# MODEL FOR SECURE TRANSMISSION OF MEDICAL TELEMONITORING DATA USING CRYPTO-STEGANO TECHNIQUES

Elizabeth Adedoyin AMUSAN[1], Oluwaseun Modupe ALADE[2], Justice Ono EMUOYIBOFARHE[3]
[1,2]Department of Cyber Security Science, Ladoke Akintola University of Technology, Ogbomoso, Nigeria
[3]Department of Information Systems, Ladoke Akintola University of Technology, Ogbomoso, Nigeria
[1]eaadewusi@lautech.edu.ng, [2]oalade75@lautech.edu.ng, [3]eojustice@gmail.com

Keywords: cryptography, healthcare, security, steganography, medical tele-monitoring

Abstract*: This research proposes a hybrid security model for the secure transmission of patients' health data in telemonitoring systems, integrating cryptography and steganography. This dual-layer defense safeguards patient health data effectively. However, specifying the application point within the telemonitoring system—comprising data collection, transmission, and storage stages—allows for a focused, efficient, and tailored implementation of security measures based on each stage's unique characteristics. The proposed technique utilizes Hill Cipher for cryptographic processes, incorporating secure key exchange. Steganography employs LSB image steganography to conceal encrypted data within a randomly chosen image. The embedded data can be retrieved using steganographic techniques and decrypted at the receiver's end with Hill Cipher decryption using a private key. This crypto-stegano technique proves effective in mitigating security concerns, offering a promising solution for safeguarding confidential medical information during telemonitoring data transmission.*

## 1. INTRODUCTION

The advent of the Internet and Internet-enabled applications (IoT), mobile wireless communication (mobile), and all other related enabling technologies have served as a platform for various information and communication technologies (ICT) service deliveries which have now resulted in the "e" (electronic) and "m" (mobile) computing paradigms. These paradigms have become the major drivers in business (as in e-business, e-commerce), banking (m-banking, e-banking), healthcare (e-health, m-health, telemedicine) and education (e-learning), etc. ICTs are at the core of the transformation of conventional, paper-based healthcare to ubiquitous healthcare providing anytime and anywhere access from any device which consequently results in considerable cost-savings and improved patient outcomes [1].

Tele-monitoring is a subset of tele-health which is an umbrella term for the set of activities connected with health, services, and methods which are remotely executed with the use of ICTs [2]. Tele-monitoring, also known as remote patient or healthcare monitoring, expands the usefulness of telemedicine by, at first, treating patients with chronic conditions and diseases by monitoring day-to-day health so that preventive and emergency care can be delivered as needed. A typical tele-monitoring system has three (3) tiers. The first is a set of physiological sensors that discern vital signs of interest and a data hub to gather same. Tier two is usually a heterogeneous network, functioning as the communication channel/infrastructure, while the third is a remote central server for storage.

Figure 1 illustrates a typical tele-monitoring system which entails continuous monitoring and transmission of data in form of vital signs like heart rate, blood pressure and any other measurement of interest to a physician/healthcare giver.

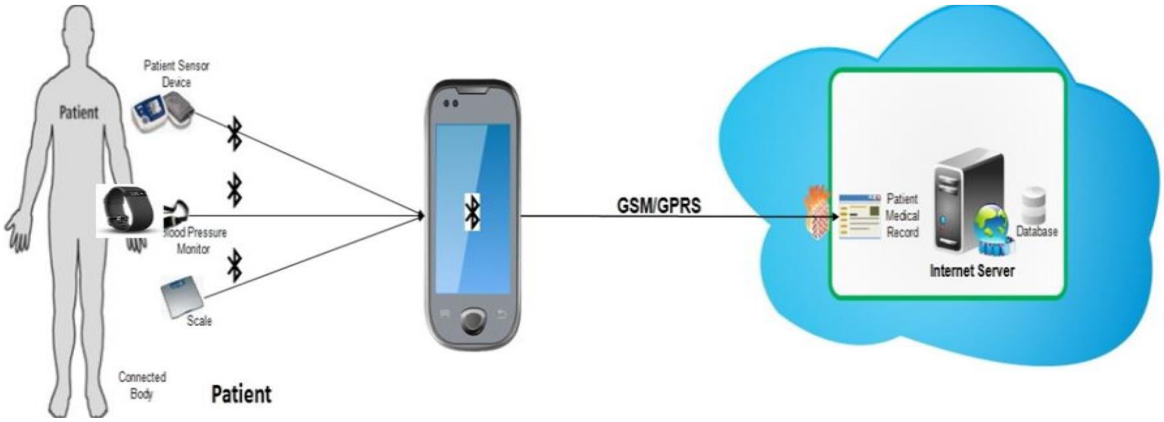


*Fig. 1 A typical health monitoring system [3]*

Since tele-monitoring systems are actualized by emerging and enabling technologies (such as IoT, mobile wireless communication, cloud computing) to improve accessibility, efficiency, availability and quality of healthcare services, they are nevertheless, vulnerable to a myriad of security attacks [4,5]. The benefits will only be achieved, however, if patients are confident in the privacy of their health-related information and if healthcare providers are confident in the security of the data gathered [6]. Any telemedicine system must be secure enough so as to gain the trust and reliability of its users [7]. Cybercriminals take advantage of the susceptibilities associated with ICTs to cause breaches in these systems at all levels. The three-tiered composition of a remote health monitoring system naturally classifies these security threats into three levels depending on their emerged level of occurrence which are: the data collection level, transmission level and the data storage level [8].

Cryptography provides a means of securing data by encryption. Encryption is the art and science of converting plaintext or message into scrambled form using various symmetric and asymmetric algorithms while steganography is the science of hiding information in communication through an innocuous carrier in an effort to conceal the existence of data from unauthorized access. Cryptography is the art of secret writing and steganography is the art of hidden communication. In other words, cryptography scrambles a message so that it cannot be understood and steganography hides the message so that it cannot be visualized [9]. In most cases, sending encrypted data over wireless channel may draw attention; hence, steganography has been used to enhance data encryption systems. The combination of both sciences through stegano-cryptographic modeling technique for secure data transmission is conjectured for better patients' data protection and preservation of its integrity from unauthorized access during transmission.

To this end, we analyzed the security and privacy threats plaguing the tele-healthcare system and then proposed the design of a secure data transmission model for a medical tele-monitoring system using a combination of cryptography and steganography techniques. The rest of this paper is organized as follows: Section 2 describes more explicitly; the security threats which healthcare systems are vulnerable to; section 3 examines the theoretical background by exploring hill cipher cryptography and image steganography followed by a brief review of related works; a design of the proposed crypo-stegano model and metrics for evaluation are presented in section 4 while section 5 concludes and establishes direction for future work.

## 2. ATTACK LANDSCAPE IN TELE-MONITORING SYSTEMS

Based on the architecture of a typical tele-monitoring system, such systems are susceptible to three (3) broad classes of security attacks as follows and as shown in Figure 2:

**a) Attacks at data collection level**

These attacks may cause several threats to data collection level such as altering information, dropping some important data, or resending data messages.

**Jamming Attack**: this relates to invasion of the attacker's radio signal with frequencies of the BAN (Body Area Networks). The consequence of this is isolation and prevention of sensor node within the range of the attacker signals from sending or accepting any message as long as the jamming signal continues [10].

**Data Collision Attack**: this happens as two or more nodes try to transmit at the same time. When a collision occurs and results in a modification of the frame header, the error-checking mechanism on the receiving end recognizes this alteration as an error, leading to the rejection of the received data. This is a huge threat to the availability of data in a body area network.

**Data Flooding Attack**: in this case, the attacker employs a repetitive strategy of broadcasting numerous connection requests to the victim node until the victim's resources are completely exhausted, thereby pushing them to their maximum capacity [11].

**Desynchronization Attack:** in this type of attack, the attacker tampers messages between sensor nodes by copying it many times using a fake sequence number to one or both endpoints of an active connection, which leads the WBAN to an infinite cycle, resulting in causing the sensor nodes transmits massages again and wastes their energy [8].

**Spoofing Attack**: this is a situation where the attacker targets the routing information to perform several disruptions such as spoofing, altering, or replay the routing information, leading to complicate the network by creating routing loops [12].

**b) Attacks at transmission level**

These pose several threats to transmission level such as spying, altering information, interrupting communication, sending extra signals to block the base station and networking traffic.

**Eavesdropping of Patient's Medical Information**: tele-monitoring systems will record patient's health data from BANs to be transmitted to the healthcare providers. Eavesdropping is a prevalent attack method for gathering information from biomedical sensors [13]. In passive eavesdropping, malicious actors listen to transmitted messages to detect sensitive information [14, 15]. Active eavesdropping involves attackers actively collecting data by sending multiple queries [16]. Attackers may also physically locate and intercept targeted hardware, such as intercepting vital signs during transmission [17]. The collected data can be used for various attacks, including fingerprinting. Active eavesdropping can exploit vulnerabilities in unsecured networks to disrupt communication between entities, such as sensor nodes or smartphones, without consent. Eavesdroppers aim to obtain critical medical data, which may be used for masquerading as the legitimate user. Some unskilled developers can easily build systems with the ability to spy on the patient's data through wireless technology.

**Man in the Middle Attacks**: the attacker intercepts a communication between the end points and exchange messages between them. The communication is completely controlled by the attacker enable him being able to read, insert and modify the data in the intercepted communication.

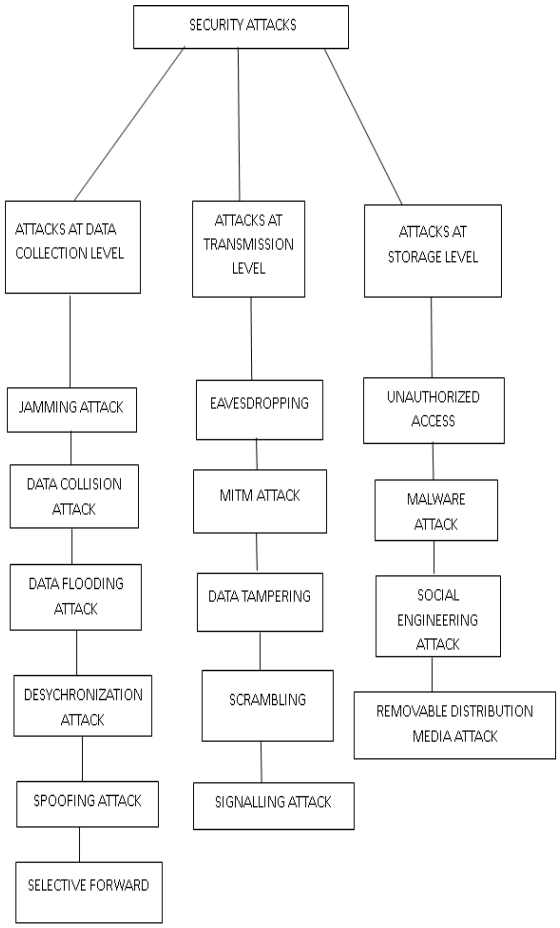


*Fig. 2 Security threats in tele-monitoring systems*

**Data Tampering Attack:** this is when a tampering attacker may damage and replace encrypted data by authorized network nodes. Any unauthorized alteration of data within the system is classified as a tampering attack. This form of attack encompasses actions like attaching external devices to manipulate data and sabotaging sensors, particularly during emergencies. Tampering attacks compromise both data confidentiality and integrity. To mitigate such threats, security measures can include combining symmetric keys with facial recognition technology or employing keyless methods, as suggested by studies [18-21].

**Scrambling Attacks:** is a kind of jamming attack on radio frequency for short intervals of time during transmission of control or management information WiMAX frames to affect the normal operation of the network. It interrupts communication that can prevent the patient's smartphone from sending data causing availability issue [22].

**Signaling Attacks**: Before patient's smart phone starts to transmit data, there is some preliminary signaling operation need to be performed with the serving base station. Signaling operations contain authentication, key management, registration, and IP-based connection establishment. The attacker can initiate a signaling attack on the serving base station by actuating extra state signals that block the base station. Thus, the excessive load on the base station results in DoS attacks, and the patient's smart phone cannot send data due to base station unavailability [8].

**c) Attacks at storage level**

These attacks may cause several threats to storage level such as modifying patient medical information or changing the configuration of system monitoring servers.

**Inference Patient's Information**: Attackers try to combine authorized information and combine them with other available data, which leads them to identify sensitive patient data such as diseases. Thus, patient's data should be anonymous to cover their identities or data before publishing/posting the data [23].

**Unauthorized access of Patient Medical Information**: this type of attack can take place by unauthorized individual without valid authentication, so patient's data will be accessed then it might cause problems such as damaging significant data. Thus, it is necessary to protect patient privacy against breaching, capturing, and misusing by unauthorized users.

**Malware Attack:** This type of attack has the ability to infect and propagate to the whole server that can cause unavailability and disruption, making system configuration unstable, resulting in system malfunctioning and communication interruption. Telemonitoring systems face various malware threats, such as botnets, backdoors, spyware, viruses, worms, and Trojans [24]. Malware attacks exploit vulnerabilities, spreading automatically through networks [25-27]. These attacks not only jeopardize the integrity and confidentiality of data but can also lead to server shutdowns via Distributed Denial of Service (DDoS) attacks. Successful malware infiltration may open backdoors, allowing unauthorized access to medical records, disclosure of patient information, or even deletion of data [28,29]. Attackers can exploit security gaps to deny access to telemonitoring devices, compromising their reliability, accuracy, and privacy. Additionally, firmware or software manipulation can result in the destruction of medical records or the compromise of telemonitoring system functionality.

**Social Engineering Attacks**: in this type of attack, a third-party attacker can gain access to the system by fooling either the patient or authorized user to access the information. Here, authorized users can also disclose patient's data to concerned parties such as Health Insurance Company for unethical personal intends.

**Removable Distribution Media Attack**: In this type of attack, it is possible to theft or loss computer or data storage medium, such as a USB flash drives, can be used to steal information and to propagate viruses in a healthcare monitoring system [8].

## 3. THEORETICAL BACKGROUND AND REVIEW OF RELATED WORKS

This section explores the two techniques of Hill Cipher Cryptography and Steganography followed in this research and also attempts a review of some related works.

### 3.1 Hill Cipher Cryptography

Hill Cipher Cryptography is a technique to protect data through the use of keys and it was created in order to generate a cipher that cannot be solved using frequency analysis techniques. It does not replace each of the same alphabets in plaintext with the same alphabet in ciphertext because it uses matrix multiplication by encryption and decryption [30]. The Hill cipher algorithm has been adjudged as one of the symmetric key algorithms that have several advantages in data encryption [31].

The basis of the Hill Cipher technique is modulo arithmetic to the matrix. In its application, Hill Cipher uses matrix multiplication techniques and inverse techniques for matrices. The key to Hill Cipher is the matrix n x n with n is the block size. The Hill cipher is also a block cipher, so, theoretically, it can work on arbitrary sized blocks. It works on multiple alphabets at the same time.

Hill cipher works as follows:

1. Assign the number to each alphabet in plain text. A = 0, B= 1….z = 25
2. Organize the plain text message as a matrix of numbers based on the above step in number format. The resultant matrix is called a plain text matrix.
3. Multiply the plain text matrix with a randomly chosen key. Note that the key matrix must be the size of n x n where n stands for the number of rows in a plain text matrix.
4. Multiply both matrices, (step 2 and step 3).
5. Calculate the mod 26 value of the above matrix, (matrix results in step 4).
6. Now translate the numbers to alphabets (0 =A, 1 =B).
7. The result of step 6 becomes the cipher-text.
8. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.

### 3.2 Steganography

Steganography is the technique in which the secret information or data is hid in such a way that its presence cannot be noticed. An intruder should not even know that a hidden information is present or not, which is the reason steganography is known as covered writing [32, 33]. Steganography is characterized by three main components which are: the message, the carrier and the password. The message is the secret text, image, video or the audio that needs to be protected through the technique of steganography [32]. The carrier is the medium through which the secret message is transferred. The password is the stego-key that protects the secret data. Usually, steganography is classified as text, audio/video or image and the most popular of all three is the image steganography in which images are used as the cover pages.

Image steganography is further divided into spatial domain image steganography and frequency domain image steganography. The former is the type of image steganography in which the data is directly embedded and hidden into images while in the latter, the frequency of the image is changed before data is embedded in it. The former uses the technique of Least Significant Bit which is much easier than the other method of steganography [34].

**Least Significant Bit (LSB) Image Steganography**

Least Significant Bit **(**LSB) is a common technique for embedding and extracting secret information to the cover image using the spatial domain of Image steganography techniques. In this algorithm least significant bit (very right bit or 8th bit of a pixel) is altered with the hidden message's bit. This bit can be thought of as redundant since its change will not be realizable with human eyes. LSB works as follows:

1. Convert the image to greyscale
2. Resize the image if needed
3. Convert the message to its ASCII value format
4. Convert ASCII value to 8-bits binary format
5. Initialize output image same as input image
6. Traverse through each pixel of the image and do the following:
    a) Convert the pixel value to binary
    b) Get the next bit of the message to be embedded
    c) Create a variable temp
    d) If the message bit and the LSB of the pixel are same, set temp = 0
    e) If the message bit and the LSB of the pixel are different, set temp = 1

f) This setting of temp can be done by taking XOR of message bit and the LSB of the pixel
g) Update the pixel of output image to input image pixel value + temp

7. Keep updating the output image till all the bits in the message are embedded.
8. Finally, write the input as well as the output image to local system.

### 3.3 **Related Works**

[35] developed a consent-based access control (CBAC) mechanism for healthcare systems. This is an authorization initiated by a patient for an intended data requester via an agreement between them. After obtaining the consent from the patient, a healthcare organization can gain access to the data, which is encrypted by a healthcare provider. This is achieved by a cryptographic primitive: conditional proxy re-encryption. With this, patient medical data is protected against access of unauthorized parties, including public data center.

A patient's diagnostic data transmission model using both color and gray-scale images as a cover carrier for healthcare based IoT environment has been proposed by [36]. The model engaged either 2D-DWT-1L or 2D-DWT-2L steganography and hybrid blending cryptographic techniques. The experimental results were evaluated on both color and gray-scale images with different text sizes. The performance was statistically evaluated.

[37] developed a block-chain-based electronic medical record access control research scheme based on the role-based access control model. Appropriate access control strategy was adopted to solve the leakage problem of the user's medical privacy information during the access process. Then, the information entropy technology was used to quantify the medical data, so that the medical data can be effectively and maximally utilized.

In [9], a hybridized approach of information security was developed for wireless communication by mixture of cryptography and steganography. They reported that the concept of differential and integral calculus has improved the encryption and decryption of information and discrete cosine transform (DCT) also increased the quality of stego-image.

[32] proposed a model of enhancing medical data security by combining the two techniques of elliptical curve cryptography (ECC) and steganography. ECC, an algebraic structure of elliptic curves over finite fields, was considered as a desired choice for being public key. With the use of both techniques, the private and secret information would be encoded then hid in a much better way and obscures medical information from a person which is not authorized to get access.

[38] examined various research studies to explore the use of intelligent techniques in health systems especially as it bothers on security and privacy issues in the current technologies. Their work highlighted both cryptographic and non-cryptographic approaches that have been used to ensure the preservation of security and privacy of health data and concluded that appropriate security solutions should be developed and maintained to protect cloud-based health information.

[39] opined that Cyber security has not gotten enough attention in the healthcare sector, despite being crucial for patient safety and a hospital's reputation and therefore, highlighted its importance, recommending cutting-edge cyber security tools, techniques and strategies to combat cyber-attacks.

In [40], the authors combined Hill cipher and LSB steganography to secure data and reported that Hill cipher needed extra security, leading to the adoption of LSB steganography. The system was evaluated using PSNR, MSE and computation time. Results indicated a minimum PSNR of 51.2907 dB, signifying good image quality. Computation time for encrypting 2000 and 6000 characters was efficient in Matlab.

Hill cipher and LSB was also utilized by [41] to encrypt text messages involving 95 characters. The encrypted message is then embedded into digital image using LSB. Quality assessment utilized 10 images of varying dimensions, along with diverse text message lengths, with MSE and PSNR values calculated.

Similarly, the work of [42] explored file encryption and security through Hill Cipher cryptography and steganography, specifically using the LSB + 1 method. The research involved testing the security applications of

cryptographic and steganographic data, particularly with the Hill Cipher method. The trial results focused on displaying data in the form of files, emphasizing data security.

Arising from the related works reviewed, the integration of cryptography and steganography emerges as a potent dual-layer defense for safeguarding patient health data. However, it is crucial to specify the application point within the telemonitoring system which typically is comprised of three stages: data collection, data transmission, and data storage. This is a strategic decision that allows for a more focused, efficient, and tailored implementation of security measures, considering the unique characteristics and challenges of that particular stage in the system. To this end, this research specifically targets the transmission stage of the telemonitoring ecosystem by designing a hybridized model to ensure secure transmission of healthcare information using both cryptography and steganography to improve the confidentiality, integrity and availability of health records in a remote health care system.

## 4. METHODOLOGY- The Model Design

This section presents the design of the proposed method in this research which combines Hill Cipher algorithm for encryption (Cryptography) and Least Significant Bit (LSB) Image steganography (Steganography). Steganography and cryptography have been noted to be individually insufficient for robust information security; therefore, a more reliable and strong mechanism can be achieved by combining both techniques which provides a measure of layered information security that meet the requirements for data transmission over communication channels. Figure 3 presents a block diagram strategy for the combination of both techniques. Figure 4 is the design of the crypto-stego based access control model and is described as follows: The proposed crypto-stegano process for securing medical data intricately combines cryptographic encryption with steganography to protect sensitive medical information during transmission. Initially, medical personnel encrypt the secret data using the Hill Cipher cryptosystem, converting it into ciphertext for security. This ciphertext is then embedded within a seemingly innocuous cover image through the least significant bit (LSB) steganographic method, creating a stego image that appears unchanged to the untrained eye but secretly contains the encrypted data. This stego image is transmitted to the intended recipient, typically a medical professional or system administrator, who can then extract and decrypt the embedded ciphertext using a private key, thereby accessing the original confidential medical information. This dual-layered security strategy, leveraging both encryption and steganography, offers a robust defense against unauthorized access and enhances the confidentiality and integrity of medical data in telemonitoring systems.

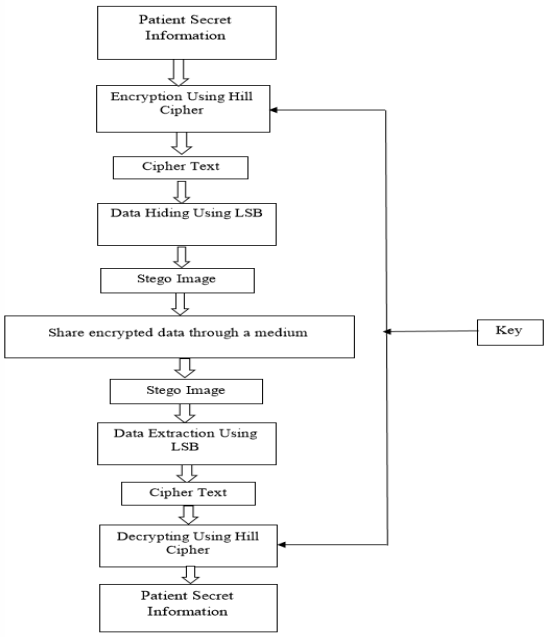


*Fig 3 Block diagram of the proposed system*

The methodology entails two main steps to secure medical data in text format stated as follows.

a) The first step will accept the patient data in plain text format as input and encrypt the plain text using Hill Cipher to generate cipher text as output. This step requires a key known as the secret key.

b) The second step will accept the output from the first step as input and embed it in a cover image using LSB to generate an output with the image called stego image.

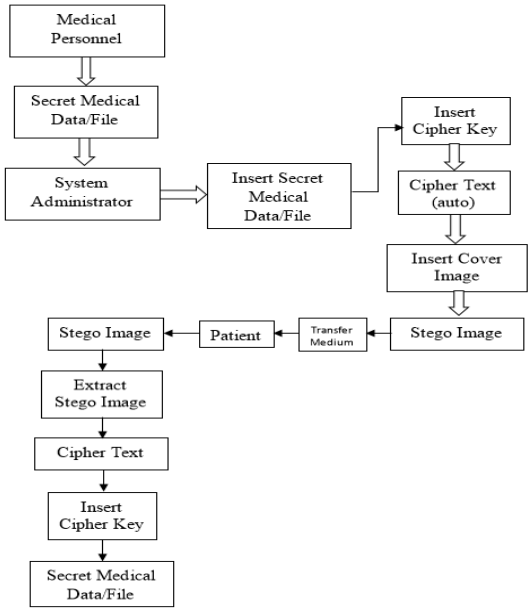


*Fig 4 The designed model*

To retrieve the secret data for the stego image, the steps involved are:

a) The first step to retrieve the secret data is to extract the cipher text from the stego image.

b) The second step to extract the secret data is to decrypt the cipher text using Hill Cipher algorithm. This step requires a secret key which corresponds to the key used during encryption.

## 5. PERFORMANCE EVALUATION OF PROPOSED HYBRIDIZED MODEL

The following performance metrics must be satisfied by the model before it can be concluded that the proposed model is efficiently improved from the existing systems.

1. **The Mean Square Error (MSE):** represents the cumulative squared error between the stego image and the original image which were calculated using equation (1).

$$\text{MSE} = \frac{\sum_{M_1N}[I_1(M_1N) - I_2(M_1N)]^2}{M*N} \qquad (1)$$

Where $I_1(M_1N) - I_2(M_1N)$ are origin image and generated optimal stego-image respectively and M x N represent the number of rows and columns in the images.

2. **Peak Signal to Noise Ratio (PSNR):** It is measured in decibels (dB). PSNR calculates the invisibility of the image by assessing the quality of the stego image. If PSNR of gray scale image larger than 36 dB then the human cannot distinguish between the cover image and the stego image. The PSNR of the system using different images would be calculated using equation (2).

$$PSNR = 10log\frac{I^2}{MSE} \qquad (2)$$

Where I represent the maximum possible value of the pixel in the image (e.g., for a gray-scale image the maximum value is 255) and MSE is the mean square error.

## 6. CONCLUSION AND FUTURE WORK

Health data should be safe and secure from unauthorized access during transmission as its integrity assists physicians to provide proper treatments. To ensure proper access control, this research highlighted the security attacks in healthcare systems and explicitly categorized them into three types depending on the emerged level in the healthcare system. These attacks may cause several threats such as altering information, dropping some important data, interrupting communication, or sending extra signals to block the base station and increasing networking traffic. Next, we presented and discussed a hybrid access control security model which combines cryptography and steganography where both methods are combined by encrypting message using cryptography and then hiding the encrypted message using steganography. The resulting stego-image can be transmitted without revealing that a secret information is being exchanged. Furthermore, even if an attacker were to beat the steganographic technique to discover the message from the stego-object, he/she would still need the cryptographic decoding key to decipher the encrypted message. Using only one of these techniques will render the electronic patient monitoring system susceptible to attacks, hence, the combination of both provide more security and robustness. In the nearest future, the designed model would be implemented for a secure medical tele-monitoring system using appropriate software process models with the capacity to guarantee confidentiality, integrity and privacy in developing country like Nigeria where the issue of digital divide is of significant

concern. Also, the envisioned model has the potential to be leveraged for audio and video (multimedia) health data transmission.

## 7. REFERENCES

[1]. Zeadally S., Isaac J. and Baig Z. "*Security Attacks and Solutions in Electronic Health (E-health) Systems*". Journal of Med Syst 40:263, pp. 262-273. DOI 10.1007/s10916-016-0597-z. 2016.

[2]. Marquez, Astudillo and Taramasco, "*Security in Telehealth Systems from a Software Engineering Viewpoint: A Systematic Mapping Study"*. IEEE Access, *Digital Object Identifier 10.1109/ACCESS.2020.2964988*. 2020.

[3]. Amusan E.A., Emuoyibofarhe O.J. and Arulogun O.T., "*Development of a Medical Tele-Management System for Post-Discharge Patients of Chronic Diseases in Resource-Constrained Settings"*. International Journal of Bio-Medical Informatics and e-Health, ISSN:2321-9017, 6(4): 1-12.2018.

[4]. Chen H., Wang J., Dong X. and Zhao C., *"Security design of ECG telemonitoring systems"*. International Conference on Computer Engineering and Application (ICCEA), IEEE. pp.707-711. DOI 10.1109/ICCEA50009.2020.00154. 2020.

[5]. Alsemmeari, R.A.; Dahab, M.Y.; Alsulami, A.A.; Alturki, B.; Algarni, S., "*Resilient Security Framework Using TNN and Blockchain for IoMT*". Electronics, 12, 2252. https://doi.org/10.3390/electronics12102252. 2023.

[6]. Kotz D., Gunter C.A., Kumar S. and Weiner J.P., "*Privacy and Security in Mobile Health: A Research Agenda*". Computers, IEEE Computer Society, pp. 22-30. 2016.

[7]. Alshammari B. M., "*A Framework for Developing Secure Internet of Medical Things: A Comprehensive Roadmap from An Artificial Intelligence Perspective"*. Journal of Theoretical and Applied Information Technology (JATIT), Vol.101. No 4, pp. 1455-1468. 2023.

[8]. Zriqat I.A. and Altamimi A.M. *"Security and Privacy Issues in Ehealthcare Systems: Towards Trusted Services"*, International Journal of Advanced Computer Science and Applications, Vol. 7, No. 9, pp. 229-236. 2016.

[9]. Chatterjee A. and Das A. K. "*Secret Communication Combining Cryptography and Steganography*". In Progress in Advanced Computing and Intelligent Engineering, Advances in Intelligent Systems and Computing. Pp. 281-291. 2018.

[10]. Aljabri, M.; Aljameel, S.S.; Mohammad, R.M.A.; Almotiri, S.H.; Mirza, S.; Anis, F.M.; Aboulnour, M.; Alomari, D.M.; Alhamed, D.H.; Altamimi, H.S. "*Intelligent Techniques for Detecting Network Attacks: Review and Research Directions"*. Sensors 2021, 21, 7070. https:// doi.org/10.3390/s21217070. 2021.

[11]. Chelli, K. "*Security Issues in Wireless Sensor Networks: Attacks and Countermeasures*" in Proceedings of the World Congress on Engineering. 2015.

[12]. Alanezi M.A. and Khan Z. F. "*Intelligent based E-healthcare Systems: Towards Security and Privacy*". International Journal of Computer Science and Network Security (IJCSNS), 19(3), pp. 16-23. 2019.

[13]. Beavers, J., Pournouri, S. *"Recent cyber-attacks and vulnerabilities in medical devices and healthcare institutions"*. Blockchain and Clinical Trial, pp. 249–267, Springer, Berlin (2019).

[14]. Kim, M., Hwang, E., Kim, J.-N. *"Analysis of eavesdropping attack in mmWave-based WPANs with directional antennas"*. Wireless Networks 23(2), 355–369 (2017).

[15]. Anh, V.T., Cuong, P.Q., Vinh, P.C. *"Context-aware mobility based on π-calculus in Internet of Thing: A survey. Context-Aware Systems and Applications"*, and Nature of Computation and Communication, Springer, Berlin, pp. 38–46 (2019).

[16]. Hamadaqa, E., Adi, W. *"Clone-resistant authentication for medical operating environment"* In: 2020 FourthWorld Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), pp. 757–762 (2020).

[17]. Alsubaei, F., Abuhussein, A., Shiva, S. *"Security and privacy in the internet of medical things: Taxonomy and risk assessment"*. In: 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops), pp. 112–120 (2017).

[18]. Alzahrani B.A, Irshad A., Albeshri A. and Alsubhi K., *"A Provably Secure and Lightweight Patient-Healthcare Authentication Protocol in Wireless Body Area Networks"*, Wireless Personal Communications, pp. 1-23, 2020.

[19]. Tutari V.H., Das B. and Chowdhury D.R., *"A Continuous Role-Based Authentication Scheme and Data Transmission Protocol for Implantable Medical Devices"*, in 2019 Second International Conference on Advanced Computational and Communication Paradigms (ICACCP), 25-28 Feb. 2019, pp. 1-6.

[20]. Bhatia T., Verma A.K. and Sharma G., *"Towards a secure incremental proxy re-encryption for e-healthcare data sharing in mobile cloud computing"*, Concurrency and Computation: Practice and Experience, vol. 32, no. 5, pp. 1-16, 2020.

[21]. G. Zheng et al., *"Finger-to-Heart (F2H): Authentication for Wireless Implantable Medical Devices"*, IEEE Journal of Biomedical and Health Informatics, vol. 23, no. 4, pp. 1546-1557, 2019.

[22]. Bonab, T.H. and Masdari M. "*Security attacks in wireless body area networks: challenges and issues*". ACADEMIE ROYALE DES SCIENCES D

OUTRE-MER BULLETIN DES SEANCES. 4(4): p. 100-107. 2015.
[23]. Partala, J., *et al*. "*Security threats against the transmission chain of a medical health monitoring system"*. e-Health Networking, Applications & Services (Healthcom), 2013 IEEE 15th International Conference on. 2013. IEEE.
[24]. Meng, W., Li, W., Zhu, L. *"Enhancing medical smartphone networks via blockchain-based trust management against insider attacks"* IEEE Trans. Eng. Manage. 67(4), 1377–1386 (2019).
[25]. Zeadally, S., Adi, E., Baig, Z., Khan, I.A. *"Harnessing artificial intelligence capabilities to improve cybersecurity"*. IEEE Access 8, 23817–23837 (2020).
[26]. Jaramillo, L.E.S. *"Malware detection and mitigation techniques: Lessons learned from Mirai DDOS attack"*. J. Inf. Syst. Eng. Manage. 3(3), 19 (2018).
[27]. Gull, S., Parah, S.A., Muhammad, K. " Reversible *data hiding exploiting Huffman encoding with dual images for IoMT based healthcare"*. Comput. Commun. 163, 134–149 (2020).
[28]. Karmakar, K.K., Varadharajan, V., Tupakula, U., Nepal, S., Thapa, C. *"Towards a security enhanced virtualised network infrastructure for Internet of Medical Things (IoMT)"*. in 2020 6th IEEE Conference on Network Softwarization (NetSoft), pp. 257–261 (2020).
[29]. Ahmad, I., Shah, M.A., Khattak, H.A., Ameer, Z., Khan, M., et al. *"FIViz: Forensics investigation through visualization for malware in Internet of Things"*. Sustainability 12(18), 7262 (2020).
[30]. Siahaan A. P. U., "*Genetic Algorithm in Hill Cipher Encryption".* International Journal of Research in Science and Technology Engineering and Mathematics, 15(1): 84–89. 2016.
[31]. Bedasa M.F. Bedada A.S. Mulatu W.B. "*Data Encryption and Decryption by Using Hill Cipher Algorithm"*. Network and Complex Systems www.iiste.org ISSN 2224-610X (Paper) ISSN 2225-0603 (Online). Vol.11, 5-16. 2020.
[32]. Hureib E.S. and Gutub A.A. "*Enhancing Medical Data Security via Combining Elliptic Curve Cryptography and Image Steganography*". International Journal of Computer Science and Network Security, 20(8): 1-8. 2020.
[33]. Duan, X., Song, H., Qin, C. and Khan, M.K., "*Coverless steganography for digital images based on a generative model*". Computers, Materials & Continua, 55(3), pp.483-93. 2018.
[34]. Denemark, T.D., Boroumand, M. and Fridrich, J., "*Steganalysis features for content-adaptive JPEG steganography*". IEEE Transactions on Information Forensics and Security, 11(8), pp.1736-1746. 2016.
[35]. Zhang, R. and L. Liu, "*Security models and requirements for healthcare application clouds*". IEEE 3rd International Conference on Cloud Computing. IEEE. 2016.
[36]. Elhoseny M., Ramírez-González G., Abu-Elnasr O.M., Shawkat S.A., Arunkumar N. and Farouk A., "*Secure Medical Data Transmission Model for IoT-Based Healthcare Systems*". IEEE Access, Special Section on Information Security Solutions for Telemedicine Applications, Vol. 6, pp. 20596-20608. 2018.
[37]. Zhao Y, Cui M, Zheng L, Zhang R., Meng L., Gao D. and Zhang Y., "*Research on electronic medical record access control based on blockchain"*. International Journal of Distributed Sensor Networks. 15(11). doi:10.1177/1550147719889330. 2019.
[38]. Sivan, R and Zukarnain, Z.A., "*Security and Privacy in Cloud-Based E-Health System*". Symmetry, 13, 742. (2021) https://doi.org/10.3390/sym13050742.
[39]. Al-Qarni E.A., "*Cybersecurity in Healthcare: A Review of Recent Attacks and Mitigation Strategies"*. *(*IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 14, No. 5, pp. 135-140. 2023.
[40]. Ajib Susanto, Ibnu Utomo Wahyu Mulyono, Muhamad Rizky Fajar Febrian and Ghaitsa Ardelia Rosyida, "*A Combination of Hill Cipher and LSB for Image Security"*. Scientific Journal of Informatics, Vol 7, No 1 (2020), pp. 155-165. DOI: https://doi.org/10.15294/sji.v7i1.24393.
[41]. Persulesy E.R and Tomasouw B.P., *"A design of a text messages security system on digital images using modified Hill Cipher and LSB method"*. In proceedings of AIP Conf. Proc. 2588, 050026 (2023) https://doi.org/10.1063/5.0125398.
[42]. Haryanto E.V., Nasution E.D., Akbar M.B. and Riza B.S., "*Application of Hill Cipher and LSB + 1 Methods for Messaging In Messages Inpicture".* Journal of Physics: Conf. Series. 1361 (2019) 012009, pp. 1-8. doi:10.1088/1742-6596/1361/1/012009.