance and making it more difficult to identify and access secret information. GANs produce realistic images that maintain the appearance of the cover image and reduce skepticism.	Due to transmission failures, using steganography with GANs in wireless sensor networks might cause noise in the retrieved data. Unauthorized access is possible since the GAN decoder lacks a protection mechanism. However, the PDF file presents an improved GAN steganography method that fixes these problems while also enhancing image quality and security.

Metchella et al [38]	Blind universal steganalysis can detect embedding strategies	The method involves carrying out concealed communication through HTTP requests using tagged URLs and IP addresses.	The first scheme has a higher capacity to accommodate secret bits compared to the second scheme when considering a 1024-bit secret, attributed to the increased information in permutations as the symbol space expands. Furthermore, the first scheme generates a significantly lower number of HTTP request sequences compared to the second scheme.	Hide text based on HTTP	X	X	The two steganography methods that are suggested in this publication work well together. Regarding the capacity of secret bit transfers and the quantity of HTTP requests made, the first strategy performs better than the second. The second method removes the time restriction by preventing a succession of HTTP requests from being dependent on one another.	The first steganography system proposed in this paper has the drawback of taking longer to execute because it executes requests to transfer the secret in a particular order. The second technique has the drawback of having less secret bit storage space and more HTTP request sequences.
Author	**A problem**	**Solve**	**Measures**	**Data hide**	**Data set**	**Future work**	**Advantage**	**Disadvantage**
Rostam et al [39]	The utilization of smart cities, which are based on the Internet of Things, application, is rapidly increasing. A key requirement of this system is privacy, which safeguards citizens from disclosure.	LSB DNA	The PSNR measure measures the quality of compressed or stego images by comparing the original image to the compressed or stego image. SSIM measures structural similarity between images, while MSE measures the difference between the original and reconstructed signals. BER bit error rate measures the number of bits incorrectly received in digital communication systems.	Text in image	UCID	X	The benefit of the suggested approach is that it uses a chaotic function to randomly select the picture block and secret data bits in order to cloak the secret data in the image. The system is made more secure by choosing secret data in random blocks and bits.	with the exception of the middle block, data genomes are concealed in block pixels. This may limit the amount of information that can be concealed in an image because only a portion of the pixels in each block are used to conceal secret data.
Khan et al [40]	Ensuring the safety and well-being of individuals has become a major concern, with approximately 421 million adverse hospitalizations annually. The healthcare industry has adopted IoT technology to gather and distribute data wirelessly and continuously to address this issue.	Blynk and RFID technology	The GSR sensors are placed on the fingers to measure skin conductance, while the the heart rate is measured using the Max 30102 sensor, while the LM 35 sensor is used for measuring is utilized to sense body temperature, and the MQ 135 sensor is used to measure the presence of CO2 gas in the air.	Text in image	X	X	RFID and steganography-based IoT-based personal healthcare systems offer a secure platform for storing and analyzing personal health data, enabling remote monitoring and prompt actions. Low-cost sensors are used to improve healthcare services, and steganography protects users' and their families' privacy and data security.	It is crucial to remember that installing such systems necessitates a sizable infrastructure and financial commitment. Additionally, there can be worries about the security and privacy of personal health information, which can be resolved by putting in place suitable security mechanisms like steganography.
	Expertise is required in the hiding process for traditional steganography.	An end-to-end deep learning network, which utilizes	PSNR MSE BPP: metrics are used to compare the performance of different probabilistic	Video in video		the proposed steganography network aims to improve resilience through the	Deep learning-based steganography offers adaptability and generalization, reducing manual effort. The	The drawback of deep learning-based steganography is that it uses a lot of processing power and training data to

Chai et al [8]		GAN and a CU (coding unit) mask.	Turing machines. They can also be used to design new probabilistic Turing machines that are more efficient and accurate.		DIV2K MS COCO	introduction of a differentiable noise layer. Future research will focus on integrating video compression features, error correction encoding techniques, and investigating prevalent attacks to ensure seamless message extraction.	convolutional neural network (CNN) selects features for information hiding and extracts information conveniently. The proposed video steganography system combines VVC coding unit masks and an attention mechanism for improved concealment and larger payload capacity.	develop neural network models. Additionally, the caliber of the cover video frames and the chosen compression technique may have an impact on how well the steganography algorithm performs. Additionally, the stego video frames' imperceptibility could not be flawless, making them susceptible to steganalysis tools' identification.
Author	**A problem**	**Solve**	**Measures**	**Data hide**	**Data set**	**Future work**	**Advantage**	**Disadvantage**
Djebbar et al [41]	The emergence of IoT has emphasized the need for adequate security measures to address the unique challenges posed by IoT and realize its potential in practical implementations.	A noise-resistant and lightweight audio steganography scheme that can securely transmit large amounts of data, which is relevant for communication in IoT networks.	The study uses GSR sensors to record skin response, Max 30102 sensor to measure heart rate and Spo2 level, and MQ 135 air quality sensor to determine the concentration of CO2 gas in the air.	Text in image	database with RFID	X	a steganography method for secure communication in IoT networks, providing benefits like a large payload capacity, excellent signal quality, and noise resistance. By intelligently adjusting phase frequencies, it achieves seamless transitions while preserving the naturalness of the modified signal, making detection difficult. Moreover, it expands the application of IoT steganography by incorporating audio signals alongside images.	The suggested system would impose additional memory and processing requirements on IoT devices, which could be restrictive for gadgets with weak computing capabilities, confined memory storage, or short battery life.
Biswas et al [42]	The objective is to implement a secure and stable network for cyber communication in Smart City applications, with a focus on intelligence and obfuscation.	using "Self-Monitoring Obfuscated IoT	MCC is a more robust measure of accuracy than accuracy, precision, and recall. It is not affected by the imbalance of classes ROC curve is used to evaluate the performance of a binary classifier. A good classifier will have a ROC curve that is close to the top left corner of the graph. PRC stands for Precision-Recall Curve. It is a graphical plot of the precision against the	Control signal in Stego image	X	X	A fresh communication method for smart cities is introduced, providing improved security, resiliency, and self-maintenance. The integration of this architecture enhances security, promotes intelligence, and utilizes tamper-resistant techniques like steganography and digital watermarking.	takes significant time, infrastructure, and resource commitments, while adding digital watermarking and steganography increases complexity and requires specialist knowledge. Although it would be difficult, compatibility with current technologies can be achieved with more study and development.

			recall. The precision is the proportion of true positives that are correctly identified, and the recall is the proportion of true positives that are identified.					

6. DISCUSSION AND FUTURE WORKDS

to maintain an acceptable level of efficiency while achieving a high level of security. The kind of information being concealed: Since some data types are more sensitive than others, they need to be protected with greater security. The amount of information that is being concealed More embedding space is needed for larger volumes of data, which can make it more challenging to conceal the data without being noticed. The capability of the system being utilized to conceal the data to compute Less powered devices will call for less expensive steganography algorithms in terms of computing. The necessary level of security is: While some applications might be able to get by with a lower level of security, others could needa high level of protection. By taking each of these elements into account, it is feasible to select a steganography technique that strikes the right balance between security and effectiveness while also satisfying the unique requirements of the application.

The potential lines of investigation for the next work in thin steganography for IoT. use of machine learning and artificial intelligence to create more reliable and effective steganography algorithms, AI and ML can be applied. For instance, AI may be used to recognize and categorize various IoT device types, while ML can be used to create algorithms that are customized to the unique properties of these devices. Adaptation to additional security technologies: To provide a more comprehensive level of security, lightweight steganography can be used with other security tools like encryption and authentication. a thorough security solution. Steganography, for instance, can be used to conceal encryption keys, aiding in the protection of data from illegal access.

The following succinctly expresses the present steganography approaches' limitations:

Limited applicability: Some steganography methods only work with specific kinds of data, such pictures or movies. This restricts their use in certain real-world scenarios.

Low embedding capacity: The amount of data that may be steganographically concealed in a cover object is frequently constrained. Applications that call for the delivery of copious volumes of confidential data may find this to be an issue.

Detectability: Advanced steganalysis tools can be used to identify some steganography techniques. The safety of the secret data may be jeopardized as a result.

Compute-intensive steganography techniques may not be appropriate for real-time applications since they are computationally complicated.

Future research can solve the following specific outstanding issues in steganography:

developing steganography methods that work with more sorts of data, such text, audio, and video. Enhancing steganography methods' ability to incorporate data while maintaining security and undetectability. creating steganography methods that are more steganalysis-resistant. steganography methods should have their computational complexity reduced to make them more appropriate for real-time applications.

To overcome the drawbacks of existing methods, new steganography techniques can be created using encryption and AI. For instance

Artificial intelligence (AI) may be utilized to create steganography methods that are better suited to the cover item and the hidden data. The security and imperceptibility of the buried data may be enhanced as a result. AI may be employed to create steganography methods that are more resistant to steganalysis. Before being buried in the cover item, the secret data might be encrypted using cryptography. The buried data may get an additional layer of protection as a result.

7. CONCLUSION

In conclusion, reviewing lightweight steganography yields a number of useful results. First of all, it increases knowledge of the technology and possible uses, encouraging more research and development efforts in the area. This opens the door for the development of more effective and safe steganography algorithms. Second, a thorough evaluation provides researchers, developers, and security experts with a better grasp of lightweight steganography and a useful resource for people wishing to learn more about the topic. The identification of research gaps through such a study also aids in the creation of more reliable algorithms and future research. Last but not least, a review's promotion of best practices makes ensuring that lightweight steganography is used responsibly and securely. Together, these results highlight the significance of promoting development and moving the profession toward improved security and effectiveness by conducting reviews in the area of light-weight steganography. We recommend technology see fit to work in the future AI can be used to develop more efficient and effective steganography algorithms. AI can also be used to develop new steganalysis techniques that can detect hidden messages.
The poll reveals the following significant findings:

A possible method for protecting IoT communication and data storage is steganography. IoT devices must use lightweight steganography methods owing to their restricted resource availability. The disadvantages of current steganography methods include their limited application, poor embedding strength, detectability, and computational complexity. Innovative and enhanced lightweight steganography approaches for IoT security may be created using AI and cryptography. There have been gaps found that need more exploration.

The survey finds the following shortcomings in lightweight steganography for IoT security that need for more study: constructing steganography methods that work with a variety of IoT data sources, including sensor data and streaming video. enhancing steganography methods' ability to incorporate data while maintaining security and undetectability.

In the context of IoT networks, creating steganography methods that are more resistant to steganalysis. steganography methods' computational complexity should be decreased to make them more suited for real-time IoT applications. constructing noise- and other impairments-resistant lightweight steganography methods for IoT contexts.

FUNDING

No funding received for this work

ACKNOWLEDGEMENT

The authors would like to thank the anonymous reviewers for their efforts.

CONFLICTS OF INTEREST

The authors declare no conflict of interest

REFERENCES

[1] F. Chen, Q. Xing, B. Sun, X. Yan, and J. Cheng, “An Enhanced Steganography Network for Concealing and Protecting Secret Image Data.,” *Entropy (Basel).*, vol. 24, no. 9, Aug. 2022, doi: 10.3390/e24091203.

[2] M. Smolarczyk, S. Plamowski, J. Pawluk, and K. Szczypiorski, “Anomaly Detection in Cyclic Communication in OT Protocols,” *Energies*, vol. 15, no. 4, 2022, doi: 10.3390/en15041517.

[3] W. Yang *et al.*, “A cancelable iris-and steganography-based user authentication system for the internet of things,” *Sensors (Switzerland)*, vol. 19, no. 13, pp. 1–15, 2019, doi: 10.3390/s19132985.

[4] Ambika, Virupakshappa, and S. Veerashetty, “Secure communication over wireless sensor network using image steganography with generative adversarial networks,” *Meas. Sensors*, vol. 24, no. August, p. 100452, 2022, doi: 10.1016/j.measen.2022.100452.

[5] L. Yu, Y. Lu, X. Yan, and Y. Yu, “MTS-Stega: Linguistic Steganography Based on Multi-Time-Step,” *Entropy*, vol. 24, no. 5, pp. 1–16, 2022, doi: 10.3390/e24050585.

[6] V. Subramaniyan, V. Sivakumar, A. K. Vagheesan, S. Sakthivelan, K. J. J. Kumar, and K. K. Nagarajan, “GANash -- A GAN approach to steganography,” 2021, [Online]. Available: http://arxiv.org/abs/2110.13650

[7] H. T. S. ALRikabi and H. T. Hazim, “Enhanced data security of communication system using combined encryption and steganography,” *iJIM*, vol. 15, no. 16, p. 145, 2021.

[8] K. K. Patel, S. M. Patel, and P. Scholar, "Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges," *Int. J. Eng. Sci. Comput.*, vol. 6, no. 5, 2016.
[9] F. Djebbar, "Securing IoT data using steganography: A practical implementation approach," *Electronics*, vol. 10, no. 21, p. 2707, 2021.
[10] F. Djebbar, "Securing iot data using steganography: A practical implementation approach," *Electron.*, vol. 10, no. 21, 2021, doi: 10.3390/electronics10212707.
[11] H. Chai, Z. Li, F. Li, and Z. Zhang, "An End-to-End Video Steganography Network Based on a Coding Unit Mask," *Electron.*, vol. 11, no. 7, pp. 1–15, 2022, doi: 10.3390/electronics11071142.
[12] H. E. Rostam, H. Motameni, and R. Enayatifar, "The Effect of DNA in Image Steganography on Privacy Preservation in Smart City," *J. Appl. Dyn. Syst. Control*, vol. 5, no. 1, pp. 68–83, 2022.
[13] A. Alarood, N. Ababneh, M. Al-Khasawneh, M. Rawashdeh, and M. Al-Omari, "IoTSteg: ensuring privacy and authenticity in internet of things networks using weighted pixels classification based image steganography," *Cluster Comput.*, vol. 25, no. 3, pp. 1607–1618, 2022.
[14] G. Borse, V. Anand, and K. Patel, "Steganography: exploring an ancient art of hiding information from past to the future," *Int. J. Eng. Innov. Technol.*, vol. 3, no. 4, pp. 192–194, 2008, [Online]. Available: http://www.ijeit.com/Vol 3/Issue 4/IJEIT1412201310_33.pdf
[15] J. Kose, O. B. Chia, and V. Baboolal, "Review and test of steganography techniques," *arXiv*, pp. 1–7, 2020.
[16] M. M. Taher, A. R. B. H. J. Ahmad, R. S. Hameed, and S. S. Mokri, "a Literature Review of Various Steganography Methods," *J. Theor. Appl. Inf. Technol.*, vol. 100, no. 5, pp. 1412–1427, 2022.
[17] M. Hariri, R. Karimi, and M. Nosrati, "An introduction to steganography methods," *World Appl. Program.*, vol. 1, no. 3, pp. 191–195, 2011.
[18] M. Warkentin, M. B. Schmidt, and E. Bekkering, "Steganography and steganalysis," *Intellect. Prop. Prot. Multimed. Inf. Technol.*, no. January, pp. 374–380, 2007, doi: 10.4018/978-1-59904-762-1.ch019.
[19] Y. Patel and P. R Patel, "Survey on Different Methods of Image Steganography," *Int. J. Innov. Res. Comput. Commun. Eng.*, vol. 3, no. 12, pp. 7614–7618, 2014.
[20] N. Hamid, A. Yahya, R. B. Ahmad, and O. M. Al-Qershi, "Image steganography techniques: an overview," *Int. J. Comput. Sci. Secur.*, vol. 6, no. 3, pp. 168–187, 2012.
[21] J. Canny, "A computational approach to edge detection," *IEEE Trans. Pattern Anal. Mach. Intell.*, no. 6, pp. 679–698, 1986.
[22] I. Galić, J. Weickert, M. Welk, A. Bruhn, A. Belyaev, and H.-P. Seidel, "Towards PDE-based image compression," in *International Workshop on Variational, Geometric, and Level Set Methods in Computer Vision*, Springer, 2005, pp. 37–48.
[23] X. Li, B. Gunturk, and L. Zhang, "Image demosaicing: A systematic survey," in *Visual Communications and Image Processing 2008*, SPIE, 2008, pp. 489–503.
[24] G. C. Kessler, "Digital steganography: hiding data within data," *IEEE Internet Comput.*, vol. 5, no. 3, pp. 75–80, 2001.
[25] N. Alifah Roslan, N. Izura Udzir, R. Mahmod, and A. Gutub, "Systematic literature review and analysis for Arabic text steganography method practically," *Egypt. Informatics J.*, vol. 23, no. 4, pp. 177–191, 2022, doi: 10.1016/j.eij.2022.10.003.
[26] J. T. Brassil, S. Low, N. F. Maxemchuk, and L. O'Gorman, "Electronic marking and identification techniques to discourage document copying," *IEEE J. Sel. Areas Commun.*, vol. 13, no. 8, pp. 1495–1504, 1995.
[27] J. Fridrich, P. Lisoněk, and D. Soukal, "On steganographic embedding efficiency," in *Information Hiding: 8th International Workshop, IH 2006, Alexandria, VA, USA, July 10-12, 2006. Revised Selcted Papers 8*, Springer, 2007, pp. 282–296.
[28] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, vol. 90, no. 3, pp. 727–752, 2010.
[29] M. Dalal and M. Juneja, "Video steganography techniques in spatial domain—a survey," in *Proceedings of the International Conference on Computing and Communication Systems: I3CS 2016, NEHU, Shillong, India*, Springer, 2018, pp. 705–711.
[30] S. Chitra and N. Thoti, "Implementation of video steganography using hash function in LSB technique," *Int. J. Eng. Res. Technol.*, vol. 2, no. 11, pp. 3396–3403, 2013.
[31] J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding for all image formats," in *Security and watermarking of multimedia contents IV*, SPIE, 2002, pp. 572–583.
[32] K. Ahsan and D. Kundur, "Practical data hiding in TCP/IP," in *Proc. Workshop on Multimedia Security at ACM Multimedia*, ACM Press New York, 2002, pp. 1–8.
[33] S. H. Sellke, C.-C. Wang, S. Bagchi, and N. Shroff, "TCP/IP timing channels: Theory to implementation," in *IEEE INFOCOM 2009*, IEEE, 2009, pp. 2204–2212.
[34] N. Kar, K. Mandal, and B. Bhattacharya, "Improved chaos-based video steganography using DNA alphabets," *ICT Express*, vol. 4, no. 1, pp. 6–13, 2018, doi: 10.1016/j.icte.2018.01.003.
[35] L. M. Adleman, "Molecular computation of solutions to combinatorial problems," *Science (80-.).*, vol. 266, no.

5187, pp. 1021–1024, 1994.
[36] R. Poisel and S. Tjoa, "Forensics investigations of multimedia data: A review of the state-of-the-art," in *2011 Sixth International Conference on IT Security Incident Management and IT Forensics*, IEEE, 2011, pp. 48–61.
[37] T. Guneysu, *Lightweight cryptography for security and privacy*. Springer, 2016.
[38] L. M. Metcheka, S. Gael, R. Ekodeck, R. Ndoundam, and S. G. Raymond, "Two secure online steganography schemes based on HTTP request sequences," *Hal.Archives-Ouvertes.Fr*, 2022, [Online]. Available: https://hal.archives-ouvertes.fr/hal-03706829/
[39] H. E. Rostam, H. Motameni, and R. Enayatifar, "The Effect of DNA in Image Steganography on Privacy Preservation in Smart City," pp. 68–83.
[40] H. A. Khan, R. Abdulla, S. K. Selvaperumal, and A. Bathich, "IoT based on secure personal healthcare using RFID technology and steganography," *Int. J. Electr. Comput. Eng.*, vol. 11, no. 4, pp. 3300–3309, 2021, doi: 10.11591/ijece.v11i4.pp3300-3309.
[41] F. Djebbar and N. Abu-Ali, "Lightweight noise resilient steganography scheme for internet of things," *2017 IEEE Glob. Commun. Conf. GLOBECOM 2017 - Proc.*, vol. 2018-Janua, no. April 2019, pp. 1–6, 2017, doi: 10.1109/GLOCOM.2017.8255039.
[42] A. Biswas, D. Das, and S. Bhattacharyya, "Self-Monitoring Obfuscated IoT Network," *Secur. Organ. within IoT Smart Cities*, no. December, pp. 119–132, 2020, doi: 10.1201/9781003018636-7.