2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN) | 979-8-3503-3802-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/CICTN57981.2023.10141472

# Securing Data in the Internet of Things (IoT) using Metamorphic Cryptography - A Survey

M. Shreyansh Narayan
*Department of CSE*
*IIIT,*
Agartala, India
shreyanshn47@gmail.com

Dr. Munesh Chandra Trivedi
*Department of CSE*
*NIT,*
Agartala, India
drmunesh.nita@gmail.com

Dr. Anil Dubey
*Department of CSE*
*ABES Eng. College,*
Ghaziabad, India
anildudenish@gmail.com

*Abstract*—**The Internet of Things (IoT) involves connecting a wide range of devices to the internet, allowing them to be controlled and monitored remotely. However, the transmission and storage of data in the IoT environment create security risks, including the possibility of unauthorized access or tampering. It is essential to use strong cryptographic and steganographic techniques to protect the confidentiality and integrity of this data. Cryptography involves using mathematical algorithms and protocols to encrypt and decrypt data to protect it from unauthorized access. Steganography is a way to hide a message within another message or piece of data to keep it from being found. Their combined usage can help to secure IoT devices and ensure the confidentiality and integrity of the data transmitted and stored in them. This paper discusses the existing implementations of metamorphic cryptography to secure data in IoT devices.**

***Index Terms—Internet of Things (IoT), Cryptography, Steganography, Metamorphic Cryptography, Data Security, Data Privacy***

## I. Introduction

The Internet of Things (IoT) is a network of physical devices connected to sensors or software, allowing them to collect and share data. This data can trigger a response or an action, such as turning off the lights or adjusting the temperature of the user's home based on their preferences. The IoT can also be used to monitor the performance and maintenance of various systems and improve efficiency and productivity. The ease of living they provide has led to the demand for IoT devices and services proliferating. This growth is driven by several factors, including the falling cost of sensors and other IoT technologies, the increasing availability of high-speed internet, and the growing need for businesses to automate and streamline operations.

However, there are many risks involved. The most severe issue is data security. In previous research, the aim was to increase the capabilities of IoT devices while little attention was paid to their security properties. IoT devices are often vulnerable to cyber-attacks. Even if the devices themselves may be secured, the security of the data that is collected or transmitted in the system can still be compromised. Another significant issue is data privacy. As more and more devices connect to the internet, there is a risk of personal data being collected and shared without the user's knowledge or consent. To counter these risks, it is essential to put in place robust data security and privacy measures.

The data transferred through IoT devices may also be confidential or personal. When transmitted over the internet, it can be intercepted by adversaries and used to gain unauthorized access to other IoT devices, which calls for data encryption in IoT devices. It can be achieved by using cryptography. Cryptography is used to convert given text into unintelligible text. It helps attain the properties of privacy, authentication, integrity, and non-repudiation.

Another technique, called steganography, can be used to mask the given data. Steganography is used to embed given data into various other mediums of data, such as images, pictures, audio, video, or text.

Metamorphic cryptography can be used to achieve a higher degree of security. Metamorphic cryptography is the culmination of cryptography and steganography. Various techniques can be used to secure the given data, depending on the feasibility of the algorithms used. While many research proposals have been presented to secure IoT devices, only a few have proposed combining cryptography and steganography. In this paper, we discuss the existing methodologies for securing IoT devices, explain the concepts of metamorphic cryptography, and state some future directions.

## II. Related Work

Several studies have been done on securing IoT devices. Few of them have recently made use of cryptography and steganography techniques.

Kalra and Sood [1] proposed an elliptic curve cryptography (ECC) based authentication scheme for IoT and cloud servers. Their protocol was based on smart authentication for embedded devices using HTTP cookies. Later, Kumari et al. [2] proposed a more secure authentication scheme for IoT and cloud servers based on ECC, which improved upon the shortcomings of the previous schemes.

Carracedo et al. [3] provided a comprehensive survey on cryptographic research related to security in IoT. Dhanda et al. [4] proposed a lightweight cryptographic scheme as a solution for resource-constrained devices in IoT. It found advanced encryption standards (AES) and elliptic curve cryptography (ECC) most suitable for the proposed scheme. V. A. Thakor et al. [5] presented a detailed view of the cost, performance, and security properties of the existing lightweight cryptographic algorithms for resource-constrained IoT devices. They concluded that ciphers such as PRESENT and CLEFIA could be used for a good balance between performance and cost, whereas SIMON and SPECK had compact implementation. However, only some algorithms could satisfy all the desired metrics, so there was an incessant need for new research.

Philjon et al. [6] proposed the technique of metamorphic cryptography, which combined the approach of cryptography and steganography. Matrix multiplication was used using a colour key and angular encryption. The original message generated a cipher image, which was then inserted into a cover image. This image was converted into an intermediate text to be encrypted and converted into the final image to be sent.

The chaotic sequence and XORing approaches were used by M. C. Trivedi et al. [7] in their proposed metamorphic cryptography scheme. They used audio files as a cover for the text. The XOR technique overcame the drawback of getting distortions while using the least significant bit (LSB) method.

Singh et al. [8] presented the usage of chaotic sequence and the XOR method in metamorphic cryptography while using video as the cover medium.

Khari et al. [9] suggested using cryptographic and steganographic techniques to secure data while transmitting on the IoT network. They used the elliptic Galois cryptography (EGC) protocol to encrypt the confidential data inserted in an image using XOR steganography after encryption. They used the Adaptive Firefly algorithm to optimise the selection of cover blocks in the image. They achieved a steganography embedding efficiency of approximately 86%. Yadav and Gupta [10] presented an approach to metamorphic cryptography using the concepts of KIMLA and DNA.

Kekre's improved multiple LSB algorithm (KIMLA) [11] and DNA methods were used to reduce distortion and increase confusion during encryption.

Kumar and Singh [12] presented a survey on the enhanced security of images after applying metamorphic cryptography. They analysed and compared the existing methods of steganography and cryptography. The video was the most suitable medium for the cover, compared to image, audio, and text. They proposed using the LSB technique for steganography, RSA, and XOR for cryptography.

Djebbar [13] presented a lightweight audio steganography algorithm to secure IoT data, to allow data protection for the increasing number of voice-enabled devices. The proposed scheme created a stego signal by hiding data in a cover signal and sending it through the IoT network. Orthogonal frequency division multiplexing (OFDM) was used to modulate the stego signal to support various wireless technologies in IoT networks. The noisy environment was then modulated by sending the stego signal across an additive white Gaussian noise (AWGN). The receiver had to demodulate the signal and then extract the embedded data.

Alsamaraee and Ali [14] proposed a scheme for securing IoT applications using cryptography and image steganography. Their scheme involved three contributions – HAC, IPM, and BIGM. Based on the ElGamal elliptic curve cryptography (ECC) and the Cubic Be´zier Curve for text secrecy, hybrid additive cryptography (HAC) was developed. Following that, the encrypted text was inserted into the cover image. Here, the image partitioning method (IPM) was used to partition the image and select random pixels for cover. The proposed bit interchange method (BGM) was used to keep the stego image identical to the original image.

## III. Cryptography

The usage of cryptography can achieve secure communication in the presence of third parties. In order to prevent unauthorized access or alteration, cryptography uses mathematical algorithms and protocols to encrypt and decrypt data.

### A. *Basic model of cryptography*

Each cryptographic algorithm consists of these parameters:

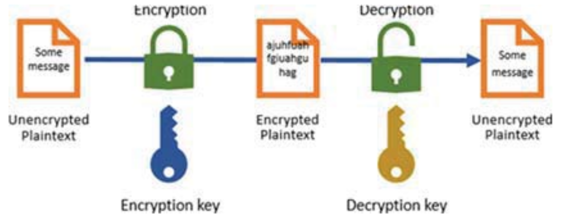

Fig. 1. Basic model of cryptography

- Plaintext: It is the secret message which is to be transmitted.
- Ciphertext: It is the message after encryption using the encryption algorithm with the key.
- Key: It is used to encrypt or decrypt the message using their respective algorithms.
- Encryption Algorithm: It is used to encrypt the secret message along with the key.
- Decryption Algorithm: It is used to decrypt the already encrypted message with the usage of the key.

These five conditions constitute a cryptosystem.

### B. *Types of cryptography*

Broadly, there are two types of cryptography:

#### 1) *Symmetric cryptography:*

It uses the same key for both encryption and decryption. The sender and receiver mutually agree to a symmetric cryptography algorithm and share the generated key. The sender encrypts the message using the key and encryption algorithm and then transmits it. The receiver decrypts the intercepted message using the same key and the decryption algorithm. It is also called secret-key cryptography since the used key must be private or known only to the sender and receiver. AES and Blowfish are two such examples of symmetric cryptography algorithms.

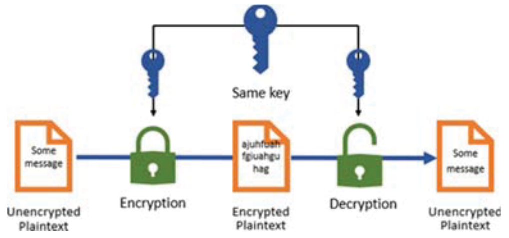

Fig. 2. Symmetric cryptography

#### 2) *Asymmetric cryptography:*

It uses a pair of keys, a public key and a private key, for encryption and decryption. Let us consider a scenario where Alice (sender) wants to send a message to Bob (receiver). Both will have to mutually agree on using some asymmetric cryptography algorithm. Here, Bob has a public key and a private key. The public key is visible to everyone, including Alice, but the private key is known only to Bob. Alice encrypts the message using the encryption algorithm and public key of Bob. Bob receives the transmitted message and then decrypts it using the decryption algorithm and his private key.

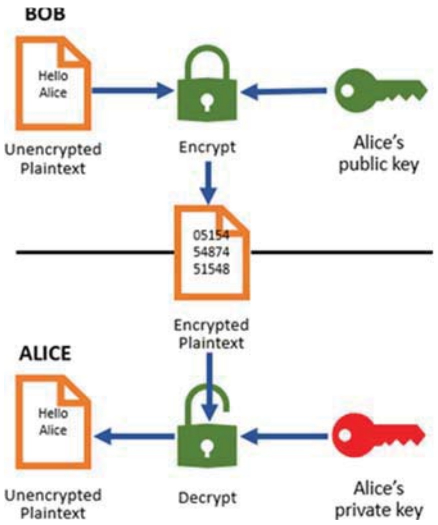

Fig. 3. Asymmetric cryptography

This type of cryptography is also known as public-key cryptography. Examples of public-key cryptography include RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography).

Some other cryptographic techniques, such as hash functions and quantum cryptography, have not been discussed in this paper.

## IV. Steganography

Steganography is the technique of concealing data within some other data. It can be used to hide a message within another message, image, audio, or video. Steganography aims to hide the presence of data from the observer. It, however, only hides the data; steganography does not encrypt the data.

### A. *Basic model of steganography*

Each cryptographic algorithm consists of these parameters:

- Payload: It is the secret message which is to be transmitted.
- Cover file: It is the data or file which is used to hide the message.
- Stego file: It is the final file which contains the message and is transmitted.
- Stego key: It is used to encrypt the cover file to get the stego file or decrypt the stego file to get the cover file along with their respective algorithms.
- Steganographic encoder: It is used to encrypt the cover file with the stego key to obtain the stego file.
- Steganographic decoder: It is used to decrypt the stego file with the stego key to obtain the cover file.

### B. *Types of steganography*

The broad classification of steganography is as follows:

- Text steganography: It involves hiding data within text words or the whitespace of a text document.
- Image steganography: It involves hiding data within the pixels of an image.
- Audio steganography: It involves hiding data within the frequencies of a sound file.
- Video steganography: It involves hiding data within the frames of a video file.
- Network steganography: It involves hiding data within the data packets transmitted over a network.

Steganography is not limited to these types; there are other ways to hide data within different media types.

Kaur et al. [15] surveyed the different steganography techniques. After comparing them, they commented on the different techniques based on factors such as robustness, imperceptibility, bit error rate, mean square error, and peak signal-to-noise ratio.

### C. *Parameters for evaluation*

Steganography is evaluated based on the following parameters:

- Embedding efficiency: It measures the number of bits of data embedded in the cover block.

$$E_{\eta} = \frac{k+1}{k}n \tag{1}$$

Here, the cover block bit is 'k', and there are 'n' total bits of data.

- Carrier capacity: It refers to the maximum number of bits that can be hidden inside the cover block. It is directly proportional to efficiency.
- Mean Square Error (MSE): It signifies the amount of distortion in the file. It shows the similarities between the cover and the stego file.

$$MSE = \frac{1}{N}\sum_{i=X,Y}^{N}(X-Y)^2 \tag{2}$$

Here, X is the cover file, Y is the stego file, and N is the total number of pixels within the file.

- Peak Signal to Noise Ratio (PSNR): It signifies the imperceptibility of the file.

$$PSNR = 10\frac{1}{N}\log_{10}\frac{256^2}{MSE} \tag{3}$$

- Time complexity: It measures the duration between the encryption and decryption process. The lesser the time complexity, more is the efficiency of the system.

## V. Metamorphic Cryptography

Metamorphic cryptography involves changing the form of the data in some way to obscure its meaning. This obscurity can be achieved through various techniques, such as altering the order of the data, adding or removing characters, or changing the structure of the data. Metamorphic cryptography aims to make it more difficult for the attacker to understand or manipulate the data, even if they can gain access to it. This paper considers 'metamorphic cryptography' to combine cryptography and steganography.

Cryptography relies on the fact that the message can be seen but not understood. Steganography relies on the fact that the presence of the message cannot be detected, but if obtained, it can be interpreted. Using both leads to more obfuscation, leading to increased security.

Cryptographic algorithms such as AES, RSA or ECC can be used to encrypt data before it can be concealed using steganography techniques. LSB, OMME, PVD, and FMO are some of the methods used for steganography after data encryption.

In this paper, we have surveyed existing methods of metamorphic cryptography and their implementation for security in IoT. A detailed description is presented in Table I, and Table II.

## VI. Conlcusion

This paper aims to provide a brief survey on the usage of metamorphic security to secure data in IoT devices before transmission over the network and the related techniques. With the rapid increase in smart IoT devices, there will be an incessant need for advances in security measures. Most of the research has mainly focused on developing lightweight cryptographic algorithms to solve this problem.

In recent times, the usage of both cryptography and steganography for securing IoT devices and the data within them has been popularized. It is because of their ability to increase robustness and confusion and achieve confidentiality and anonymity. Further improvements can be made in the available schemes to attain higher security degrees while also maintaining feasibility.

## References

[1] S. Kalra and S. K. Sood, "Secure authentication scheme for IoT and cloud servers," Pervasive and Mobile Computing, vol. 24, p. 210, Dec.2015.

[2] S. Kumari, M. Karuppiah, N. Kumar, X. Li, F. Wu, and N. Kumar, "A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers," The Journal of Supercomputing, vol. 74, no. 12, p. 6428, Dec. 2018.

[3] J. M. Carracedo et al., "Cryptography for Security in IoT," The Internet of Things, Oct. 2018.

[4] S. S. Dhanda, B. Singh, and P. Jindal, "Lightweight Cryptography: A Solution to Secure IoT," Wireless Personal Communications, vol. 112, no. 3, p. 1947, Jan. 2020.

[5] V. A. Thakor, M. A. Razzaque, and M. R. A. Khandaker, "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities," IEEE Access, vol. 9, p. 28177, Jan. 2021.

[6] J. T. L. Philjon and N. V. Rao, "Metamorphic cryptography &amp;#x2014; A paradox between cryptography and steganography using dynamic encryption," International Conference on Recent Trends in Information Technology, Jun. 2011.

[7] M. C. Trivedi, S. Mishra, and V. K. Yadav, "Metamorphic cryptography using strength of chaotic sequence and XORing method," Journal of Intelligent and Fuzzy Systems, vol. 32, no. 5, p. 3365, Jan. 2017.

[8] N. Singh, M. C. Trivedi, V. K. Yadav, and V. K. Singh, "Metamorphic cryptography considering concept of XOR and chaotic sequence: Using video as medium," International Conference on Information Technology and Electrical Engineering, Oct. 2017.

[9] M. Khari, A. K. Garg, A. H. Gandomi, R. Gupta, R. Patan, and B. Balusamy, "Securing Data in Internet of Things (IoT) Using Cryptography and Steganography Techniques," IEEE transactions on systems, man, and cybernetics, vol. 50, no. 1, p. 73, Jan. 2020.

[10] V. Yadav and I. K. Gupta, "A hybrid approach to metamorphic cryptography using KIMLA and DNA concept," International journal of computational systems engineering, vol. 5, no. 4, p. 218, Jan. 2019.

[11] H. B. Kekre, A. Athawale, and U. Athawale, "Increased cover capacity using advanced multiple LSB algorithms," International Conference & Workshop on Emerging Trends in Technology, Feb. 2011.

[12] R. Kumar and N. Singh, "A Survey Based on Enhanced the Security of Image Using the Combined Techniques of Steganography and Cryptography," Social Science Research Network, Mar. 2020.

[13] F. Djebbar, "Securing IoT Data Using Steganography: A Practical Implementation Approach," Electronics, vol. 10, no. 21, p. 2707, Nov. 2021.

[14] S. Alsamaraee, A. S. Ali, "A crypto-steganography scheme for IoT applications based on bit interchange and crypto-system," Bulletin of Electrical Engineering and Informatics, vol. 11, no. 6, p. 3539, Dec. 2022.

[15] H. Kaur, J. Rani, "A Survey on different techniques of steganography," Jan. 2016.

TABLE I. Review Of Metamorphic Cryptographic Techniques

| Reference | Method(s) | Description | Advantage | Future Scope | Results |
|---|---|---|---|---|---|
| Philjon et al. [6] | Matrix multiplication + Angular encryption | A colour key is taken, represented as a matrix. A point P on the image is considered a reference point. For each character in the message, some operations are performed on a chosen pixel with respect to P and the value obtained is XORed with the ASCII value of the character. It is then used to obtain RGB values of the new pixel in the cipher image.<br>A cover image is used to create a cipher image. XOR operations are performed on the RGB values of the cover and cipher images. The resulting value is then converted to an intermediate text.<br>This intermediate text is again encrypted using the previously used encryption algorithm to generate the final cipher image. | It uses cryptography and steganography to achieve a higher degree of security.<br>In this algorithm, encryption takes place twice since the message is encrypted to get a cipher image, which is converted to an intermediate text with a cover image to be encrypted again. | The final image is not identical to the cipher image. After converting to intermediate text, the cipher image is again encrypted to get the final image. So, the final image does not satisfy the properties of steganography of concealing the changes. | The final image had some extra pixels and was distinguishable from the original.<br>They suggested using Portable Network Graphics (PNG) format because they consume less space, even if the image size increases. |

| | | | | | |
|---|---|---|---|---|---|
| M. C. Trivedi et al. [7] | Chaotic sequence + LSB + XOR | The proposed algorithm encrypts text using index-based chaotic sequences and then uses LSB and XOR methods to conceal it in an audio file.<br>The plaintext is converted to ASCII, which is then converted to its binary format. It is encrypted using an index-based chaotic sequence. It is then converted to a matrix vector and converted to binary. On the other hand, a cover audio file is also converted to its binary format.<br>The LSB of the audio file is replaced with the XOR of the resultant text vector and LSB of the audio file. | Chaotic sequence increases randomness such that altering a single bit shifts the arrangement to a large extent.<br>XOR is used with LSB to reduce distortion in the cover file, leading to identical plots of the cover and stego audio files. | Although similar, the method used does not reduce the time taken to hide text files in audio files drastically when compared to the simple LSB method.<br>The time taken increases mainly with the increase in the size of the audio cover file. | The time taken to hide a text file of size 4 KB in audio files of varying sizes (ranging from 20 KB to 144 KB) is 2.069 seconds. |
| Singh et al. [8] | Chaotic sequence + XOR | The algorithm uses video as a cover medium for steganography.<br>The plaintext is encrypted using chaotic sequence and then converted to binary. A video frame is selected using chaotic sequence. The cipher text is embedded into it using the XOR method to obtain the stego video. | The histogram analysis shows very minute differences in the stego frame, which are not observable to the naked eye. The time taken for encryption and decryption varies very little compared with the increase in the number of bits. | The time elapsed in payload processing varies with plaintext size, albeit minimal.<br>The distortion in the cover frame and the changes in the histogram can be minimized. | The average encryption time for the varying number of bits (from 40 to 1200) is 11.707 seconds.<br>The average PSNR and MSE for four different videos are 23.268825 and 447.7672, respectively. |
| Khari et al. [9] | EGC + XOR | The plaintext is encrypted using EGC. It is encrypted using chaotic neural network. Matrix XOR steganography is performed on the ciphertext before it is stored on the cloud. Here, H.264 video file is used as a cover. The cover blocks in the cover frame are chosen using the adaptive Firefly optimization method. The stego file is then sent through the IoT network. | The loss in video compression ratio is reduced with the supreme progressive film coding model. The embedded plaintext requires authorization because of the presence of the ECC secret key. | Other methods for steganography, such as KIMLA, can be used, which may increase confusion. | The efficiency of steganography is 86%. The PSNR performance is 32.42% better than LSB. The carrier capacity is 0.33% better than LSB. |
| Yadav and Gupta [10] | DNA + KIMLA | Plaintext is converted to ASCII, which is further converted to binary. Then DNA encryption procedure is used to encrypt them. Again, the encrypted text is converted to ASCII, followed by binary.<br>A cover image is selected whose pixel values are converted from decimal to binary. The KIMLA method hides the final binary data of plaintext in the pixels of the cover image. | The usage of DNA and KIMLA creates high confusion and more robustness. The histogram analysis shows less difference between the original and stego images. | There is a significant increase in time when compared to other methods, such as LSB, due to DNA encoding. | The average time taken to encrypt data is 63.81% more in the proposed approach than in LSB. |
| Kumar and Singh [12] | Review on metamorphic cryptography (LSB, DES, AES, RSA) | They observed that the number of redundant bits also increases with an increase in the file size, thereby making it easier to embed data. In the LSB technique, data is converted to binary which is then replaced with the LSB of the cover file. This method has a high payload capacity. They discussed DES, AES, and RSA techniques for encryption. | Metamorphic cryptography ensures data confidentiality and hides its presence in the first place. Using the XOR method reduces distortion in the cover file, thereby making it look more identical to the original file. | They focused on embedding text in other mediums, such as audio, video, and image. It can be extended to embed video in a cover video while aiming for less distortion.<br>Also, techniques for random frame selection are required to increase confusion. | Video file is found to be the best medium for cover.<br>Using LSB for steganography and RSA with XOR for cryptography was suggested as one of the techniques. |

TABLE II. REVIEW OF METHODS FOR SECURING DATA IN IOT

| Reference | Method(s) | Description | Advantage | Future Scope | Results |
|---|---|---|---|---|---|
| Kalra and Sood [1] | ECC | The embedded device first registers with the cloud server, which stores a cookie on the device. Then the device sends a login request to the server during connection. Then the server and device mutually authenticate each other using ECC parameters and agree on a shared session key. All the subsequent messages communicated between them are XORed with this session key. | The proposed protocol is resistant to replay attacks, MITM (Man-In-The-Middle) attacks, cookie theft attacks, eavesdropping, and brute force attacks. | It is susceptible to insider attacks and offline password-guessing attacks. It does not meet the requirements for mutual authentication, session key agreement, or device anonymity.<br>It also does not achieve forward secrecy. | The computation cost of the protocol is 4x(time for one hashing operation) + 4x(time for elliptic curve multiplication).<br>The communication cost is 1280 bits. |

| | | | | | |
|---|---|---|---|---|---|
| Kumari et al. [2] | ECC | The tamper-proof device registers with the cloud server after sending a computed result through a secure channel. Then the server computes a cookie for the device along with other security parameters. The device computes the ECC points for each login and sends the login request. Then the cloud server computes the cookie and other information and verifies it with the received one. Upon matching, a mutually agreed session key is used for further communication. | It is resistant to replay attacks, MITM (Man-In-The-Middle) attacks, insider attacks, stolen verifier attacks, impersonation attacks, and brute force attacks, among others. | The security of the proposed scheme is greatly based on the usage of tamper-resistant embedded devices, the absence of which may cause security implications. | The computational cost of the proposed scheme is approx. 17.824 x 103 µs. The storage cost for three messages of 1760 bits is 480 bits. |
| Carracedo et al. [3] | Survey on cryptography for security | They described the various threats to the security of IoT – MITM (Man-In-The-Middle) attack, DoS (Denial-of-Service) attack, node replication, camouflage, malicious code, eavesdropping and injection of fraudulent packets. Coding theory can be used to reduce errors during the transmission of data over the IoT network.Various cryptosystems can be used to prevent some of the attacks. | Lightweight cryptographic algorithms such as PRESENT can be used in resource-constrained devices due to their high chip efficiency and low power consumption.<br>Furthermore, broadcast encryption allows only the intended recipients to receive the ciphertext. | Algorithms like RSA are based on the factorization problem, so advanced research in it might pose a threat to them.<br>The eventual arrival of quantum computers will put most cryptographic schemes at risk. | The practical implications of resource-constrained IoT devices call for lightweight cryptographic algorithms. Thus, many symmetric cryptographic algorithms have been proposed for security in IoT. |
| Djebbar [13] | Audio steganography (OFDM + AWGN) | This scheme hides the payload in a cover signal before transmission over the IoT network.<br>The cover signal is divided into several frames. FFT is applied to each frame, and the magnitude spectrum is separated. The payload is embedded in the phase spectrum. The new phase is multiplied by its magnitude to get the stego spectrum. Then inverse FFT (iFFT) is applied to it to get the stego signal.<br>The stego signal is modulated using orthogonal frequency division multiplexing (OFDM). An additive white Gaussian noise (AWGN) is sent over it before transmission. | The proposed algorithm is suitable for IoT systems because it is lightweight, noise resilient, and has a large payload-carrying capacity.<br>Low frequencies are used for data embedding because of their better SNR. | The proposed scheme uses audio as the cover medium. In future work, it can be extended to other mediums of data, such as video. | For a payload up to 24 Kbps, the SegSNR value ranges from 42 to 48 dB, and the PESQ ranges from 4.38 to 4.41.<br>The usage of 64–QAM achieves better throughput than other modulations, i.e., 1Mbps at an SNR of 10 dB.<br>AER in speech, music and video is 31.96%, 35% and 36.2%, respectively. |
| Alsamaraee and Ali [14] | Cryptography – HAC (ECC + CBC)<br>Steganography – IPM + BIGM | A session key is generated, which is used to encrypt the plaintext with the help of ECC. The session key is encrypted using the Bezier curve, and the result is sent to the receiver along with the cipher text. Huffman coding compresses the data before embedding it in the cover image.<br>The image partitioning method (IPM) is used to identify the cover pixels through random pixel distribution based on the Hénon Map function.<br>The bit interchange method (BIGM) ensures that the stego image remains the same as the original and reduces distortion. | The proposed scheme uses session keys and a framework agreement between the transmitter and the receiver.<br>It preserves the integrity and prevents replaying.<br>Using three random control functions during image partitioning increases the complexity by roughly equal to 2100. | The proposed scheme may be extended in future works to hide data in other mediums, such as audio or video. | The average PSNR for the proposed algorithm is 70.422, which is 18.34% more than that of LSB.<br>It has an average MSE of 0.426, which is 89.62% less than that of LSB. |