International Journal of Innovation, Creativity and Change. www.ijicc.net
Volume 11, Issue 1, 2020

Medical Image Steganography Framework for Confidentiality in IoTs Based Health Care Applications

Monanad Najm Abdulwahed[a], [a]Materials department, University of Technology, Baghdad, Iraq, Email: [a]mohanadnajmabdulwahed@gmail.com

The extensive interchange of data visualised to take place in dispersed IoTs is susceptible to result in privacy and authentication results at the cyberspace position. The objective of this study is the preservation of privacy and confidentiality of data in uncertain surroundings during multimedia exchanges 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 proposed work is based on bit invert system (BIS), and three random control parameters have been suggested, a random selection process was performed using Henon map function (HMF) to stop against cybercrimes challenges. For increase in the security level, the affine cipher was used to encrypt the data and Huffman method to minimize the encrypt data prior to the embedding for increasing payload ability. The outcome of the proposed scheme is very high vigor of the conveyed details linking two nodes, inclusive of signal processing and the region-oriented strikes, occurring at the same time or standalone. Rotation strikes, cropping, histogram equalisation, and sharpening, results in great vigor with SSIM near to unity. For another remarkable/collaborated strikes, the mean SSIM is more than 0.98. The average PSNR resulting of several cover images is more than 60 dB consisting of distinct payload capacity. The investigated outcomes reveals the advantage of the suggested perspective compared to other modern methods.

Key words: *Image Steganography, IoT, Secure medical data, Random function, Affine cipher.*

Introduction

The network revolution provides easiness in digital communication and a remarkable increase in its users in the last decades. Meanwhile, it has become a challenge for the security factor of data transmission over the public network. Numerous hazards must also be considered. Being that much attention has been given to telemedicine technologies data, there is a need to ensuring the security of such medical data and this has become a source of concern lately as a result of unauthorised access to medical data (which is a major form of cybercrime). Patients' rights are often violated when such important data is stolen. Therefore, medical descriptions must preserve confidentiality to safeguard patients' confidence in the services of health care institutions. Medical institutions can store patient's health records as electronic files in (electronic health records, EHR) in large databases (Kuang,2009). Sensitive patient information such as their personal data, diagnosis reports, vital signs, and laboratory reports can be stored as EHR. Such information will serve as the patients' medical history and will command convenience on both sides (patients and clinicians). The information can also be transmitted via modern communication channels, including both local and wide area networks. medical images constitute more than 90 % of medical data stored in EHRs. These images, X-ray, magnetic resonance pictures, endoscopy images, including recordings, etc. are processed and relayed following the Digital Imaging and Communications in Medicine (DICOM) standard. The confidentiality of victim's data in DICOM file must be ensured to prevent any form of alteration or manipulation, including unauthorised copying; the copyright of such information must be protected as well (Usman, and Soo,2017). To ensure the confidentiality of medical data, they must be secured in every possible way. The confidentiality of patient data in DICOM file must be ensured to prevent any form of alteration or manipulation, including unauthorised copying; the copyright of such information must be protected as well (Usman, and Soo,2017). To ensure the confidentiality of medical data, they must be secured in every possible way. This protection can be provided using security features like Firewalls, an encryption technique, virtual private networks (VPN), and cryptography or steganography techniques with IoT systems.

Linking smart objects and cloud policies have resulted in a wholly managed internet boundary known as the Internet of Things (IoT); with the aim to transform the modern environment technologically (Usman, and Soo,2017). The IoT is a vigorous interconnection of essentially linked material objects, creating a Smart Cyberspace, objectively to create huge connection, effective computation with an instant evaluation of information. A thoroughly designed IoT provides benefits regarding application inclusive of lower utilisation of energy, intensified certainty, automation control, and undemanding services. Regarding the benefits, greater interest has been exhibited within the recent few years at industrial locality level hence many models have been suggested at both industrial and executive extents (MOHAMMED, et al.,2018; Hashim,2018). For instance, the ehealthcare arena ensures

efficient service delivery through the inclusion of IoT supported CBS – cloud-based services. Likewise, the linking of geo sensors via an IoT structure leads to the huge real-time gathering of geographical data with regards to woodland plantations, soil and disasters like swamping, tremors among others (Domain,2018).

Among the swapped data within a dispersed IoT structure is information related to medical, banking and discrete files taking the appearance of images, text documents and recordings obtained from a variety of sensors and processed /cached by the system. For a better, smart and sturdy structure completely encompassing an implementation with relation to control and intelligence, there must be reliability, security, and efficiency in terms of computation (., Mohd Rahim, and Mohd Shafry,2017; Sabah et al.2018). Many attacks result too via the transfer of information using insecure means due to the full computerisation of the structures. As a result of the huge data transfers in IoT structures, recent problems in the form of certainty, discreteness, security and authentication should be confronted at cybercrime (Mahdi,2019; Sabah, et al.,2019). In IoTs there are chances of easy access, copying, exploitation, and dissemination of digitalised data with the multiplication of probability of attacks on multimedia (Ahmadian, and Habib,2011). The current level of data security standards is still immature with numerous reports on constant data violations from big international organisations. The estimated yearly economic loss resulting from cyber strikes and data raid is 1 trillion US dollars as per the Global Risks Report 2018 (Mohammad S., et al.,2006).

The violations are in different areas like healthcare and defence cannot be tolerated due to greater sensitivity of the data proportion; therefore any little change could lead to deadly judgment (Megias, and Mohammed,2011). Sadly, healthcare is not left either. A ransomware strike in the DB of the Pacific Alliance Medical Center PAMC, resulted in the violation of the medical data of 266,123 victims (Jinyuan, et al.,2018). A lot of other comparable incidences might be established (Baziyad, and Ibrahim,2018; Huffman,1952). The disappearance of data linked to the privacy of many customers results in critical issues for affected companies, as this leads to charging of huge fines by many legal administrations (Santhoshi, et al.,2015). An estimate of 5 billion dollars results yearly from legal suits and post violation rectifications in US healthcare (Anita, et al.,2016). This being the cause for companies paying millions to several security organisations to conceive methods to minimise loss. To be able to recover losses, and levy fines on perpetrators, there is the provision of copyrights of intellectual possessions in the courts (Wei Lu, and Wei,2014).

The requirement for legitimate persons is to conceive a genuine technique for claiming copyrights in case of violations. This means certainty difficulties encountered during data dissemination via many links require improved quality of service (QoS) from information managing divisions. Moreover, there is a necessity for methods that support honesty and

authenticity to safeguard copyright and make certain on secure and legitimate utilisation of digitalised documents (Hashim, et al.,2018). Lack of data privacy, confidentiality and authenticity and privacy would lead to low adoption of IoT applications (Dominic, and Crina Raţiu,2014). Data hiding methods are highly efficient for maintaining authentic and private secure dialogue (Khan, et al.,2015). An information concealing method covers the significant digital information of a client in any cover media like a picture or audio form from some unauthorised attacker.

For an improved level of privacy of data transfer in IoTs, medical image a steganography scheme has been proposed using individual and double pixel allocation schemes, three random functions and bit invert system (BIS). Preceding the embedding scheme and to intensify the security level, the affine cipher was used to encrypt the patient data and Huffman coding to minimise the encrypt data and increasing payload ability.

The remaining part of this study is arranged as below: section II provided an overview of the related works, while section III briefly describes the proposed work and its methodology. This section also detailed the systematic explanation of the proposed method, focusing more on the data embedding and extraction frameworks. The results and evaluation of the proposed methodology were presented in section IV, while section V provided the conclusion of the study.

Related Work

a- Background of Framework

The certainty and discreetness of data dissemination in an IoT related implementation entail stronger and secure designs. A variety of methods have been suggested for prevention of unauthorised gain of multimedia data. However, security with relation to cyber-attacks is a persisting difficulty in distributed IoT structures. The most significant way to provide secure data transmission in an IoT structure and guard against intellectual structures, there must be a guard against cyber strikes. A reliable picture allocation method of objects with cloud structure linked with IoTs is shown (Hwan Jie, et al.,2015). The suggested method entails shadow images initiated from data and inserted in an object likeness via 24-are notional idea. Its limit is the lack of adoption of a security method, the standalone protective method is hiding and when algorithm violation occurs, data is endangered.

Spatial domain-based picture information covering technique for acquiring the broadcasting of Internet Protocol (IP) camera pictures of IoT object is shown (Li, et al.,2019). This method utilises the idea of inverted (ILSB) to encode the images prior broadcasting into different gadgets or selected cloud correlating with an IoT structure. On the contrary, these information covering methods lack inspection for extraction efficiency concerning cyber attacks.

A High capacity (EHR) details concealing mechanism was suggested for the IoT directed E-healthcare implementation (A., et al.,2019). The concealment of information in a medical picture is attained via modular computational functions together with PRM- Pixel Repetition Method. Various SD-spatial domain methods are available in (Jobin, and Varghese Paul.,2016). In as much as these methods are computationally systematic, the security presented to the discrete information is regarded as insufficient for the present and upcoming incidences.

Likewise, a blind and strong watermark method depending on the (CNN) is suggested at (Seung-Min, et al.,2017). Nevertheless, this procedure provides simple inadequate vigour as opposed to many attacks. Moreover, an improved level of robustness is achievable via inserting a watermark in the transformed arena. Few of the famous modified arenas with implementation of the watermarking procedures are inclusive of DCT, DWT, and IWT (Ling-Yuan, and Hwai,2015) The procedures depend on the hybrid collaboration of these modified areas resulting in improved complexity, minimal imperceptive and payload to improve robustness (Nasir N., et al.,2019).

The security of the watermark is a significant consideration during the development of a watermarking procedure. With a correct conceived security method, unauthorised access would exhibit meaningless information during a violation of extraction algorithm. The additional security safeguard is significant in the present world because of the availability of higher processing multimedia gadgets to unlicensed personnel (Zheng, and Jiwu Huang,2015). Despite the used of encryption algorithms such as: Advanced Encryption Standard (AES), Data Encryption Standard (DES) and Rivest–Shamir–Adleman (RSA), for security improvement, they exhibit unsuitability characteristic for application in digital pictures, even with their distinctive characteristics like vigorous connections with adjacent pixels, improved redundancy and larger structures (Prerna, and Abhishek Sachdeva.,2013).

A reliable medical detail sharing model incorporating a synthesis union of AES and RSA has been suggested for IoT-based healthcare structures (Mohamed, et al.,2018). Besides encoding the medical details, the procedure conceals the details in a second-level DWT band of a cover picture. Despite the achievement of a simple favourable discernible quality of the stego image, the fulfilment in existence of diverse regularly resulting strikes lacks evaluation. The outcome of the merging of AES and RSA is more encryption period and hence unsuitable for resource-restricted instant implementations in an IoT domain. There are popularity and utilisation of chaotic maps for security reasons in various structures ascribed by their features like greater susceptibility to original variables, pseudo-randomness and non-linear behaviour (Xingyuan, and Kang,2014).

In reference (Junlin, et al.,2015) there is the utilisation of Arnold cat map for encryption of the watermark prior to inserting in a colour image. The procedure entails Quaternion Discrete Fourier Transform (QDFT) and enhanced Uniform Log-Polar Mapping (IULPM). Despite good embedding capacity and imperceptibility of the procedure, there is poor vigour regarding Gaussian noise, sifting and few geometric strikes. Moreover, weak security is issued by the Arnold encryption method because of low keyspace and invariably familiar algorithm (Zheng, and Jiwu,2015) Furthermore, enhancement of security is possible through the incorporation of more than one chaotic maps following each other with reliance on the necessitated proportion of security.

A secure watermarking procedure exists as described in reference (Nazir A., et al.,2018). The method utilises dual-encryption with the form of two chaotic maps. The injection precedes behind administering DCT on the 8x8 blocks by combining, from two adjacent blocks, a pair of DC coefficients. The power of vigour is ascertained through an embedding element whose value places the length of guard bands in the middle of the areas determined by watermark bits. There is poor performance regarding few areas oriented geometric strikes even with the high robustness offered by the procedure for filtering, compression, and noisy attacks. The disadvantage is as a result of injecting watermark bits though the utilisation of neighbouring adjacent 8 x 8 blocks. Therefore, during region-based strikes like trimming or rotation, the image information is lost. Moreover, the watermark also is erased and tampered with because of two coefficients utilise watermarking data in two, blocks that entail 128 coefficients, further tampering.

The security method utilised the Arnold Chaos encryption lacks efficiency due to small key structure and enhancement in difficulty with a high number of iterations of Arnold encryption. Moreover, security is possible via the manipulation of all keys and not an alteration of one key.

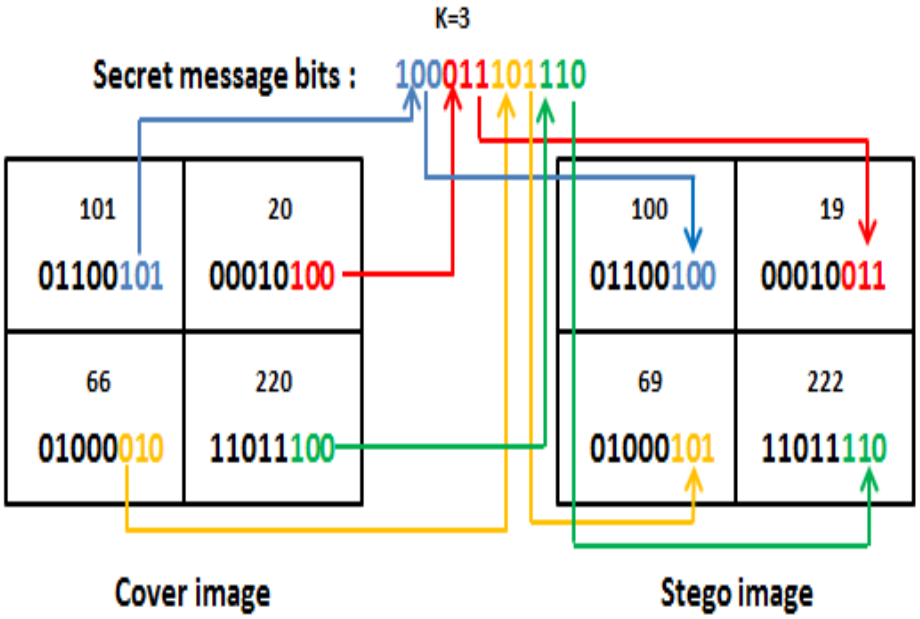
Hence a secure and strong data encapsulation method is suggested in this study to conquer the restrictions linked with the newly suggested procedure. The objective is securing the privacy and confidentiality of the details to provide dissemination of reliable medical data in the IoT structure by combining information hiding and cryptography procedures. A comprehensive exploration of the suggested procedure is analysed in section 3.

b. least significant bit substitution (LSB)

Least significant bit (LSB) substitution is a conventional and simple method exploited to insert secret data within a cover image (Domain,2015). While this process is ongoing, it is possible to overwrite the binary representation of the secret data. With regards to the grey-scale images whose pixels possess just a single value differing from 0 into 255 and the bit

depth of 8 bits, the bit of the secret information cannot be converted into binary bits because they are utilised instantly to substitute the cover object's image (Hashim, et al.,2019). Pertaining the colour images that possess 3 routes (RGB) and the bit depth of 24 bits, the cover object (image) is initially divided into 3 channels prior embedding the secret information in each of the channels. Finally, the three paths are merged so as to produce the stego image. The modification of the LSB bits does not allow the HVS to detect the stego-image (Mohammed Mahdi, et al.,2018). Since a distinct kind of the LSB substitution method is utilized in the proposed scheme, a mathematical expression of the method is provided with adequate details. This mathematical expression aims to provide deeper insight into the central idea of the scheme in section 3.

Figure 1. Possible pixel value transitions with LSB substitution



Diverse embedding percentage (EP) of LSB which includes 6.25%, 12.5%, 18.75% and 25% which means 0.5, 1.0, 1.5 and 2 bpp respectively are used based on the capacity that is to be embedded. Through the use of a simple instance, a comprehensive explanation of the central idea of the LSB-based steganography is provided in figure 1.

$$P_c = \begin{cases} P_s - 1 \ ,if\ A \neq LSB\ (P_s) \text{ and } P_s \text{ is Even} \\ P_s + 1 \ ,if\ A \neq LSB\ (P_s) \text{ and } P_s \text{ is Odd} \\ P_s \quad\ ,if\ A = LSB\ (P_s) \end{cases} \qquad (1)$$

Where, P_c and P_s represent the stego and cover image pixel values, respectively, and A is the desired bit value of the secret message (Mustafa Sabah, et al.,2019).

A method that ensures imperceptible visual data hiding in Positron emission tomography (PET) images were presented by (Nambakhsh,2011), using ECG images as the secret images. In this study, multi-resolution wavelet decomposition was used in selected PET image sections which are believed to be unnoticeable to the human eye. Another study (Mohammad S. et al.,2006), proposed the use of lossless compression approach for embedding medical data. Here, embedding was executed after utilising the embedded zero-tree wavelet (EZW) algorithm to compress the original image. In (Mohammad S. et al.,2006), a watermarking procedure that boasts the combination of data compression, encryption and watermarking was presented. This approach applied the image moment theory to radiology images. The framework incorporated DICOM data as a watermark for medical images' embedment. Another study has provided a reversible data embedding technique for medical images (Megias, and Mohammed,2013). This approach works by splitting the image into tiles before shifting their histograms between their lowest and highest frequencies. The embedment of the secret data is then performed at the pixel with the maximum frequency; this ensures maximisation of the payload hiding capacity.

c. Random function

Many studies have been carried out in steganography to develop, novel methods through which messages can be secured using steganography (Wei Lu, and Wei,2014). To enhance data privacy, many such studies have used the random technique because of its higher efficiency and ease of use. The following are the advantages of a randomised algorithm:

- Rapid and ease, or even both for diverse problems.
- Easy implementation.
- Rapid with high probability and/or
- Produces optimum output with very high probability.

In the literature, it has been found that several authors have leveraged the advantages of the random maps function, with each having its shortcomings and strengths. Based on behaviour, there are diverse kinds of random maps in existence, and they include, NUBASI (Santhoshi, et al.,2015), Arnold scrambling (Anita, et al.,2016), LDA (Wei Lu, and Wei,2014), Henon map (Dominic, and Crina,2014), and Knight Tour (Khan, et al.,2015). In normal random maps, the number is selected using a single parameter, with the initial condition of this function being (single) is 10^{15}, while the possibility of discovering these numbers is 2^{50} (Tayarani-N, and Mehdi,2015). Three random maps are used for the allocation of pixels to maintain the proposed work.

D. Steganography in Medical Image

ECG signal used to host a secret record of patients in (Anukul, et al.,2019) by applying Bernoulli's chaotic map to choose the appropriate position for embed secret medical report; LPF filter used in both encode and decode signal of ECG. System medical image retrieval designed to find Rejoin Of Interest (ROI) to get features used for embedding in steganography system based on image retrieval after concealing introduced by (Peter, et al.,2019). Telemedicine developed using frequency domain of wavelet transform in terms of watermarking, three levels of DWT used to embed secret information within the high pass and low pass of sub-band in stego image suggested by (Rajan, and S.,2019). Blowfish algorithm modified to secure both text record and medical image using power function to encrypt the secret information; Unified Average Changing Intensity (UACI) with Number of Pixel Change Rate (NPCR) manipulate to make the system more robust against attack introduced by (Oluwatobi, et al.,2019). Coefficients of Discrete Cosine Transform (DCT) help to achieve good results of dividing the cover image into 8 × 8 windows pixel with no overlapping between them; frequency domain is helpful special with watermarking technique suggested by (A., et al.,2019). The goal here to find a new method to overcome the disadvantages of existing methods and improved the results, detail methodology presented in the next section.

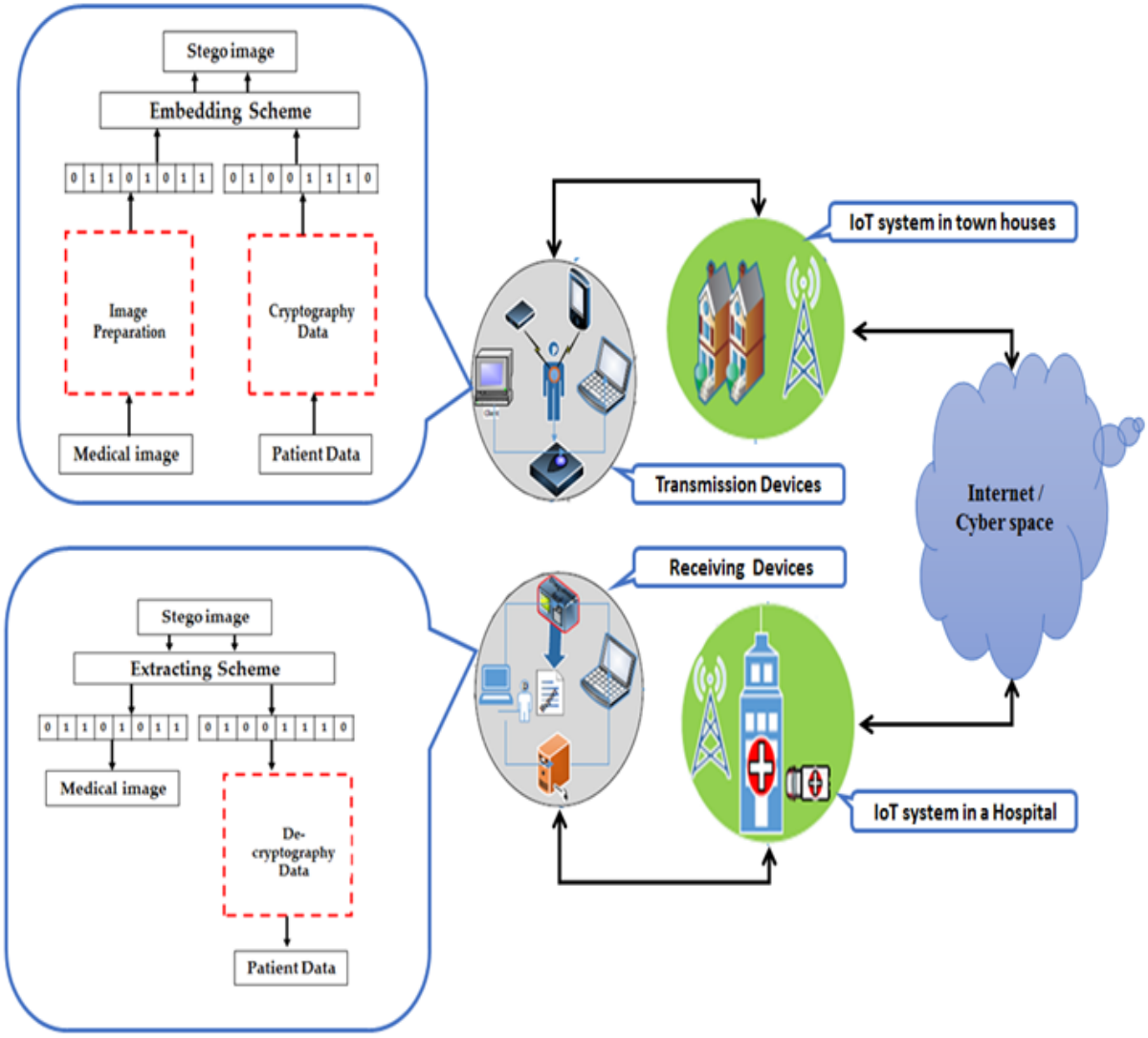
Proposition and Methodology

This part provides a discussion on the suggested method for conserving data confidentiality when disseminating in IoT. Data confidentiality is significant in IoT because of the passing of information via multiple hops and is possible through a reliable encoding procedure. Therefore, the many combinations of gadgets, services, and interconnections, linked through a plethora of data create provision for privacy breach caused by the ease of data availability in an IoT connection [8]. Therefore, a reliable data transfer model for a secure IoT connection is suggested as shown in Figure 2. This is a visualisation of the scenario in healthcare employing an IoT distributed structure over various settlements and municipalities.

The three leading phases of data hiding structure entail:

1- sender position (Patient side): processes information to achieve security and privacy,
2- Cyberspace (Internet layer) **-** network or storage space vulnerable to strikes and information exploitation.
3- Receiver position (Hospital side) **-** obtains and decodes confidential information from the stego image.

Figure 2. Suggested Hiding data and extraction scheme for broadcasting between IoT gadgets

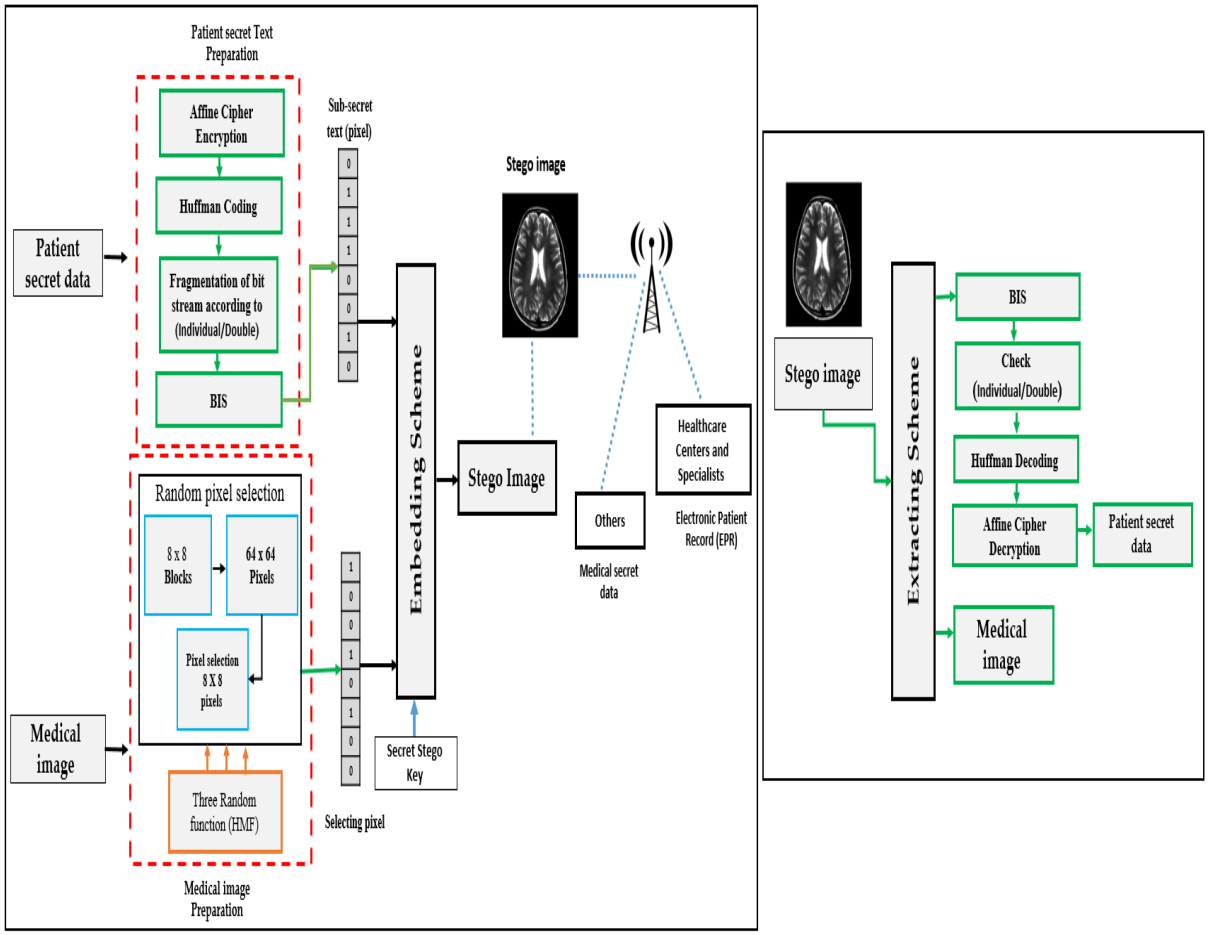


The postulated technique employed the medical image in terms of the spatial domain depending on different techniques (three variables random functions, Huffman Coding, affine cipher) to securing a larger size of data and significant security by given a stego object (image). The major intent of this study is designing and developing a scheme that can give a better security level to the secret data without losing the stego-image quality. Figure 3 illustrates the entire proposed hiding data.

There are five sub-schemes in the proposed scheme: A) the affine cipher which is used for patient data cryptography; this guarantees enhanced security; B) the Huffman Coding for compressing the encrypted data before embedding; C) Bit invert system (BIS) for checking the similarity between the bits of the original image and the patient data; D) the data embedding

scheme which variably hides the encrypted patient details in the medical image to generate the stego images which are bound to be forwarded to the designated users; E) the retrieval/extraction scheme which is utilised to retrieve the embedded data from the received stego object (image) for usage. These algorithms are briefly reviewed in section 3

Figure 3. The proposed diagram illustrating the hiding data scheme



A- Affine Cipher

The affine cipher formula can be interpreted as standard switch cipher which is controlled by a rule that letter will be replaced by another letter. The function used to encipher each letter is (ax+b) mod (26), where b is the shift-magnitude. According to the affine cipher first, alphabets of size 0...m-1 are mapped to integers. Then, modular arithmetic is used to transfer the integer in a fashion that each plaintext letter corresponds to another integer, which represents another cipher-text letter. For single letter encryption, the function used is mentioned as:

$$E(x) = (ax + b) \mod m, \quad (2)$$

Where “a” and “b” are the keys of the cipher and m is the size of alphabets. The value “a” will be chosen in a way that it comprises of “m”. The decryption function for a single letter is mentioned as:

$$D(x) = a^{-1}(x - b) \mod m, \quad (3)$$

Where a^{-1} is the modular multiplicative opposite of m modulo, that is, to satisfy the rule:

$$1 = aa^{-1} \mod m. \quad (4)$$

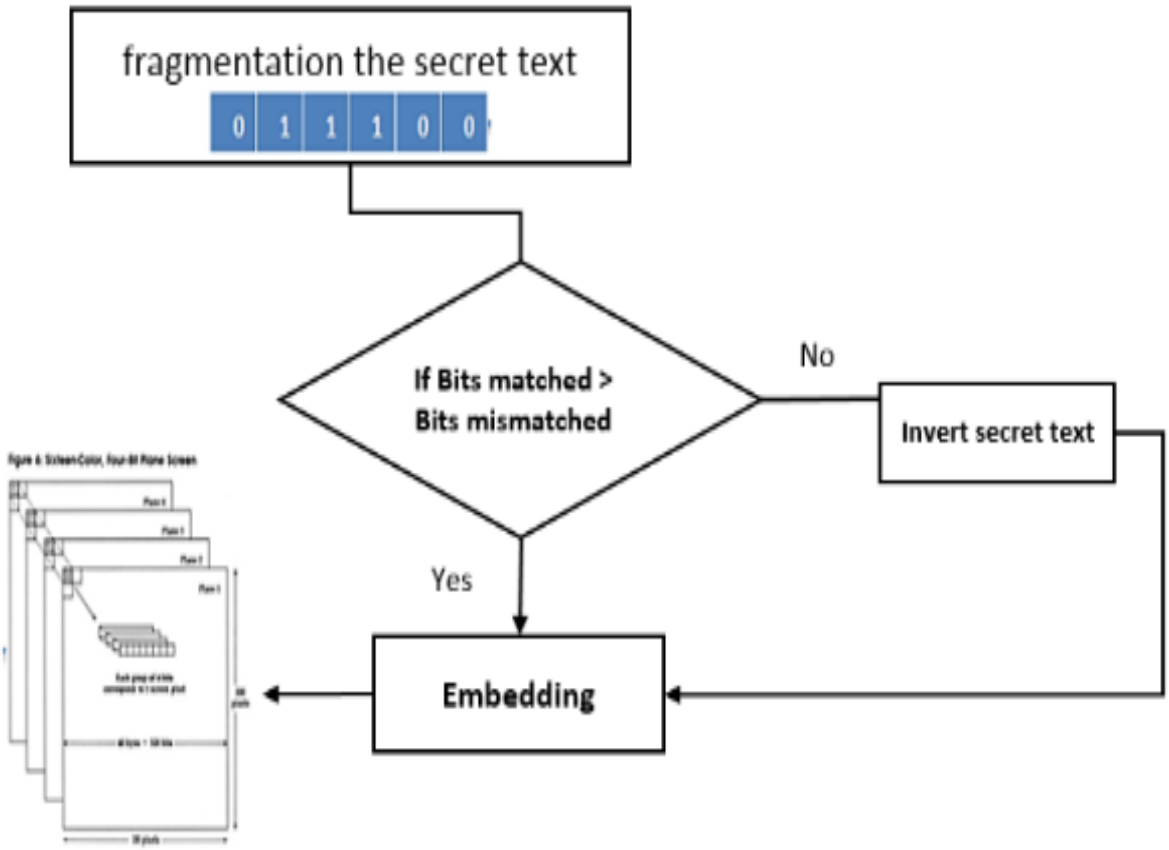
A. Huffman Coding

Huffman coding (HC) is among the common data compression methods which consider a kind of prefix code. David Huffman using the redundant letters in the text [16] developed it in 1952. HC is mainly suitable for lossless data compression and was used in this study for secret data compression before the embedding. This adopted compression phase in this work is more efficient in comparison to the other compression methods.

B. Bit invert system (BIS)

After selecting the pixels, these pixels are arranged as a sub-window of 8 x 8 pixels as shown in figure 2, then take the LSB of each pixel that is now ready for embedding. On the other hand, the secret data fragments the blocks of 64 bits. At this stage, the bits (from LSB of pixels of the image) are replaced with 64 bits (from the secret data).

Figure 4. Bit invert system process



Bit invert system (BIS) is used to check the match between bits in original image and bits of the secret data before the replacement, if several matching bits is less than mismatched bits, then invert secret data and embed it, otherwise embed secret bits directly. Figure 4, explains the BIS before the embedding process.

C. Embedding process

Embedding Process
Input: C_IMG (Cover image). S_BIT (Secret text).
Case a: 1. Read and change Se_Bits into binary. 2. Perform the Affine Cipher to Se_Bits 3. Use Huffman coding to compression the (Se_Bits). 4. Determine the magnitude of Se_Bits (Number of bits 262144). 5. BIS 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 *bl*ocks. 3. Choose block randomly via using first variable of HMF-1. 4. Use second variable of HMF-2 to select the 64 x 64 pixels 5. Use third variable of HMF-3 to select the destination pixel.
Case c: 1. Generate H vector and organize based on Double/Individual. 2. Comment on the LSB of each pixel. 3. Generate loop L=1:N. 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 are embedded
Output: EM_BIT (Stego-image).

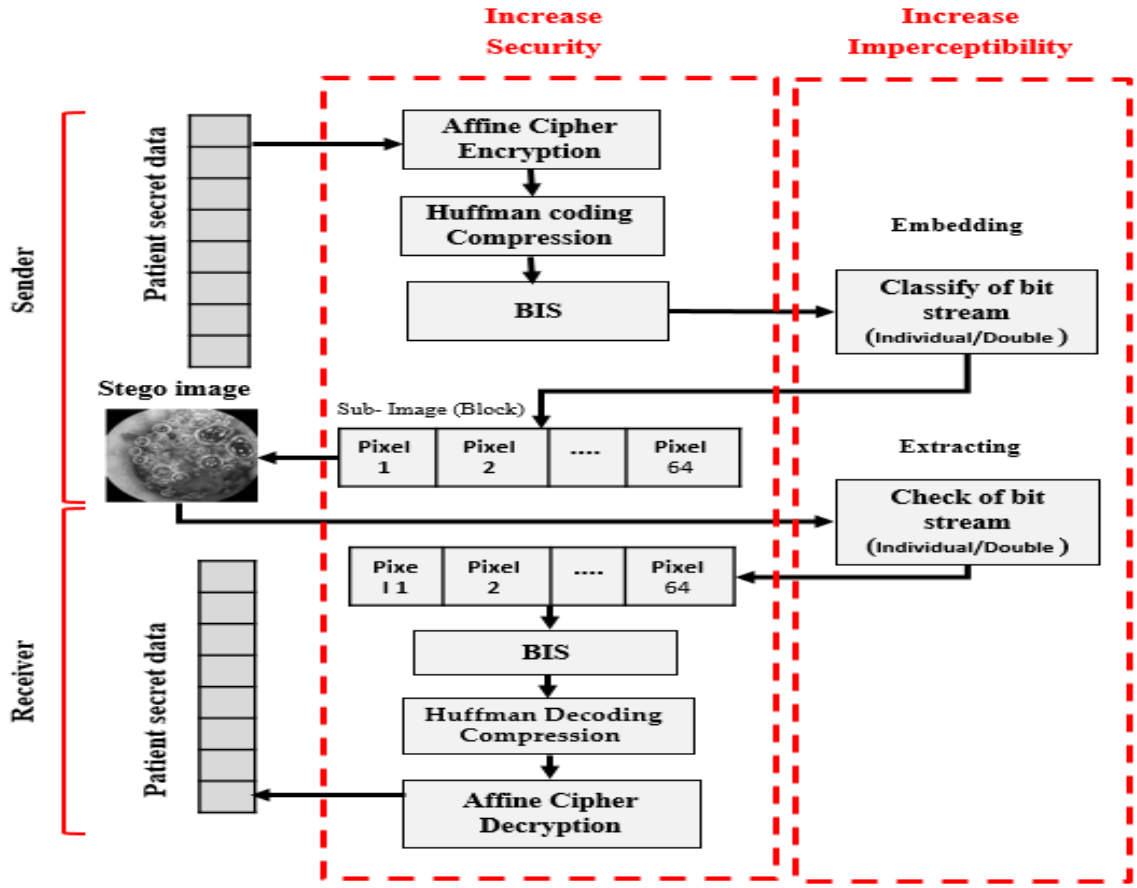
The EP is employed to hide the compressed discrete information in the LSB part of the carrier via a secret key. The two steps of the embedding process are block selected and embedding data. Both steps are executed simultaneously when embedding the secret data into the carrier image. The cover image (512 * 512) was the first partition into 8 × 8 blocks with each block having 64×64 pixels. A random collection procedure was performed using a Henon map function (HMF-1) to select random blocks. The sub-blocks (each of 64 * 64 pixels block) were selected using the second variable of HMF-2. Finally, the third variable of HMF-3 was used to select the 8 * 8 pixels block that can give the last destination.

D. Retrieval/Extraction process

The extracting process aims in getting data from the LSB pixels and needs to precede the process postulated and built within the embedment procedure. It is situated in the other receiver, which comprises guidelines with the agreement between two parties through stego

key to direct the processes. The extracting procedure is identical to the embedment but in the opposite form, this implies that the LSB components of pixels evaluate pixel in terms of individual or double. Double value of pixel comprises 0 in LSB because of binary impact values and 1 individual pixel value of 1. The majority of information regarding the parameters is shown through the block and image partitioning, in conjunction with the fragment of a secret message. This is referred to as public information, while the technique preceding the embedding procedure is called private information. In this, the extracting and embedding attained two major goals, which are imperceptibility and security; this is illustrated in Figure 5.

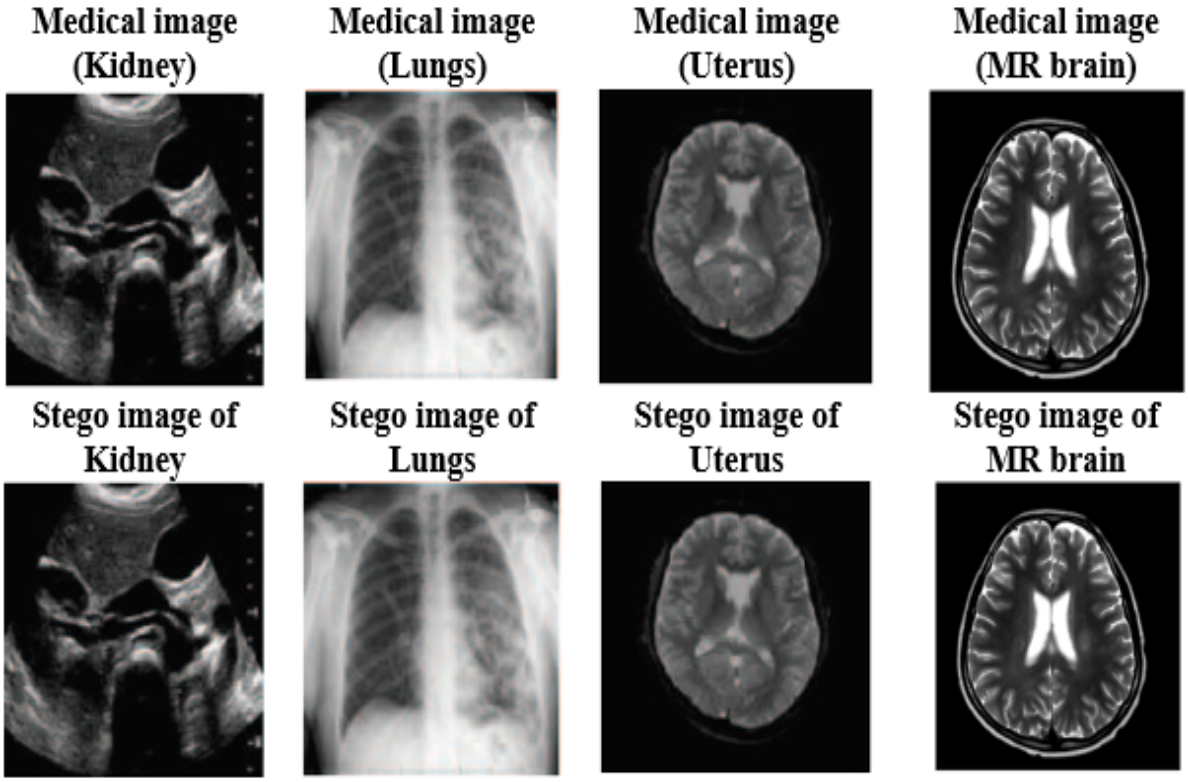
Figure 5. The main objectives of the proposed scheme.



Result and Evaluation

In the result performed in this study, the use of MATLAB tool alongside four standard images that are contained in Figure 11 was employed. The images with size (512 x 512) were obtained from different databases. The experimental results are obtained by considering the large capacity of each image for the respective techniques. The different stego-images for the proposed technique with embedding percentage (EP) = 2 are contained in Figure 6.

Figure 5. The first row has the original medical image, of size 512 x 512 pixels, the second row has the stego image of the first row.



The proposed approach has been evaluated using different parameters such as PSNR, EC, bits per pixel (BPP) and Structural Similarity Index (SSIM). In order to check the robustness of the suggested technique against attack, BER was used.

E. Evaluate based on EC, PSNR, BPP, and SSIM

The embedding capacity EC is defined as the ratio of the number of message bits to the number of cover pixels [6, 8]. This is directly related to the number of pixels used in the scheme that is proposed in this study as a different number of message bits are embedded by one pixel.

$$C = \frac{\textit{The number of message bits}}{\textit{The number of cover images's pixels}} \qquad (5)$$

In the current study, diverse payload capacities were used and presented as a percentage to be in accordance with that of recent studies in this field. For more clarification, the following is given:

- The 16384 Bytes which is equal to 6.25% for a given image 512 x 512, meaning that every two pixels = 16 bits, so 1/16 = 6.25% when 1 bit of two pixels is embedded.
- The 32768 Byte which is equal to 12.5% for a given image 512 x 512, meaning that every pixel = 8 bits, so 1/8 = 12.5% when 1 bit of one pixel is embedded.
- The 49152 Byte which is equal to 18.75% for a given image 512 x 512, meaning that every two pixels = 16 bits, so 3/16 = 18.75% when 1.5 bit of one pixel is embedded.

The method for image quality evaluation is determined by peak signal to noise ratio (PSNR), which is calculated after the process of embedding to compare original and stego images. The process of embedding data is considered imperceptible to the human vision system (HVS) if the result of PSNR calculation is equal to or greater than 30db [14]. By applying the following equations, PSNR can be calculated.

$$\boldsymbol{PSNR = 10log_{10}\left(\frac{255}{MSR}\right)} \qquad \textbf{(6)}$$

Where, MSE is mean square error, which is calculated by the following equation:

$$\boldsymbol{MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}(x_{ij} - y_{ij})} \qquad \textbf{(7)}$$

In measuring the similarity between the original image and the stego-image, the use of SSIM is utilized [15]. Eq. (8) is used in computing the similarity. The range of SSIM value is from -1 to 1. If the SSIM value is 1, it means that there is no difference between the original image and the stego-image.

$$\boldsymbol{SSIM = \frac{(2P_O\,Q_S + C_1)(2\sigma_{OS} + C_2)}{(P_O^2\,Q_S^2 + C_1)(\sigma_O^2 + \sigma_S^2 + C_2)}} \qquad (8)$$

For the original image and the stego-image, they represent the mean pixel value, variance, and standard deviation, respectively. rOS represents the covariance between the original image and the stego-image while the constant c1 = k1L and c2 = k2L. For the grayscale image, k1 = 0.01, k2 = 0.03, and L = 255.

Table 1: Results for Proposed Scheme With 6.25% of EP

Cover image 512 x 512	Proposed Scheme (6.25%)					
	PSNR	**EC**	**Bpp**	**SSIM**	**BER**	**BER-P**
Kidney	72.20	131,072	0.5	1	0.01383	1.38%
Lungs	72.11	131,072	0.5	1	0.01386	1.38%
Uterus	72.40	131,072	0.5	1	0.01380	1.38%
MR brain	72.40	131,072	0.5	1	0.01382	1.38%
Average	**72.28**	**131,072**	**0.5**	**1**	**0.01382**	**1.38%**

Table 2: Results for Proposed Scheme with 12.5% of EP

Cover image 512 x 512	**Proposed Scheme (12.5%)**					
	PSNR	**EC**	**Bpp**	**SSIM**	**BER**	**BER-P**
Kidney	66.62	265,144	1	0.99	0.01500	1.50%
Lungs	66.44	265,144	1	0.99	0.01504	1.50%
Uterus	66.68	265,144	1	0.99	0.01499	1.49%
MR brain	66.55	265,144	1	0.99	0.01502	1.50%
Average	**66.56**	**265,144**	**1**	**0.99**	**0.01488**	**1.48%**

Table 3: Results for Proposed Scheme with 18.75% of EP

Cover image 512 x 512	**Proposed Scheme (18.75%)**					
	PSNR	**EC**	**Bpp**	**SSIM**	**BER**	**BER-P**
Kidney	61.18	393,216	1.5	0.99	0.01633	1.63%
Lungs	61.20	393,216	1.5	0.99	0.01634	1.63%
Uterus	61.33	393,216	1.5	0.98	0.01631	1.63%
MR brain	61.26	393,216	1.5	0.99	0.01632	1.63%
Average	**61.25**	**393,216**	**1.5**	**0.99**	**0.01632**	**1.63%**

F. Robustness Evaluation against Bit Error Rate (BER)

The robustness of the proposed scheme was evaluated using a bit error rate (BER). Robustness refers to the ability of the secret bits to resist attacks. The value of PSNR is inverted to obtain the bit error rate using the following equation:

$$BER = \frac{1}{PSNR} \qquad (9)$$

The section of the original cover image's qubits that are converted during the process of steganography is determined by the BER. In the case whereby the PSNR is 50 dB, the BER would be 0.02, i.e., alterations have been made to 2% BER-P of bits during the process.

Tables 1,2 and 3 present the results of the calculated BER, PSNR, EC, SSIM, BER-P and Bpp in the simulation of the current study.

Conclusion

Due to fast expansion and increasing attention in medical data, it can effortlessly be snatched or captured in the course of storing, dissemination or acceptance via internet and network. These cybercrimes can be avoided when securing medical details. A certain and vigorous information hiding methods for maintaining security and confidentiality of information in the process of transmission in an IoT structure has been discussed in this study. The proposed medical image steganography scheme based on BIS and three random control parameters have suggested, to stop against cybercrimes challenges and maintaining a high level of security in an IoT environment. To increase the security level, the affine cipher was used to encrypt the data and Huffman coding to minimise the encrypt data prior to the embedding for increasing payload ability. Two major elements bring the effectiveness of the technique: first, inspecting harmonisation of secret bits with LSB and mapping to decide 0- and 1-bits during embedding, and second, subdividing the secret data to trace and map every bit in stego image. The security of the injected data was protected by employing a current security module, suggested in the undertaken study. The outcome from the suggested procedure can accomplish protected confidentiality of patient data. Testing has been done due to the reason that every single bit alteration in the key, provides no clue regarding the plain text. The objective of the submitted work is the provision of secure information from multimedia gadgets substituted as visual sensors in IoT surrounding. In future, different kinds of gathered information from a variety of IoT gadgets will be chosen and enhanced data interchange methods will be submitted for a disseminated IoT administration.

REFERENCES

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

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

HASHIM, MOHAMMED, et al. "A Review and Open Issues of Multifarious Image Steganography Techniques in Spatial Domain." *Journal of Theoretical & Applied Information Technology* 96.4 (2018).

Hashim, Mohammed Mahdi, et al. "Performance evaluation measurement of image steganography techniques with analysis of lsb based on variation image formats." *International Journal of Engineering & Technology* 7.4 (2018): 3505-3514.

Domain, W. T. I. S. "A review and open issues of diverse text watermarking techniques in spatial domain." *Journal of Theoretical and Applied Information Technology* 96.17 (2018).

Mahdi Hashim, M. O. H. A. M. M. E. D., Mohd Rahim, and Mohd Shafry. "Image Steganography Based on Odd/Even Pixels Distribution Scheme and two Parameters Random Function." *Journal of Theoretical & Applied Information Technology* 95.22 (2017).

Hashim, Mohammed Mahdi, et al. "An extensive analysis and conduct comparative based on statistical attach of LSB substitution and LSB matching." *International Journal of Engineering & Technology* 7.4 (2018): 4008-4023.

Mahdi, Mohammed Hashim, et al. "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*. Vol. 518. No. 5. IOP Publishing, 2019.

Taha, Mustafa Sabah, et al. "Wireless body area network revisited." *International Journal of Engineering & Technology* 7.4 (2018): 3494-3504.

Taha, Mustafa Sabah, et al. "Combination of Steganography and Cryptography: A short Survey." *IOP Conference Series: Materials Science and Engineering*. Vol. 518. No. 5. IOP Publishing, 2019.

Nambakhsh, Mohammad-Saleh, Alireza Ahmadian, and Habib Zaidi. "A contextual based double watermarking of PET images by patient ID and ECG signal." *Computer methods and programs in biomedicine* 104.3 (2011): 418-425.

Nambakhsh, Mohammad S., et al. "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, 2006.

Fallahpour, Mehdi, D. Megias, and Mohammed Ghanbari. "Reversible and high-capacity data hiding in medical images." *IET Image Processing* 5.2 (2011): 190-197.

Tao, Jinyuan, et al. "Towards robust image steganography." *IEEE Transactions on Circuits and Systems for Video Technology* 29.2 (2018): 594-600.

Rabie, Tamer, Mohammed Baziyad, and Ibrahim Kamel. "Enhanced high capacity image steganography using discrete wavelet transform and the Laplacian pyramid." *Multimedia Tools and Applications* 77.18 (2018): 23673-23698.

Huffman, David A. "A method for the construction of minimum-redundancy codes." *Proceedings of the IRE* 40.9 (1952): 1098-1101.

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

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

Feng, Bingwen, Wei Lu, and Wei Sun. "Secure binary image steganography based on minimizing the distortion on the texture." *IEEE transactions on Information Forensics and Security* 10.2 (2014): 243-255.

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

Muhammad, Khan, et al. "A Secure Method for Color Image Steganography using Gray-Level Modification and Multi-level Encryption." *TIIS* 9.5 (2015): 1938-1962.

Aziz, Mahdi, Mohammad H. Tayarani-N, and Mehdi Afsar. "A cycling chaos-based cryptic-free algorithm for image steganography." *Nonlinear Dynamics* 80.3 (2015): 1271-1290.

Pandey, Anukul, et al. "Bernoulli's Chaotic Map-Based 2D ECG Image Steganography: A Medical Data Security Approach." *Medical Data Security for Bioengineers*. IGI Global, 2019. 208-241.

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

Sivaprakash, Asokan, Samuel Nadar Edward Rajan, and S. Selvaperumal. "A Novel Robust Medical Image Watermarking Employing Firefly Optimization for Secured Telemedicine." *Journal of Medical Imaging and Health Informatics* 9.7 (2019): 1373-1381.

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

Parah, Shabir A., et al. "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, 2019. 47-70.

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

Li, Li, et al. "Distortion less secret image sharing scheme for Internet of Things system." *Cluster Computing* 22.1 (2019): 2293-2307.

Parah, Shabir A., et al. "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* (2018).

Abraham, Jobin, and Varghese Paul. "An imperceptible spatial domain color image watermarking scheme." *Journal of King Saud University-Computer and Information Sciences* (2016).

Mun, Seung-Min, et al. "A robust blind watermarking using convolutional neural network." *arXiv preprint arXiv:1704.03248* (2017).

Hsu, Ling-Yuan, and Hwai-Tsu Hu. "Blind image watermarking via exploitation of inter-block prediction and visibility threshold in DCT domain." *Journal of Visual Communication and Image Representation* 32 (2015): 130-143.

Hurrah, Nasir N., et al. "Dual watermarking framework for privacy protection and content authentication of multimedia." *Future Generation Computer Systems* 94 (2019): 654-673.

Guo, Jianting, Peijia Zheng, and Jiwu Huang. "Secure watermarking scheme against watermark attacks in the encrypted domain." *Journal of Visual Communication and Image Representation* 30 (2015): 125-135.

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

Wang, Xingyuan, and Kang Guo. "A new image alternate encryption algorithm based on chaotic map." *Nonlinear dynamics* 76.4 (2014): 1943-1950.

Ouyang, Junlin, et al. "Color image watermarking based on quaternion Fourier transform and improved uniform log-polar mapping." *Computers & Electrical Engineering* 46 (2015): 419-432.

Loan, Nazir A., et al. "Secure and robust digital image watermarking using coefficient differencing and chaotic encryption." *IEEE Access* 6 (2018): 19876-19897.

Elhoseny, Mohamed, et al. "Secure medical data transmission model for IoT-based healthcare systems." *IEEE Access* 6 (2018): 20596-20608.

Falah.Y.H.Ahmed,Muthukumaran a/l Thiruchelvam, and Muhammad Irsyad Abdullah (2019). Improvement of Vehicle Management System (IVMS). IEEE International Conference on Automatic Control and Intelligent Systems, Scopus .

Dhafer Sabah Yaseen, Shamala A/P Batumalai, Falah Y H Ahmed and Sim Liew Fong (2019). Improved Disabled Mobile Aid Application for Android : Health and Fitness Helper for Disabled People. 2019 IEEE 10th Control and System Graduate Research Colloquium (ICSGRC), Scopus.

Falah.Y.H.Ahmed,Muthukumaran a/l Thiruchelvam, and Muhammad Irsyad Abdullah (2019). Improvement of Vehicle Management System (IVMS). IEEE International Conference on Automatic Control and Intelligent Systems, Scopus .

Dian Nugraha and Falah Y. H. Ahmed (2019). Advancement parking application using MEAN stack: A narrative review (FIRST 2018 Conference in Palembang Indonesia Scopus.

Sim Liew Fong, Amir Ariff Azham bin Abu Bakar, Falah Y.H Ahmed, Arshad Jamal (2019). Smart Transportation System Using RFID (Proceedings of the 2019 8th International Conference on Software and Computer Applications) publisher ACM 579-584. Scopus.

Sim Liew Fong, David Chin Wui Yung, Falah YH Ahmed, Arshad Jamal (2019). Smart City Bus Application with Quick Response (QR) Code Payment (Proceedings of the 2019 8th International Conference on Software and Computer Applications) publisher ACM 248-252. Scopus.

Falah Y.H. Ahmed, Omar Ahmed Mahmood, Ahmed Sabeeh Yousif (2019). Comparison between improved histogram shifting and LSB (bit-plan mapping) in digital watermarking techniques (International Journal of Engineering & Technology) Science Publishing Corporation, Pages5322-5326 /4/7. Scopus.

Dian Nugraha and Falah Y. H. Ahmed (2019). MEAN stack to enhance the advancement of parking application: A narrative review. IOP science (Journal of Physics: Conference Series) 1088/1742-6596/1167/1/012075,V 1179.

Scopus.

Falah Y.H. Ahmed & Siti Mariyam Shamsuddin (2019). Spikeprop Deep Learning with Multiple Weights Optimization of Differential Evolution and Particle Swarm Optimization (Hindawi Publishing journal of Computational Intelligence and Neuroscience) 7547924 in ISI Impact Factor 0.430