Efficient Security and Authentication for Edge-Based Internet of Medical Things

Shabir A. Parah, Javaid A. Kaw, Paolo Bellavista⬛, *Senior Member, IEEE*, Nazir A. Loan⬛, G. M. Bhat, Khan Muhammad⬛, *Member, IEEE*, and Victor Hugo C. de Albuquerque⬛, *Senior Member, IEEE*

Abstract—Internet of Medical Things (IoMT)-driven smart health and emotional care is revolutionizing the healthcare industry by embracing several technologies related to multimodal physiological data collection, communication, intelligent automation, and efficient manufacturing. The authentication and secure exchange of electronic health records (EHRs), comprising of patient data collected using wearable sensors and laboratory investigations, is of paramount importance. In this article, we present a novel high payload and reversible EHR embedding framework to secure the patient information successfully and authenticate the received content. The proposed approach is based on novel left data mapping (LDM), pixel repetition method (PRM), RC4 encryption, and checksum computation. The input image of size $M \times N$ is upscaled by using PRM that guarantees reversibility with lesser computational complexity. The binary secret data are encrypted using the RC4 encryption algorithm and then the encrypted data are grouped into 3-bit chunks and converted into decimal equivalents. Before embedding, these decimal digits are encoded by LDM. To embed the shifted data, the cover image is divided into 2×2 blocks and then in each block, two digits are embedded into the counter diagonal pixels. For tamper detection and localization, a checksum digit computed from the block is embedded into one of the main diagonal pixels. A fragile logo is embedded into the cover images in addition to EHR to facilitate early tamper detection. The average peak signal to noise ratio (PSNR) of the stego-images obtained is 41.95 dB for a very high embedding capacity of 2.25 bits per pixel. Furthermore, the embedding time is less than 0.2 s. Experimental results reveal that our approach outperforms many state-of-the-art techniques in terms of payload, imperceptibility, computational complexity, and capability to detect and localize tamper. All the attributes affirm that the proposed scheme is a potential candidate for providing better security and authentication solutions for IoMT-based smart health.

Index Terms—Authentication, COVID-19, emotion care, imperceptibility, Internet of Medical Things (IoMT), reversibility, security, smart health.

Shabir A. Parah, Javaid A. Kaw, and Nazir A. Loan are with the Department of Electronics and Instrumentation Technology, University of Kashmir, Srinagar 190006, India (e-mail: shabireltr@gmail.com; javaidkaw@gmail.com; nazirloan786@gmail.com).

Paolo Bellavista is with the Department of Computer Science and Engineering, University of Bologna, 40136 Bologna, Italy (e-mail: paolo.bellavista@unibo.it).

G. M. Bhat is with the Department of Electronics Engineering, Institute of Technology, University of Kashmir (Zakura Campus), Srinagar 190006, India (e-mail: drgmbhat@gmail.com).

Khan Muhammad is with the Department of Software, Sejong University, Seoul 143-747, South Korea (e-mail: khan.muhammad@ieee.org).

Victor Hugo C. de Albuquerque is with the LAPISCO, Federal Institute of Education, Science and Technology of Ceará, Fortaleza 60811-905, Brazil, and also with the ARMTEC Tecnologia em Robótica, Fortaleza 60811-341, Brazil (e-mail: victor.albuquerque@ieee.org).

Digital Object Identifier 10.1109/JIOT.2020.3038009

I. INTRODUCTION

IN the last decade, e-healthcare has turned out to be one of the most important service areas that has attracted the attention of the research community worldwide [1]. The health and emotional care industry are progressing exponentially because of the new data communication and automation technologies.

This healthcare revolution known as "smart health" has made it possible for doctors to monitor and diagnose patients remotely, for physical and emotional ailments, and has paved a way for doctors to remotely operate certain kinds of surgeries as well [2]. Smart health uses technological concepts, such as cyber–physical systems (CPSs), Internet of Service (IoS), Internet of Medical Things (IoMT), Internet of Health Things (IoHT), Artificial Intelligence, and multi-access edge computing (MEC) [1], [3]–[5]. Due to multiple benefits of edge computing paradigm in an IoMT-driven smart health, massive data processing, such as heterogeneous distributed architecture, the requirement of mobility support, etc., the conventional data security and authentication mechanisms of cloud computing are no longer suitable for data security in IoMT edge paradigm. Also, in an IoMT edge paradigm, a user loses physical control over his private data as it is outsourced to the edge server separating its ownership and control. This leads to potential threats of the data breach and illegal data operations, such as copy, delete, and disseminate. As a result of data outsourcing, the data integrity in the edge paradigm could also be compromised. To create a sustainable edge paradigm ecosystem concerning security it is important to come up with some new solutions which prevent attraction from malicious attackers.

Smart healthcare involves the exchange of patient data between two or more experts placed at different global locations. It is being used as an effective tool for patient care during the ongoing COVID-19 pandemic. Unfortunately, the data breaches are increasing exponentially with every passing

day as a result of of hacking attacks. The healthcare sector observed a whopping 41.4 million patient records being breached in the year 2019 alone. As per the highly reliable Protenus breach Barometer, the breaches saw a sharp increase of nearly about 300% compared to the year 2018 in which about 15 million patient record breaches had been reported [6]. The situation is not different in the year 2020. As reported, Florida Orthopedic Institute reported a data breach involving records of 640 000 patients in July 2020. A similar security attack that resulted in a breach of 550 000, patient records was reported in June 2020 by Elite Emergency Physicians [7]. In a smart health system, a compromise with patient data integrity cannot be tolerated at all. It assumes an extra significance during the ongoing COVID-19 pandemic times when the use of smart health is playing an important role in patient care and cure while maintaining the mandatory physical distancing. To address these threats, suitable data confidentiality, integrity, and authentication schemes need to be put forward to protect the private patient data. At present, data confidentiality and authentication are mainly implemented using various data encryption techniques.

Classically, cryptographic solutions are used to ensure the security of multimedia data [8]. In cryptography, the message is scrambled such that it cannot be revealed to ill-intentioned third parties. An emerging trend for securing information focuses on combining cryptographic and steganographic approaches [9]. Steganography differs from cryptography in many ways; among them, data are not disguised into an unreadable form, hence it attracts less attention from the adversary. Lately, steganography—also referred to as data hiding (DH)—is receiving the attention of researchers and is gaining momentum for various applications. In a typical image-based DH system, the content of interest is inserted in cover images imperceptibly and then transmitted to the destination without compromising its security and robustness.

Thereby, the design goals of a typical DH technique include covert communication, watermarking, authentication, and intellectual property rights (IPRs) protection. The requirements of a DH system are payload, robustness, imperceptibility (perceptual transparency), and computational cost. In terms of deployment, a critical factor in a real-time data processing system is computational complexity. Steganography places an emphasis usually on the payload, security, imperceptibility, and computational complexity. In the case of watermarking the major focus is on robustness. Usually, DH is implemented in two domains: 1) pixel and 2) transform domain. The former can accommodate more data and is computationally less complex, whereas the latter features high robustness but is computationally more complex than its pixelwise counterpart. An e-healthcare setup is supposed to deal with real-time situations, so algorithms and methods designed for its application must be computationally efficient, capable of content authentication, and secure [10], [11].

The diagnostic information of a patient could be thought to be composed of two main components: 1) patient history (which would include prescriptions, medical reports, etc.) and 2) diagnostic imagery, such as X-ray and magnetic resonance images. For safely conveying patient data to a remote location, the following criteria should be met.

1) Security of electronic health record (EHR) while its transmission from source to destination.
2) The receiver should be able to authenticate the received content and localize any tamper in the content.
3) No diagnostic information should be lost due to pre- and post-EHR and medical imagery processing.
4) The processing time should be reduced to comply with real-time computational requirements.

This work proposes a novel framework that aims to address all the above requirements by embedding patient data in medical images. The key contributions of the proposed approach can be summarized as follows.

1) A left data mapping (LDM) mechanism is developed, which maps an arbitrary bit sequence to a corresponding shifted sequence that results in less deterioration, hence better security for a given quantum of hidden data. The principal objective of the use of LDM is to achieve high imperceptibility irrespective of high embedding capacity. In addition to this, embedding and extraction time reduces considerably with the help of LDM.
2) We have elaborated on an innovative block checksum computation mechanism for localized tamper detection. The developed mechanism can detect tamper in any 2×2 block. Furthermore, a fragile watermark has been utilized to facilitate early tamper detection.
3) The proposed system is devoid of any transformation and has been purely implemented in the pixel domain. As a result, information embedding and extraction times have been drastically reduced in comparison to the state of the art. The lightweight cost of the proposed solutions makes them particularly suitable for an edge-enabled deployed environment.

The remainder of this article has been structured as follows. A detailed related work is presented in Section II. The need for patient data security in COVID—19 has been presented in Section III, while the proposed RIH system is described in Section IV. Section V reports an extensive set of experiments and discusses results obtained therefrom. Finally, we end this article with conclusive remarks and an outline of future research work.

II. RELATED WORK

The exponential rise in multimedia technology and heavy data traffic has emerged as a catalyst for research surge in the area of multimedia security [12], [13]. Smart health involves voluminous multimedia content exchange. The use of Industry 4.0 in health technology has yielded a higher technological diversification of the area [14], [15]. High capacity RIH in medical images for smart healthcare systems is currently gaining huge interest from the research community around the globe. To date, various RIH techniques have been realized using assorted concepts, such as interpolation, compression, histogram-bin-shifting, and difference expansion. However, RIH techniques using interpolation have garnered more attention because of their high capacity, imperceptibility, and

low computational overhead. The main purpose of interpolation is to enlarge the image size. Various interpolation-based approaches have been reported so far. The first interpolation-based RIH scheme for grayscale images using neighbor mean interpolation (NMI) was reported in [16]. The authors made use of neighborhood pixels for interpolation and generation of the cover image. However, this technique can accommodate reduced payloads and poor imperceptibility. Also, based on interpolation, Luo *et al.* [17] presented a reversible watermarking technique in which sample and nonsample pixels were utilized for embedding purposes. However, the payload of this approach remained low because pixels that resulted in overflow or underflow problems were not used for embedding purposes. Qui *et al.* [18] presented an extended generalized integer transform (GIT)-based adaptive RIH approach where more data bits are concealed in smooth blocks when compared to nonsmooth blocks.

Prediction error expansion and histogram-based RIH algorithms have been presented in [19]–[21], providing a good imperceptibility yet at a low embedding capacity. An additive interpolation and error-expansion-based RIH scheme has been reported in [22] for medical images. An average peak signal-to-noise ratio (PSNR) of 49 dB for an average payload of 38 545 bits has been reported by the authors. Moreover, the computational cost is increased due to the adoption of particle swarm optimization (PSO) and GA as inner processing modules. A high capacity, computationally efficient RIH technique has been reported in [23]. In this scheme, the secret message to be hidden is image dependent: the more edges exist in an image, the more message bits can be embedded, but at the cost of perceptual quality (imperceptibility). Ahad *et al.* [24] have proposed a high capacity RIH technique for medical images. The technique offers stego-images of high perceptual quality, but the capacity is very low [0.75 bits per pixel (bpp)] and it further reduces to 0.5 bpp when incorporating watermark or keeping scope for temper detection. A transform domain-based reversible watermarking technique has been presented in [25], where high-frequency coefficients are used for information embedding. This technique provides better quality watermarked images but is computationally expensive. For the healthcare system, a reversible message embedding technique has been presented in [12], where EHR is embedded imperceptibly into the medical images. The technique offers a very high payload of about 2.25 bpp, however, its imperceptibility is comparatively low. Reversible information hiding technique using interpolation by splines on the three directional mesh has been reported in [13]. Lu [14] has proposed a very interesting reversible DH approach using interpolation, modulus function, and reencoding strategy. The technique offers a high payload of about 3 bpp, however, its imperceptibility is comparatively poor. A high capacity reversible message embedding technique based on the right–left shift has been presented in [15]. The payload of this method is high but the perceptually quality is not up to the mark. The capability to detect and localize tamper is one of the important features of an information embedding system. The tamper detection and correction techniques are usually block based.

A thorough literature review reveals that most of the reported reversible message embedding techniques have the drawback of lesser payload, high computational complexity, and tamper detection capability. In this work, we tried to resolve this issue of lesser payload and higher computational cost, while retaining reversibility (to facilitate proper diagnosis) by utilizing pixel repetition method (PRM) instead of conventional interpolation-based solutions. Furthermore, LDM has been used to provide better imperceptivity and hence better security. Tamper detection ability has been acquired by inserting a fragile watermark in the spatial domain.

III. COVID-19 AND NEED FOR SECURITY FRAMEWORK

The COVID-19 pandemic revealed the caveats in the digital health infrastructure, which has led to the effort to overhaul the entire e-health system with the help of networked technology such as IoMT. The IoMT is a medical specific type of IoT that can facilitate digital health during the COVID-19 pandemic by providing a management database for the patients, healthcare organizations, and government institutions. IoMT makes use of sensors and network connectivity, which helps in providing meaningful communication between patients and specialists. For a specialist to provide medical suggestions, diagnosis, and possible treatment strategies, the clinical image analysis is actively performed.

An integrated global virtual-care consultation is particularly important at the time of a crisis like the COVID-19 pandemic. The number of affected patients is increasing at an alarming rate as such a proper computer-aided diagnostic platform can assist the radiologists and other front-line workers to help prevent possible breakdowns of medical systems. The computed tomography (CT) scans of patients with COVID-19 show clinical findings of lung abnormalities and pneumonia. The important observations include ground-glass opacities, consolidation, linear opacities, and crazy-paving pattern. Furthermore, the real-time reverse transcription-polymerase chain reaction (RT-PCR), which is currently used to test for COVID-19, can in some cases provide false negative tests. It has been investigated that the chest CT scan can manifest these above-mentioned abnormalities even earlier than the time-consuming RT-PCR test. The chest X-ray, CT scan has been identified as a predominant tool for COVID-19 diagnosis, screening, and measurement of severity of the disease. In such a scenario medical image analysis along with proper storage and security of the medical data can be integrated to provide efficient medical care services to these patients. Patient data security and authentication framework using DH can thus help in improving the security and efficiency of the overall IoMT-based smart health system.

IV. PROPOSED METHOD

The proposed system has been developed to provide a high degree of security to EPR, besides reducing the overall computational overhead. The block diagram of the proposed system is presented in Fig. 1.

The cover image "*C*" has been generated from the input image "*I*" by PRM. As later discussed in Section IV-A, the
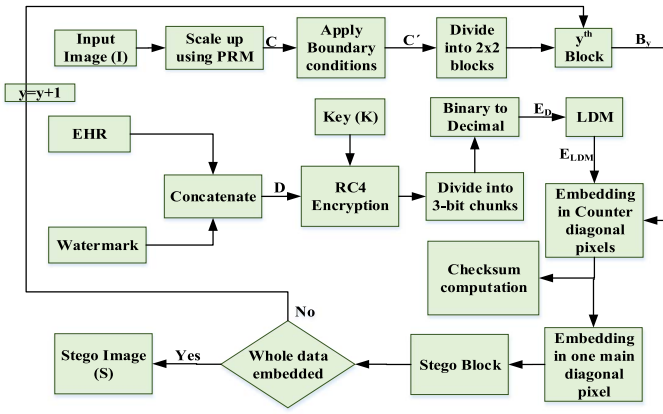
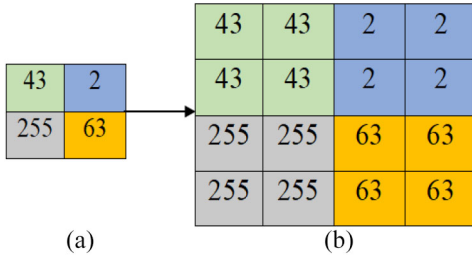Fig. 1.   Block diagram of proposed RIH system.

Fig. 3.   Proposed implementation of LDM.

Fig. 2.   (a) Original block: (b) Scaled up block after PRM.

TABLE I
PIXEL MODIFICATION IN CONVENTIONAL AND PROPOSED LDM SCHEME

Secret data to be embedded	Data embedding through the addition			
	Conventional		Proposed	
	Stego Pixel	| Ps-Pc|	Stego Pixel	| Ps-Pc|
0	$P_s=P_c+0$	0	$P_s=P_c-4$	4
1	$P_s=P_c+1$	1	$P_s=P_c-3$	3
2	$P_s=P_c+2$	2	$P_s=P_c-2$	2
3	$P_s=P_c+3$	3	$P_s=P_c-1$	1
4	$P_s=P_c+4$	4	$P_s=P_c-0$	0
5	$P_s=P_c+5$	5	$P_s=P_c+1$	1
6	$P_s=P_c+6$	6	$P_s=P_c+2$	2
7	$P_s=P_c+7$	7	$P_s=P_c+3$	3
Average absolute difference	28/8=3.5		----	16/8=2.0

use of PRM results in the generation of a 2×2 block from each seed pixel. The EHR and watermark data are first encrypted using RC4 encryption as in [26]. The encrypted bitstream to be inserted in the cover image is divided into chunks of 3 bits. Each 3-bits chunk has been represented by its decimal equivalent {0, 1, 2, 3, 4, 5, 6, 7}. As described in Section IV-B, LDM is utilized to improve the imperceptibility and payload of stego-images. Boundary conditions imposed to handle undesired pixel values are discussed in Section IV-C.

The proposed scheme is further capable of tamper detection with precise localization ability. This has been achieved by utilizing checksum bits in every 2×2 block. A detailed description of checksum computation and its embedding is presented in Section IV-D. A fragile watermark (logo) is also embedded in the cover image for content authentication. The process of embedding and extraction of secret data (patient data, checksum bits, and watermark) is shown in detail in Section IV-D and IV-E, respectively.

A. Pixel Repetition Method

Let us consider an input image I of size $M \times N$. PRM has been utilized to form the cover image C of size $2M \times 2N$. As exemplified in Fig. 3, this has been done by converting each seed pixel into a 2×2 block by repeating the pixel. Let $I(k, l)$ and $C(i, j)$ be a seed pixel of the input image, and the resultant cover image pixels, respectively. The equations given below are utilized for generating the cover image (a scaled-up version of the input image)

$$C(i, j) = I(k, l) \tag{1}$$
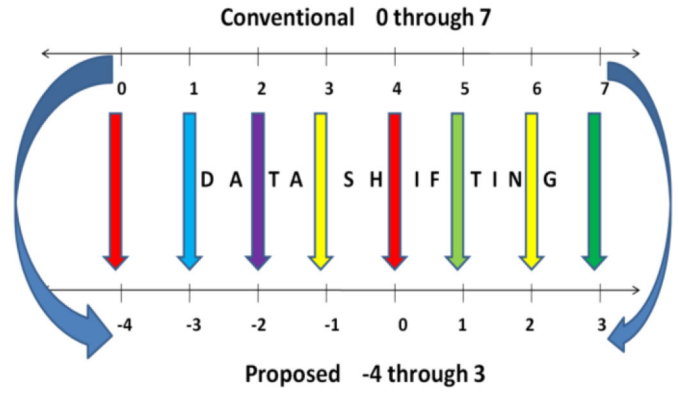$$C(i, j + 1) = I(k, l) \tag{2}$$

$$C(i + 1, j) = I(k, l) \tag{3}$$
$$C(i + 1, j + 1) = I(k, l) \tag{4}$$

with $k = 1, 2, 3, \ldots, M, l = 1, 2, 3 \ldots, N, i = 1, 3, 5 \ldots, 2M$, and $j = 1, 3, 5 \ldots, 2N$.

As seen in Fig. 2, a 2×2 block is generated from a seed pixel by repeating its value, thereby coining the name of the PRM [23], [24].

B. Left Data Mapping

LDM is a novel approach to improve payload while imprinting a lesser deterioration in a cover image. The secret message to be hidden is transformed into 3-bit chunks, which are generally represented by a decimal value ranging from 0 to 7. In the proposed LDM implementation, the data is shifted four steps toward the −ve axis of the number line. The entire range of digits that results from the 3-bit chunks, i.e., 0 through 7, are mapped to −4 through 3 (100 through 011). Fig. 3 depicts that the digits 0, 1, 2, 3, 4, 5, 6, and 7 after a four-step shift toward −ve axis of the number line are mapped to a new set of values −4, −3, −2, −1, 0, 1, 2, and 3, respectively. The embedding of shifted data results in less distortion to the cover image compared to the embedding of unshifted data.

This statement can be better understood by comparing the two-data embedding scenarios (i.e., unshifted and shifted data), as presented in Table I.

Algorithm 1 Processing of Boundary Conditions

Input: Cover image (C)

IF $C(i, j) \geq 253$ **THEN**
  Replace $C(i, j) \leftarrow C(i, j) - 3$
ELSEIF $C(i, j) \leq 3$ **THEN**
  Replace $C(i, j) \leftarrow C(i, j) + 4$
ELSEIF $3 < C(i, j) < 253$
  NoOp
END

Output: Modified Cover image (C)

As shown in this table, the patient data are directly added to the cover image pixel "Pc." For data digits, 2 to 7, the magnitude of the difference between the stego-pixel "Ps" and the cover image pixel "Pc" is less in the proposed scheme compared to the conventional one. If all the decimal symbols are equally probable, the proposed scheme produces a net average difference of 2.0 units only, while the conventional scheme results in a net average difference of 3.5 units, between stego-pixel and cover pixel. This validates the argument that the proposed technique distorts a cover image pixel by a small factor in comparison to its conventional counterpart. Therefore, the LDM plays a significant role in retaining the quality of the stego-image in the proposed approach.

C. Boundary Conditions

To overcome the undesirable pixel values (out of range pixel values due to the addition of decimal values corresponding to 3-bit message chunks), the boundary conditions for the cover image are so set that the resultant pixel falls within the grayscale pixel value range (0 to 255) even after LDM is applied. The set of conditions defined in Algorithm 1 has been applied to an arbitrary pixel, $C(i, j)$ of the cover media. It is pertinent to mention that boundary conditions are set before data embedding in the cover image.

D. Data Embedding

The process of data embedding involves inserting secret data (EHR), the fragile watermark for tamper detection/localization, and the checksum bits for authentication. The steps involved in the data embedding process are discussed in detail in Algorithm 2.

E. Data Extraction

The data extraction involves the inverse process of data embedding. The data retrieved at the receiving end contain covert EHR information, fragile logo, and the checksum bits. The retrieved watermark and EHR bits are mapped back to their original values using inverse mapping. This is followed by the application of an inverse RC4 algorithm to decrypt the message. Furthermore, for tamper detection, the checksum is again computed from the received stego-image and, then it is compared with the extracted checksum. The mismatch between the two indicates the tampering of the image. To reconstruct the original image, the seed pixels are collected from all the 2×2 blocks.

Algorithm 2 Embedding Algorithm

Input: Input image ($I_{M \times N}$), Encryption Key (K), EHR, and Watermark (W)

Step 1: Take an input image (I).
Step 2: Generate a Cover image ($C_{2M \times 2N}$) from the input image using PRM as discussed in Section (IV-A), resulting in $C(i, j) = I(k, l)$,
where $i = 2k - 1, 2k$ and $j = 2l - 1, 2l$. This equation results in a 2x2 block corresponding to each pixel $I(k, l)$ that can be written as

$$\begin{bmatrix} C(2k-1, 2l-1) & C(2k-1, 2l) \\ C(2k, 2l-1) & C(2k, 2l) \end{bmatrix} = I(k, l).$$

Step 3: Concatenate the EHR and watermark bits to make a single sequence "D" of size 1x 6MN. Represent the checksum bits for every block separately.
Step 4: Select an encryption key (K) and then encrypt the data row vector (D) using the RC4 algorithm. The obtained result is again a row vector represented as $E = Encryption\ (D, K)$.
Step 5: Group the encrypted data (E) into three-bit chunks and let the xth chunk be represented by $E_C(x)$, defined as $E_C(x) = E(r: r + 2)$, where $r = 1, 4, 7, 10, 13, \ldots, 2MN-2$ and $x = floor(r/3) + 1$.
Step 6. Convert every binary chunk by its respective decimal equivalent (i.e., 0 through 7). Let the decimal equivalent vector be denoted by (E_D), then $E_D(x) = decimal\ (E_C(x))$.
Step 7: Apply LDM to the decimal equivalent vector (E_D) as described in Section (IV-B). The data vector obtained after LDM can be represented by E_{LDM}, which is given as $E_{LDM} = E_D - 4$.
Step 8: Apply boundary conditions to cover image pixels $C(a, b)$ to limit the pixel value between 0 and +255 as discussed in Section (IV-C), i.e.,

$$\text{For } mod([a, b], 2) \neq 1$$
$$C'(a, b) = \begin{cases} C(a, b) - 3, & \text{for } C(a, b) \geq 253 \\ C(a, b) + 4, & \text{for } C(a, b) \leq 3 \\ C(a, b) = C(a, b), & \text{for } 3 < C(a, b) < 253 \end{cases}$$

Where $a = 1, 2, 3, 4, 5 \ldots, 2M$ and $b = 1, 2, 3, 4, 5, \ldots 2N$.
Step 9: Divide the modified cover C' into 2x2 blocks and let the yth be represented by 'B_y,'(where, $y = 1, 2, 3, \ldots, MN$).
Step 10: Embed two digits of encrypted secret data sequence into the block 'B_y' which results in an intermediate stego block 'B_y'.' The data is embedded into the counter diagonal pixels, leaving the main diagonal pixels untouched, given as

'B_y''$(1, 1) = B_y(1, 1)$//sparing the pivot/seed pixel '$B_y'(1, 1)$
  to ensure reversibility
'B_y''$(1, 2) = B_y(1, 2) + E_{LDM}(2y - 1)$//patient data embedded
'B_y''$(2, 2) = B_y(2, 1) + E_{LDM}(2y)$//patient data embedded
'B_y''$(2, 2) = B_y(2, 2)$//sparing this pixel for checksum digit
  embedding (to ensure tamper detection)

To facilitate the content authentication and tamper detection at the receiver side, the Checksum of each intermediate Stego-block is computed and then embedded into it. The checksum of an arbitrary intermediate Stego-block "B_y" is computed by using the following equation:

$$ChkS(y) = \left[\left(\left(\sum_{p=1}^{2} \sum_{q=1}^{2} B_y'(p, q) \right) mod 8 \right) - 4 \right].$$

Step 11: Embed the checksum digit "ChkS(y)" into the intermediate Stego-block pixel $B_y'(2, 2)$ such that $B_y'(2, 2) = B_y'(2, 2) + ChkS(y)$. The embedding of checksum digit completes the embedding process in the block and therefore the block B_y' is termed as stego-block.
Step 12: Repeat Step 10 to 11 until complete data (EHR bits, fragile watermark bits, and checksum bits) are embedded in the cover image to obtain a Stego-image "S."

Output: Stego image (S)

V. EXPERIMENTAL RESULTS AND DISCUSSION

To evaluate our work, we use two of the most commonly used test image data sets (that include both medical images and general test images) from the related literature [24]. The size of the input and cover test images used is (256×256)

and (512 × 512), respectively. In addition, 150 images of size (385 × 512) from the UCID database [27] have also been used to test our approach. For authentication, the fragile binary logo used is of size (64 × 64). It is worth mentioning here that the proposed approach of RIH could work with any kind of grayscale general and medical images [28], [29]. The algorithm is not specific to the used test images only but is of general applicability. Simulations have been carried out using MATLAB R 2014a on windows-7 (64-bit) platform with Intel Pentium CPU processor working at 2.13 GHz and with 2-GB RAM.

The objective quality of the stego-images has been evaluated by using image quality indices PSNR and structural similarity measure index (SSIM). The PSNR and SSIM have been defined as in [23] and [24]. To cater to the real-time computational demands of a smart e-healthcare system, both the embedding and the extraction time are reduced by implementing the scheme in the pixel domain. The content authentication ability of our technique has been evaluated by computing bit error rate (BER) and normalized cross-correlation (NCC) between embedded and extracted data after the stego-images have gone through various image processing operations. The proposed approach DH has been evaluated for payload, imperceptibility, fragility, and computational complexity for different images. Simulation results have been compared to several state-of-the-art DH schemes.

A. Payload Analysis

In the proposed RIH approach, nine EHR/checksum/logo bits have been concealed in every 2 × 2 block of the cover image excluding the seed pixel. For a seed image of size $M \times N$, the total number of bits "n" that could be hidden in the corresponding cover image of size $P \times Q$ is computed as

$$n = 3((P \times Q) - M \times N) \tag{5}$$
$$\text{or } n = 3(2M \times 2N - MN) \text{ as } P = 2M \text{ and } Q = 2N$$
$$\text{or } n = (9MN). \tag{6}$$

The total number of bits that could be hidden in a cover image equals to $9MN$ bits. The number of bits that could be hidden per pixel of the cover image is calculated as

$$n_{\text{bpp}} = \frac{9MN}{PQ} = \frac{9MN}{4MN} = \frac{9}{4} = 2.25 \text{ bpp.} \tag{7}$$

Therefore, the proposed scheme can hide 2.25 bpp. The possible payload of the proposed approach for various images is presented in Table II. It is worth to mention that when tamper detection and localization is incorporated, the maximum EHR that can be embedded is 1.5 bpp.

The payload of the proposed approach for medical images has been compared with many existing state-of-the-art approaches. Results presented in Fig. 4 reveal that our scheme offers a higher payload when compared to most of the techniques under comparison.

TABLE II
OBJECTIVE PERFORMANCE PARAMETERS IN TERMS
OF PAYLOAD, PSNR, SSIM, AND BER

| Images	Payload (bits)	PSNR (dB)	SSIM	BER (%)
Image 1	589824	41.94	0.9493	0
Image 2	589824	41.98	0.9462	0
Image 3	589824	41.74	0.9509	0
Image 4	589824	41.97	0.9672	0
Image 5	589824	41.98	0.9573	0
Image 6	589824	41.99	0.9493	0
Image 7	589824	41.96	0.9684	0
Image 8	589824	41.99	0.9651	0
Image 9	589824	41.98	0.9817	0
Image 10	589824	41.99	0.9643	0
Image 11	589824	41.97	0.9727	0
Average (11 images)	**589824**	**41.95**	**0.9611**	**0**
Average (150 images)	**589824**	**41.98**	**0.9675**	**0**
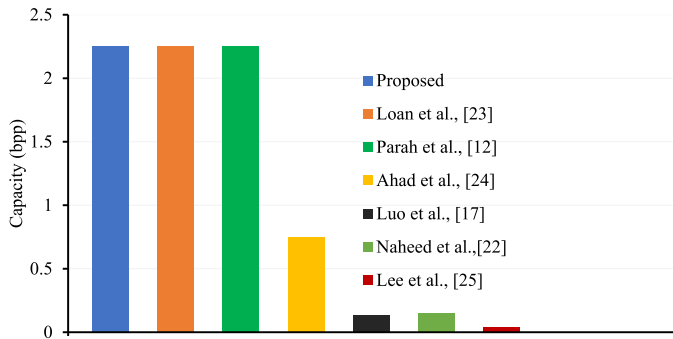
Fig. 4. Payload comparison in bpp for medical images.

B. Imperceptibly Analysis

One of the important characteristics of an ideal information embedding system is that the perceptual quality of the cover image must be retained even after high capacity data embedding. The LDM technique adopted in this scheme guarantees high-quality stego-images by changing the pixels of the cover image with a lower value than conventional LSB embedding schemes. The subjective quality analysis of each stego-image is shown in Fig. 5, whereas the objective quality parameters obtained are reported in Table III.

Table III clearly states that our scheme can produce high-quality Stego-images. This has also been validated by an average PSNR of 41.95 dB for an embedding capacity of 2.25 bpp obtained for the 11 test images shown in Fig. 5. Moreover, the logo and the secret message are extracted from the stego-images without any error as shown in Fig. 5. The perceptual quality of the proposed stego-images has been compared with several existing state-of-art approaches. Tables III and IV clearly show that our approach of RIH provides good quality stego-images irrespective of very high embedding capacity. Average PSNR and SSIM values obtained for 1000 images taken from the UCID database are 41.9822 and 0.9711, respectively, and for the other 150, general and medical images these values are 41.9811 and 0.9675, respectively, which indicate high-quality stego-images.
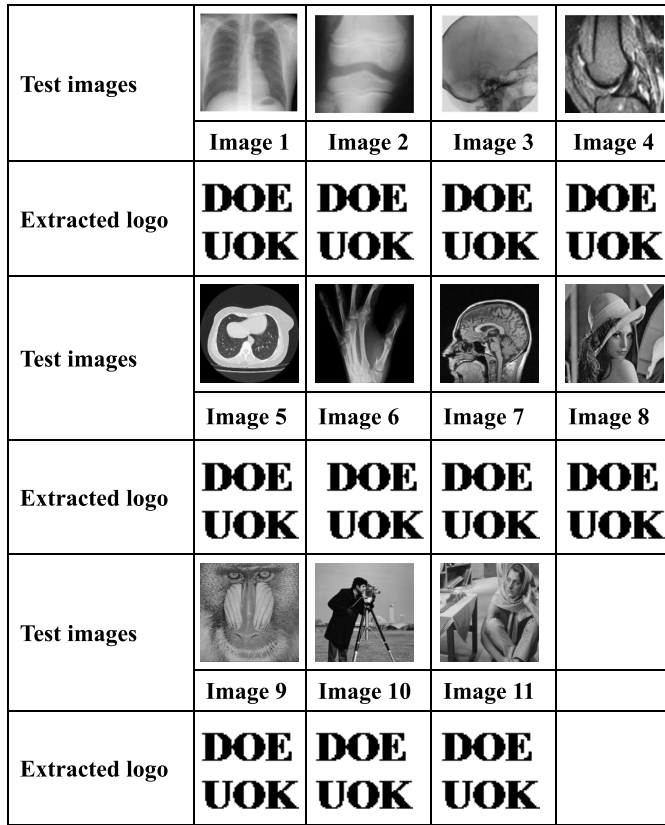
Test images	Image 1	Image 2	Image 3	Image 4
Extracted logo	DOE UOK	DOE UOK	DOE UOK	DOE UOK
Test images	Image 5	Image 6	Image 7	Image 8
Extracted logo	DOE UOK	DOE UOK	DOE UOK	DOE UOK
Test images	Image 9	Image 10	Image 11	
Extracted logo	DOE UOK	DOE UOK	DOE UOK	

Fig. 5. Stego-images and corresponding extracted logos.

C. Authentication Analysis

The authentication of medical and general images is very important in many applications. For example, in the case of a typical e-healthcare system, the medical images need to be shared with a distant doctor along with the EHR. In such a critical scenario, the authentication of medical images/EHR is vital for the final diagnosis. In our proposed framework, we have embedded a fragile watermark in the spatial domain to enable the receiver to decide if the received content is authentic or not. In case of a signal processing or geometric attack on stego-images, the receiver is unable to extract the logo successfully, hence the receiver is informed that the content received is not legitimate.

It is to be kept in mind that the size of the fragile logo is lower when compared to concealed data. As such, it can facilitate early tamper detection. This could be achieved by extracting the logo first. In case the receiver can extract the correct logo, it could proceed with the extraction of the EHR. Otherwise, it can ask for an automatic retransmission request. The authentication analysis has been done by distorting the stego-image using different image processing operations, such as Gaussian noise, salt and pepper noise, histogram equalization, median filtering, sharpening, and low-pass filtering. Table V shows the extracted logos and their respective objective quality parameters, such as BER and the number of tempered blocks.

We next compare the degree fragility of the proposed scheme to that of the scheme by Ahad *et al.* [24], which is the only background reference that has reported quantitative fragility

TABLE III
COMPARISON OF CAPACITY, PSNR, AND SSIM FOR MEDICAL IMAGES

Image	Scheme	Capacity (bits)	PSNR (dB)	SSIM
Image 1	Proposed	589824	**41.94**	**0.9493**
	Loan et al., [23]	589824	38.08	0.9065
	Proposed	196608	**46.77**	**0.9829**
	Ahad et al., [24]	196608	46.36	0.9815
	Proposed	38700	**53.84**	0.9969
	GA scheme [22]	38700	49.01	0.9985
	PSO scheme [22]	38390	49.00	0.9985
	Luo et al., [17]	36060	48.94	0.9985
	Lee et al., [25]	10882	48.42	0.9988
Image 2	Proposed	589824	**41.98**	**0.9462**
	Loan et al., [23]	589824	38.89	0.9077
	Proposed	196608	**46.74**	0.9815
	Ahad et al., [24]	196608	46.36	0.9878
	Proposed	38700	**53.78**	0.9965
	GA scheme [22]	38700	49.01	0.9985
	PSO scheme [22]	38390	49.00	0.9985
	Luo et al., [17]	36060	48.94	0.9985
	Lee et al., [25]	10882	48.42	0.9988
Image 3	Proposed	589824	**41.74**	**0.9509**
	Loan et al., [23]	589824	38.35	0.9133
	Proposed	196608	**46.75**	0.9817
	Ahad et al., [24]	196608	46.36	0.9823
	Proposed	38700	**53.87**	0.9969
	GA scheme [22]	38700	49.01	0.9985
	PSO scheme [22]	38390	49.00	0.9985
	Luo et al., [17]	36060	48.94	0.9985
	Lee et al., [25]	10882	48.42	0.9988
Image 4	Proposed	589824	**41.97**	**0.9672**
	Loan et al., [23]	589824	38.33	0.9328
	Proposed	196608	**46.76**	**0.9879**
	Ahad et al., [24]	196608	46.37	0.9806
	Proposed	38700	**53.82**	0.9976
	GA scheme [22]	38700	49.01	0.9985
	PSO scheme [22]	38390	49.00	0.9985
	Luo et al., [17]	36060	48.94	0.9985
	Lee et al., [25]	10882	48.42	0.9988
Image 6	Proposed	589824	**41.99**	**0.9493**
	Loan et al., [23]	589824	37.36	0.7198
Image 7	Proposed	589824	**41.96**	**0.9684**
	Loan et al., [23]	589824	35.45	0.9352

results. The results are shown in Fig. 6 for Image 1 of Table V. We note that the higher the obtained BER is after attacking an information hiding system, the more fragile the system is concluded to be. From Fig. 6, our scheme is more fragile to various attacks to those under comparison and hence can detect easily that an attack has taken place during data transit.

D. Tamper Localization

The proposed scheme can localize any tempered block at a resolution of 2×2. Fig. 7 illustrates the localized portions of different stego images. The checksum digit calculated for a 2×2 block has been embedded in the designated pixel for such purpose in each block. The localization of tempered blocks has been achieved by comparing the extracted checksum with that of the calculated value from the corresponding 2×2 block at the receiver. In case of mismatch, if any, between the two

TABLE IV
COMPARISON OF CAPACITY, PSNR, AND SSIM FOR GENERAL IMAGES

Image	Scheme	Capacity (bits)	PSNR (dB)	SSIM
Image 8	Proposed	589824	**41.99**	0.9651
	Parah et al., [12]	589824	35.71	NA
	Benhfid et al., [13]	474716	40.37	NA
	Wang et al., [15]	463995	32.01	NA
	Proposed	414187	**44.57**	0.9791
	Loan et al., [23]	414187	44.02	NA
	Lu [14]	786432	36.03	NA
	Proposed	196608	**46.77**	0.9867
	Ahad et al., [24]	196608	46.36	0.9869
	Proposed	**381940**	**45.27**	0.9814
	Qui et al., [18]	381940	27.34	NA
	Proposed	10002	**59.91**	0.9992
	Li et al., [19]	10000	61.02	NA
	Li et al., [20]	10000	59.78	NA
	Ou et al., [21]	10000	59.75	NA
	Proposed	**300**	74.06	1
	Qui et al., [18]	236	70	NA
Image 9	Proposed	589824	**41.98**	0.9817
	Parah et al., [12]	589824	29.96	NA
	Proposed	477102	**43.45**	0.9878
	Loan et al., [23]	477102	39	NA
	Wang et al., [15]	422052	31.33	NA
	Benhfid et al., 13]	771542	29.71	NA
	Lu [14]	786432	35.99	NA
	Proposed	196608	**46.75**	0.9947
	Ahad et al., [24]	196608	46.37	0.9932
	Proposed	**381940**	**45.25**	0.9929
	Qui et al., [18]	381940	26.53	NA
	Proposed	10002	**59.87**	0.9999
	Li et al., [19]	10000	56.25	NA
	Li et al., [20]	10000	53.96	NA
	Ou et al., [21]	10000	55.21	NA
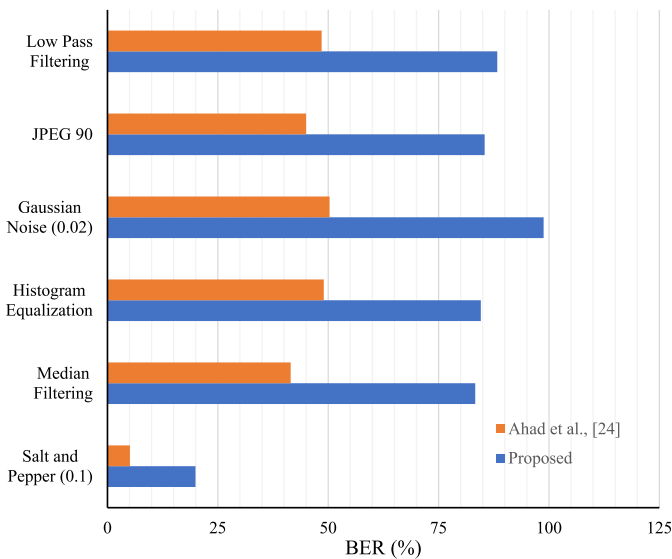
Fig. 6. Fragility comparison in terms of BER of our scheme with Ahad *et al.*,[24].

Fig. 7. Localized portions of stego-images with different *copy-paste* attacks.

E. Data Extraction and Recovery of the Seed Image

As the seed pixels of the cover image has not been modified while DH, therefore, all the seed pixels from the stego-image are collected to produce the seed image. The resultant seed image obtained is the same as the original image. Furthermore, the hidden, secret information is extracted and the PSNR value of the resulting seed image with respect to the original image is infinity, which reveals that the reversibility of the proposed RIH system is flawlessly accomplished. Besides, the secret message is retrieved easily from the stego-image by subtracting the respective seed pixel from each stego-pixel of a 2×2 block.

F. Computational Complexity

As mentioned in the introduction, the development of computationally efficient algorithms for critical applications is a highly desirable design target. Reduced computational complexity is more important in electronic healthcare applications,

checksums, the corresponding block is labeled as tampered. Otherwise, no error is assumed to have occurred. This feature allows for a proper, timely decision making, and hence could advocate for a better e-healthcare.
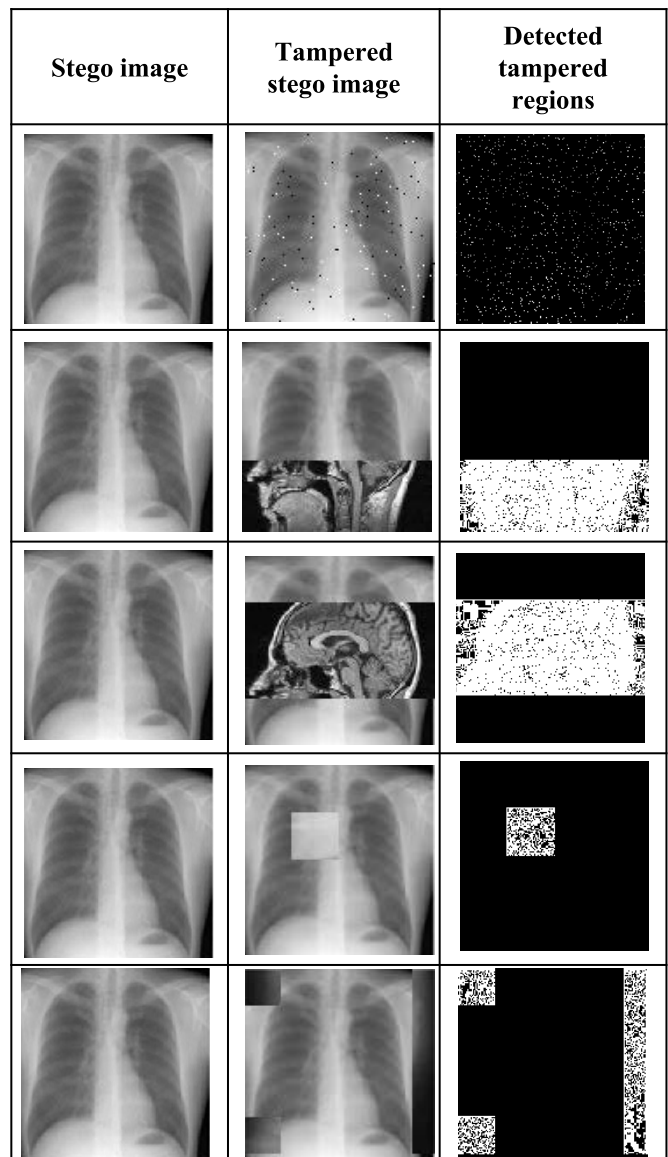
TABLE V
PARAMETERS FOR AUTHENTICATION ANALYSIS IN TERMS OF BER AND NUMBER OF TEMPERED BLOCKS

Attacks	Image 1			Image 8		
	Extracted logo	BER (%)	Number of tampered blocks	Extracted logo	BER (%)	Number of tampered blocks
No Attack	DOE UOK	0	0	DOE UOK	0	0
Median Filtering (MF)		83.314	53014		87.577	55703
Salt and Pepper (SAP) (0.1)	DOE UOK	19.951	21280	DOE UOK	19.087	21185
Histogram Equalization (HE)		84.5757	48264		83.2367	47177
Gaussian Noise (GN) (0.01)		98.7853	64782		98.88	64829
JPEG 90		85.4378	53516		86.9942	56933
Low Pass Filtering (LPF)		88.3041	51550		90.8498	57144

which deal with real-time data. The use of spatial domain technique PRM in the proposed scheme results in a considerable reduction in computational cost while obtaining the cover image from the seed image. Additionally, all processes, including EHR embedding have been carried out using simple arithmetic, devoid of any transformation techniques, which contributes further to the computational efficiency of the overall approach. In quantitative terms, we have carried out an analysis of the embedding and extraction time required for a payload of 2.25 bpp over a data set of 6, 150, and 1000 images, and the results have been presented in Table VI.

The experimental results obtained for our scheme have been compared to [13], as to the best of our knowledge, such a timing analysis has been done only in this prior work. It has been found that our scheme results in less average embedding and extraction times when compared to those reported in this reference. The values reported in [23] for average embedding and extraction time (for a payload of 2.25 bpp) are 3 and 9.6 s, respectively, which are significantly higher than 0.9115 and 3.02 s as observed for our proposed technique. The results presented in Table VI clearly show that our technique is computationally efficient and as such it is highly suitable for real-time e-healthcare applications.

VI. CONCLUSION

The exponential rise in the development of technology and networked infrastructure has led to the realization of smart health and emotional care. For the development of a successful smart healthcare setup, there are many challenges at the administrative as well as technological level. Some of the major challenges at the technological level are privacy,

TABLE VI
COMPUTATIONAL ANALYSIS FOR THREE DATA SETS COMPRISING 6, 150, AND 1000 IMAGES, AT AN EMBEDDING CAPACITY OF 2.25 BPP

Image name	Embedding time (sec)	Extraction time (sec)
Image 1	0.9531	2.9060
Image 2	0.9219	2.9812
Image 3	0.9688	3.1094
Image 4	0.8281	3.0130
Image 8	0.8906	3.1563
Image 9	0.9063	2.9844
Average per image (6 images)	**0.9115**	**3.0251**
Average per image (150 images)	**0.3481**	**2.327**
Average per image (1000 images)	**0.1946**	**1.9163**
Average [13]	**3.0000**	**9.6000**

security, and authentication of critical healthcare data. The privacy and integrity of patient data have achieved more significance in the ongoing COVID-19 pandemic. This article addresses the privacy and integrity issues of patient data by proposing a new high payload, reversible, and computationally efficient scheme for EHR security and authentication. The proposed solution provides double-layer security to the embedded EHR, comprising of patient physiological vitals and history by hiding it in the medical images: the first security layer is provided by RC4 encryption and the second one by information embedding. A novel technique based on LDM has been developed and utilized to improve payload for a given imperceptivity level. In addition to EHR, a fragile logo has been inserted into the cover medium, to facilitate content authentication at the receiver end. The reversibility has been ensured utilizing PRM. The use of PRM coupled

with spatial-domain embedding results in lesser computational cost in comparison to the state of the art. We have also used checksum generation and checksum embedding to enable the proposed scheme to detect and localize the tamper if any. Experimental results have shown a better performance of our RIH scheme compared to many state-of-the-art schemes in terms of imperceptibility, payload, computational complexity, and capability to detect tamper. Given the various attributes of the proposed scheme, it could serve as a potent candidate for patient data security and support the existing smart health systems to do better in the unprecedented times of COVID-19.

Data secrecy or data security has a positive impact on society as it can benefit clients in numerous ways, leading to new potential clients. Research shows that 89% of businesses believe that optimized data security has led to better client loyalty and trust. With the advent of the digital revolution most of the potent fields of life, such as banking, commerce, health, etc., have been tremendously influenced. This has resulted in sectors, such as e-banking, e-commerce, e-health, etc. For faithful and effective operations, the security of data involved in such sectors is of prime concern. The work presented here deals with the security of patient records in smart health. Through extensive experiments, it has been shown that the proposed work outperforms the state of the art and is believed to have a positive impact concerning the security concerns in smart healthcare services and society.

References

[1] H. Habibzadeh, K. Dinesh, O. Rajabi Shishvan, A. Boggio-Dandry, G. Sharma, and T. Soyata, "A survey of healthcare Internet of Things (HIoT): A clinical perspective," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 53–71, Jan. 2020.

[2] M. Chen, W. Li, Y. Hao, Y. Qian, and I. Humar, "Edge cognitive computing based smart healthcare system," *Future Gener. Comput. Syst.*, vol. 86, pp. 403–411, Sep. 2018.

[3] X. Li, S. Liu, F. Wu, S. Kumari, and J. C. Rodrigues, "Privacy preserving data aggregation scheme for mobile edge computing assisted IoT applications," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4755–4763, Jun. 2019.

[4] C. Zhu, J. C. Rodrigues, V. C. M. Leung, L. Shu, and L. T. Yang, "Trust-based communication for the industrial Internet of Things," *IEEE Commun. Magazine*, vol. 56, no. 2, pp. 16–22, Feb. 2018.

[5] C. M. J. M. Dourado, S. P. P. Da Silva, R. V. M. Da Nóbrega, P. P. R. Filho, K. Muhammad, and V. H. C. De Albuquerque, "An open IoHT-based deep learning framework for online medical image recognition," *IEEE J. Sel. Areas Commun.*, early aceess, Aug. 31, 2020, doi: 10.1109/JSAC.2020.3020598.

[6] *2020 Breach Barometer*. Accessed: Sep. 27, 2020. [Online]. Available: https://www.protenus.com/resources/2020-breach-barometer

[7] *The 10 Biggest Healthcare Data Breaches of 2020*. Accessed: Sep. 27, 2020. [Online]. Available: https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2020

[8] K. K. R. Choo, S. Gritzalis, and J. H. Park, "Cryptographic solutions for industrial Internet-of-Things: Research challenges and opportunities," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3567–3569, Aug. 2018.

[9] C. Zhu, H. Nicanfar, V. C. M. Leung, and L. T. Yang, "An authenticated trust and reputation calculation and management system for cloud and sensor networks integration," *IEEE Trans. Inf. Forensics Security*, vol. 10, pp. 118–131, 2015.

[10] H. Wang, S. Wu, M. Chen, and W. Wang, "Security protection between users and the mobile media cloud," *IEEE Commun. Mag.*, vol. 52, no. 3, pp. 73–79, Mar. 2014.

[11] Z. Sheng, H. Wang, C. Yin, X. Hu, S. Yang, and V. C. M. Leung, "Lightweight management of resource-constrained sensor devices in Internet of Things," *IEEE Internet Things J.* vol. 2, no. 5, pp. 402–411, Oct. 2015.

[12] S. A. Parah, J. A. Sheikh, J. A. Akhoon, and N. A. Loan, "Electronic health record hiding in images for smart city applications: A computationally efficient and reversible information hiding technique for secure communication," *Future Gener. Comput. Syst.*, vol. 108, pp. 935–949, Jul. 2020.

[13] A. Benhfid and Y. Taouil, "Reversible steganographic method based on interpolation by bivariate linear box-spline on the three directional mesh," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 32, pp. 850–859, Sep. 2020.

[14] T.-C. Lu, "Interpolation-based hiding scheme using the modulus function and re-encoding strategy," *Signal Process.*, vol. 142, pp. 244–259, Jan. 2018.

[15] W. Wang, J. Ye, T. Wang, and W. Wang, "A high capacity reversible data hiding scheme based on right-left shift," *Signal Process.*, vol. 150, pp. 102–115, Sep. 2018.

[16] K. Jung and K. Yoo, "Data hiding method using image interpolation," *Comput. Stand. Interfaces*, vol. 31, no. 2, pp. 465–470, 2009.

[17] L. Luo, Z. Chen, M. Chen, X. Zeng, and Z. Xiong, "Reversible image watermarking using interpolation technique," *IEEE Trans. Inf. Forensics Security*, vol. 5, pp. 187–193, 2010.

[18] Y. Qiu, Z. Qian, and L. Yu, "Adaptive reversible data hiding by extending the generalized integer transformation," *IEEE Signal Process. Lett.*, vol. 23, no. 1, pp. 130–134, Jan. 2016.

[19] X. Li, W. Zhang, X. Gui, and B. Yang, "Efficient reversible data hiding based on multiple histograms modification," *IEEE Trans. Inf. Forensics Security*, vol. 10, pp. 2016–2027, 2015.

[20] X. Li, W. Zhang, X. Gui, and B. Yang, "A novel reversible data hiding scheme based on two-dimensional difference-histogram modification," *IEEE Trans. Inf. Forensics Security*, vol. 8, pp. 1091–1100, 2013.

[21] B. Ou, X. Li, Y. Zhao, R. Ni, and Y.-Q. Shi, "Pairwise prediction-error expansion for efficient reversible data hiding," *IEEE Trans. Image Process.*, vol. 22, no. 12, pp. 5010–5021, Dec. 2013.

[22] T. Naheed, I. Usman, T. M. Khan, A. H. Dar, and M. F. Shafique, "Intelligent reversible watermarking technique in medical images using GA and PSO," *Optik Int. J. Light Electron Opt.*, vol. 125, no. 11, pp. 2515–2525, 2014.

[23] N. A. Loan, S. A. Parah, J. A. Sheikh, J. A. Akhoon, and G. M. Bhat, "Hiding electronic patient record (EPR) in medical images: A high capacity and computationally efficient technique for e-healthcare applications," *J. Biomed. Informat.*, vol. 73, pp. 125–136, Sep. 2017.

[24] F. Ahad, S. A. Parah, J. A. Sheikh, and G. M. Bhat, "Hiding clinical information in medical images: A new high capacity and reversible data hiding technique," *J. Biomed. Informat.*, vol. 66, pp. 214–230, Feb. 2017.

[25] S. Lee, C. D. Yoo, and T. O. N. Kalker, "Reversible image watermarking based on integer-to-integer wavelet transform," *IEEE Trans. Inf. Forensics Security*, vol. 2, pp. 321–330, 2007.

[26] A. Mousa and A. Hamad, "Evaluation of the RC4 algorithm for data encryption," *Int. J. Comput. Sci. Appl.*, vol. 3, no. 2, pp. 44–56, 2006.

[27] *UCID Image Dataset*, Loughborough Univ., Loughborough, U.K., Jan. 2013. [Online]. Available: http://homepages.lboro.ac.uk/cogs/datasets/ucid/data/ucid.v2.tar.gz

[28] *The USC-SIPI Image Database*. Accessed: Nov. 29, 2018. [Online]. Available: http://sipi.usc.edu/database/database.php? volume=misc

[29] *Open Access Biomedical Image Search Engine (OPENi)*. Accessed: Nov. 29, 2018. [Online]. Available: https://openi.nlm.nih.gov/index.php

Shabir A. Parah received the M.Sc., M.Phil., and Ph.D. degrees in electronics from the University of Kashmir, Srinagar, India, in 2004, 2010, and 2013, respectively, in the field of signal processing and data hiding.

He is currently working as an Assistant Professor with the Department of Electronics and Information Technology, University of Kashmir. He has published more than 100 research papers in International/National journals and conference proceedings. His fields of interests are multimedia signal processing, secure communication, digital watermarking, steganography, artificial intelligence, image processing and analysis, Internet of Things, IIoTs, and Industry 4.0.

Javaid A. Kaw received the Ph.D. degree in electronics from the University of Kashmir, Srinagar, India, in 2020.

He is currently serving at the Department of Electronics and Instrumentation Technology, University of Kashmir. He has published several papers in reputed journals and conferences in his areas of research. His research interests include image processing, steganography, and Industry 4.0.

G. M. Bhat received the M.Sc. degree in electronics from the University of Kashmir, Srinagar, India, in 1987, and the Ph.D. degree in electronics from Aligarh Muslim University, Aligarh, India, in 1996.

He is a Full Professor and the Head of the Department of Electronics Engineering, Institute of Technology, Zakoora, India. He has published more than hundred research papers in international and national journals and conference proceedings. His present research interests include secure message communication, neural networks, and signal processing techniques for communication.

Paolo Bellavista (Senior Member, IEEE) received the Ph.D. degree in computer science engineering from the University of Bologna, Bologna, Italy, in 2001.

He is currently a Full Professor of distributed and mobile systems with the University of Bologna. He is also currently the Scientific Coordinator of a large H2020 big data innovation action called IoTwins about distributed digital twins for the manufacturing industry. His research activities span from pervasive wireless computing to location/contextaware services and from edge cloud computing to middleware for Industry 4.0 applications.

Prof. Bellavista serves on the Editorial Boards of the IEEE COMMUNICATION SURVEYS AND TUTORIALS, *ACM Computing Surveys*, the IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, *Pervasive Mobile Computing* (Elsevier), and *Journal on Network and Computing Applications* (Elsevier). He is a Senior Member of ACM.

Khan Muhammad (Member, IEEE) received the Ph.D. degree in digital contents from Sejong University, Seoul, South Korea, in 2018.

He is currently an Assistant Professor with the Department of Software, Sejong University. He is also serving as a Professional Reviewer for over 100 well-reputed journals and conferences. His research interests include medical image analysis (brain MRI, diagnostic hysteroscopy, and wireless capsule endoscopy), information security (steganography, encryption, watermarking, and image hashing), video summarization, computer vision, fire/smoke scene analysis, and video surveillance. He has registered more than ten patents and authored or coauthored more than 140 papers in peer-reviewed international journals and conferences in the above research areas.

Dr. Muhammad is also an Editorial Board Member of *Journal of Artificial Intelligence and Systems*, *Internet of Things and Cyber–Physical Systems Journal*, and *Mathematics of Computation and Data Science*.

Nazir A. Loan received the M.Sc. degree in electronics from the University of Kashmir, Srinagar, India, in 2014, and the Ph.D. degree from the University of Kashmir in 2019, under the Government of India INSPIRE Scheme.

He has published papers in reputed journals of IEEE, Elsevier, and Springer. His research interests include cyber security, image processing, cryptography, video analytics, IoT, and Industry 4.0.

Victor Hugo C. de Albuquerque (Senior Member, IEEE) graduated in mechatronics engineering from the Federal Center of Technological Education of Ceará (CEFETCE), Fortaleza, Brazil, in 2006, the M.Sc. degree in teleinformatics engineering from the Federal University of Ceará, Fortaleza, in 2007, and the Ph.D. degree in mechanical engineering from the Federal University of Paraíba, João Pessoa, Brazil, in 2010.

He is a Professor and a Senior Researcher with the LAPISCO/IFCE, and ARMTEC Tecnologia em Robótica, Brazil. He is a specialist, mainly, in IoT, machine/deep learning, pattern recognition, and robotica.