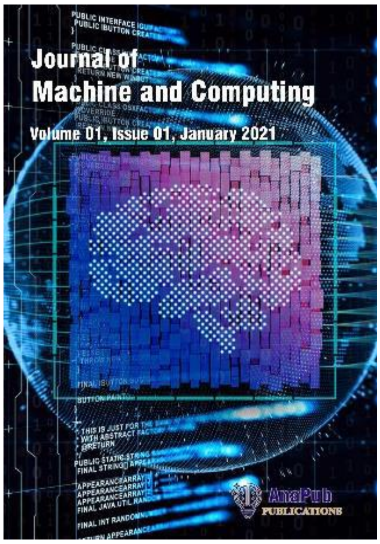
Journal Pre-proof

A Secure Authentication Algorithm for Medical IoT using Steganography and Cryptography



Wubie Engdew Hailu, Ravindra Babu Bellam, KrishnaPrasad B, Sarwani Theeparthi J L, Raghavendra Gowda and Subramanian Selvakumar

DOI: 10.53759/7669/jmc202505032

Reference: JMC202505032

Journal: Journal of Machine and Computing.

Received 31 August 2024

Revised form 30 October 2024

Accepted 27 November 2024

A Secure Authentication Algorithm for Medical IoT using Steganography and Cryptography

[1]Wubie Engdew Hailu, [2]Ravindra Babu Bellam, [3]B. KrishnaPrasad, [4]J L Sarwani Theeparthi, [5]Raghavendra Gowda, [6]Subramanian Selvakumar*

[1,6] Faculty of Computer Engineering, Bahir Dar Institute of Technology, Bahir Dar University, Ethiopia.
[2] Faculty of Computer Science Engineering, School of Electrical Engineering & Computing (SoEEC), Adama Science and Technology University (ASTU), Adama, Ethiopia.
[3]Department of Computer Science and Engineering, Koneru Lakhmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India
[4]Department of Computer Science & Engineering , Aditya University, Surampalem, India
[5]Department of Computer Science and Engineering ,Vardhaman College of Engineering, Shamshabad, Hyderabad ,India

[1] wubieeng21@gmail.com, [2]ravindrababu4u@yahoo.com,
[3]bkrishnaprasad@kluniversity.in,[4]sarwani.theeparthi@acet.ac.in, [5]goudru@gmail.com, [6]sscseau9@bdu.edu.et
Corresponding author : sscseau9@bdu.edu.et

Abstract - The advent of cloud computing and the Internet of Things (IoT) has facilitated the ability of medical practitioners to remotely monitor patients in real-time, thus enabling the provision of healthcare services in the comfort of patients' homes. To streamline this process, it is imperative to keep patient medical data in the cloud. However, storing medical information in the cloud poses a security risk due to the possibility of cyberattacks. As a result, the effective worldwide adoption of intelligent healthcare systems relies on a strong security mechanism. In addition, the use of restricted resources in health devices in IoT-enabled healthcare systems requires the installation of a combination of steganography and cryptography to protect these applications. The amalgamation of steganography and encryption diminishes susceptibilities and poses a formidable obstacle for trespassers attempting to get access to confidential data. This work proposes a security system that utilises the Diffie and Hellman algorithm for secret key sharing, as well as the Least Significant Bit (LSB) steganography principle and Deoxyribo Nucleic Acid (DNA) cryptography for encryption and decryption. The system is implemented using MATLAB 2018a tools. An evaluation is conducted on the encryption time, throughput, Peak Noise to Signal Ratio (PSNR), and Mean Square Error (MSE) of the proposed system. The suggested system has superior security and efficiency compared to the Advanced Encryption Standard and LSB algorithms, as confirmed by the performance evaluation.

Keywords-Authentication, Cryptography, Least Significance Bit, DNA Cryptography, Medical Internet of things, Steganography, One Time Pad

I. INTRODUCTION

Today, the contemporary society is defined by the continuous utilization of technology to enhance the standard of living. IoT refers to technology designed to improve the quality of life (QoL). It facilitates the communication and connection of physical items, people, virtual environments, and information, resulting in the creation of practical environments like smart cities, smart transportation, smart healthcare, and smart energy [1]. The medical industry is anticipated to experience a proliferation of new eHealth IoT devices and applications in the coming years as the widespread adoption of the IoT takes place. Healthcare applications and devices are expected to manage sensitive private information, such as personal healthcare data. Global data networks connect healthcare smart devices, enabling access from anywhere and at any time. Hence, attackers may potentially focus on the healthcare sector. To effectively deploy the Internet of Things (IoT) in healthcare, it is crucial to identify and assess the distinct features of IoT security and privacy. This includes examining security vulnerabilities, needs, countermeasures, and threat models, specifically in the context of healthcare [2]. IoT is primarily designed to handle healthcare and medical care as one of its creative application areas [3]. The Internet of Things (IoT) has the capacity to transform the medical domain by facilitating the creation of diverse applications, such as remote health monitoring, management of chronic illnesses, exercise programmes, and senior care. As a result, a range of medical gadgets, sensors, and diagnostic and imaging devices are often considered to be intelligent things or devices that are an essential part of the Internet of Things. People expect healthcare services to enhance their quality of life. The security problem impacting the IoT environment has recently attracted significant consideration from research experts. To secure this paradigm, we have to consider five dimensions: operating system/firmware, hardware, networking, software and data maintained and generated within the system. Some vulnerabilities of IoT are Deficient physical security, inadequate authentication, insufficient audit mechanisms and unnecessary open ports [4].

II. Related Works

In cryptography, the encryption and decryption processes use either the same key or a different key. The cryptographic system encrypts the information, producing a cypher output that may be incomprehensible to an unintended user without knowledge of the key. Encryption is a widely used technique for ensuring secure data transfer because it offers distinct security advantages. Nevertheless, it causes the covert communications to become incomprehensible and artificial, making them insignificant. These incomprehensible signals often attract the attention of unwanted onlookers [5][28]. Steganography is a technique used to hide data within many types of media, such as text, images, protocols, audio, and video files. Its purpose is to facilitate secure and secret communication by concealing the presence of data[27]. Steganography does not serve as a substitute for cryptography; rather, it strengthens security by using its ability to create uncertainty. A steganographic system conceals information within regular cover media to avoid arousing suspicion from hackers [6], [7]. The study undertaken by Oduguwa and Arabo [3] introduces a practical design and prototype that serves as a feasible option for both password-based and password-less authentication systems, marking a deviation from previous research.

Deoxyribonucleic acid (DNA) Cryptography is the practice of securely hiding data within DNA sequences. It further explains the utilization of DNA as a medium for storing information and the application of contemporary biotechnology as a means to transform plain text into coded text. The properties of DNA are employed for a diverse range of scientific and cryptographic applications. The task of gaining access is tough because of the two layers of security offered by the complexity of biological systems and the computational challenges involved [8].

Presently, a substantial quantity of patients' medical photos and information are conveyed among different entities for examination and assessment by physicians who are geographically scattered. Any unauthorised alteration of this information can lead to inaccurate assumptions and wrong diagnoses. Therefore the safeguarding of patient information and medical data has long been a key issue [9]. Trujillo et al. introduced a comprehensive chaotic encryption method to enhance the security and confidentiality of transmitting medical images from healthcare Internet of Things (H-IoT) devices connected to the Internet via the message queuing telemetry transport (MQTT) protocol [20]. Kamarudin et al. examine the present condition of authentication systems in the Internet of Things (IoT), focusing on recognising patterns and detecting changes [22].

We propose the need for a more efficient cryptographic technique for medical sensors, as current algorithms like AES and RSA demand substantial computational time and memory. We have developed a security solution that protects patient information from attackers by combining DNA cryptography and LSB steganography methods. This method was specifically developed to streamline the delivery of patient information across an unsecured connection. Here the secret medical data is first converted to binary representation; then the values are encoded to DNA bases. Steganography hides the existence of medical information by hiding it in image so it can maintain the integrity of the information. The method of embedding cipher text with image, mechanism of converting binary data to DNA bases and develop security mechanism to medical information are some mechanisms addressed in this paper.

III. System Model

The main objective of this research is to develop security algorithm by joining steganography and cryptography to solve the problem of illegal medical data access.

In this proposed system design, first sender and receiver share one-time pad key using Diffie and Hellman algorithm; the message will be encrypted using DNA Cryptographic algorithm and then the encrypted message (not the plain data) is embedded inside a cover image using LSB steganography. Random generated One-time pad key is used for decrypting and encrypting the medical information. The merging of these two approaches will strengthen the security of the concealed data. Stego images are created by incorporating encrypted data and a cover image. We can convey these images without jeopardizing the confidentiality of the secret data we receive. In addition, the cryptographic decryption process would be required to encrypt the already encrypted data, even if an adversary were able to successfully overcome the steganographic methodology and identify the contents from the stego-object.

A Graphical User Interface (GUI) programme is developed using MATLAB 2018a to streamline the process of sharing keys, encrypting data, and integrating the resulting cypher text into a cover image. The application will retrieve the binary data and present the randomly created OTP key and medical data. Afterwards, the binary data is transformed into DNA bases, namely A, C, G, and T, in order to produce cypher text. The encrypted text is produced using DNA cryptography and then concealed within the cover image using LSB steganography. Finally, a steganographic image will be created and sent to the recipient through an unsecured channel. The proposed architecture mainly consists of the following modules: Key Sharing/Distribution, Secret Key Generation, Encryption Module, Steganography Module, Decryption Module.

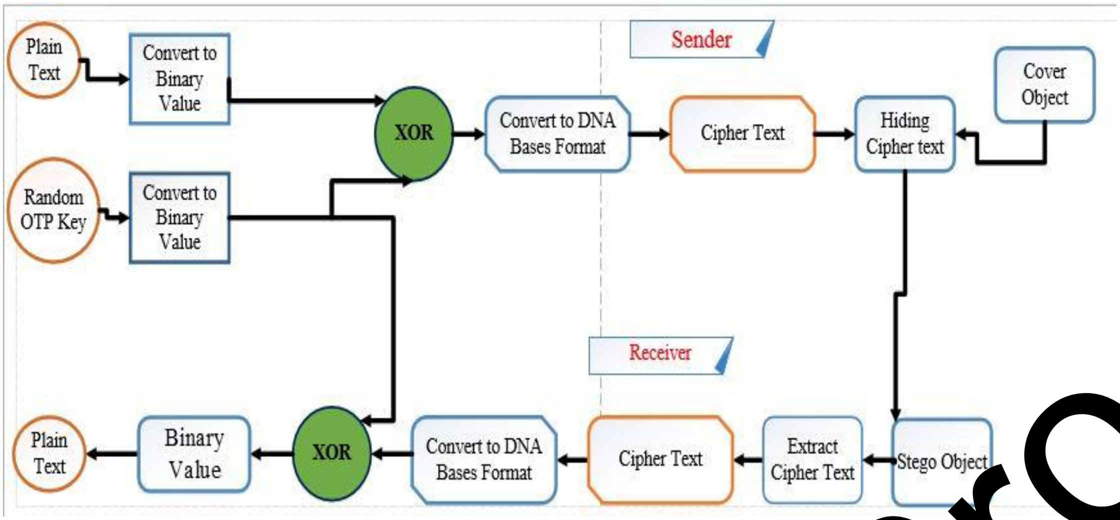


Fig 1. Block Diagram of Proposed System

Due to the unbreakable nature of OTP the proposed work use key for encryption of plain text at the sender and decryption of cipher text at the receiver. In the developed GUI we inserted OTP key manually equal to the length of plain text both for encryption and decryption.

3.1. Steganography Module

Today, digital photographs are omnipresent on the Internet due to their ease of collection and distribution. Therefore, steganography applications commonly use image files, with their specific features depending on the used formats. Since the human eye cannot detect subtle alterations in color or patterns, it is possible to embed text or graphic files into the steganographic image without being perceptible.

The least significant bit (LSB) is the most commonly used method for embedding information in modern digital steganography. This technique is probably the most direct approach for incorporating data into an image, and it is highly efficient [10]. This concealment method is based on the concept that least significant bit (LSB) in an image is unaffected by any alterations or random noise fluctuations in the image. The suggested model utilises the Least Significant Bit (LSB) algorithm to hide encrypted text, and incorporates lossless compression techniques to guarantee the accurate preservation of the original image data. The least significant bit (LSB) of the Red colour is used to determine whether each cypher bit will replace the LSB of the blue or green colour. The embedded message within the cover image can be hidden using the following method:

Convert the cipher text to streams of binary bits
Convert each RGB colors of a pixel to binary bits
XOR each embedded key bit with LSB of Red color
If result is 1
substitute the LSB of Green color with the first bit of the cipher text and
LSB of Blue color with the second bit of cipher text
Else
substitute the LSB of Blue color with the first bit of the cipher text and
LSB of Green color with the second bit of cipher text
Similarly substitute the next bits of the cipher bits

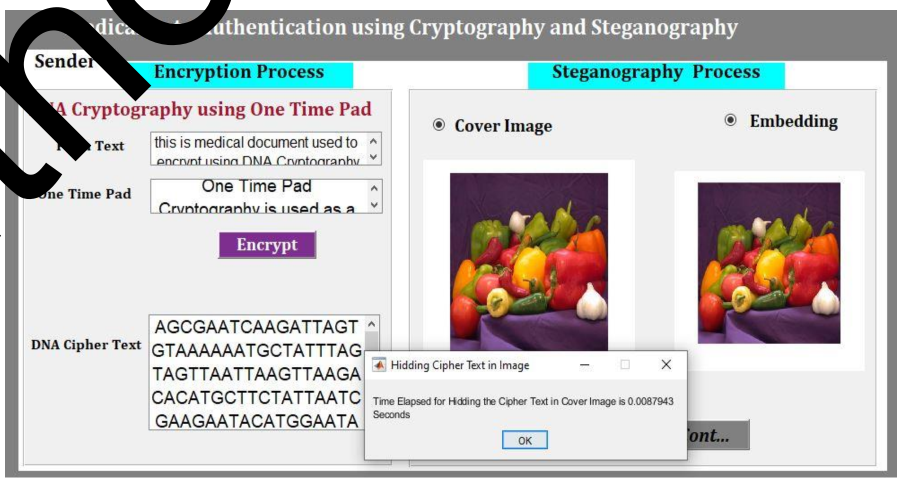


Fig 2. Ciphering and Embedding Process of proposed Algorithm

3.2. Extraction Process

The cipher text is obtained from the stego-image by applying the same key that was used during the embedding process. The embedding procedure is the same as the process of expanding the key and extracting the cypher text from the stego-image. The encrypted text is obtained from the steganographic image that was previously created during the process of embedding, using the identical secret key. To decrypt the cypher text, the user must feed the stego image into the decoding algorithm via the graphical user interface (GUI) together with the secret key. Steganalysis refers to the extraction of plaintext from a stego-image [11]. The data extraction algorithm is the inverse of the ciphering process. To extract encrypted data, one must access the stego-image file and analyze each pixel's RGB color value. The least significant bits (LSBs) of the green and blue channels in the stego-image are extracted until the terminator characters are found, following the established technique. The least significant bits (LSB) that were extracted are added to the array and transformed to a decimal number, representing the binary value of the encrypted message. Every entry in the array, which is 8 bits in size, is transformed into a character and then shown in the text editor. Every entry in the array, which is 8 bits in size, is transformed into a character and then shown in the text editor. Thus, the message that is regained from the image is actually encoded form of the original message. Then data retrieved is then sent to decryption.

3.3. Deciphering Process

The deciphering process employs the same technique as ciphering technique but in opposite direction. The same key used during enciphering process is used to decipher the original plain text. This key will be expanded in the same fashion as the encryption process. But the last expanded block of keys will be used in the first round.

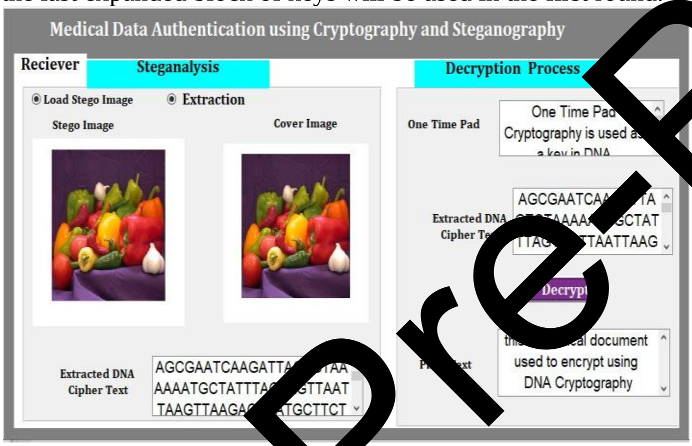


Fig 3. Extractions and Deciphering Process of the New Algorithm

4. Result and Discussion

It is necessary to perform various tests after the completion of the design and implementation of the algorithm to validate its operation. The Functionality test and speed test will be performed on the new algorithm to validate its operation.

4.1. Functionality Test

Functional testing is performed on the designed new algorithm to verify whether it can function as required. The proposed system is implemented using a MATLAB code and a GUI is developed to encrypt a sample of plain text using the one-time pad and then it will be embedded in a true color JPG image file. Using the same key cipher text will be extracted from the stego-Image and then it will be deciphered to retrieve the original plain text. The Figure 4. shows the ciphering and deciphering process. First plain text and cipher text enter by sender, then it is encrypted to DNA cipher. Load cover image and hide DNA cipher with cover image.

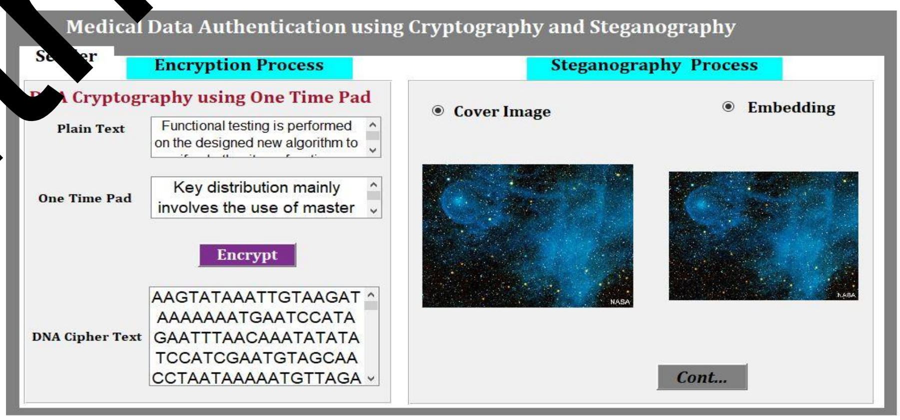


Fig 4. Encryption Functional Test of the proposed system

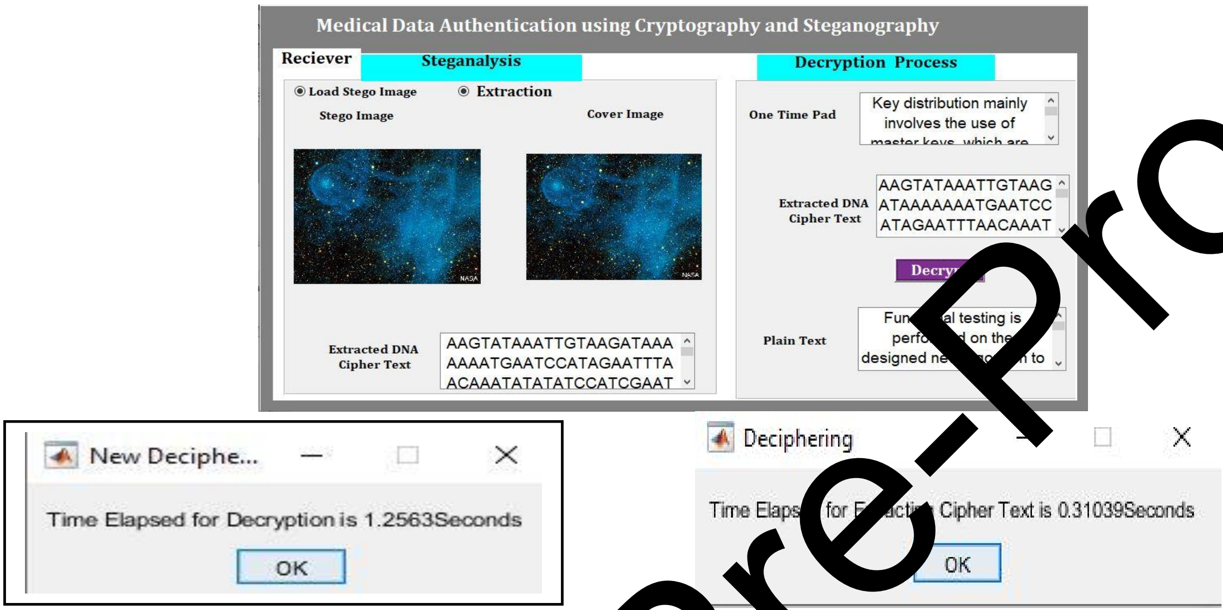
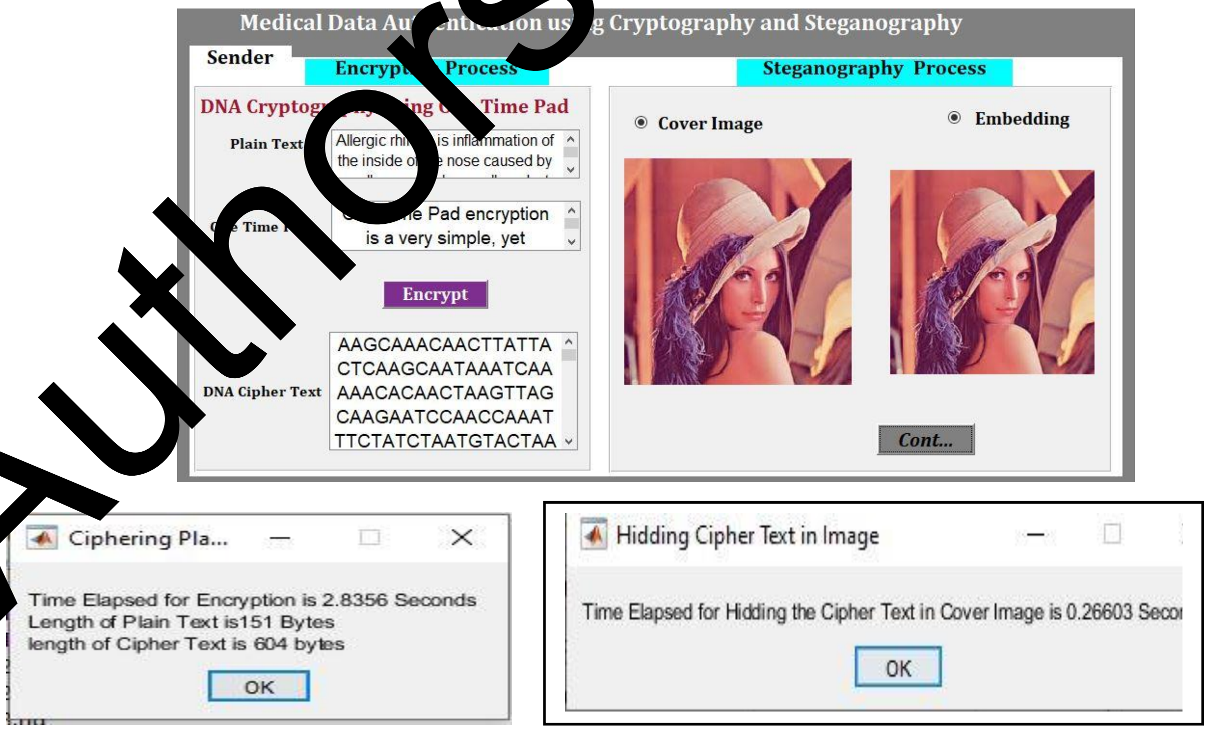


Fig 5. Decryption Functional Test of the proposed system

4.2. Repeated Tests

Repeated test is performed on the designed new algorithm to verify whether it performs as required for different plain texts and one-time pad keys. The functionality test was performed repeatedly for 15 different plain texts with the same one-time pad keys and different keys for each plain text. The encrypted plain text will be hidden into the cover image. Finally, the extracted cipher text from stego-image will be decrypted using the same key and cross checked with the original plaintext.



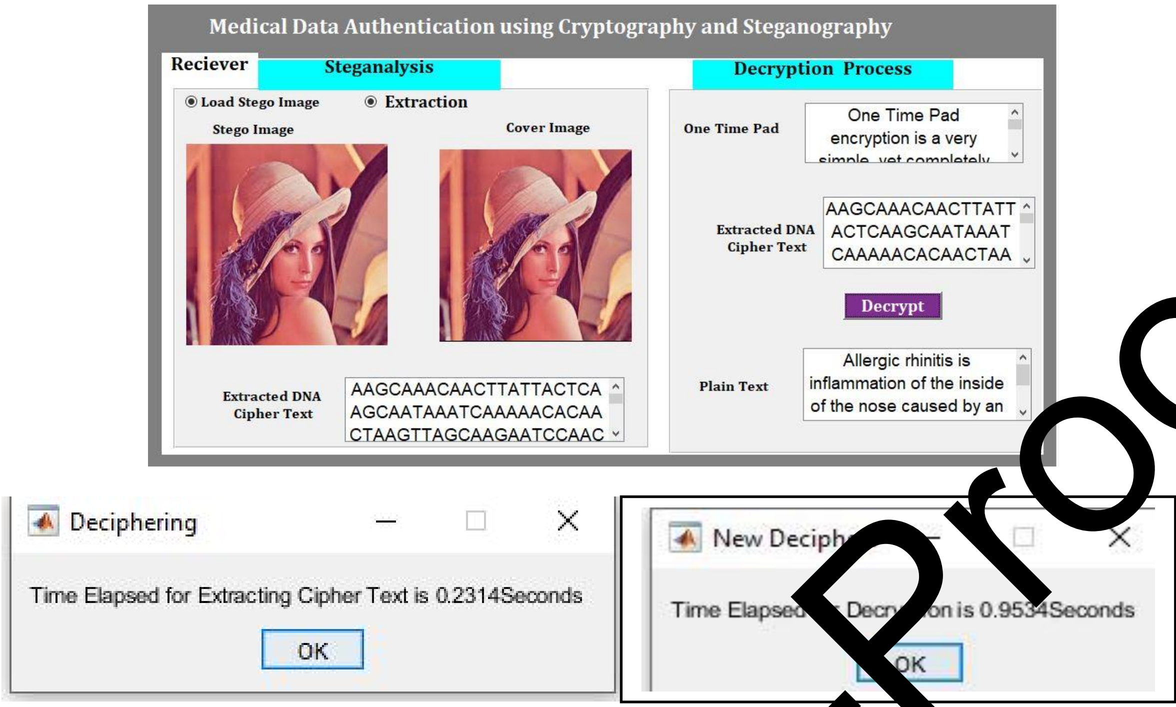


Fig 6. Repeated Functional Testing

4.3. Encryption time

The duration needed by the algorithm to transform regular text into ciphertext is known as encryption time. It is used to measure the encryption speed of the algorithm. The encryption time in most encryption techniques is primarily influenced by the complexity of the algorithm, the size of the plaintext and the secret key. In this proposed system a number of encryption times of the encryption algorithm were collected for different plain text size using the same secret key and then the relationship between size of plain text and encryption time will be analyzed.

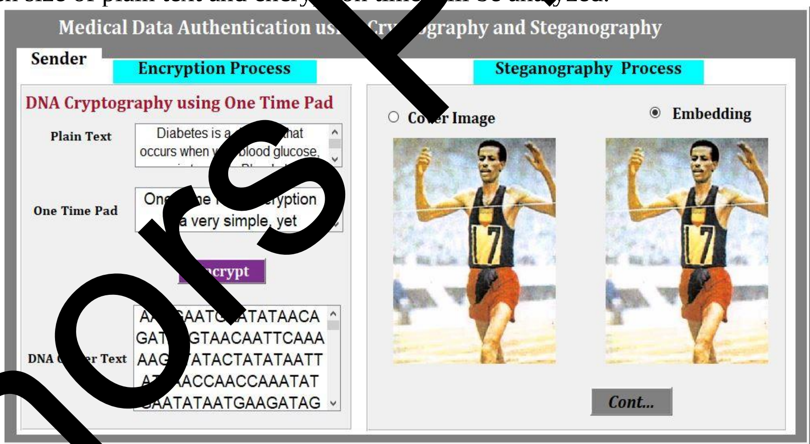


Fig 7. New algorithm Encrypting and Hiding Process

Fig 8. Time elapsed for encryption and Data Size Indicator

The time taken to elapse for encryption and the length of plain text and length of cipher text are located in Figure 9. Figure 9 and Figure 10 depict the encryption and concealment procedure of the data-hiding graphical user interface (GUI), accomplished by employing Advanced Encryption Standard Cryptography and Least Significant Bit of Steganography.

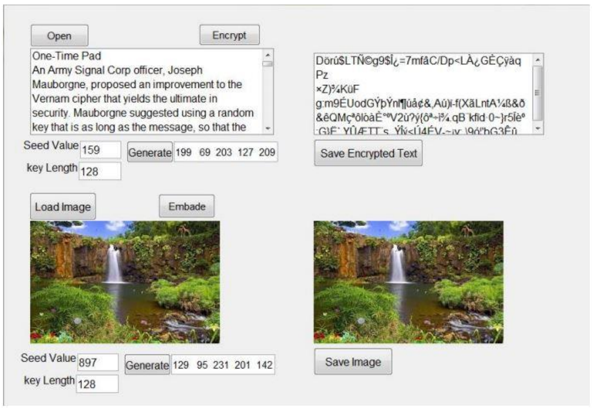


Fig 9. AES- LSB encryption and hiding process

Fig 10. AES-LSB Time, Round Number, And Data Size Indicator

Table 1 shows different encryption times and their respective plain text size of the new proposed system and AES LSB algorithm.

Table 1. Encryption Time Vs. Data Size

	Size in byte	1248	2512	3760	5008	6256	7504	10000
Time in Seconds	New Algorithm	3.29	5.31	[illegible]	[illegible]	11.41	14.33	18.14
	AES- LSB	4.5	7.2	10.1	[illegible]	14.2	16.2	20.5

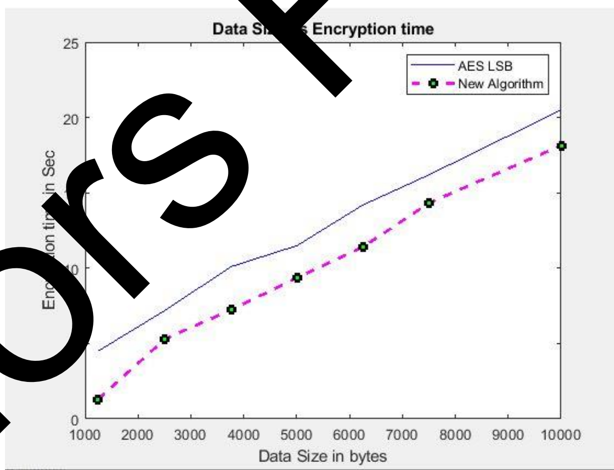


Fig 11. Encryption Time Vs. Size of Encrypted Data

The encryption time of the new proposed is varying at all data size not in uniformity and increasing as data size increases. The encryption time of new algorithm is better than that of AES LSB algorithm. The better encryption time of new proposed system is obtained due to number of rounds used in AES algorithm require much encryption time.

4.4. Encryption Throughput

Encryption throughput is a quantitative measure of the total amount of plaintext that is successfully turned into ciphertext during the encryption process. It functions as a measure of the speed at which the encryption process is happening. Mathematically, it is calculated by dividing the total number of bytes in the plain text that has been converted to cypher text by the length of the encryption process. An established technique for assessing throughput entails the transmission of data from the input (source) to the output (destination). Determine the difference between the initial and final times using the timer. Subsequently,

$$\text{Encryption throughput} = \frac{\text{number of bytes completed}}{\text{encryption time}}$$

Table below shows the effect of the change of plain text size on encryption throughput.

Table 2. *Encryption* Throughput Vs. Data Size

	Size in byte	1248	2512	3760	5008	6256	7504	10000
Throughput	**New Algorithm**	967.44	1087.45	1164.09	1148.62	1156.53	1185.47	1228.50
	AES- LSB	277.33	348.89	372.28	435.48	440.56	463.21	487.80

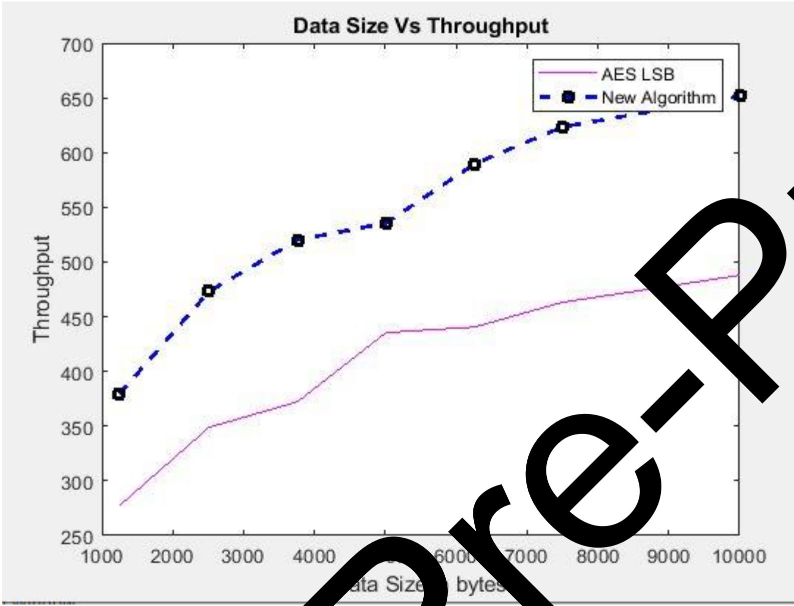


Fig 12. Throughput Vs. Data Size

The above Figure 12 shows throughput of AES LSB and the new proposed system for varying data size. Throughput of the proposed algorithm is greater than that of AES LSB because of the new algorithm encryption time is less than AES LSB. So, more the throughput; more the speed of the algorithm & less will be the power consumption.

4.5. Steganography Encryption Time

The steganography algorithm needs a certain duration to effectively conceal the confidential message within the stego-image. The length of time it takes for the process to complete depends on the complexity of the algorithm, the size of the secret key, and the size of the secret message. The cover image in Table 5.3 has different sizes of embedded encrypted text, and the time it took to encrypt each size was recorded. It is used to measure throughput of the steganography algorithm. The dimension of the image used as a cover image is 800 x 600 pixels.

Table 3. Data Size Vs. Embedding Time

Size in byte	1248	2512	3760	5008	6256	7504	10000
Time in Sec	3.549	4.678	6.867	8.681	9.853	11.214	14.213

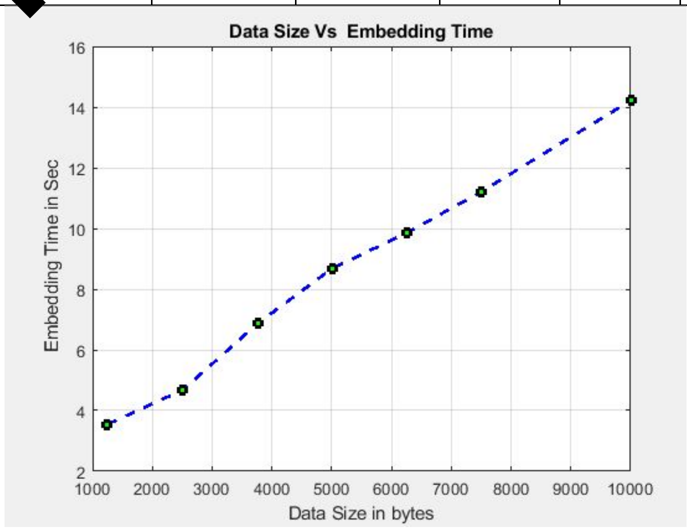


Fig 13. Hidden Data Size Vs. Encryption Time

4.6. Steganography Throughput

It measures the total number of bytes of the secret message successfully hidden to stego-image within a given period of time. It is given by the following formula.

$$Throughput = \frac{number\ of\ bytes\ hidden\ in\ the\ cover\ images}{embedding\ time}$$

Table 4. Throughput vs hidden data size

Size in byte	1248	2512	3760	5008	6256	7504	10000
Throughput	351.65	536.98	547.55	576.96	634.94	669.16	703.59

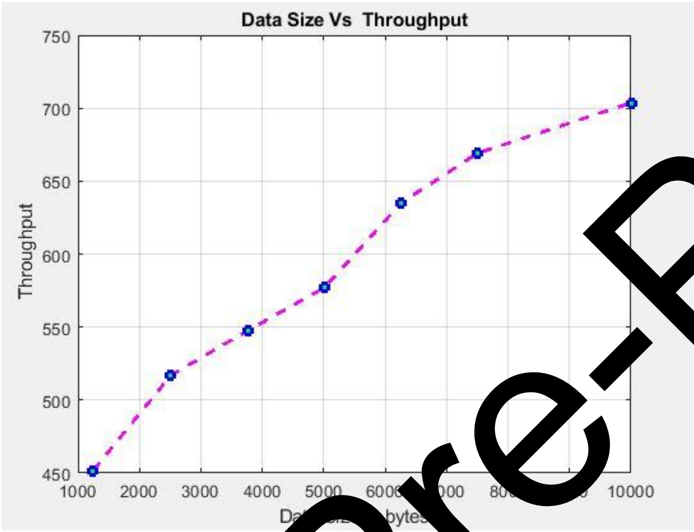


Fig 14. Throughput Vs. Hidden Data Size

In Figure 11. Throughput of hidden data decreased dramatically. The throughput and encryption time are inversely proportional. The reason is that the encryption time is minimum initially at packet size of 1936 bytes.

4.7. Mean Square Error (MSE)

The Mean Square Error is the metric used to measure the difference between the original image and the distorted or chaotic image. Typically, the mean squared error (MSE) will rise as the amount of confidential data grows, leading to a corresponding decrease in the peak signal-to-noise ratio (PSNR). Hence, the trade-off demonstrates that an augmentation in PSNR leads to a reduction in MSE and vice versa. PSNR values below 30 dB suggest a pretty low quality, and the distortion caused by concealment can be easily noticeable. However, it is recommended to utilize the PSNR (Peak Signal-to-Noise Ratio) for assessing the stego-image, with a minimum fidelity requirement of 40 dB [13].
The Mean Squared Error (MSE) is a quantitative measure that assesses the degree of similarity or dissimilarity between two photographs. These findings indicate that photographs of higher quality have a reduced Mean Squared Error (MSE) value and less distortion compared to the original image.

$$MSE = \frac{1}{M \cdot N} \sum_{i=0}^{M} \sum_{j=0}^{N} (x(i,j) - y(i,j))^2$$

Where
M- Total number of rows
N- Total number of columns
(i, j)- (rows, columns)
x- cover Image
y- stego Image

4.8. PSNR (Peak Signal to Noise Ratio) value

The Peak Signal-to-Noise Ratio (PSNR) is a commonly employed metric for assessing the quality of a picture. It is primarily utilised to quantify the imperceptibility of concealed data in stego-images (Shamim & Kattamanchi, 2016). PSNR is a measure of the signal-to-noise ratio, which quantifies the impact of noise on the fidelity of a signal's representation by comparing the maximum power of the signal to the power of the corrupting noise. PSNR is commonly represented using a logarithmic decibel scale (Ali, Sohrawordi, & Uddin, 2019). A greater PSNR value indicates that the reconstruction possesses superior quality. In this case, the noise refers to the error that occurs during the process of embedding, whereas the signal represents the original data.

$$PSNR = 10\ (255 * 255/MSE)$$

Table 5. PSNR value of an Image for Varying Data Size

Size in byte	936	1248	2512	3760	5008	6256	7504	10000
PSNR Value	68.32	66.93	65.35	62.18	60.40	57.92	56.25	53.67

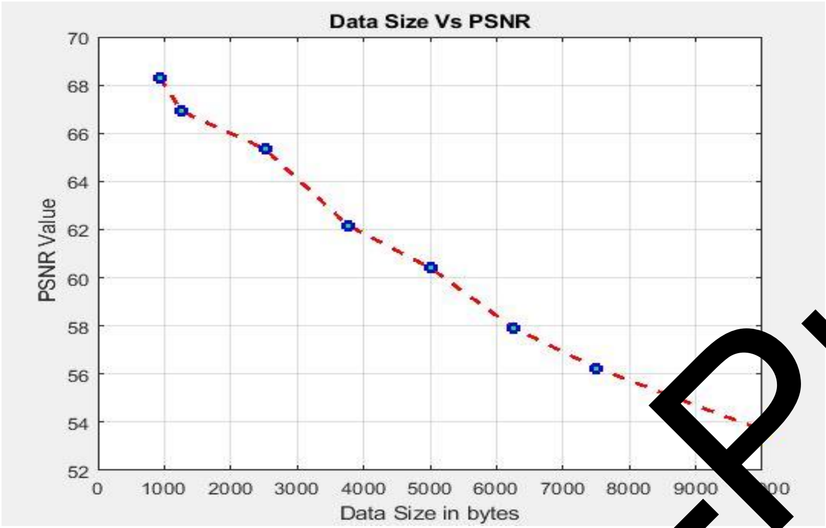


Fig 15. PSNR value Vs. Embedded Data Size

Based on the statistical distortion analysis conducted between cover-image and the stego-image, the result shows that for all plain text sizes in the experiment and different images, the PSNR is above 50db. This proves that the stego-images created by the new developed steganography algorithm have even higher quality. i.e. it produces less perceptual distortion and higher PSNR. Based on Encryption performance and Steganography performance this proposed system is better than existing AES LSB algorithm.

The suggested system utilizes the ideas of steganography and cryptography to guarantee the security of medical data. DNA cryptography is an emerging and highly promising topic within data security. The data is encoded using the binary system, which consists of two numbers, '0' and '1'. Nevertheless, DNA molecules, which serve as the natural carriers of information, encode data using four bases: 'A', 'T', 'G', and 'C'. A small amount of DNA molecules has the capacity to store all the info in the world. The utilization of DNA cryptography, in combination with a one-time pad key, is implemented to augment the security of medical data.

The functional test and repeated tests show that the developed encryption algorithm and steganography algorithm can properly encrypt the plain text and hide the cipher text in cover image. It was tested for different plain texts and different one-time pad keys. The cipher text was embedded in different cover images. Finally, the cipher text was extracted from the stego-image using the developed extraction algorithm and the cipher text is decrypted using the DNA cryptography decryption algorithm. For all cases the decrypted plain text is exactly the same as that of the original plain text.

Now a day a lot of images are transmitted through internet and shared among different peoples through the social network. So, it is possible to transfer valuable information through the internet without giving any clues by imbedding the information in images with very small (acceptable) distortion as shown by the PSNR test. Even if the attackers can be able to extract the information from the image it is encrypted using strong encryption algorithm. The performance of this proposed system measured by encryption time, throughput, and energy consumption are almost better than AES LSB algorithm.

V. Conclusion

Performance analysis is done on the new proposed system to determine how properly the algorithm processes the encryption, decryption and steganography operations based on some predefine analysis metrics. Using these metrics, the cryptographic algorithm will be compared with the existing DNA cryptography algorithm, which is currently accepted as a strong encryption algorithm. The steganography algorithm will be measured using the most common image quality measuring standard PSNR. The performance metrics used to measure and compare the performance of the proposed system are divided in to Encryption Performance Analysis and Steganography Performance Analysis.

References

[1]. N. M. M. AbdElnapi, N. F. Omran, A. A. Ali and F. A. Omara, "A survey of internet of things technologies and projects for healthcare services," 2018 International Conference on Innovative Trends in Computer Engineering (ITCE), Aswan, Egypt, 2018, pp. 48-55, doi: 10.1109/ITCE.2018.8316599.

[2]. Kumar, M., Kumar, A., Verma, S.; Bhattacharya, P., Ghimire, D.; Kim, S.-h., Hosen, A.S.M.S. Healthcare Internet of Things (H-IoT): Current Trends, Future Prospects, Applications, Challenges, and Security Issues. Electronics 2023, 12, 2050.

[3]. Oduguwa, T.; Arabo, A. Passwordless Authentication Using a Combination of Cryptography, Steganography, and Biometrics. Preprints 2024, 2024011466. https://doi.org/10.20944/preprints202401.1466.v1

[4]. Rahimi Moosavi, Sanaz & Nguyen gia, Tuan & Rahmani, Amir M. & Nigussie, Ethiopia & Virtanen, Seppo & Isoaho, Jouni & Tenhunen, Hannu. (2015). SEA: A Secure and Efficient Authentication and Authorization Architecture for IoT-Based Healthcare Using Smart Gateways. Procedia Computer Science. 52. 10.1016/j.procs.2015.05.013.

[5]. Paul, S. P., & Vetrithangam, D. (2023). A Full-Scale Analysis on Challenges and Issues of Next Generation (5G) Communication in Heterogeneous Wireless Network Based Enterprise Applications. Journal of Theoretical and Applied Information Technology, 101(11).

[6]. Jacob, Grasha & Murugan, Annamalai. (2013). DNA based Cryptography: An Overview and Analysis. International Journal of Emerging Sciences. 3. 36-42.

[7]. Liu, Y.; Hao, X., Ren,W., Xiong, R., Zhu, T., Choo, K.-K.R.; Min, G. (2023), A Blockchain-Based Decentralized, Fair and Authenticated Information Sharing Scheme in Zero Trust Internet-of-Things. IEEE Trans. Comput., 72, 501–512.

[8]. Mao,W., Jiang, P., Zhu, L. (2023), BTAA: Blockchain and TEE-Assisted Authentication for IoT Systems. IEEE Internet Things J., 10, 12603–12615.

[9]. Bułat, R.; Ogiela, M.R. (2023), Personalized Context-Aware Authentication Protocols in IoT. Appl. Sci., 13, 4216.

[10]. Tanveer, M., Badshah, A., Khan, A.U., Alasmary, H., Chaudhry, S.A. (2023), CMAF-IIoT: Chaotic map-based authentication framework for Industrial Internet of Things. Internet Things, 23, 100902.

[11]. Ali, F.M., Yunus, N.A.M., Mohamed, N.N., Daud, M.M., Sundararajan, E.A. (2023), A Systematic Mapping: Exploring Internet of Everything Technologies and Innovations. Symmetry, 15, 1964.

[12]. Zhang, Y., He, D., Vijayakumar, P., Luo, M., Huang, (2023), X. SAPFS: An Efficient Symmetric-Key Authentication Key Agreement Scheme with Perfect Forward Secrecy for Industrial Internet of Things. IEEE Internet Things J., 10, 9716–9726.

[13]. Jacob, Grasha & Murugan, Annamalai. (2013). DNA based Cryptography: An Overview and Analysis. International Journal of Emerging Sciences. 3. 36-42.

[14]. Vitthal, Phad & Bhosale, Rajkumar & Archana, Panhalkar. (2012). A Novel Security Scheme for Secure Data using Cryptography and Steganography. International Journal of Computer Network and Information Security. 4. 10.581 jcnis.2012 .06.

[15]. El-Moursy, A & Elmogy, Mohammed & Atwan, Ahmed. (2018). DNA-based cryptography: motivation, progress, challenges, and future. 3.

[16]. Bani Salameh, Jamal. (2019). A New Approach for Securing Medical Images and Patient's Information by using A hybrid System. International Journal of Network Security. 19. 28-39.

[17]. Laskar, Shamim. (2012). High-Capacity data hiding using LSB Steganography and Encryption. International Journal of Database Management Systems. 4. 57-68. 10.5121/ijdms.2012.4605.

[18]. Ansari, Arshiya & Mohammadi, Mohammad & Parvez, Mohammad. (2019). A Comparative Study of Recent Steganography Techniques for Multiple Image Formats. International Journal of Computer Network and Information Security. 11. 11-25. 10.5815/ijcnis.2019.01.02.

[19]. Mehndiratta, A. (2017). Data Hiding System Using Cryptography & Steganography: A Comprehensive Modern Investigation . International Research Journal of Engineering and Technology (IRJET), 397-403.

[20]. D.A. Trujillo-Toledo et. Al., (2023), Real-time medical image encryption for H-IoT applications using improved sequences from chaotic maps, Integration Journal, 90, 131-145, https://doi.org/10.1016/j.vlsi.2023.01.0

[21]. Bułat, Radosław, and Marek R. Ogiela. (2023), "Personalized Context-Aware Authentication Protocols in IoT" Applied Sciences 13, no. 7: 4216. https://doi.org/10.3390/app13074216

[22]. Kamarudin, Nazhatul Hafizah, Nur Hanis Sabrina Suhaimi, Fadilla Atyka Nor Rashid, Mohd Nor Akmal Khalid, and Fazlina Mohd Ali. (2024). "Exploring Authentication Paradigms in the Internet of Things: A Comprehensive Scoping Review" Symmetry 16, no. 2: 171. https://doi.org/10.3390/sym16020171

[23]. Shalini Dhar, Ashish Khare, Ashutosh Dhar Dwivedi, Rajani Singh, (2024) Securing IoT devices: A novel approach using blockchain and quantum cryptography, Internet of Things, 25, https://doi.org/10. 6/j.iot.2023.101019.

[24]. Hashim, Mohammed Mahdi, Suhad Hasan Rhaif, Ali Abdulwahhab Abdulrazzaq, Adnan Hussein Ali and Mustafa Sabah Taha. (2020) "Based on IoT Healthcare Application for Medical Data Authentication: Towards A New Secure Framework Using Steganography." IOP Conference Series: Materials Science and Engineering, 81

[25]. Y. Jiang et al., "Secure Data Transmission and Trustworthiness Judgement Approaches Against Cyber-Physical Attacks in an Integrated Data-Driven Framework," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 52, no. 12, pp. 7799-7809, Dec. 2022, doi: 10.1109/TSMC.2022.3164024.

[26]. Dhawan, S., & Gupta, R. (2020). Analysis of various data security techniques of steganography: A survey. Information Security Journal: A Global Perspective, 30(2), 63 https://doi.org/10.1080/19393555.2020.1801911

[27]. Zekrifa, D. M. S., Saravanakumar, Nair, Pachiappan, K., Vetrithangam, D., Kalavathi Devi, T., ... & Rukmani Devi, S. (2024). Securing energy horizons: Cloud driven based machine learning methods for battery management systems. Journal of Intelligent & Fuzzy Systems, (Preprint), 1-15.

[28]. Neshenko, N., B Harb, Crichi o, J., Kaddoum, G., & Ghani, N. (2019). Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. IEEE Communications Surveys & Tutorials, 21, 2702-2733.