Based on IoT Healthcare Application for Medical Data Authentication: Towards A New Secure Framework Using Steganography

Mohammed Mahdi Hashim¹,², Suhad Hasan Rhaif³, Ali A. Abdulrazzaq³, Adnan Hussein Ali⁴, Mustafa Sabah Taha⁵,⁶

¹Technical Engineering College, Middle Technical University, Baghdad, Iraq.  
²Faculty of Engineering, Uruk University, Baghdad, Iraq.  
³Technical Instructors Training Institute, Middle Technical University, Baghdad, Iraq.  
⁴Institute of Technology, Middle Technical University, Baghdad, Iraq.  
⁵School of Computing, Facility of Engineering, University Technology Malaysia, Johor Bahru, Malaysia.  
⁶Basrah Oil Training Institute, Ministry of Oil, Iraq.

Abstract. With increasing transmission of sensitive information over the dispersed IoTs, security of sensitive patient’s contents is becoming more challenging and has been enthusiastic area of research since last decades. Evolution in the concealment of data was reflected in the medical field specifically on medical images. Hide information technology in the image is called steganography. The objective of this study is the preservation of privacy and confidentiality of data in uncertain surroundings during multimedia exchange joining two IoT hops. For attacker hindrance and, provision of data confidentiality, a resilient multilevel security perspective depending on information hiding and cryptography is suggested. The existing schemes have limitations related to the equilibrium trade-off amid two variables (medical image quality and security). In addition, the direct embedment of the secret data into the images and further subtraction of an encrypted data from it often enables the intruders to easily detect and extract the hidden information. Based on these factors, we proposed a multilevel security based on 3¹th random iterations with chosen a procedure was implemented using Henon function to stop against cybercrimes challenges. The patient information is going through the preparation stage (different steps) before the embedding algorithm in order to increase the security. Superior results achieved with this study in term of imperceptibility and security the reason is to choose the right method in the right place. Satisfying results, gained when benchmarking our results with existing one in literature through the same criteria.

Keywords: IoT Healthcare, Medical Image Steganography, Henon Map Function, Encryption, RBF.

1. Introduction

Because of evolution massive the internet the main important element in information communication is information security and how to secure the transferred data. However, the security and privacy of transmitted data over the Internet have become an issue, especially over the public network and as such, several hazards ought to be considered. With the much attention given to telemedicine technologies data. So, security and privacy are necessary to ensure the data this has generated much concern within
the research community lately due to the rate of un-authored access to such medical information that has led to the violation of the rights of patients. Hence, medical descriptions must ensure the confidentiality of such data to retain patients’ confidence in the healthcare institutions. Sensitive patient’s health records, like laboratory reports, ECG data, diagnosis records can be stored in large databases as electronic files (in electronic health records, EHR) [1] and be considered as the medical history of the related patients, thereby commanding convenience on both sides. Alternatively, the collected data can be communicated among the concerned parties using modern information communication channels like wide or local area networks. Medical images accounts for 92% of medical records (information) that are stored in EHRs images. So, these images are processed and relayed following the recommended approach by the Digital Imaging and Communications in Medicine (DICOM) standard to ensure the privacy of such records (information) and its protection from manipulation or copyright violation [2]. Hence, it is important to secure medical data in all possible ways to ensure the confidentiality. Such security can be provided using security features such as information security techniques (steganography, watermarking and encryption) with IoT systems.

The connectivity between smart objects and cloud policies have resulted in a wholly managed internet boundary known as Internet of Things (IoT). The aim of this new paradigm is to achieve technological transformation of the modern environment [2]. IoT refers to the smart interconnection of essentially linked objects in order to create a Smart Cyberspace, achieve great connectivity and effective computation with quick information evaluation. A perfectly designed IoT comes with several application-related-advantages, such as reduced energy utilization, improved certainty, automation control, and undemanding services. It has also attracted industrial interest within the recent few years; hence, many models have been recommended at both executive and industrial levels [3, 4]. For example, e-healthcare guarantees efficient service delivery as it incorporates IoT supported CBS – cloud-based services. Similarly, geo sensors interconnection via an IoT framework can facilitate real-time geographical data collection, such as woodland plantations data, soil data, disaster-related data, such as swamping, tremors, etc. [5].

Different forms of data are propagated via IoT structure; such data forms are related to medical and military information and these are normally in the forms (text documents, image, video, audio and recordings) sourced from many sensors and processed via an application. Achieving a better, smart and sturdy structure that completely encompasses an implementation with relation to control and intelligence demands the assurance of the reliability, security, and efficiency of the computation [6,7]. Several attacks can also occur due to information propagation via an insecure channel; such attack can come from the full computerization of the structures. Owing to the volume of data propagated via IoT structures, it is necessary to address the associated problems, especially those that related to the certainty, discreteness, security, and authentication of the system [9]. IoT platforms can provide an avenue for easy access, copying, exploitation, and dissemination of digitalized data, thereby increasing the chances of multimedia attacks [8,10].

Currently, the level of data security standards remains immature as there are still numerous cases of constant data violations on the side of big international organizations. Yearly, the estimated economic loss due to cyberattacks and data raid amount so over 1 trillion USD as per the Global Risks Report 2018 [11]. These violations are encountered in different areas such as healthcare and defense and are not tolerated in these sectors due to the sensitivity of such healthcare and defense-related data where a slight change can lead to erroneous decisions [13]. For instance, a ransomware attack on the records of PAMC caused the violation of the privacy for the medical data of 266,123 victims [14]. Other comparable incidences have also been raised in [15-16]. Such violations in the privacy of the data of many customers could cause critical issues for the affected companies and could have huge financial implications in the form of litigations [17]. In the US healthcare, it is estimated that about 5 billion USD is spent yearly on legal suits and post violation rectifications [18]. This results in many companies contracting several security organizations to provide them with services that could help to reduce loss. There is also provision for the protection of copyrights of intellectual properties in the courts, as well as for the recovery of losses imposition of fines on perpetrators [19]. However, there is a need for the legitimate persons to conceive a genuine technique for claiming copyrights in case of violations. This implies that the information managing divisions need to improve on the difficulties
encountered during data propagation via many channels. There is also a need for techniques that will support honesty and authenticity to protect copyright and ensure the security and legitimate use of digitalized contents [8].

Among the issues that could limit the adoption of IoT applications are lack of data privacy, data confidentiality, and data privacy, and data authenticity [20]. Data embedding methods are robust in ensuring the authenticity and privacy of private communication [21] as they can conceal the vital digital information of a client in a cover object (such as picture or audio) from unauthorized access.

Medical image steganography schemes have been proposed for improving the level of privacy of data transfer in IoTs; this involves the use of both single- and double-pixel allocation frameworks, 3 random functions, and a RBF system. The patient data was first encrypted using the affine cipher prior to embedment to intensify the security level while Huffman coding was used to minimize the encrypted data in order to increase the payload.

The rest of this research is structured as follows: section II Theoretical background for proposed framework was described while in section III, the proposed framework is discussed in detail. In section IV, the results achieved from the evaluation of the proposed work were given in details. Finally, the conclusions drawn from the study were presented in Section V.

2. Theoretical Background
2.1. Environment of the study
Steganography consists of two main parts sender and receiver; certain media take the message from sender and deliver it into receiver side. Many terms in steganography used such as cover image which mean the original image not including anything-pure image, process of inserting or hiding secret message inside cover image called embedding [27]. Embedding process produce image contain secret data inside it this image called stego image, after transferring stego image in trusted channel at the other side second party (receiver) will receive stego image and make reverse process of embedding called extracting to reveal secret message from stego image, to extract data from image need coding information stored in secret key called stego key. Structure of the system illustrate in Figure 1.

![Figure 1. Structure of steganography system](image)

Sender sends stego image through channel, stego image should be look like original image without any doubt (innocent image) because of preventing any hacker or intruder to recognize there is a secret inside it. Any distortion in stego image create suspicion to the intruder and distortion comes from two things first weakness in embedding method; second increasing the amount of payload capacity which mean image carry too much amount of secret message [28]. Secret message convert into binary before embedding to get ability and compatibility with cover image. Converting secret message into binary decomposition allow it to be in form of bytes, and each byte consists of 8-bits as normal but of necessity embedding some time these serial of bits that come from secret message will segmented into more or less number of bits [29]. First contribution in this study lies here and will discuss in detail in methodology, while second contribution located within image decomposition. Cover image in general consists of pixels (PICture CELl) which is consider the basic components, this pixel reflect the illuminate of the image and consists of number value not exceed 256 and in binary represented as $2^8$, each value in the pixel reflected by 8-bits in binary decomposition. Image includes two types of
illumination color and gray; gray image consists of one channel pixel, which mean the pixel has one numeric value [30]. Steganography system embed secret information in different manners in particular with image due to different media need different technique, type of steganography will explain next section.

2.2. Classification of Information Hiding

Hiding information take different forms in term of placing data within media, there are three main forms considered when talking about data security [31]. Cryptography is changing the data itself by scrambling under certain condition, as if he was openly challenging and no need to hide secret coding because power of encryption method. Watermarking to a certain extent look like steganography and main different by choosing the media of cover and secret. In steganography, many hosting media used to cover secret message as shown in Figure 2. Each cover media has advantage and disadvantage in text media imperceptibility is good but gain less capacity due to text can carry less amount of data while video and audio can use large amount of data accompanied by a few of security exactly the contrary with protocol that has high degree of security with less capacity.

![Figure 2. Classification of steganography within information hiding](image)

There are two main categories in image steganography spatial and transform (frequency) domain, techniques between them is very different in method and results. Image in transform domain is more robust and secure than other but lake in capacity and imperceptibility; spatial domain is more flexibility and researchers can contribute in such area like blue ocean therefore we can notice that most of the existing researchers considered this case. Spatial domain focusing on pixels value specially Least Significant Bit (LSB). The human eye does not distinguish the minimum difference in illumination (less than 30), LSB of the pixel got impact of $2^0, 2^1, 2^2, 2^3$ which equal to 8 pixel value. As shown in Figure 3.
Most of the previous research was mainly adopted LSB in embedding process and contributed in spatial domain while frequency domain still far from innovation. This study carried out novel method can open horizons to recover steganography and improve both security and imperceptibility. Now can stand on one class of hierarchical steganography (which is image); for more clearance will discuss in detail within methodology later in this manuscript.

2.3. Background of framework

To achieve a secure and accurate propagation of data via an IoT-related platform requires a stronger and secure framework design. Several methods have been proposed for multimedia data protection from unauthorized access; however, security from cyber-attacks remains a persisting difficulty in distributed IoT structures. The obvious way of providing secure data transmission via an IoT structure and guard against violations is to guard against cyberattacks. A previous study [28] has provided a reliable picture allocation method of objects with cloud structure linked with IoTs [28]. However, this method suffers from lack of a security method; the standalone security method is embedding, and data is endangered when the algorithm is violation.

The research by [29] presented a spatial domain-based picture information covering techniques for acquiring the broadcasting of Internet Protocol (IP) camera pictures of IoT object. This method relies on the idea of inverted ILSB for image decoding before broadcasting to different gadgets or selected cloud connected to an IoT structure. On the contrary, these information embedding methods lack inspection for extraction efficiency in terms of cyberattacks.

Another study by [30] provided a high capacity (EHR) information embedding technique IoT-related e-healthcare implementation. This system achieves information embedment in a medical picture using modular computational functions with Pixel Repetition Method (PRM). Previous studies have provided different SD-spatial domain methods as well [31, 32]. Being that these methods are computationally systematic, the security of the discrete information is considered insufficient for both current and future incidences.

Similarly, the study by [33] presented a blind and strong CNN-based watermarking method which provides simple inadequate vigor as opposed to many attacks. However, this method can achieve an improved level of robustness by inserting a watermark in the transformed arena. Among the famous modified methods for watermarking implementation are DCT, DWT, and IWT [34, 35, 36]. The procedures are a hybridization of these modified areas, resulting in improved complexity, minimal imperceptible and payload, and improved robustness [37, 38].

During the development of a watermarking procedure, the security of the watermark is a significant consideration. A well-conceived security method will prevent unauthorized access as the real information content will not be extracted if the extraction algorithm is violated. The improvement of the security mechanism is significant in the present world due to the access of unlicensed personnel to higher processing multimedia gadgets [40, 39].

The study by [45] reported a reliable medical detail sharing model for IoT-based healthcare structures that comprises of a combination of AES and RSA. In addition to the encoding of the medical details, the procedure also conceals the details with the second part of DWT of the cover image. This system succeeded in achieving a simple favorable discernible quality of the stegoimage, it
was not evaluated in the presence of different consistent attacks. The combination of AES and RSA resulted in prolonged encryption period; hence, it is not suitable for resource-restricted instant implementations in an IoT domain. The use of chaotic maps for security improvements in various structures has received attention due to their features such as greater susceptibility to original variables, pseudo random, and non-linear behavior [41].

According to [42], Arnold cat map was used for watermark encryption prior to insertion in a color image. The procedure entails QDFT and EULPM. The procedure suffers from poor vigor in terms of Gaussian noise, sifting and few geometric attacks despite achieving good embedding capacity and imperceptivity. The Arnold encryption method also offered weak security because of low key space and invariably familiar algorithm [39]. Furthermore, security enhancement is possible by incorporating more chaotic maps based on the expected level of security.

The report in [43] described a secure watermarking procedure that utilizes dual-encryption two chaotic maps. The injection precedes the administration of DCT on the 8x8 blocks via combination from the two adjacent blocks and a pair of DC coefficients. The vigor strength is ascertained through a hiding element that have value places the length of guard bands in a middle of the areas determined by watermark bits. The performance of the system was poor in few geometric attacks despite its great performance on filtering, compression, and noisy attacks. The poor performance is due to the insertion of the watermark bits using the neighboring adjacent 8 x 8 blocks as the image information is lost during region-based attacks such as trimming or rotation. The watermark can also be erased and tampered with as the two coefficients utilize watermarking data in two blocks that entail 128 coefficients, hence, further tampering.

Arnold Chaos encryption-based security methods lack efficiency due to the small key structure and enhancement is difficult with a high number of iterations of Arnold encryption. However, the security can be improved by manipulating all the keys and not alteration of one key. Hence, this study suggests a secure and strong data embedding method to address the issues of the newly suggested procedures. This study aims at securing the privacy and confidentiality of medical data dissemination in IoT frameworks using a combination of information hiding and cryptography procedures. Section III provides a detailed description of the suggested procedure.

2.4. Steganography in Medical Image.

A study by [23] utilized ECG signal to host a secret record of patient; the study selected the appropriate position for embedding the secret medical report using Bernoulli's chaotic map. LPF filter was used in encoding and decoding the ECG signal. Another study by [24] introduced a medical image retrieval system which was designed for finding the Region of Interest (ROI) in order to get features that will be used for steganography processes after embedment [24]. Researchers in [25] suggested the use of the DWT with telemedicine in watermarking model. They utilized 3 phases of DWT for embedment a secret data in high and low of sub-band within host object (host image).

A modification of the Blowfish algorithm was presented by [26] for protecting the security of medical images and text record; they suggested the use of power function for secret information encryption. They also introduced the manipulation of the UACI with (NPRC) in order to improve a security of the method vs. attacks. As per [27], coefficients of DCT are helpful in achieving perfect outcomes when partitioning the cover images into 8 x 8 pixel; with no overlapping among them; they also submitted that transform domain is more helpful with watermark techniques. In this study, the major aim is to develop a new method that will address the challenges of the existing methods and improve the results.

3. Methodology

The proposed framework for conserving data confidentiality when disseminating in IoT is discussed in this section. Data confidentiality is important in IoT since information is propagated via several hops. The combination of many gadgets, services, and interconnections linked through plethora of data creates rooms for privacy breach in IoT due to the ease of data accessibility. Hence, data confidentiality can be achieved in such scenario through a reliable encoding procedure [8]. In line with this, a reliable data transfer model for a secure IoT connection is proposed in this study as depicted in
Figure 4 which is a visualization of the scenario in healthcare that employs an IoT distributed structure over various settlements and municipalities. There are three major phases of data embedding processes; these are:

a) Sender position (Patient side): The information is processed to ensure its privacy and security.
b) Cyberspace (Internet layer) – The network or storage space which may be prone to attacks and information exploitation.
c) Receiver position (Hospital side) - Decodes the secret information from a stego-image.

The medical image in proposed work is employed in terms of the spatial domain; various approaches were used to ensure the security of the huge data size and improve the security of the achieved stego image. This study mainly aims at designing and developing a scheme which can provide a perfect security level of secret data without compromising the image quality of the stego-image. The entire proposed information hiding approach is illustrated at Figure 5.

The proposed work is comprised of 5 main sub-schemes as follows: i) The affine cipher used for patient data cryptography to ensure data security; ii) Huffman Coding for encrypted data compression prior to embedding; iii) RBF system for ascertaining the similarity among the bits of an original cover image and the patient secret bits; iv) Hiding scheme for embedding the result of AC encrypted patient information within a medical image to produce a stego images. v) The extraction process for retrieval embedded patient bits from the stego image. The next section briefly reviewed these algorithms.
3.1. **Affine cipher AC**

The formula of AC is represented like a standard switching cipher controlled via the concept of the letter being replaced by another letter, and each letter is encrypted using the function \((a x + b) \mod m\) [27]. So, \(b\) is the size. Regarding the AC, laters of size \((0, \ldots, (m-1))\) are first mapped to combines prior to the transfer of the integer (modular arithmetic). To encrypt each alphabet letter, the formula calculate as follows:

\[ E(x) = (ax + b) \mod m, \]  

(1)

So, \((a)\) and \((b)\) represented as encryption key, while \((m)\) is represented as the amounts for alphabets. The \((a)\) is selected in the manner which it includes \((m)\). For each letter, the decryption formula calculate as follows:

\[ D(x) = a^{-1}(x - b) \mod m, \]  

(2)

Where \(a^{-1}\) is the modular multiplicative opposite of \(m\) modulo, i.e., to satisfy the rule:

\[ 1 = aa^{-1} \mod m, \]  

(3)

3.2. **lossless Compression (LC-HC)**

Huffman coding (HC) is one of a most lossless compression approach that employs as a prefix code. HC was first reported via (David Huffman at "1952") using the frequenc letters within texts [16]. The HC is ideal for the compression of lossless data but more effective while compared to the exist techniques for data compression. The HC used to compress the patient’s secret information prior to the hiding process.

3.3. **Reverse Bit Function (RBF)**

Having selected the random pixels, the next step is to arrange them as sub-pixels of (8 x 8 pixels) to hiding in LSB of each pixel. On the other hand, the patient's data fragments into blocks of 64 bits. At this stage, the hiding procedure via replace the bits from LSB of sub-pixels of (8 x 8 pixels) within 64 bits from the patient's secret data.

The RBF is used to check the similarity among the secret bits pairs prior to the replaced; if the number of (matching bits) is lower than the (mismatched bits), in this case, the patient's secret data will be inverted before embedding, otherwise, the secret bits will be directly embedded. The bit invert system before the embedding process is explained in Figure 6.
In additional clarification, before replacement check the match between bits in original medical image and bits of patient's secret data, if number of matching bits less than mismatched bits then reverse secret data and embed it, otherwise embed secret bits directly. As shown in Figure 7 in this figure red color bits refer to mismatched bits and green bits refers to matched bits.

**Figure 6.** Reverse bit function (RBF).

**Figure 7.** Embedding process with RBF

3.4. Embedding process (EP)
The EP is required to hide the compressed patient's secret data within a (LSB) part of pixel. This is done in two steps, 1) selection pixel randomly, 2) Data embedding. These steps are performed simultaneously, firstly, medical image that has size (512 * 512) is fragmented into (64 blocks) each block has 4096 pixels. Henon map function is a random function used the three times in order to increase the security. The Henon map function (HMF-1) is used to selected one block randomly of (64 blocks), while the selection of the sub-blocks (4096 pixels) is done utilizing the second parameter of HMF-2. Lastly, the selection of the (64) pixels that can determine the last destination, which is done using the third variable of HMF-3.

**Embedding Process**

| Input: | C_IMG (Cover image). |
|--------|---------------------|
| S_BIT  | (Secret text).      |

**Case a:**
1. Read and change S_BIT to (0,1) binary system.
### 3.5. Retrieval/Extraction process.

The aim of the extraction process is to get data from the LSB pixels; hence, it must be done after the EP at the receiver end. It comprises of guidelines with contact among two sides via a secret key to improve the procedure. It is performed in a similar manner as the embedment process but in the reverse format, meaning that a LSB part of a pixels can recognize the pixels (individual, double). In LSB, the double pixel means start with (0) due the binary values and the individual pixel (1) vice versa. Most of the patient secret data are detect during the image partitioning, together with the segment of a patient secret data. Hence, the two major aims of extraction and embedment processes are imperceptibility and security. Figure 8 is achieving the objectives of this study in detail.

1. Perform the Affine Cipher to Se_Bits
2. Use Huffman coding to compression the (Se_Bits).
3. Determine the magnitude of Se_Bits (Number of bits 262144).
4. RBF procedure:
   - If S_BIT matched > S_BIT mismatched, do embedding directly.
   - If S_BIT matched < S_BIT mismatched, invers S_BIT then embedding.

**Case b:**
1. Choose C_IMG (512 * 512).
2. Partition C_IMG into 64 blocks.
3. Choose block randomly via using first variable of HMF-1.
4. Use $2^{th}$ parameter of HMF-2 to select the 64 x 64 pixels
5. Use $3^{th}$ parameter of HMF-3 to get a destination pixel.

**Case c:**
1. Generate H vector and organize based on Double/Individual.
2. Selected the LSB layers for pixel.
3. Generate loop L=1: W.
4. Receive S_BIT (1 or 0).
5. Embedding procedure (EM_BIT)
   - a- If pixel is double and S_BIT is 0 and, do in nothing
   - b- If pixel is individual and S_BIT = 0, replace LSB position vale with 0.
   - c- If pixel is double and S_BIT is 1, replace LSB position vale with 1.
   - d- If pixel is individual and S_BIT is 1, do in nothing.
6. P = P +1.
7. Iterate the step 5 till whole S_BIT of secret bits is embedded

Output: EM_BIT (Stego-image).
4. Result and Evaluation.
This experiments in this study were performed in the MATLAB platform using four standard images (size = 512 x 512) sourced from different databases (refer to Figure 9). The results were obtained by considering the payload of a medical image for the related methods. Figure 8 depicted the utilized stego medical images for the suggested work when BPP (1.5). Different parameters were employed for the evaluation of the proposed work, such as (BPP), (PSNR) and (SSIM), while (BER) was used to check for the robustness of the suggested technique against attacks.
Figure 9. Illustration the host medical image and stego medical image, with size (512 * 512).

4.1. Evaluate based on capacity and imperceptible parameters (SSIM, EC, bpp, PSNR).

The amount of Embedding Capacity (EC) is the amount of secret patient’s bits to the amount of host medical image (pixels) [6, 8]. It is a direct expression of number of pixels utilized in the proposed work since one pixel can embed different numbers of message bits.

\[
EC = \frac{\text{The number of message bits}}{\text{The number of cover images' pixels}}
\]  

(4)

This study used different payload capacities and is presented as a percentage. These EC are used with existing methods that used for comparison with our work, for more clarification table 1 is discussed EC in detail.

Table 1. Illustration the different payload capacities used in proposed work.

| EC by Bytes | EC By Bits | EC percentage | BPP  | Description               |
|------------|------------|---------------|------|---------------------------|
| 1.         | 16384      | 131072        | 6.25%| 0.5                       |
| 2.         | 32768      | 265144        | 12.5%| 1                         |
| 3.         | 49152      | 393216        | 18.75%| 1.5                       |

The peak signal-to-noise ratio (PSNR) was used as a metric to measure the image quality; this ratio is determined after the EP to match the original medical image and stego image (pixels). A PSNR of >= 30db implies that the data embedding process is imperceptible to HVS [14]. The PSNR is calculated as follows:

\[
PSNR = 10 log_{10} \left( \frac{255}{MSE} \right)
\]  

(5)

Where, the MSE is the mean square error presented as follows:

\[
MSE = \frac{1}{mn} \sum_{i=1}^{m} \sum_{j=1}^{n} (x_{ij} - y_{ij})
\]  

(6)

The SSIM is used to determine the similarity among the cover image and the stego-image [15]. This similarity level is calculated using Equation (8) and the value ranges from -1 to 1, where SSIM value of 1 implies no difference among the stego medical image and cover medical image.

\[
SSIM = \frac{(2P_Q Q + c_1)(2\sigma_{QQ} + c_2)}{(P_Q^2 Q^2 + \sigma_Q^2 + \sigma_Q^2 + c_2)}
\]  

(7)

Where SSIM represent the mean pixel value, variance, and standard deviation respectively for the original image and the stego-image, and rOS is the covariance between both images. \(c_1 = k1L\) and \(c_2 = k2L\) are constants; where \(k (1) = (0.01)\), \(k (2) = (0.03)\), and \(L = (255)\) for grayscale image.

Table 2. Proposed scheme result based on different evaluation parameters when BPP equal (0.5).
4.2. Robustness Evaluation Using (BRE)

The Bit Error Rate BER was used to evaluate the robustness of the proposed scheme in this study. Robustness expresses the capability of the secret patient’s bits to against attacks. It involves an inversion of the (PSNR) value in order to obtain the BER; this inversion is performed as follows:

$$BER = \frac{1}{PSNR}$$  \hfill (8)

The BER expresses the section of a medical cover image qubits changed through the steganography procedure. When the PSNR is 50 dB, the BER would be 0.02, i.e., 2% BER-P of bits has been altered during the process. The calculated of all evaluation parameters during the implementation process in this study are presented in Tables 2, 3 and 4, where Table 5 showed the outcomes results using PSNR at 0.5 BPP and 1 BPP for proposed framework and other methods. Observable, the proposed work achieved better PSNR when compared to [6], [46], [47] and [48] as it hides the secret message by manipulating the LSB of every pixel.

To make the comparison more clearly figure 10 is showed the graphical representation of the PSNR for different EC (bits).
Figure 10. Comparison of PSNR for proposed work based on different EC (Bits)

Table 5. Experimental result among existing methods and proposed work when BPP equal (0.5 , 1)

| Standard images 512 x 512 | PSNR | BPP | Hashim et al. [6] | Muhammed et al. [46] | Seyyedi et al. [47] | Jiang et al. [48] | Proposed work |
|---------------------------|------|-----|-------------------|----------------------|--------------------|-----------------|---------------|
| Lena                      |      | 0.5 | 71.44             | 53.91                | 69.21              | N/A             | 72.30         |
|                           |      | 1   | 66.63             | 51.13                | 65.09              | 50.84           | 67.30         |
| Baboon                    |      | 0.5 | 71.21             | 53.89                | 69.10              | N/A             | 72.22         |
|                           |      | 1   | 65.85             | 51.14                | 65.19              | 50.37           | 66.50         |
| Papers                    |      | 0.5 | 72.10             | N/A                  | N/A                | N/A             | 72.24         |
|                           |      | 1   | 67.61             | 51.13                | N/A                | 50.62           | 67.72         |
| Cameraman                 |      | 0.5 | 71.20             | 53.88                | 69.09              | N/A             | 72.15         |
|                           |      | 1   | 67.23             | 51.11                | 65.12              | 51.61           | 67.51         |

The standard images commonly used by previous scholars were also employed in this study for comparison sake; these images include “Lena”, “Papers”, “Cameraman”, and “Baboon” gray scale images with size 512*512. In order to have a comparison between the proposed framework and existing methods with 1 BPP a graphical representation of the PSNR is shown in Figure 11.
Figure 11. Comparison of PSNR for proposed work and existing methods based on BPP

5. Conclusion
The increased attention given to medical data has also increased its susceptibility to threats and attacks during storing, dissemination, or acceptance via the Internet and network. However, such threats can be avoided by securing such medical details. This study has discussed several information hiding methods that can ensure the security and confidentiality of information during transmission in an IoT structure. The existing schemes have limitations related to the equilibrium trade-off among two variables (medical image quality and security). In addition, the direct embedment of the secret data into the images and further subtraction of an encrypted data from it often enables the intruders to easily detect and extract the hidden information. Based on these factors, we proposed a multilevel security based on random iterations with chosen a procedure was implemented using Henon function to stop against cybercrimes challenges. The patient information is going through the preparation stage (different steps) before the embedding algorithm to improve security evaluation.

The major objective of this research is to provide security to information from multimedia gadgets substituted as visual sensors in IoT surrounding. Future studies will focus on the use of different kinds of information from different IoT gadgets, as well as submitting the enhanced data exchange methods for disseminated IoT administration. The major objective of this research is to provide security to information from multimedia gadgets substituted as visual sensors in IoT surrounding. Finally benchmarking with the most important researches in literature regarding steganography presented.

References
[1] Kuang, Li-Qun, Yuan Zhang, and Xie Han. 2009 Watermarking image authentication in hospital information system. 2009 International Conference on Information Engineering and Computer Science. IEEE.

[2] Usman, Muhammad Arslan, Muhammad Rehan Usman, and Soo Young Shin. 2017 Quality assessment for wireless capsule endoscopy videos compressed via HEVC: From diagnostic quality to visual perception. Computers in biology and medicine 91, pp. 112-134.

[3] Hashim, Mohammed, et al. 2018 A Review and Open Issues of Multifarious Image Steganography Techniques in Spatial Domain. Journal of Theoretical & Applied Information Technology 96 (4).

[4] Hashim M. Mahdi, et al. 2018 Performance evaluation measurement of image steganography techniques with analysis of lsb based on variation image formats. International Journal of Engineering & Technology 7 (4), pp. 3505-3514.

[5] Domain, W. T. I. S. 2018 A review and open issues of diverse text watermarking techniques in spatial domain. Journal of Theoretical and Applied Information Technology 96 (17).

[6] Mahdi Hashim, M., Mohd Rahim, and Mohd Shafry. 2017 Image Steganography Based on Odd/Even Pixels Distribution Scheme and Two Parameters Random Function. Journal of Theoretical & Applied Information Technology 95 (22).

[7] Hashim, Mohammed Mahdi et al. 2018 An extensive analysis and conduct comparative based on statistical attach of LSB substitution and LSB matching.” International Journal of Engineering & Technology 7 (4), pp. 4008-4023.

[8] Mahdi, Mohammed Hashim et al. 2019 Improvement of Image Steganography Scheme Based on LSB Value with Two Control Random Parameters and Multi-level Encryption. IOP Conference Series: Materials Science and Engineering. 518 (5).

[9] Taha, Mustafa Sabah et al. 2019 Combination of Steganography and Cryptography: A short Survey. IOP Conference Series: Materials Science and Engineering 518 (5).

[10] Nambakhsh, Mohammad-Saleh, Alireza Ahmadian, and Habib Zaidi. 2011 A contextual based double watermarking of PET images by patient ID and ECG signal. Computer methods and programs in biomedicine 104 (3), pp. 418-425.
[11] Nambakhsh, Mohammad S., et al. 2006 A novel blind watermarking of ECG signals on medical images using EZW algorithm. 2006 International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE.

[12] Usman, Muhammad Arslan, and Muhammad Rehan Usman. 2018 Using image steganography for providing enhanced medical data security. 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC). IEEE.

[13] Fallahpour, Mehdi, D Megias, and Mohammed Ghanbari. 2011 Reversible and high capacity data hiding in medical images. IET Image Processing 5 (2), pp. 190-197.

[14] Tao, Jinyuan, et al. 2018 Towards robust image steganography. IEEE Transactions on Circuits and Systems for Video Technology 29 (2), pp. 594-600.

[15] Rabie, Tamer, Mohammed Baziyad, and Ibrahim Kamel. 2018 Enhanced high capacity image steganography using discrete wavelet transform and the Laplacian pyramid. Multimedia Tools and Applications 77 (18), pp. 23673-23698.

[16] Huffman, David A. 1952 A method for the construction of minimum-redundancy codes. Proceedings of the IRE 40 (9), pp. 1098-1101.

[17] Bhatt, Santhoshi, et al. 2015 Image steganography and visible watermarking using LSB extraction technique. 2015 IEEE 9th International Conference on Intelligent Systems and Control (ISCO). IEEE.

[18] Pradhan, Anita, et al. 2016 Performance evaluation parameters of image steganography techniques. 2016 International Conference on Research Advances in Integrated Navigation Systems (RAINS). IEEE.

[19] Feng, Bingwen, Wei Lu, Wei Sun. 2014 Secure binary image steganography based on minimizing the distortion on the texture. IEEE transactions on Information Forensics and Security 10 (2), pp. 243-255.

[20] Bucerzan, Dominic, and Crina Raţiu. Image processing with android steganography. International Workshop Soft Computing Applications. Springer, Cham, 2014.

[21] Muhammad, Khan, et al. 2015 A Secure Method for Color Image Steganography using Gray-Level Modification and Multi-level Encryption. TIIS 9 (5), pp. 1938-1962.

[22] Aziz, Mahdi, Mohammad H. Tayarani-N, and Mehdi Afsar. 2015 A cycling chaos-based cryptic-free algorithm for image steganography. Nonlinear Dynamics 80 (3), pp. 1271-1290.

[23] Pandey, Anukul, et al. 2019 Bernoulli’s Chaotic Map-Based 2D ECG Image Steganography A Medical Data Security Approach. Medical Data Security for Bioengineers, 2019, pp. 208-241.

[24] Eze, Peter, et al. 2019 Integrity Verification in Medical Image Retrieval Systems using Spread Spectrum Steganography. Proceedings of the 2019 on International Conference on Multimedia Retrieval. ACM.

[25] Sivapraeksh, Asokan, Samuel Nadar Edward Rajan, and S. Selvaperumal. 2019 A Novel Robust Medical Image Watermarking Employing Firefly Optimization for Secured Telemedicine. Journal of Medical Imaging and Health Informatics 9 (7), pp. 1373-1381.

[26] Akande, Noah Oluwatobi, et al. 2019 Electronic Medical Information Encryption Using Modified Blowfish Algorithm. International Conference on Computational Science and Its Applications. Springer, Cham, 2019.

[27] Parah, Shabir A., et al. 2019 Realization of an adaptive data hiding system for electronic patient record, embedding in medical images. Security in smart cities: models, applications, and challenges. Springer, Cham, 47-70.

[28] Yin, Joanne Hwan et al. 2015 Internet of Things: Securing data using image steganography. 2015 3rd International Conference on Artificial Intelligence, Modelling and Simulation (AIMS). IEEE.

[29] Li, et al. 2019 Distortion less secret image sharing scheme for Internet of Things system. Cluster Computing 22 (1), pp. 2293-2307.

[30] Parah, Shabir A., et al. 2018 Electronic Health Record hiding in Images for smart city applications: A computationally efficient and reversible information hiding technique for secure communication. Future Generation Computer Systems.
[31] Abraham, Jobin, and Varghese Paul. 2016 An imperceptible spatial domain color image watermarking scheme. *Journal of King Saud University-Computer and Information Sciences*.

[32] Wang, yang, et al. 2014 A new robust color image watermarking using local quaternion exponent moments. *Information sciences 277*, pp. 731-754.

[33] Mun, Seung-Min, et al. 2017 A robust blind watermarking using convolutional neural network. *arXiv preprint arXiv 17* (4), pp. 03248.

[34] Hsu, L. Yuan, and Hwai-Tsu Hu. 2015 Blind image watermarking via exploitation of inter-block prediction and visibility threshold in DCT domain. *Journal of Visual Communication and Image Representation 32*, pp. 130-143.

[35] Zhang, Zhi, C. Y. Wang, and Xiao Zhou. 2016 Image watermarking scheme based on DWT-DCT and SSVD. *Int. J. Secur. Appl 10*, pp. 191-206.

[36] Verma, Vivek Singh, Rajib Kumar Jha, and Aparajita Ojha. 2015 Significant region based robust watermarking scheme in lifting wavelet transform domain. *Expert Systems with Applications 42* (21), pp. 8184-8197.

[37] Hurrah, Nasir N. et al. 2019 Dual watermarking framework for privacy protection and content authentication of multimedia. *Future Generation Computer Systems 94*, pp. 654-673.

[38] Benoraira, Ali, Khier B, and Noureddine Boucenna. 2015 Blind image watermarking technique based on differential embedding in DWT and DCT domains. *EURASIP Journal on Advances in Signal Processing 2015* (1), pp. 55.

[39] Guo, Jianting, Peijia Zheng, Jiwu Huang. 2015 Secure watermarking scheme against watermark attacks in the encrypted domain. *Journal of Visual Communication and Image Representation 30*, pp. 125-135.

[40] Mahajan, Prerna, and Abhishek Sachdeva. 2013 A study of encryption algorithms AES, DES and RSA for security. *Global Journal of Computer Science and Technology*.

[41] Wang, Xingyuan, Kang Guo. 2014 A new image alternate encryption algorithm based on chaotic map. *Nonlinear dynamics 76* (4), pp. 1943-1950.

[42] Ouyang, Junlin, et al. 2015 Color image watermarking based on quaternion Fourier transform and improved uniform log-polar mapping. *Computers & Electrical Engineering 46*, pp. 419-432.

[43] Loan, Nazir A., et al. 2018 Secure and robust digital image watermarking using coefficient differencing and chaotic encryption. *IEEE Access 6*, pp. 19876-19897.

[44] Elhoseny, Mohamed, et al. 2018 Secure medical data transmission model for IoT-based healthcare systems. *IEEE Access 6*, pp. 20596-20608.

[45] Muhammad, Khan, Jamil Ahmad, Haleem Farman, Zahoor Jan. 2016 A new image steganographic technique using pattern-based bits shuffling and magic LSB for grayscale images. *arXiv preprint arXiv 16* (1), pp. 01386.

[46] Seyyedi, Seyyed Amin, Vasili Sadau, and Nick Ivanov. 2016 A Secure Steganography Method Based on Integer Lifting Wavelet Transform. *IJ Network Security 18* (1), pp. 124-132.

[47] Jiang, Nan, Na Zhao, and Luo Wang. 2016 LSB based quantum image steganography algorithm. *International Journal of Theoretical Physics 55* (1), pp. 107-123.