International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

Review on Lightweight Cryptography Techniques and Steganography Techniques for IOT Environment

Sangeetha Supriya Kola
Research Scholar,
Christ University, Kengeri, India.
e-mail: sangeetha.supriya@res.christuniversity.in

Dr. Jeno Lovesum S. P
Associate Professor,
Christ University, Kengeri, India.
e-mail: jeno.lovesum@christuniversity.in

Abstract— In the modern world, technology has connected to our day-to-day life in different forms. The Internet of Things (IoT) has become an innovative criterion for mass implementations and a part of daily life. However, this rapid growth leads the huge traffic and security problems. There are several challenges arise while deploying IoT. The most common challenges are privacy and security during data transmission. To address these issues, various lightweight cryptography and steganography techniques were introduced. These techniques are helpful in securing the data over the IoT. The hybrid of cryptography and steganography mechanisms provides enhanced security to confidential messages. Any messages can be secured by cryptography or by embedding the messages into any media files, including text, audio, image, and video, using steganography. Hence, this article has provided a detailed review of efficient, lightweight security solutions based on cryptography and steganography and their function over IoT applications. The objective of the paper is to study and analyze various Light weight cryptography techniques and Steganography techniques for IoT. A few works of literature were reviewed in addition to their merits and limitations. Furthermore, the common problems in the reviewed techniques are explained in the discussion section with their parametric comparison. Finally, the future scope to improve IoT security solutions based on lightweight cryptography and steganography is mentioned in the conclusion part.

Keywords-Internet of Things; Block cipher; Steganography; Lightweight security solutions

I. INTRODUCTION

The IoT has grown as the greatest evolving technology for the modern world and achieved research related to artificial intelligence [45]. It is generally like the system connecting the machines, computers, mechanical or digital devices, objects, or the users allocated with a specific ID [46]. It establishes the relaying between the human and the machine. In simple, the concept of the IoT is operating the surrounding appliances with remote control. It gives great influence and the sense of humans' attitudes in daily life [47].

In an IoT environment, the system or users are connected to share information and achieve the assigned task [48, 49]. The core aim of the IoT is to attain a reliable and secure exchange of information. Although it has made life easier, the safeguard of exchanging information has attracted major attention [50]. Crisis detection at the network is important for the safe sharing of information. For the user's privacy, such material is important [51]. A third person can easily access the users' information without the safety controls [54]. The cyber security risk also became the greater barrier to the development of the industrial IoT [62].

To address these issues, the IoT enables authentication and identification approaches for preserved communication and sharing [61]. The cryptography approach can easily authenticate the information. Cryptography utilizes a set of procedures called ciphers or cryptography algorithms for decryption and encryption to enhance data sharing and communication security. Cipher suits are used for encryption, authentication, and key sharing. The lighter version of cryptography is named lightweight cryptography (LWC), which integrates algorithms and block ciphers [55]. It is simple and more efficient than typical cryptography. A block cipher is currently the most extensively used light cryptographic primitive. It offers extremely tight security to IoT equipment and can be used for encryption, authentication, hashing, and the production of random bits. Moreover, the block cipher design is simpler to comprehend than the stream cipher. Designing a lightweight block cipher is difficult because there are trade-offs between efficiency, cost, and security [56].

Another approach that shares the additional safety to the sharing of information is called steganography. In cryptography, the data are encrypted and sent. In steganography, the encrypted messages are hidden, which are non-susceptible to hackers. In digital steganography, typical encryption is used. One key rule in steganography is that the transformed data is injected into the jpeg image [57]. The steganography system needs three apparatuses: secret data, stego, and cover object. The outcome of the embedded cover image is called a stego-image.

Similarly, for the different cases like text, audio and video embedding, outcomes are stego-text, stego-audio, and stego-video. If the three processing parameters, security, image quality, and capacity, are satisfied, steganography is said to be

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

the good one [58]. Usually, the steganography methods hide an equal proportion of secretive data in every pixel of the cover image. Therefore, it causes the same embedding intrusion at the cover object. But, each pixel resulted in difficult geometrical dependencies among the images and degraded the image grade [59]. To address these challenges, various efficient steganography processes are introduced. Combining these two methods can secure the data from hackers or attackers during the transmission over the open channeled network and enhance the secured data [60].

II. LIGHTWEIGHT CRYPTOGRAPHY TECHNIQUES

Various cryptographic solutions are researched for sensitive information protection, but some techniques exhibit more challenges and limitations for the IoT environment. Lightweight cryptography brings and advantages of efficient area and solving power issues. Both commercialized and industrial IoT experience harmful attacks that affect privacy. For the prevention of such disasters, various cryptographic mechanisms are researched.

Moshin et al. [5] introduced a lightweight multi-hop IoT structure protection protocol. Here, the protocol uses the link fingerprint generated by the indicators of the nodes in IoT. The safeguard measures of the data transmission are increased by the correlation coefficient, computed by matching generated fingerprints. Less energy is consumed. The addition of adversarial nodes gives a low correlation coefficient. To meet the resource constraints of the authentication protocol, Tai-Hoon et al. [6] suggested an authentication scheme named extended Lightweight Signcryption Protocol with Keccak (LiSP-XK). It achieved better efficiency and low complexity for authentication. Yanan et al. [8] created a single directional proxy re-signature framework to safeguard the mobile payment agreement. This technique has adopted the idea of a batch verification scheme to control the scalability issue of the millions of customers in the pay platform of IoT. It achieved very efficient mobile transactions. Yaxing et al. [9] suggested a safe and enhanced remote monitoring system called SRM based on the technology of trustworthy computing to enhance the remote monitoring assistance in the IoT environment.

Additionally, a heartbeat protocol is proposed to handle the complex key repeal problem. To analyze the security issues of the IoT, Yue et al. [11] designed a new power distribution security framework based on a Trusted Cryptographic Module (TCM). It provides a safe network and offers a stable execution in the power network. It ensures security by the measurement of integrity and the monitoring status. To overcome the delay issues in the IoT security framework, Abbas et al. [12] explained drone-based applications. It applies a zone-based infrastructure named Drone-based Delegated Proof of Stake (DDPOS) in the drone environment. This infrastructure needed re-authentication. The addition of blockchain technology provides the key, hash, and transaction for specific drones. Here, the drones enabled P2P communication and migration of different regions to secure the recorded data of every region. The limitation is that the geographical range affects the system's performance and raises a side effect from the speed parameter of the drone. Also, the drone environment is used by Basurab et al. [13] for battlefield surveillance.

Craig and Andrea [14] put forward a multi-layered network for data transport security of the cellular network. Various security functional elements build this architecture, providing a preserved end-to-end channel communication. The radio carriers ensure security. IP addressing will not help to prevent the public from accessing the available information through the public. Xing et al. [15] devised a lightweight encryption procedure centered on Layered Cellular Automata (LCA) to protect real-time surveillance videos. It is eight layered infrastructures extracted the RoIs block for the initialization. The encryption takes place synchronously and independently. It can avoid brute force and statistical attacks, has easy implementation, and is efficient. The half-shift transformation indirectly affects the cells.

To focus the trust, security, and the over sea communication in Industrial IoT (IIoT), a lightweight blockchain-based platform for IIoT (BPIIoT) was introduced by Bai et al. [19]. It comprised both on and off-chain platforms. Here, network delay and load are reduced. The main limitation of the blocking technology is once it is recorded, the information gets deleted. Mitha et al. [20] invented the RoadRunneR-128 (RRR-128), the LW block cipher operated on 8-bit platforms. It ensures the prevention of various cryptographic attacks. It utilizes the lesser area and provides satisfied throughput. Sooyeon et al. [22] developed a key agreement besides a two-factor authenticating structure for the 5G integrated networks. It prevents the number of known attacks and provides more security attributes. In the future, it will be tested on the devices of the 5G integrated WSN for IoT.

TABLE I. COMPARISON OF ASYMMETRIC AND SYMMETRIC KEY CRYPTOGRAPHY

characteristics	**Cryptography methods**	
	Symmetric key cryptography	***Asymmetric key cryptography***
key	same key for both decryption and encryption	Different key
Encryption/decryption speed	Very fast	Slower
Number of keys	Equal to the square of the number of participants	Same as participant counts
Usage	Used for decryption and encryption except for digital signatures.	It can be used for digital signatures and also
Hardware complexity	Low complexity due to the simple operations	More complexity due to the high computational algorithms
Examples	Block Ciphers: TEA, SIMON, PRESENT, 3DES, DES, Blowfish, AES, RECTANGLE, Twofish, KATAN, Humming Bird, Curupira Stream cipher: Grain 128 Chacha, WG-8, Espresso, Trivium,	DSA, ECC, RSA

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

Guangyu [25] presented an IoT-controlled electrocardiogram (ECG) managing framework with protected data transmission. It proposed two frameworks: lightweight, secure IoT (LS-IoT) and Lightweight Access Control (LAC). Here, the battery energy consumption is reduced. Tallat et al. [27] introduced an optimized lightweight encrypting scheme based on genetics for medical data security in IoT. It maintains the confidentiality of the data by lightweight telemetry transport protocol. However, sometimes the debugging is difficult. Safiullah et al. [35] introduced a new scheme, Gimili, a versatile method for hashing and a lightweight authenticated encrypting system for authentication protocols. It mitigates the different potential attacks on RFID applications. Mohamed and Lei [36] evaluated the performance of blockchain technology in the IoT environment. Yi et al. [52] established homomorphic encryption to secure the lottery computation protocol. The two kinds of cryptography mechanisms are explained as follows, and their comparison is given in Table 1.

A. Asymmetric key cryptography

It is also named public key cryptography, and the architecture is shown in Figure 1. This schematic required pairs of private and public keys. The keys used for the decrypting and encrypting functions are different for asymmetric. Its process is slower than the symmetric key. The encryption key is longer than the key used in symmetric.

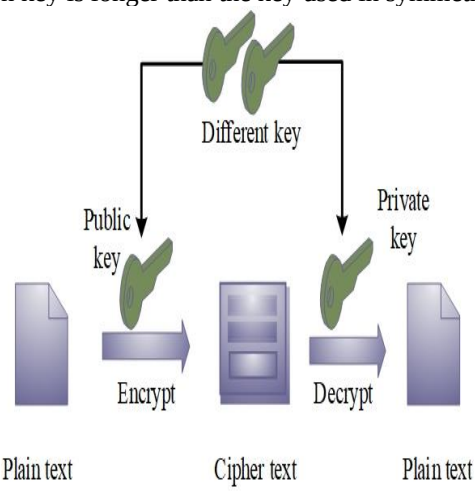

Figure 1. Asymmetric key cryptography

Krishna et al. [24] explained a hybrid encrypting approach using the RSA algorithm. It enhances the privacy preservation of numerous real-world technologies such as social networks, bank accounts, etc., and the security is improved by two-factor authentication. Additionally, Sai et al. [31] created the RSA-based LWC system to communicate efficiently, consistently, and comprehensively about medicines and vaccines for diminishing birth defects and fetus death. However, it sometimes fails or needs a third party to verify the public key dependency. Jyoti et al. [1] introduce the Elliptic variety Galois Cryptography (EGC) protocol to encrypt confidential data from various healthcare resources. Traun and Vineet [37] have made both software and hardware implementations of DH, Elliptic Curve Diffie Hellman (EC-DH), and RSA algorithm. Among all, EC-DH has attained greater performance in all the attributes like low power, lightweight and robustness in the IoT platform. To prevent DoS attacks, Dahee et al. [53] use the public key cryptography technique.

B. Symmetric key cryptography

It is also called secret or shared key cryptography, and the architecture is shown in Figure 2. In the IoT environment, most symmetric key cryptography is due to its operating speed. Here, the key used for both the encryption and decryption is the same. The most important primitives are hashing blocks and stream ciphers. A stream cipher is in which the key size is the same as the data. At the same time, the block ciphers use several phases of transformation determined by a symmetric key and have a set number of bits. It converts a more significant number of bits than the stream cipher and the complexity is simple. So, it is suitable for IoT architectures. A few symmetric key cryptography works of literature are reviewed as follows.

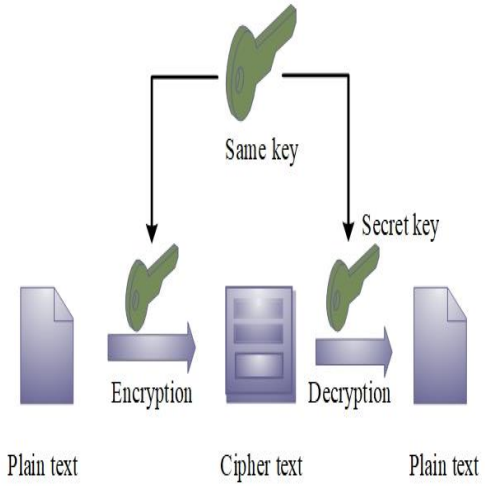

Figure 2. Symmetric key cryptography

Prakasam et al. [2] designed an efficient cryptography technique for numerous IoT devices. It utilized the 8-bit manipulation principle. It exhibits weight in small quantities and maximum security features. Bassam et al. [3] suggested a unique ultra-lightweight cryptographic algorithm named SLIM for the Radio Frequency Identification (RFID) application. It is the Feistal structure-based 32-bit block cipher. It is a symmetric block cipher utilizing an identical key for decryption and encryption. It gives excellent performance for both hardware and software. It cannot be operated on 4-bit components. Lein et al. [4] introduced a new data encrypting scheme named path-oriented data encryption for wireless sensor networks (WSNs). This encryption technique protects the data by grouping pairwise shared keys. It allows multiple network nodes to forward data and takes minimum time for encryption. Sometimes, invalid pairwise keys in some inner nodes are used to prevent the recipient from retrieving the data. Also, for the prevention of the sinkhole attack in the WSN, Huda et al. [64] developed a threshold sensitivity based protocol. At the base station verification phase, the cluster head id is sent in the encrypted format. It is efficient for various injection and modification attacks. Hongbing [7] designed the lightweight encryption algorithm called PRESENT for the vehicle information transmitting protocol to prevent data hacking and tampering. It ensures data safety and

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

transmission. For the dynamic key update, the algorithm utilizes the different communications among the server and device, which is roughly a one-time pad and enhances the security. Certain thread is caused if the business requirements are not properly handled. The properties of cryptographic block ciphers are tabulated in Table 2.

TABLE II. BLOCK CIPHERS PROPERTIES

Block cipher	Block size(bit)	Key size(bit)	Number of rounds	Features
Blowfish	64	32-448	16	Flexible, enhanced security
AES	128	128, 192, 256	10, 12, 14	Flexible, enhanced security
3DES	64	112, 118	48	Flexible, enhanced security
DES	64	64	16	Flexible but not highly secure
Twofish	128	128, 192, 256	16	Not able to break remotely
Humming Bird	16	256	4	Suitable for WSN or RFID tags, greater speed, low power consumption
LED	64, 128	64, 128	-	RFID tags transmissions, simple hardware implementation
SIMON	32~128	64~256	32~2	Flexible, enhanced security, easy implementation
Curupira	96	96 , 144, 192	96, 144, 192	Minimum space for S-boxes
KATAN	32, 48, 64	80	256	Lesser throughput, higher energy consumption, efficient n hardware than software
PRESENT	128	80, 128	32	Encrypts small amounts of data
TWINE	64	80,128	36	Enough speed, Ultra-lightweight
RECTANGLE	64	80	25	High throughput, suitable for hardware
TEA	64	128	32	An increased number of iterations provides greater security

Musa et al. [16] designed a security advisor for the IoT hardware platforms. It is composed of three attributes: security requirements, guidelines, and the attributes of LWCA. It serves as a road map for secure IoT development. The absence of sufficient LWCAs is the fundamental constraint of this effort. RECTANGLE block ciphers provide great efficient encryption and speed performance. So, Abdul et al. [21] extended the RECTANGLE with a 3D cipher and named it 3D RECTANGLE. It shows the highest performance than its actual version. It attains a better throughput. However, its cost is high. Palwasa and Damai [23] developed a parallel pipelined hybrid KATAN cipher. Rizwan [28] developed a Symmetric Cipher relay on EXlusive OR and Permutation for visual media encryption. Gauvrav et al. [10] modelled a new hybrid system combining the cryptographic mechanisms group operations (GRP) and S-box of PRESENT. The utilization of the PRESENT S-box diminishes the gate complexity. Hongzhen et al. [63] created an identity based cryptography for the security of the wireless healthcare environment. It used the aggregate signature as an encrypting key without using parings and encrypted by an elliptic curve mechanism.

For selecting the best lightweight block ciphers in the group of 10 ciphers such as HIGHT, Klein, Scalable Encryption Algorithm (SEA), Lightweight Encryption Algorithm (LEA), Advanced Encryption Standard (AES-128), mCrypton, Camellia, NOEKEON, and Tiny Encryption Algorithm (TEA)and PRESENT-80 Ning et al. [29] analyzed the hybrid Multiple criteria decision-making (MCDM). However, the result of the cipher may vary according to the technology chosen for processing the ciphers. So, it does not give a correct prediction.

III. ADVANCED STANDARD ENCRYPTION (AES)

AES was an iterative cipher that Joan and Vincent first introduced. This algorithm works on variable key length and block size. Ex. 32-bit multiples.

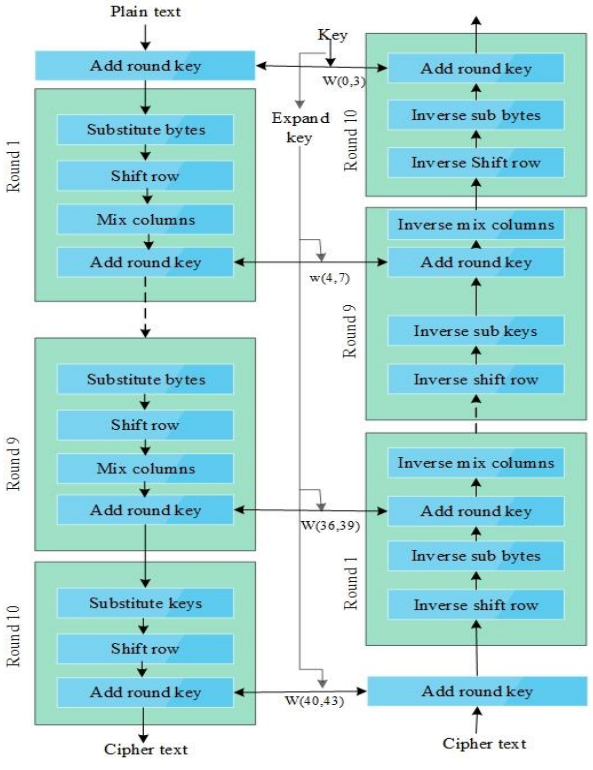

Figure 3. 10 rounds of AES – 128 (Block Diagram)

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

One of the key attributes of the AES algorithm is it is not based on any feistal structure. Instead, it is based on an S-P network in which the entire input block is arranged as 4×4 bytes called state and processed in the number of rounds. For example, ten rounds are required for a 128-bit key, as described in Figure 3.

According to the dimension of the key, the number of rounds is assigned. Some of the AES-based encryption techniques for IoT are discussed below. Yiqun et al. [17] modelled a reconfigurable cryptographic processor named Recryptor. Also demonstrated the optimized AES, finite field multiplication and reduction (FFMR), and the hash function of keccak. Recryptor is an efficient solution in energy, throughput, programmability, and balancing area metrics. In the 32-bit processor, the operation of keccak is slow. Weik and Selcuk [18] proposed on-chip CoRe regulators. The differential power analysis (DPA) resistance and the lightweight AES leverage the proposed regulator. The security is measured based on the clock frequency and switching frequency of the regulator. The comparison of software and hardware security solutions is performed in Table 3.

TABLE III. COMPARISON OF HARDWARE AND SOFTWARE SECURITY SOLUTIONS

Hardware security solution	Software security solution
Inside the security environment, the keys are segregated.	The number of keys lives across backups and systems
High integrity	Less integrity
Depending on the system's security	Not depend on operational services
The fluctuation in power consumption can be masked.	Not resistant to power analysis attacks
Less susceptible	More susceptible
Provides memory space protection	Memory space is not secure.

Saleh et al. [26] created a hybrid cloud infrastructure for sensitive and non-sensitive data encryption. Here the data is burst into two sections. One section undergoes RC6-based encryption, the next section is encrypted by Fiestal structure, and the non-sensitive data is encrypted by the AES scheme. Security was ensured by both public and private clouds. However, the compression of the key does not work for high-grade information and is a very time-consuming process. To fight against CPA attacks, Weize et al. [32] developed a lightweight masked AES scheme. Here, the false key-based masking is utilized for the unsafe AES engine.

IV. STEGANOGRAPHY

Today, many people share audio, text, video, and image information over the IoT medium. These media are utilized as a cover source to conceal data for preserved confidential data transmission. It conceals the private information in another file where only the recipient knows the presence of data.

The steganography method is explained in Figure 4. Some steganography techniques are described as follows, and the advantages and disadvantages are noted in Table 4.

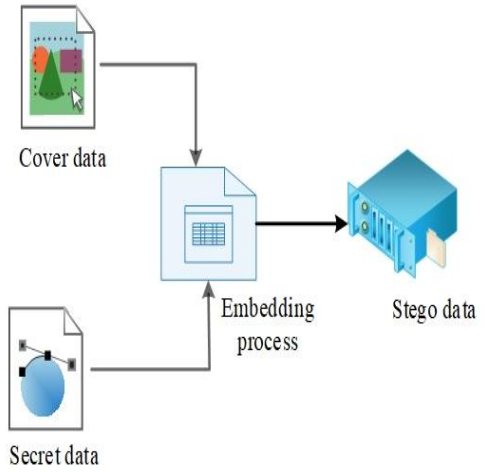

Figure 4. Steganography

TABLE IV. ADVANTAGES AND DISADVANTAGES OF A FEW STEGANOGRAPHY TECHNIQUES

Author	Method	Cover object	Advantages	disadvantages
Subash et al. [38]	PECT	Text	Less storage requirement and time complexity	Defective is needed to send again
Jyoti et al. [1]	OM-XOR	Image	Provided a high-level data security	Increased time complexity
Sachin et al. [33]	OFN	Image	It shows higher image quality and security	At the encryption stage huge amount of noise is added
Rouhan et al. [43]	cycleGAN	Image	It guarantees image grade and performance efficiency.	Learns only one-to-one mapping
Osma and Abbas [30]	modern algorithm	Video	Low complexity	It has quite an effect on the quality of the video
Karthika and Vidhya [39]	ANN	Video	It gives secure help to the customers	Fewer edge lines are picked
Rahem et al. [40]	SWT, SVD	Video	Very high robustness against attacks	Reduced image quality
Mohammed et al. [41]	LISS	Audio	low computational complexity	Low quality
Shunzhi et al. [42]	GAN	Audio	Produce high-fidelity steganographic audio	The function related to the information of a specific group is not encoded.
Yixiang et al. [44]	ERSTEG	Modified Packets (MP)	Provides greater payload replacement	High complexity

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

A. Text Steganography

It is the steganography technique of hiding secret information in text files. Some of the text steganography techniques are reviewed as follows. Subash et al. [38] presented a text steganography method named Parallel Encrypting by Cover Text (PECT) by embedding the secret text into the cover text. Here, the cover data is $1/4^{th}$ of the secret message ratio, and the data exactness is checked on the receiving end.

B. Image Steganography

It is termed as the concealing of data in the image source. In digital steganography, the image is the major used cover source because of its digital bit representation. In this technique, the information is hidden by the pixel intensities. To embed the encrypted knowledge into images, Jyoti et al. [1] an optimized matrix XOR coding steganography, is used. In this steganography method, for the optimization of the canopy parts among the image, an adaption firefly algorithm is activated. It provided high-level data security. Sachin et al. [33] proposed a new optimized fuzzy network (OFN) for secured and increased-quality steganography. Here the image is encrypted based on decomposition, and the encryption and steganography scenario is combined by IoT. The proposed steganography shows higher image quality and security. However, at the encryption stage huge amount of noise is added. Rouhan et al. [43] introduced an image steganography working on cycleGAN for privacy preservation in IoT. It guarantees the grade of the image and better performance.

C. Video Steganography

Osma and Abbas [30] used steganography and watermarking schemes to manage the video copyright by injecting the encrypted logo into it with the modern algorithm. However, it has quite an effect on the quality of the video. Karthika and Vidhya [39] proposed the security enhancement of the video steganography for the Raspberry Pi IoT based on artificial neural networks (ANN). It processed the data collected from the USB webcam. It gives secure help to the customers. Rahem et al. [40] proposed an efficient video steganography technique in the principle of decomposition and transform. Here, the structural variation between the stego video and the cover video is 99%.

D. Audio Steganography

It is the approach where the sensitive data are concealed in audio files such as AU, MP3, and WAV. The audio signal is the cover source for hiding sensitive data in most wireless mediums. Fatiha et al. [34] introduced a lightweight IoT steganography scheme (LISS) with quality noise resilience and high payload audio. It achieves low computational complexity and can constrain all IoT devices. Mohammed et al. [41] studied the detection accuracy of sensitive messages in video steganography techniques in the 5G-enabled IoT. Shunzhi et al. [42] proposed a machine learning-based lightweight audio steganography algorithm. This model works based on adversarial training. It consists of three layers: encoding for message embedding, decoding and the discriminator for determining the carriers that employ the secret message.

E. Network Steganography

It hides the information by utilizing network architecture in the cover objects, like IP, ICMP, TCP, or UDP. The channels in the OSI model where steganography can be applied. Some of the conventional steganography techniques lack security during the data transferring stage. So Yixiang et al. [44] introduced a new network steganography method named an Error-correcting Retransmission STEGanography algorithm "ERSTEG" for the data transmitting security in the 5G IoT network. Here the packets in the network are encoded by AES. However, this system is complex.

V. DISCUSSION

In the IoT environment, security is a major concern for many researchers. It is very hard to detect the best solution for all types of IoT applications. IoT connects numerous devices. So some techniques need to process the high weight and provide enhanced protection. Additionally, it should be less complex and have a surface area and fast-acting security. Therefore this paper reviewed a few cryptography techniques suitable for IoT applications in providing better security during sensitive data transmission. The recorded values for different AES techniques are given in Table 5.

TABLE V. COMPARISON OF A FEW AES TECHNIQUES

Reference	Data-path	Tech	Frequency (MHz)	Cycles	Area (mm2)	Throughput	Power (mW)	Energy/bit (pJ/bit)
[17]	8 bit	40 nm	28.8 MHz	16	0.128	-	-	12.8
[18]	8 bit	130 nm	200 MHz	10	-	-	-	-
[32]	4 bit	130 nm	196.4 MHz		2.61	1.81%	0.24	-

In the cryptographic technique, the block cipher is identified as more effective than the stream ciphers. It provides better security, and multiple block cipher will survive in the IoT environment. Additionally, the hardware and software implementation comparisons are included. Further, the different types of steganography are reviewed. The steganography can be carried out in 5 ways by varying the cover objects, including image, video, text audio, and network packet. However, some factors, such as robustness, mean square error, imperceptibility, payload capacity, and signal-to-noise ratio, may affect the efficiency of the steganography method. The comparison of these parameters is described in Table 6.

TABLE VI. METRICS COMPARISON OF STEGANOGRAPHY APPROACHES

Author	Method	Peak signal-to-noise ratio (PSNR)	Mean square error (MSE)	Payload capacity
Jyoti et al. [1]	OM-XOR	70dB	0.02	15 bpp
Sachin et al. [33]	OFN	60.82dB	0.6537	0.7 to 2.3 bpp

Osma and Abbas [30]	modern algorithm (MA)	57dB	0.12	17 bpp
Mohammed et al. [41]	LISS	57.2dB	0.14	-
Shunzhi et al. [42]	GAN	60dB	0.05	-

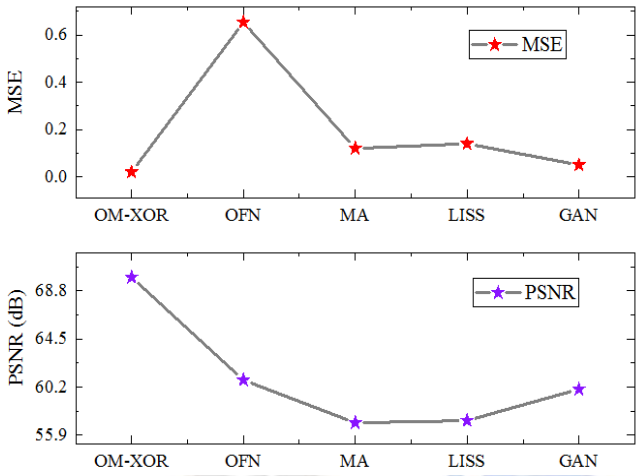

Figure 5. PSNR and MSE comparison

The graphical representation of the PSNR and MSE assessment is illustrated in Figure 5. In this comparison, the method OM-XOR scored a high PSNR value of 70dB, and MA achieved a lower PSNR rate of 57dB. Similarly, in the MSE comparison, the OM-XOR method achieved the very low error of 0.02, and OFN model results the greater error of 0.6357. Here the OM-XOR is the image steganography method; from this comparison it is quite clear that, in steganography the embedding of the confidential messages in the image gives the higher PSNR with low error values for the used cover images.

VI. CONCLUSION

In this review, lightweight security solutions for the IoT network are discussed. Various asymmetric and symmetric cryptographic mechanisms have been studied here. And also various AES-based security solutions have been studied. Compared to all other cryptographic mechanisms, AES provides enhanced security and all suitable for all IoT applications. It is the most trusted and researched block. Additionally, this paper elaborated on some of the recent works on steganography for IoT security solutions. Each methodology has different advantages and disadvantages. Efficient steganography must provide high payload capacity, data embedding and reconstruction without any intrusion and provide better quality and security. Here the GAN-based solutions have proved the efficient security services and hiding ratio for image-based steganography. In future, focus on the AES mechanism to provide a better lightweight IoT solution and an optimized technique for increasing the efficiency of the steganography method. Also, the hybrid of cryptography and steganography methods will be focused on.

REFERENCES

[1] 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 Trans. Syst. Man Cybern. vol. 50, no. 1, pp. 73-80, 2019 Mar 27. doi: https://doi.org/10.1109/TSMC.2019.2903785.

[2] P. Prakasam, M. Madheswaran, K. P. Sujith and M. S. Sayeed, "An enhanced energy efficient lightweight cryptography method for various IoT devices," ICT Express, vol. 7, no. 4, pp. 487-92, 2021 Dec 1. doi: https://doi.org/10.1016/j.icte.2021.03.007.

[3] B. Aboushosha, R. A. Ramadan, A. D. Dwivedi, A. El-Sayed and M. M. Dessouky, "SLIM, a lightweight block cipher for Internet of health things," IEEE Access, vol. 8, pp. 203747-57, 2020 Nov 6. doi: https://doi.org/10.1109/ACCESS.2020.3036589.

[4] L. Harn, C. F. Hsu, Z. Xia and Z. He, "Lightweight aggregated data encryption for wireless sensor networks (WSNs)," IEEE Sensors Letters, vol. 5, no. 4, pp. 1-4, 2021 Mar 3. doi: https://doi.org/10.1109/LSENS.2021.3063326.

[5] M. Kamal, "Lightweight security and data provenance for multi-hop Internet of Things," IEEE Access, vol. 6, pp. 34439-48, 2018 Jul 2. doi: https://doi.org/10.1109/ACCESS.2018.2850821.

[6] T. H. Kim, G. Kumar, R. Saha, W. J. Buchanan, T. Devgun, R. Thomas, "LiSP-XK, extended lightweight signcryption for IoT in resource-constrained environments," IEEE Access, vol. 9, pp. 100972-80, 2021 Jul 15. doi: https://doi.org/10.1109/ACCESS.2021.3097267.

[7] H. Tao, "Design and implementation of vehicle data transmission protocol based on PRESENT algorithm," In 2021 IEEE Asia-Pacific Conf. on Image Processing, Electr. and Comput. (IPEC) IEEE, pp. 968-971, 2021 Apr 14. doi: https://doi.org/10.1109/IPEC51340.2021.9421220.

[8] Y. Chen, W. Xu, L. Peng, H. Zhang, "Lightweight and privacy-preserving authentication protocol for mobile payments in the context of IoT," IEEE Access, vol. 7, pp. 15210-21, 2019 Jan 20. doi: https://doi.org/10.1109/ACCESS.2019.2894062.

[9] Y. Chen, W. Sun, N. Zhang, Q. Zheng, W. Lou, Y. T. Hou, "Towards efficient fine-grained access control and trustworthy data processing for remote monitoring services in IoT," IEEE Trans. Inf. Forensics Secur., vol. 14, no. 7, pp. 1830-42, 2018 Dec 6. doi: https://doi.org/10.1109/TIFS.2018.2885287.

[10] G. Bansod, N. Raval, N. Pisharoty, "Implementation of a new lightweight encryption design for embedded security," IEEE IEEE Trans. Inf. Forensics Secur., vol. 10, no. 1, pp. 142-51, 2014 Oct 29. doi: https://doi.org/10.1109/TIFS.2014.2365734.

[11] Y. Sun, J. Yang, B. Zhou, W. Chen, L. Chen, X. Xu, "Research on the Security of Power Distribution Internet of Things Based on TCM," In 2020 7th Intern. Forum on Electrical Eng. Automation (IFEEA) IEEE, pp. 656-660, 2020 Sep 25. doi: https://doi.org/10.1109/IFEEA51475.2020.00140.

[12] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, H. Karimipour, G. Srivastava, M. Aledhari, "Enabling drones in the Internet of things with decentralized blockchain-based security," IEEE Internet Things J., vol. 8, no. 8, pp. 6406-15, 2020 Aug 10. doi: https://doi.org/10.1109/JIOT.2020.3015382.

[13] B. Bera, A. K. Das, S. Garg, M. J. Piran, M. S. Hossain, "Access control protocol for battlefield surveillance in drone-assisted IoT environment," IEEE Internet Things J., vol. 9, no. 4, pp. 2708-21, 2021 Jan 4. doi: https://doi.org/10.1109/JIOT.2020.3049003.

[14] C. Lee, A. Fumagalli, "Internet of things security-multilayered method for end to end data communications over cellular networks," In 2019 IEEE 5th World Forum on Internet of Things (WF-IoT) IEEE, pp. 24-28, 2019 Apr 15. doi: https://doi.org/10.1109/WF-IoT.2019.8767227.

[15] X. Zhang, S. H. Seo, C. Wang, "A lightweight encryption method for privacy protection in surveillance videos," IEEE Access, vol. 6, pp. 18074-87, 2018 Apr 2. doi: https://doi.org/10.1109/ACCESS.2018.2820724.
[16] M. G. Samaila, J. B. Sequeiros, T. Simoes, M. M. Freire, P. R. Inacio, "IoT-HarPSecA, a framework and roadmap for secure design and development of devices and applications in the IoT space," IEEE Access, vol. 8, pp. 16462-94, 2020 Jan 13. doi: https://doi.org/10.1109/ACCESS.2020.2965925.
[17] Y. Zhang, L. Xu, Q. Dong, J. Wang, D. Blaauw, D. Sylvester, Recryptor, "A reconfigurable cryptographic cortex-M0 processor with in-memory and near-memory computing for IoT security," IEEE J. Solid-State Circuits, vol. 53, no. 4, pp. 995-1005, 2018 Feb 5. doi: https://doi.org/10.1109/JSSC.2017.2776302.
[18] W. Yu, S. Köse, "A voltage regulator-assisted lightweight AES implementation against DPA attacks," IEEE Transactions on Circuits and Systems I, Regular Papers, vol. 63, no. 8, pp. 1152-63, 2016 Jul 7. doi: https://doi.org/10.1109/TCSI.2016.2555810.
[19] L. Bai, M. Hu, M. Liu, J. Wang, "BPIIoT, A light-weighted blockchain-based platform for industrial IoT," IEEE Access, vol. 7, pp. 58381-93, 2019 May 1. doi: https://doi.org/10.1109/ACCESS.2019.2914223.
[20] M. Raj, K. S. Joseph, J. Tomy, K. S. Niveditha, A. Johnson, R. Nandakumar, M. Raj, "Design and implementation of IP core for RoadRunneR-128 block cipher," In 2017 Intern. Conf. on Public Key Infrastructure and its Applications (PKIA) IEEE. Pp. 57-62, 2017 Nov 14. doi: https://doi.org/10.1109/PKIA.2017.8278961.
[21] A. A. Zakaria, A. H. Azni, F. Ridzuan, N. H. Zakaria, M. Daud, "Extended RECTANGLE algorithm using 3D bit rotation to propose a new lightweight block cipher for IoT," IEEE Access, vol. 8, pp. 198646-58, 2020 Nov 3. doi: https://doi.org/10.1109/ACCESS.2020.3035375.
[22] S. Shin, T. Kwon, "Two-factor authenticated key agreement supporting unlinkability in 5G-integrated wireless sensor networks," IEEE Access, vol. 6, pp. 11229-41, 2018 Jan 23. doi: https://doi.org/10.1109/ACCESS.2018.2796539.
[23] P. W. Shaikh, I. W. Damaj, "Analysis of Pipelined KATAN Ciphers under Handle-C for FPGAs," In 2018 International Conference on Innovations in Information Technology (IIT) IEEE, pp. 163-168, 2018 Nov 18. doi: https://doi.org/10.1109/INNOVATIONS.2018.8606012.
[24] M. K. Sai, N. Alapati & Sivaramakrishna, R. Teja, B. Kolla, "A Hybrid Approach for Enhancing Security in IOT using RSA Algorithm, HELIX," vol. 9, pp. 4758, 2019.
[25] G. Xu, "IoT-assisted ECG monitoring framework with secure data transmission for health care applications," IEEE Access, vol. 8, pp. 74586-94, 2020 Apr 15. doi: https://doi.org/10.1109/ACCESS.2020.2988059.
[26] S. Atiewi, A. Al-Rahayfeh, M. Almiani, S. Yussof, O. Alfandi, A. Abugabah, Y. Jararweh, "Scalable and secure big data IoT system based on multifactor authentication and lightweight cryptography," IEEE Access, vol. 8, pp. 113498-511, 2020 Jun 16. doi: https://doi.org/10.1109/ACCESS.2020.3002815.
[27] T. Jabeen, H. Ashraf, A. Khatoon, S. S. Band, A. Mosavi, "A lightweight genetic based algorithm for data security in wireless body area networks," IEEE Access, vol. 8, pp. 183460-9, 2020 Oct 5. doi: https://doi.org/10.1109/ACCESS.2020.3028686.
[28] R. A. Shah, M. N. Asghar, S. Abdullah, N. Kanwal, M. Fleury, "SLEPX, An efficient lightweight cipher for visual protection of scalable HEVC extension," IEEE Access, vol. 8, pp. 187784-807, 2020 Oct 12. doi: https://doi.org/10.1109/ACCESS.2020.3030608.
[29] L. Ning, Y. Ali, H. Ke, S. Nazir, Z. Huanli, "A hybrid MCDM approach of selecting lightweight cryptographic cipher based on ISO and NIST lightweight cryptography security requirements for Internet of health things," IEEE Access, vol. 8, pp. 220165-87, 2020 Nov 30. doi: https://doi.org/10.1109/ACCESS.2020.3041327.
[30] O. Q. Al-Thahab, A. A. Hussein, "Implementation of Stego-Watermarking Technique by Encryption Image Based on Turbo Code for Copyright Application," In2020 1st. Information Technology to Enhance e-learning and Other Application (IT-ELA) IEEE, pp. 148-153, 2020 Jul 12. doi: https://doi.org/10.1109/IT-ELA50150.2020.9253112.
[31] B. D. Anudeep, R. S. Devi, V. K. Thenmozhi, R. Amirtharajan, P. Praveenkumar, "IoT with Light Weight Crypto System for Primary Health Centers to Minimize Fetus Death, Birth Defects and Premature Delivery in Solamadevi Village Trichy District," In2020 International Conference on Computer Communication and Informatics (ICCCI) IEEE, pp. 1-4, 2020 Jan 22. doi: https://doi.org/10.1109/ICCCI48352.2020.9104180.
[32] W. Yu, S. Köse, "A lightweight masked AES implementation for securing IoT against CPA attacks," IEEE Transactions on Circuits and Systems I, Regular Papers, vol. 64, no. 11, pp. 2934-44, 2017 May 31. doi: https://doi.org/10.1109/TCSI.2017.2702098.
[33] S. Dhawan, C. Chakraborty, J. Frnda, R. Gupta, A. K. Rana, S. K. Pani, "SSII, secured and high-quality steganography using intelligent hybrid optimization algorithms for IoT," IEEE Access, vol. 9, pp. 87563-78, 2021 Jun 14. doi: https://doi.org/10.1109/ACCESS.2021.3089357.
[34] F. Djebbar, N. Abu-Ali, "Lightweight noise resilient steganography scheme for Internet of Things," InGLOBECOM 2017-2017 IEEE Global Communications Conference, pp. 1-6, 2017 Dec 4. doi: https://doi.org/10.1109/GLOCOM.2017.8255039.
[35] S. Khan, W. K. Lee, S. O. Hwang, "A flexible Gimli hardware implementation in FPGA and its application to RFID authentication protocols," IEEE Access, vol. 9, pp. 105327-40, 2021 Jul 26. doi: https://doi.org/10.1109/ACCESS.2021.3100104.
[36] M. A. Ferrag, L. Shu, "The performance evaluation of blockchain-based security and privacy systems for the Internet of Things, A tutorial," IEEE Internet Things J., vol. 8, no. 24, pp. 17236-60, 2021 May 6. doi: https://doi.org/10.1109/JIOT.2021.3078072.
[37] T. K. Goyal, V. Sahula, "Lightweight security algorithm for low power IoT devices," In 2016 international conference on advances in computing, communications and informatics (ICACCI) IEEE, pp. 1725-1729, 2016 Sep 21. IEEE. doi: https://doi.org/10.1109/ICACCI.2016.7732296.
[38] S. Panwar, M. Kumar, S. Sharma, "Text Steganography Based on Parallel Encryption Using Cover Text (PECT)," Internet of Things and Connected Technologies. Springer International Publishing, pp. 303-313, 2020. doi: https://doi.org/10.1007/978-3-030-39875-0_32.
[39] P. Karthika, P. Vidhya Saraswathi, "IoT using machine learning security enhancement in video steganography allocation for Raspberry Pi," J. Ambient Intell. Humaniz Comput., vol. 12, pp. 5835-44, 2021 Jun. doi: https://doi.org/10.1007/s12652-020-02126-4.
[40] R. A. El-Shahed, M. N. Al-Berry, H. M. Ebied, H. A. Shedeed, "Robust Video Steganography Technique Against Attack Based on Stationary Wavelet Transform (SWT) and Singular Value Decomposition (SVD)," In Proceedings of Third Intern. Conf. on Sustainable Computing, SUSCOM 2021 Springer Singapore, pp. 257-266, 2022. doi: https://doi.org/10.1007/978-981-16-4538-9_26.
[41] M. J. Alhaddad, M. H. Alkinani, M. S. Atoum, A. A. Alarood, "Evolutionary detection accuracy of secret data in audio steganography for securing 5G-enabled Internet of things," Symmetry, vol. 12, no. 12, pp. 2071, 2020 Dec 14. doi: https://doi.org/10.3390/sym12122071.
[42] S. Jiang, D. Ye, J. Huang, Y. Shang, Z. Zheng, "SmartSteganogaphy, Lightweight generative audio steganography model for smart embedding application," J. Netw. Comput. Appl., vol. 165, pp. 102689, 2020 Sep 1. doi: https://doi.org/10.1016/j.jnca.2020.102689.
[43] R. Meng, Q. Cui, Z. Zhou, Z. Fu, X. Sun, "A steganography algorithm based on CycleGAN for covert communication in

the Internet of Things," IEEE Access, vol. 7, pp. 90574-84, 2020. doi: https://doi.org/10.1109/ACCESS.2019.2920956.
[44] Y. Fang, K. Tu, K. Wu, Y. Peng, J. Wang, C. Lu, "Securing Data Communication of Internet of Things in 5G Using Network Steganography," In Artificial Intelligence and Security, 6th International Conference, ICAIS 2020, Hohhot, China, July 17–20, 2020, Proceedings, Part II 6 Springer International Publishing, pp. 593-603, 2020. doi: https://doi.org/10.1007/978-3-030-57881-7_52.
[45] A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider, M. Hamdi, "A survey on security and privacy issues in edge-computing-assisted Internet of things," IEEE Internet Things J., vol. 8, no. 6, pp. 4004-22, 2020 Aug 10. doi: https://doi.org/10.1109/JIOT.2020.3015432.
[46] E. Lee, Y. D. Seo, S. R. Oh, Y. G. Kim, "A Survey on Standards for Interoperability and Security in the Internet of Things," IEEE Commun. Surv. Tutor., vol. 23, no. 2, pp. 1020-47, 2021 Mar 19. doi: https://doi.org/10.1109/COMST.2021.3067354.
[47] B. Liu, Z. Su, Q. Xu, "Game theoretical secure wireless communication for UAV-assisted vehicular Internet of Things," China Commun., vol. 18, no. 7, pp. 147-57, 2021 Jul 26. https://doi.org/10.23919/JCC.2021.07.012.
[48] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, Y. A. Bangash, "An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security," IEEE Internet Things J., vol. 7, no. 10, pp. 10250-76, 2020 May 26. doi: https://doi.org/10.1109/JIOT.2020.2997651.
[49] M. N. Bhuiyan, M. M. Rahman, M. M. Billah, D. Saha, "Internet of things (IoT), A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities," IEEE Internet Things J., vol. 8, no. 13, pp. 10474-98, 2021 Mar 1. doi: https://doi.org/10.1109/JIOT.2021.3062630.
[50] M. Bansal, M. Nanda, M. N. Husain, "Security and privacy aspects for Internet of Things (IoT)," In2021 6th international conference on inventive computation technologies (ICICT) IEEE, pp. 199-204, 2021 Jan 20. doi: https://doi.org/10.1109/ICICT50816.2021.9358665.
[51] F. Tian, X. Chen, S. Liu, X. Yuan, D. Li, X. Zhang, Z. Yang, "Secrecy rate optimization in wireless multi-hop full duplex networks," IEEE Access, vol. 6, pp. 5695-704, 2018 Jan 17. doi: https://doi.org/10.1109/ACCESS.2018.2794739.
[52] Y. Sun, Z. Lin, Y. Ma, "A lottery SMC protocol for the selection function in software defined wireless sensor networks," IEEE Sens. J., vol. 16, no. 20, pp. 7325-31, 2016 Mar 9. doi: https://doi.org/10.1109/JSEN.2016.2540002.
[53] D. Kim, S. An, "PKC-Based DoS attacks-resistant scheme in wireless sensor networks," IEEE Sens. J., vol. 16, no. 8, pp. 2217-8, 2016 Jan 19. doi: https://doi.org/10.1109/JSEN.2016.2519539.
[54] P. Tedeschi, S. Sciancalepore, R. Di Pietro, "Security in energy harvesting networks, A survey of current solutions and research challenges," IEEE Commun. Surv. Tutor., vol. 22, no. 4, pp. 2658-93, 2020 Aug 18. doi: https://doi.org/10.1109/COMST.2020.3017665.
[55] B. Seok, J. C. Sicato, T. Erzhena, C. Xuan, Y. Pan, J. H. Park, "Secure D2D communication for 5G IoT network based on lightweight cryptography," Appl. Sci., vol. 10, no. 1, pp. 217, 2019 Dec 27. doi: https://doi.org/10.3390/app10010217.
[56] K. Tsantikidou, N. Sklavos, "Hardware Limitations of Lightweight Cryptographic Designs for IoT in Healthcare," Cryptography, vol. 6, no. 3, pp. 45, 2022 Sep 1. doi: https://doi.org/10.3390/cryptography6030045
[57] A. Miri, K. Faez, "Adaptive image steganography based on transform domain via genetic algorithm, Optik," vol. 145, pp. 158-68, 2017 Sep 1. https://doi.org/10.1016/j.ijleo.2017.07.043.
[58] N. Kaur, S. Behal, "A Survey on various types of Steganography and Analysis of Hiding Techniques," International journal of engineering trends and technology, vol. 8, pp. 388-92, 2014 May;11.
[59] O. F. Wahab, A. A. Khalaf, A. I. Hussein, H. F. Hamed, "Hiding data using efficient combination of RSA cryptography, and compression steganography techniques," IEEE access, vol. 9, pp. 31805-15, 2021 Feb 18. doi: https://doi.org/10.1109/ACCESS.2021.3060317.
[60] D. Bi, S. Kadry, P. M. Kumar, "Internet of things assisted public security management platform for urban transportation using hybridized cryptographic-integrated steganography," IET Intell. Transp. Syst., vol. 14, no. 11, pp. 1497-506, 2020 Nov. doi: https://doi.org/10.1049/iet-its.2019.0833.
[61] P. Gao, R. Yang, X. Gao, "Research on" Cloud-Edge-End" Security Protection System of Internet of Things Based on National Secret Algorithm," In2019 IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC) IEEE, vol. 1, pp. 1690-1693, 2019 Dec 20. doi: https://doi.org/10.1109/IAEAC47372.2019.8997741.
[62] H. Chen, M. Hu, H. Yan, P. Yu, "Research on industrial internet of things security architecture and protection strategy," In2019 International conference on virtual reality and intelligent systems (ICVRIS) IEEE, pp. 365-368, 2019 Sep 14. doi: https://doi.org/10.1109/ICVRIS.2019.00095.
[63] H. Du, Q. Wen, S. Zhang, "An efficient certificateless aggregate signature scheme without pairings for healthcare wireless sensor network," IEEE Access, vol. 7, pp. 42683-93, 2019 Mar 25. doi: https://doi.org/10.1109/ACCESS.2019.2907298.
[64] H. A. Babaeer, S. A. Al-Ahmadi, "Efficient and secure data transmission and sinkhole detection in a multi-clustering wireless sensor network based on homomorphic encryption and watermarking," IEEE Access, vol. 8, pp. 92098-109, 2020 May 14. doi: https://doi.org/10.1109/ACCESS.2020.2994587.