BioGecko

Vol 12 Issue 02 2023

ISSN NO: 2230-5807

A DETAILED SURVEY OF SECURE IMAGE TRANSMISSION TECHNIQUES IN IOT: RECENT ADVANCES AND FUTURE TRENDS

[1]P.Shobana, [2]Dr.D.Kannan,
[1]Ph.D Scholar, Department of Computer Science and Applications, Pollachi College of Arts and Science, Pollachi and
Assistant Professor in Information Technology, Sree Saraswathi Thyagaraja College, Pollachi

[2]Dr.D.Kannan, Principal, Pollachi College of Arts and Science, Pollachi

Abstract: The upsurge in the Internet of Things (IoT) adoption has accelerated incorporation and expanded the Internet's reach beyond computers, tablets, and mobiles to a wide range of physical devices. It is challenging to secure sensitive data transferred by IoT due to hostile conditions and unique properties of IoT. Furthermore, IoT has security problems that traditional networks still need to address. As a result, security is a primary concern for IoT, and numerous security factors should be researched. Many security systems for reliable image transmission have been developed and researched. However, existing security algorithms have flaws. It may be susceptible to threats such as replay attacks and user privacy invasion, severely limiting its wide acceptance by end consumers. This article compares current encryption techniques regarding user scenarios, standout features, and limitations. This study also examines the pros and cons of image encryption techniques regarding IoT services.

Keywords: *Internet of Things (IoT), Cryptography, Biometric images, Medical images, security and privacy, and Message Queuing Telemetry Transport (MQTT).*

1. INTRODUCTION

The IoT is undoubtedly among the most exciting topics in the research, public, and private sectors. While the traditional internet allows for information exchange between a small number of devices and living beings, IoT integrates all types of connected "Things" into an extensive network of interconnected computing intelligence without the interference of a human [1]. An IoT paradigm comprises various functional blocks that facilitate various smart object functions such as sensing, actuation, identification, management, and communication [2]. It creates these devices available to all internet-connected users [3]. IoT devices can use the user's Internet Protocol (IP) address to send and receive data over a network. IoT applications are expanding rapidly in all key sectors, including healthcare, military, government, education, security, surveillance, banking systems, and so on. They produce massive amounts of sensitive images, which are transferred via the internet [4]. These images include more details and are more likely to reveal personal information. As a result, image security is critical for maintaining image anonymity by safeguarding sensitive data from intruders. This can be accomplished by transforming the original image to another unintelligible format before sending it to the recipient.They generate vast quantities of sensitive images and urgently need to protect the enormous data generate [5]. With IoT devices' increasing utilization, security has become a significant concern in IoT networks. It causes opponents to launch a barrage of attacks. Images must be encrypted before transmission to resist hackers and attackers [6]. With far too little awareness of IoT security risks among IoT device users and vendors, these IoT devices are becoming a source of potential risks.

Cryptography is among the most critical aspects for any data transferred over a wireless channel; it is the method that safeguards information from third-party interference and translates it into an unreadable format. Due to particular actual characteristics of the digital image, such as the high correlation among both picture elements (pixels) and large data volume, classical cryptographic algorithms such as Rivest cipher 4 (RC4), advanced encryption standard (AES), data encryption standard (DES), and so on, encrypting the image and converting it to an unintelligible form is inadequate. Furthermore, image security based on biometric authorization employs physiological and behavioral characteristics of a person as characteristics that are not easily misapplied or thieved. Fingerprint, face, palm, iris, hand veins, and DNA are some of the most commonly used physiological attributes. Some common behavioral characteristics include gait, signature, and voice. Cryptology employs the chaos system, which has numerous advantages. The compressed and encrypted images, on the other hand, are susceptible to bit errors, which can deteriorate the quality of the transmitted image. This encourages us to conduct a comprehensive survey to clarify the current state-of-the-art image transmission over IoT security and privacy solutions. It is also important to identify research directions issues and propose future research directions based on a general review of the field. The organization of the current survey is shown in fig.1.

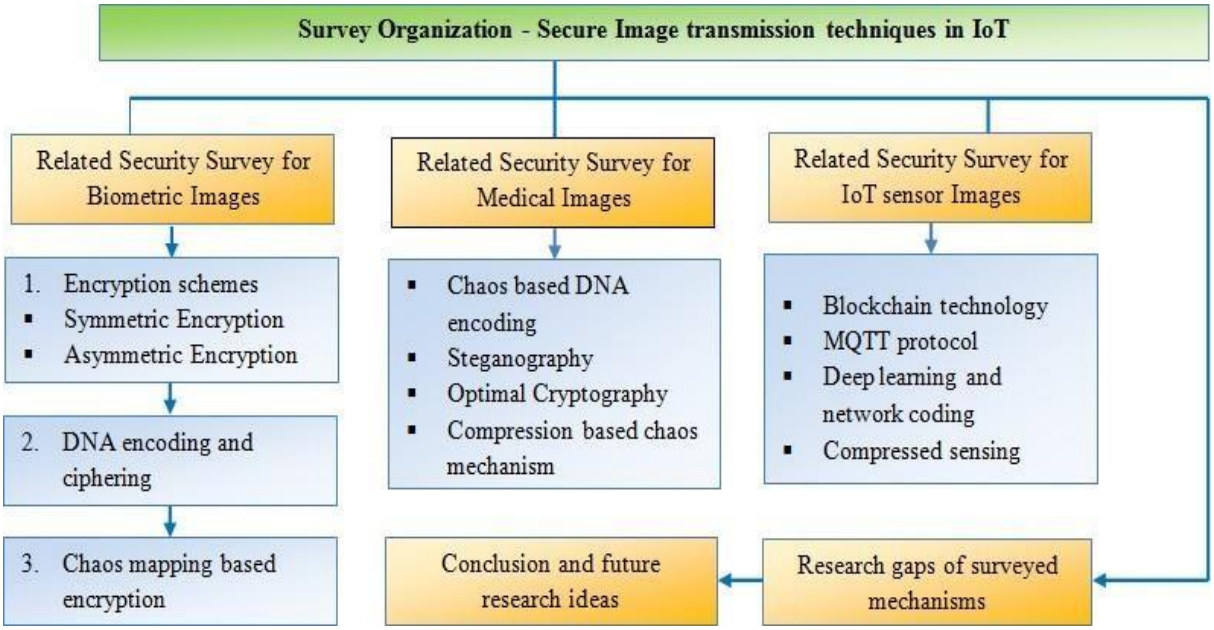

Figure 1: Survey organization

The rest of the survey paper is coordinated as follows: Section 2 portrays the various techniques used for image transmission over IoT, and Section 3 provides the survey paper's conclusion.

2. SURVEY OVER ON SECURE IMAGE TRANSMISSION IN IOT

Because of the widespread use of IoT in various fields such as military, civil, and healthcare, industry and academic researchers have been drawn to this field. This section conducts a literature review of existing secure image transmission methods in IoT and proposes a technique to transfer the secure image.

Security of biometric image in IoT

IoT applications have recently started to use biometric individuality for authentication. The distinctiveness of an individual is derived from physiological and behavioral characteristics such as fingerprint, facial recognition, iris scanning, and hand geometry, with no passwords or numbers to remember. The integrity and confidentiality of biometric templates during storage and transmission are critical because they contain critical information about the physical identity of the users. Some authors offer biometric image security solutions.

Muhammed Golec *et al.* [4] presented a biometric-based authentication approach, BioSec, to address the security and privacy-related issues in IoT. The biometric used to provide authentication of IoT users was a fingerprint. In addition, to ensure the security of the biometric data (fingerprint), an encryption technique, say advanced encryption standard with the 128-bit key module, was presented. The security of the user biometric data was maintained in both the database and transmission medium. This way, the technique offered security to the IoT environment and the user's biometrics data. The performance of the techniques was analyzed regarding processing time, and the presented AES technique outperformed other related schemes. **Rajendran Sujarani *et al.* [6]** recommended a lightweight bio-cryptosystem to provide security to the biometric templates in IoT applications. The approach worked in three phases: key generation, confusion and diffusion. Initially, a 2-dimensional logistic sine map was utilized to perform a key generation process. Then, diffusion-based DNA encoding and ciphering were used to ensure the data integrity and diminish the burden of the encryption process. The outcomes proved that the technique was robust and achieved a satisfied level of security with lower computational complexity.

ShadiYoosefianDezfuliNezhad *et al.* [7] suggested an encryption method for fingerprint biometric images using DNA sequence and chaotic tent map. Initially, the fingerprint image was encrypted using the DNA sequences. The DNA-encrypted image was further encrypted by applying the XOR operator and chaotic mapping sequences to them. The average entropy for the final encrypted fingerprint image was obtained as a final step. The results showed that the technique attained good data encryption results and worked well against common attacks in the network. **Khaled Loukhaoukha *et al.* [8]** recommended a fingerprint image encryption approach to protect biometric images from replay attacks. The method was based on the operations of the wavelet domain, such as permutation and diffusion. Initially, a one-level lifting wavelet transforms integer-to-integer process was performed on the input biometric image. The approximation and detailed sub-band coefficients of the wavelet-transformed images were then divided into blocks and permuted using the permutation key. Finally, the method generated the encrypted image by arranging the encrypted sub-bands. The outcomes showed that the technique was effective and robust against common attacks.

Noha A. Hikal and Marwa M. Eid [9] presented a hybrid chaotic map-based encryption technique to secure palm print biometric images. The chaotic hybrid map was the combination of different chaotic maps that were applied to the specific control parameters of the biometric image. In addition, they are designed to overcome the difficulties of confusion and diffusion and to offer a larger key space. The results proved that the technique worked well against several well-known attacks in the network, such as brute force, statistical, and differential attacks. From the results of encryption and decryption time, it was also observed that the approach was more applicable in real-time network scenarios than other related schemes. Fig. 2 shows the general working process followed in biometric images to offer security to them.

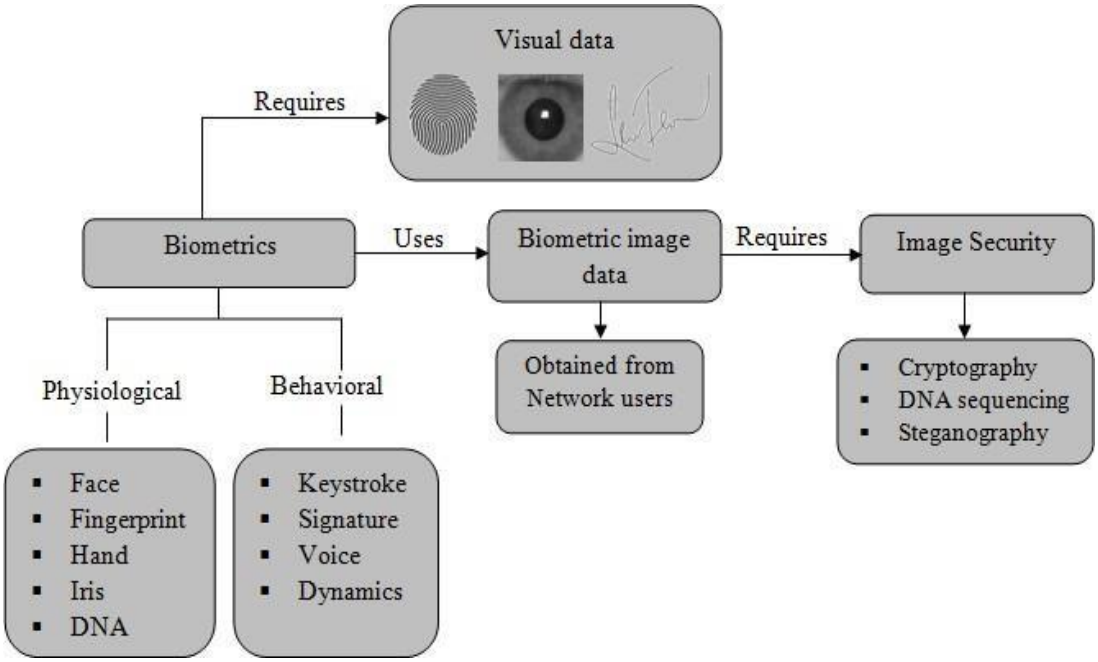

Figure 2: Working process of biometric image security schemes

Security of medical image in IoT

Medical images are essential for diagnosing diseases in IoT-based e-healthcare applications, so transmitting medical images over networks and storage in cloud-based services is critical. As a result, it is critical to developing an efficient mechanism to ensure the integrity and confidentiality of patient medical images transmitted and stored in an IoT environment. Among the solutions are the following:

Sujarani Rajendran and ManivannanDoraipandian [10] presented a chaos-based medical image data transmission system for securing IoT-based healthcare applications. Initially, a message digest method was applied to input medical images to generate a Lorenz chaotic map seed key. Then the Lorenz map was iterated to produce the chaotic key series for further proceedings. Next, the author applied a dual confusion technique, namely, row by row and column by column on the input medical image. Finally, the dual diffusion procedure was carried out by applying binary reverse and complement functions. Furthermore, the XOR operation was applied between the Lorenz chaotic key and diffusion image. The simulation outcomes showed that the technique attained better results against several attacks and satisfied the security needs of IoT-based healthcare applications. **S. ArunaDeepthi*et al.* [11]** developed a secure medical image (brain MRI) transmission scheme for IoT networks using a hybrid autoencoder (HAE) and Restricted Boltzmann machines (RBM) approach. Initially, the medical images transferred via the IoT environment were compressed using the HAE and RBM. Then to securely share the medical images in the IoT, Raspberry Pi and messaging queue telemetry transport protocol were utilized. The outcomes showed that the technique achieved better results regarding security than that of similar existing approaches.

Joshua C. Dagadu*et al.* [12] suggested a hybrid chaotic DNA diffusion strategy for providing security to medical images. The suggested method contained three operations: two chaotic maps, hashing, and DNA XOR operations. Initially, MD5 hashing technique was applied to the input medical image to get the hash image. This generated hash value was used to generate the initial condition and control parameter of the chaotic maps used in this system for encryption. Two chaotic maps, namely the Bernoulli shift and Zigzag map, were utilized to generate the encryption key matrices. Finally, a diffusion

operation (row by row) was performed between the input image matrices and the generated chaotic encryption key matrices using the DNA XOR function to generate an encrypted medical image. The outcomes demonstrated that the scheme was robust and protected the data from various attacks. **BassemAbd-El-Atty*et al.* [13]** recommended a medical image security protocol using quasi-quantum walks-based steganography for cloud-based e-healthcare systems. The quasi-quantum walks are utilized to choose the pixel locations in the input carrier image and embed secret bits in them. The bits embedded carrier image using quasi-quantum walks were considered a final stego image for transmission. The technique showed superior performance regarding image quality, security, and embedding capacity, and the technique was secure against data loss attacks. **Mohamed Elhoseny *et al*. [14]** presented an optimal encryption scheme to secure medical images in an IoT environment. The system used an elliptical curve cryptography technique to encrypt and decrypt the medical images. The key was selected optimally to enhance the security of the cryptographic algorithm using a hybrid optimization technique such as the grasshopper and particle swarm optimization technique. The optimal key-based encryption scheme provided higher security to the medical images in IoT.

Security of other types of images in IoT

Also, people have done much research on other types of secure image transmission (i.e. surveillance, satellite, cropped images, etc.) and have made some achievements. Table 1 compares the advantages and disadvantages of the traditional method for secure image transmission.

Table 1: Comparison of current existing works

Author Name and Ref. no	**Technique used for image security**	**Advantages**	**Drawbacks**
Astrid Maritza González-Zapata *et al*. [15]	MQTT protocol for neuron images	It was convenient because of its low cost and aptness to encrypt the data.	It did not increase the randomness of the chaotic sequences and also the computational cost is high by using MQTT protocol
Yunfa Li *et al*. [16]	Blockchain technology for surrounding scene images	Secure against various kinds of network attacks and if data was tampered or altered it was immediately informed to the data owner.	Sometimes, the data was stolen when the public blockchain mechanism was used. In addition, the blockchain mechanism did not allow us to modify the data quickly because if we need to change the data means, it is necessary to rewrite the codes in all blocks. This process results in a time-Consuming and expensive mechanism.
S. Ramana*et al*. [17]	MQTT protocol for captured image by an	The system was worked better against replay and	MQTT permits the data to pass in both

	IoT	man-in-the-middle attacks.	directions between clients and servers efficiently; however, the protocol did not use any encryption methodology to protect the data, so third parties quickly attacked the image when performing transmission.
Prince Waqas Khan and YungcheolByun [18]	Blockchain technology for industrial IoT images	Protected the data from leakage and offered better security.	When using blockchain as an image security model, correcting a mistake or adjusting the image data stored in the blockchain is difficult, this results in higher energy dependence and implementation costs.
Quoc-Tuan Vien*et al.* [19]	Deep learning and network coding for high resolution images	Lower data transmission bandwidth with higher performance efficiency.	The noise density level increased in the image when performing data transmission, which significantly lessened the performance and was unsuitable for multi-scale images.
Renjith V. Ravi *et al.* [20]	2D exponential cosine transform and Latin square for underwater images	Lower computational overhead.	It took more time to perform encryption and decryption compared to the other studies examined in this paper.
Lixiang Li *et al.* [21]	Compressed sensing method for the images captured by an IoT sensors	Less memory storage and higher data transmission rate.	The major demerit of the compressed sensing approach is its insufficient toleration in low signal-to-noise ratio and its heavy computational burden.

3. RESEARCH GAPS

When the user data (image) is transferred via an unsecured channel like IoT, it is necessary to protect it from several network attacks and attackers. Many kinds of security approaches were developed previously to ensure the security of the user images transferred via the IoT platform. This section lists the problems and challenges the above-surveyed techniques face in providing image security. Some techniques were developed to offer security to the biometric user images. The symmetric encryption, AES, used in [4] can be complicated when encryption and decryption take place in different locations, necessitating the movement of the key. A system that only has access to the secret key can decrypt a message using symmetric cryptography, which is faster. It does, however, have a transportation issue with keys. Because before transmitting the data to the destination, the private key must be shared with the receiver. There is a high possibility of attacking the key between the communications, so this transmission is unsafe. Therefore, personally exchanging keys would be the only secure method. The techniques developed in [6 and 7] used the conventional form of chaotic maps for key generation, so the schemes were deterministic and could be hacked by phase space reconstruction.

The wavelet-based approach for offering biometric image security takes more time to execute the algorithm, and its encryption efficiency is low [8]. It is suggested to use optimization techniques like particle swarm and genetic algorithms to improve the encryption efficiency and adaptive ability of the wavelet domain. Some existing works offered security for medical images transferred via the IoT network. However, some methods [10 and 11] were not secure enough to transmit the medical images via the unsecured channel; so it needs to be investigated additionally to increment the security level. The difficulties faced by DNA sequencing [13] are its simple structure and the absence of a secure theory. The conventional optimization used in [14] for key generation suffered from local optima and convergence issues. So the key generated using the model was not optimal in encryption. The MQTT protocol-based image transmission produced a minimum battery loss and minimum bandwidth in a transmission medium. However, the MQTT protocol-based solutions have slower transmitted cycles than other protocols [15, 17]. So, it is imperative to have well-defined hybrid security algorithms for secure image transmission to allow legitimate users to access the various resources from the IoT environment. The solutions given in [16, 18 to 20] have the problems of higher execution time, limited computing resources, less efficiency in encryption and decryption and the possibility of being attacked by hackers when used in a public transmission medium.

4. CONCLUSION

Preserving image security has become an essential issue since images are transmitted over the Internet frequently. This paper surveys the recent methodologies proposed by various researchers to provide security to the different kinds of images transferred via an unsecured channel like IoT and cloud. The survey of the techniques includes symmetric and asymmetric encryption schemes, chaos mapping-based schemes, DNA sequencing-based encryption methods and other types of protocols for the images, such as medical, biometric, underwater, and sensor-captured images. The techniques are surveyed based on their purpose, the framework used, and steps involved, results achieved, and drawbacks and challenges they faced while performing transmission. Most of the techniques achieved better and satisfactory results; however, they still face security issues in the transmission channel. The key parameters to focus on the future research for providing image security are security, execution time, computational resources, and improved versions of the encryption approaches. In addition, from the survey, only limited studies were focused on biometric image transmission in IoT. The traditional biometric attributes used to provide security are fingerprint, palm print, gait, speech and face. Compared to other techniques, such as hashing and encryption-based authentication, biometric-based authentication provides a higher level of security to the user data in any network. However, the biometric template stored in the databases may be vulnerable to attacks. As a result, the suggested enhancements will be provided in the future alongside security mechanisms that effectively apply to biometric images and other algorithms for sophisticated IoT

systems.

REFERENCES

1. Dang, L. M., Piran, M. J., Han, D., Min, K., & Moon, H. (2019). A survey on internet of things and cloud computing for healthcare. *Electronics*, *8*(7), 768.
2. Kassab, W. A., &Darabkh, K. A. (2020). A–Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions and recommendations. *Journal of Network and Computer Applications*, *163*, 102663.
3. Yang, W., Wang, S., Sahri, N. M., Karie, N. M., Ahmed, M., & Valli, C. (2021). Biometrics for Internet-of-Things security: A review. *Sensors*, *21*(18), 6163.
4. Golec, M., Gill, S. S., Bahsoon, R., & Rana, O. (2020). BioSec: A biometric authentication framework for secure and private communication among edge devices in IoT and industry 4.0. *IEEE Consumer Electronics Magazine*.
5. Dr. D. Kannan and Mrs. P. Shobana (2022). Survey based on image security using various methodologies under networking system. *International Journal of Research and Analytical Reviews*, 9(1), 2349-5138.
6. Sujarani, R., Manivannan, D., Manikandan, R., &Vidhyacharan, B. (2021). Lightweight bio-chaos crypt to enhance the security of biometric images in internet of things applications. *Wireless Personal Communications*, *119*(3), 2517-2537.
7. Nezhad, S. Y. D., Safdarian, N., & Zadeh, S. A. H. (2020). New method for fingerprint images encryption using DNA sequence and chaotic tent map. *Optik*, *224*, 165661.
8. Loukhaoukha, K., Refaey, A., Zebbiche, K., &Shami, A. (2018). Efficient and secure cryptosystem for fingerprint images in wavelet domain. *Multimedia Tools and Applications*, *77*(8), 9325-9339.
9. Hikal, N. A., & Eid, M. M. (2020). A new approach for palmprint image encryption based on hybrid chaotic maps. *Journal of King Saud University-Computer and Information Sciences*, *32*(7), 870-882.
10. Rajendran, S., &Doraipandian, M. (2021). Chaos based secure medical image transmission model for IoT-powered healthcare systems. In *IOP Conference Series: Materials Science and Engineering* (Vol. 1022, No. 1, p. 012106). IOP Publishing.
11. Deepthi, S. A., Rao, E. S., &Giriprasad, M. N. (2022). Secure MRI Brain Image Transmission Using IOT Devices Based on Hybrid Autoencoder and Restricted Boltzmann Approach. *Journal of Sensors*, *2022*.
12. Dagadu, J. C., Li, J. P., & Aboagye, E. O. (2019). Medical image encryption based on hybrid chaotic DNA diffusion. *Wireless Personal Communications*, *108*(1), 591-612.
13. Abd-El-Atty, B., Iliyasu, A. M., Alaskar, H., & Abd El-Latif, A. A. (2020). A robust quasi-quantum walks-based steganography protocol for secure transmission of images on cloud-based E-healthcare platforms. *Sensors*, *20*(11), 3108.
14. Elhoseny, M., Shankar, K., Lakshmanaprabu, S. K., Maseleno, A., &Arunkumar, N. (2020). Hybrid optimization with cryptography encryption for medical image security in Internet of Things. *Neural computing and applications*, *32*(15), 10979-10993.
15. González-Zapata, A. M., Tlelo-Cuautle, E., Cruz-Vega, I., & León-Salas, W. D. (2021). Synchronization of chaotic artificial neurons and its application to secure image transmission under MQTT for IoT protocol. *Nonlinear Dynamics*, *104*(4), 4581-4600.
16. Li, Y., Tu, Y., Lu, J., & Wang, Y. (2020). A security transmission and storage solution about sensing image for blockchain in the Internet of Things. *Sensors*, *20*(3), 916.
17. Ramana, S., Bhaskar, N., Murthy, M. R., & Devi, G. R. (2021). A Two-Level Protocol For Secure Transmission Of Image Using IOT Enabled Devices. *Webology (ISSN: 1735-188X)*, *18*(5).
18. Khan, P. W., & Byun, Y. (2020). A blockchain-based secure image encryption scheme for the industrial Internet of Things. *Entropy*, *22*(2), 175.

19. Vien, Q. T., Nguyen, T. T., & Nguyen, H. X. (2021). Deep-NC: A secure image transmission using deep learning and network coding. *Signal Processing: Image Communication*, *99*, 116490.
20. Ravi, R. V., Goyal, S. B., Aggarwal, A., &Bhala, T. (2022). Secure Image Transmission Using 2D ECT and Latin Square Algorithm for IoUT Systems. *Procedia Computer Science*, *215*, 299-308.
21. Li, L., Wen, G., Wang, Z., & Yang, Y. (2019). Efficient and secure image communication system based on compressed sensing for IoT monitoring applications. *IEEE Transactions on Multimedia*, *22*(1), 82-95.