Journal of Engineering Technology
Volume 6, Issue 2, July. 2018, PP. 42-54
RESEARCH ARTICLE -ENGINEERNG TECHNOLOGY

A secured healthcare system using private blockchain technology

C. Ananth[1], M. Karthikeyan[2], N. Mohananthini[3]

[1,2] Assistant Professor / Programmer, Dept. of Computer and Information Science, Annamalai University, India.
[3] Assistant Professor, Dept. of Electrical and Electronics Engg., Muthayammal Engg. College, Rasipuram, India.

Abstract: Introduction, The Electronic Medical Record (EMR), in the healthcare system, is a precious source of healthcare intelligence. The EMRs maintain a protected and permanent system which needs to be repeatedly shared among the peers. The sharing of EMR is a necessary step to offer smart and improved healthcare system service. Sharing the EMR, between the places or institutions, is a challenging task. The current sharing methods, to effectively manage and protect the medical records, have been insufficient. **Methodology:** The Blockchain technology, mostly, used by a distributed database, enables the digital currency as Bitcoin. This technology quickly ascends the inflated expectations to the peak. The excitement about using the private Blockchain technology, in the healthcare system is, also growing. The private Blockchain technology provides an immutable shared and transparent history of all the transactions to construct the applications with accountability, transparency, and trust. **Result:** This technology presents a unique opportunity to develop secure and trustable records management to be shared with the healthcare system. **Conclusion:** In this paper, we present our perspectives on private Blockchain technology in the healthcare system. The distributed ledger blocks form three various scenarios such as primary care, cross-disciplinary referral and multidisciplinary approach using different watermarking techniques.

Keywords: cross-disciplinary referral, healthcare system, multidisciplinary approach, primary care, private blockchain technology, watermarking.

1 Introduction

The EMR, in the health care system, usually provides general information such as Physician details, treatment history and personal information about a patient collected by the individual medical practice. The EMR needs to improve and secure communications from one place to another place. In reality, the healthcare system has more data branches than any other sectors and more than 95% of the medical organizations surveyed indicate they had been victims of a cyber attack. The EMRs are being stolen and sold in dark-net markets where they are ten times more expensive than credit card data [1]. A big challenge for healthcare systems data being smarter is how to assemble, analyze, besides ensuring integrity and security and storing the personal healthcare systems data without any privacy violations. The mentioned challenges can be solved by using the Blockchain technology.

The Blockchain technology is extremely popular nowadays; the name itself indicates the Blockchain as a chain of blocks contains information. This technique was regionally described in 1991 by the group of re-structures and was regionally extended to timestamps digitized documents. It is not possible to tamper with them almost like a notary. However, it was first described by Satoshi Nakamoto in 2009 [2] to create digital cryptocurrency as Bitcoin. The Blockchain is a distributed

ledger that is completely open to anyone [3]. Once the block is created, the information can never be erased or altered because of every single transaction is verified by all the group members.

The authors [4] conclude with the point that Blockchain applications focus on 80.50% of the papers in Bitcoin system and 19.50% deals with other applications such as healthcare, law enforcement, online music, smart contracts and voting. It is essential to find the present applications developed by using Blockchain technology. Recognizing the different applications help us to understand other directions and ways of using of the Blockchain technology. This technology raises its own privacy and security concerns now as it offers a new concept for distributing the information [5]. When used, the Blockchain's potential, in the healthcare system, is greatly weighed by these limitations. Therefore, the proposed work explores the Blockchain technology applied to healthcare system.

1.1 Motivation

Many researchers, who studied Blockchain technology, have proposed solutions to solve only the issues related to cryptocurrency application. It is necessary to find the other applications using Blockchain technology. Hence, the Blockchain technology, applicable to the healthcare system, is adopted. The method for creation of the each and every block in the Blockchain technology is same. The requirements of the healthcare systems are considered and proposed by the method for the creation of each and every block by applying different watermarking techniques.

1.2 Benefit of the proposed work

Generally, the Electronic Medical Records are exchanged, from one place to the required place, through unsecured open networks; but it poses a threat resulting in undesirable outcomes. Considering this fact, the Electronic Medical Records are used in the proposed Blockchain Technology and multiple watermarking schemes. This is important for addressing different problems like higher security, transparency and to preserve the privacy of patients. The block diagram of Blockchain functioning is shown in Fig. 1.

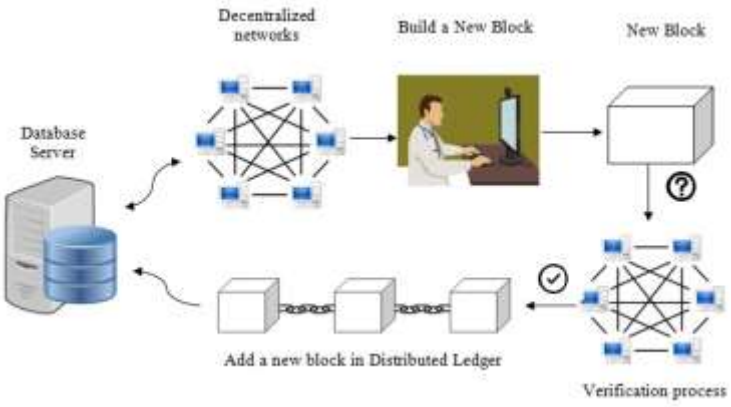

Figure. 1. Overview of Blockchain functioning principle

2 Related works

In multiple industries, an emerging innovative model enables faster, more efficient and highly secured business-to-business and business-to-consumer transactions. Those who are involved, in health care programmes believe that the same distributed database technologies can drive similar results within the industry. Many major innovations recognize the fact that confusion and hype can mask the potential of real world applications. Known as Blockchain technologies, these solutions can support many existing healthcare processes at a fundamental level. The creation of secured, trusted, portable healthcare records that have a high degree of integrity and fidelity can be trusted across the healthcare continuum [6].

Ariel Ekblaw et. al. [7] proposed a novel and decentralized record management system to handle the EHRs, using the Blockchain technology. Their system gives patients a comprehensive, immutable log and easy access to their medical information across the providers and treatment sites. Xiao Yue et. al. [8] Proposed centric access model ensures the patients to control their healthcare data on their own; simple, unified indicator – centric schema makes it possible to organize all kinds of personal health care data practically and easily. Their method also indicates the fact that MPC is one promising solution to enable an interested third party to conduct computation over patient data without violating privacy.

The Blockchain technology, along with some of its significant features and benefits, is discussed in [9]. The technology, still evolving with a lot of scope for different domains and industries, is set to change the world. But, it is not free from challenges; some of them have been highlighted too. Although Blockchain is the technology behind Bitcoin, its use is not limited to financial domain only. The year 2016 revealed Blockchain as more disruptive technology in the retail industry than any other industry and, in 2017, the Blockchain was gradually becoming the dominant hype phrase for retailing.

Deepayan Bhowmik and Tian Feng [10] proposed a novel watermarking based multimedia Blockchain framework that can address some of the issues. The unique watermark information contains two pieces of information as cryptographic hash that contains transaction histories and an image hash that preserves the retrievable original media content. Once the watermark is extracted, the first part of the watermark is passed to a distributed ledger to retrieve the historical transaction trial and the latter part is used to identify the edited / tampered regions. Alevtina Dubovitskaya et. al. [11] presented the perspectives on Blockchain based healthcare data management, in particular, for the EMR data sharing between the healthcare providers and the research studies. The framework helps manage and sharing the EMR data for the care of cancer patients. Their proposed work can significantly reduce the turnaround time for the EMR sharing and improve the decision making for medical care, and reduce the overall cost.

3 Preliminaries

3.1 Blockchain technology

The Blockchain technology presents a shared, immutable and transparent record of all the communications to build the applications with trust, transparency and accountability. This technology provides a unique opportunity to develop a trustable and secured EMR data sharing and supervision system.

The Blockchain technology has three types as indicated below [12]:

Public: The public Blockchains have ledgers to notice every person on the internet and any person can verify and add a block of transactions to the Blockchain.

Private: The private Blockchains allow only specific persons in the organization to verify and add transaction blocks, but every person on the internet is normally allowed to view.

Consortium: The consortium Blockchains allow only a group of organizations (like banks) which can verify and add transactions, but the ledger can open or restricted to selected groups.

For the above three types, the private Blockchain technology excitements are suitable in the proposed method. Hence, we can choose to utilize the private Blockchain technology.

3.2 Dual tree - complex wavelet transform (DT – CWT)

The traditional implementation of the Complex Wavelet Transform (CWT) is a simple extension of the Discrete Wavelet Transform (DWT). That is, only a single tree of filters with complex coefficients is used [13]. Since such filters have an asymmetric response for positive and negative frequencies, it is complicated to design them with perfect reconstruction properties, and complex filters which satisfy perfect reconstruction tend to amplify noise during the reconstruction stage [14]. The Dual Tree implementation of the CWT utilizes two filter trees, each with real coefficients, to provide the real and the imaginary parts of the complex coefficients independently. The redundancy thus remains at 2:1. This execution allows us to design the perfect reconstruction of the filters. In 2-D signals, the two tree work on the rows followed by the columns of the data [15]. Therefore, the redundancy is increased to 4:1. At each resolution, there are six subbands, rather than three as in the DWT.

3.3 Image based techniques

Hari et. al. [16] developed the Adaptive Kernel Possibilistic C-Means (AKPCM) with Cuckoo Search Optimization (CSO) and the dismissal of anomalies joined with the level set method. The algorithms were experimented over diverse sorts of images and the fragmented results show relatively good results when compared to the native methods. The Semantic Annotation of the image based on Golden Face Analysis is also incorporated in the design strategy for providing an additional benediction of enhanced image analysis and a variety of image operations in [17]. Suganthi et. al. [18] proposed an efficient approach for patch-based image in painting by exploitation of geodesic distance metric. This technique is used to improve the speed and performance of any patch primarily based in painting methodology.

3.4 Multiple watermarking

The multiple watermarks are intended to convey different information at the same time. They should satisfy several goals like robustness, security and imperceptibility [19]. In multiple watermarking, more than one watermark is embedded into the original image. The multiple watermarking is used to boost the robustness with many different methods in which the embedded information is not easily lost [20].

Journal of Engineering Technology
Volume 6, Issue 2, July. 2018, PP. 42-54
RESEARCH ARTICLE -ENGINEERNG TECHNOLOGY

Amit Kumar Singh [21] presented a new robust hybrid multiple watermarking technique using a fusion of DWT, DCT, and SVD. Their proposed method simple encryption algorithm is used to save execution time during embedding and extraction processes. Their proposed method may find potential application in the prevention of theft related to patient identity in medical applications.

The proposed method uses the hybrid embedding and extraction of equations:

$$I_W(i,j) = I(i,j) + (\alpha \times I(i,j) + \beta) \times (W(i,j))) \quad (1)$$

$$W(i,j) = I_W(i,j) - I(i,j)) \Big/ (\alpha \times I(i,j) + \beta) \quad (2)$$

Where,

I_W = Watermarked Image, W = Physician's information, I = Patient's details and α = Scaling factor

4 The proposed method

The proposed method discussed three scenarios of DT-CWT based multiple watermarking schemes using private Blockchain technology in the healthcare system. The block diagrams of embedding and extraction method are shown in Fig. 2 and Fig. 3. The three scenarios are discussed below,

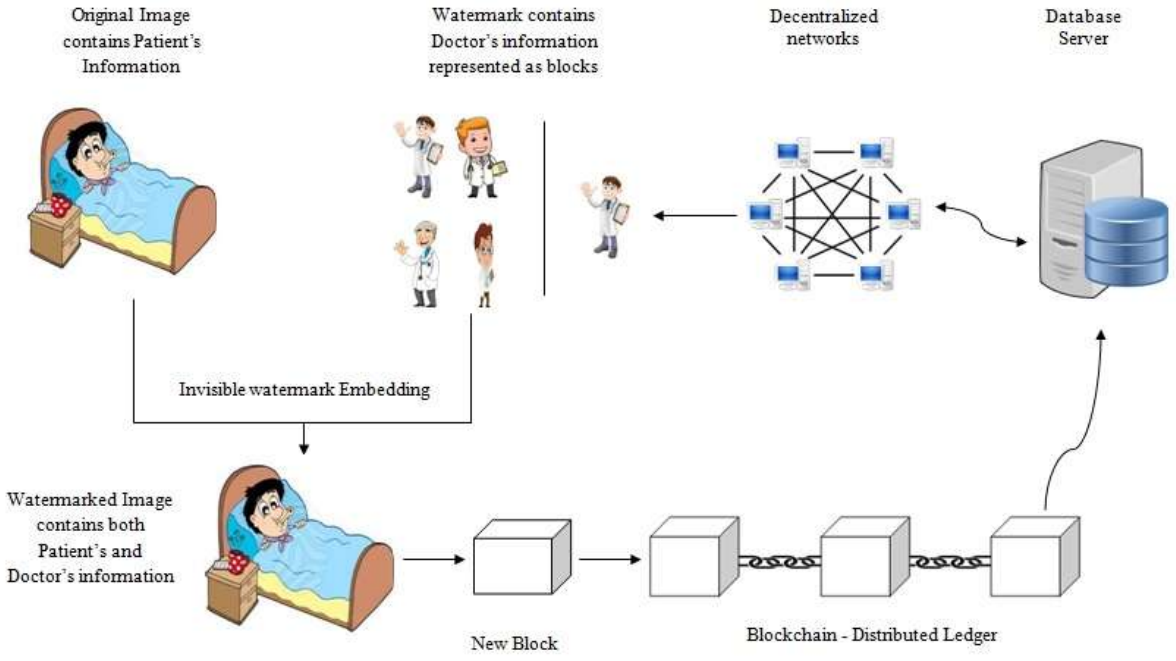

Figure. 2. The block diagram of embedding method

Journal of Engineering Technology
Volume 6, Issue 2, July. 2018, PP. 42-54
RESEARCH ARTICLE -ENGINEERNG TECHNOLOGY

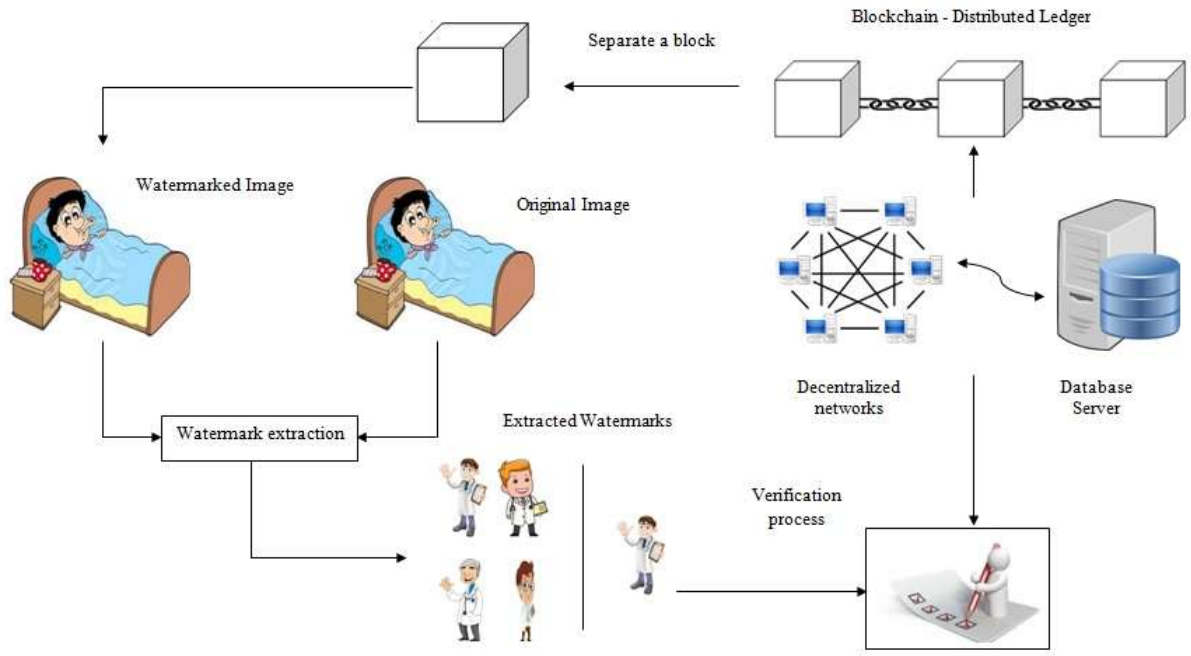

Figure. 3. The block diagram of extraction method

4.1 Scenario 1: Primary care

Arrangement of the scope and skills of training which define a primary care physician includes the factors like fundamental analysis and treatment of basic diseases and medical conditions. Diagnostic techniques contain interviewing the patient to gather information about the present symptoms, previous medical history and other health details, followed by a physical examination. Fig. 4 shows the creation of block 1 as primary care.

The patient's details are decomposed by 2 levels using DT-CWT. The Physician's information is embedded using equation (1). The inverse wavelet transform is performed to get the watermarked image. The inverse process of a watermark concealing process is to recover the physician's information from a block1 using equation (2).

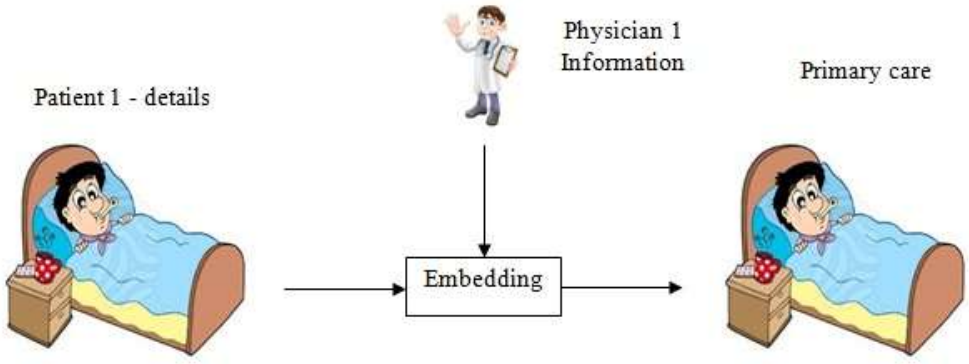

Figure. 4. Creation of genesis block as primary care

Journal of Engineering Technology
Volume 6, Issue 2, July. 2018, PP. 42-54
RESEARCH ARTICLE -ENGINEERNG TECHNOLOGY

4.2 Scenario 2: Cross-disciplinary referral

In healthcare system, a referral is the transfer of care for a patient from one clinic or physician to another by request. Its major goal is to improve and streamline the communication among primary care physicians, specialists and any other health providers involved in a patient's care. Fig. 5 shows the creation of block 2 as a cross-disciplinary referral. This method is the most straight forward method. The embedding steps are examined, rolled back and re-applied using the DT-CWT. It allows the way to find out the order in which the physician's information is embedded. In this scenario, the EMR, as the referral, may be embedding the information concerning both the patient and the physician. In case another referral occurs, each time the corresponding physician information can be embedded. In this watermarking technique, the multiple physicians' information is embedded using one after another using the equation (1) and then the information are extracted from one after another from the block2 using equation (2).

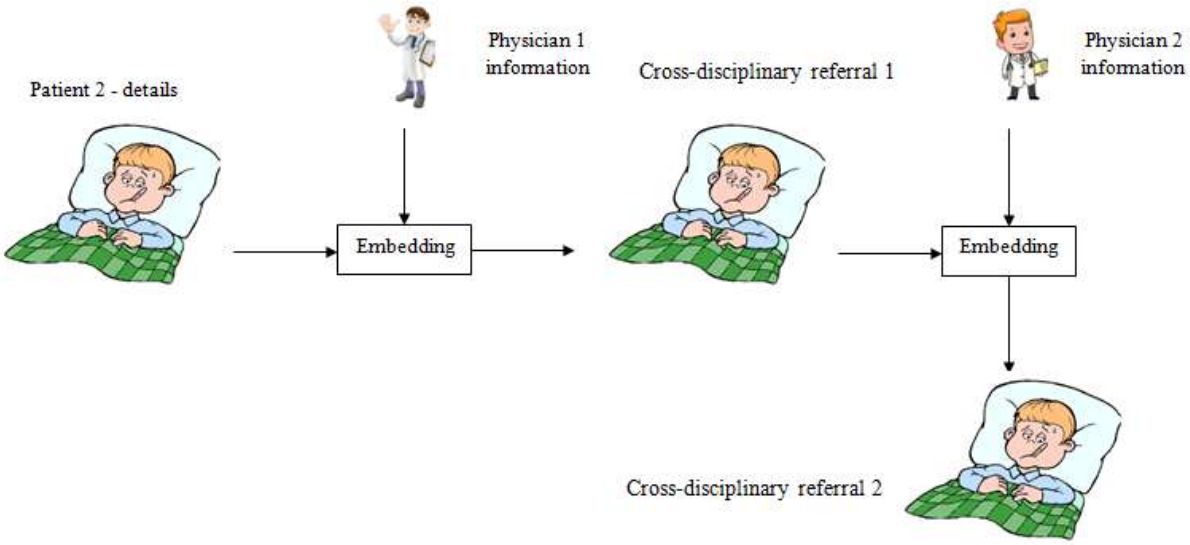

Figure. 5. Creation of block 2 as cross-disciplinary referral

4.3 Scenario 3: Multidisciplinary approach

Multidisciplinary approach is an integrated team-care of a patient. Each of the healthcare physicians, who belong to various disciplines, can provide particular services to the patient. This co-ordinates their services and gets the team working together towards a specific set of goals. Fig. 6 shows the creation of block 3 as a multidisciplinary approach.

In this method, the patient's details as well as the two physicians', belonging to different disciplines, are embedded at the same time using the equation 1. In the extraction process, the physician information is extracted from the block3 using equation 2.

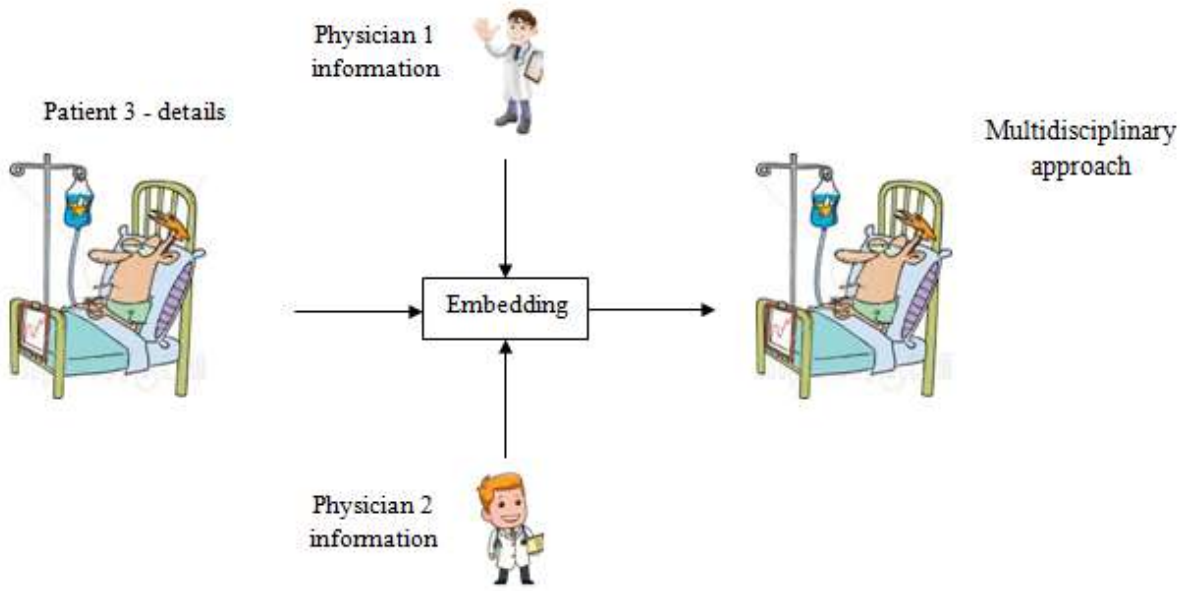

Figure. 6. Creation of block 3 as multidisciplinary approach

4.4 Healthcare system using Blockchain technology

Fig. 7 shows the overview of healthcare system using the Blockchain technology. It contains three blocks, such as primary care (genesis block), cross-disciplinary referral (block 2) and multidisciplinary approach (block 3). Each block has separate hash and the hash of the previous block. Subsequently, block 3 points the block 2 and the block 2 points the block 1. The initial block is a special, it cannot point the previous block because it is the initial one. Hence, the initial block is called the genesis block. If any change occurs in any block, it will make all the following blocks are invalid, since it no longer has the capacity to store the valid hash of the previous block. Hence, it is not possible to change any block in the distributed ledger of the Blockchain technology.

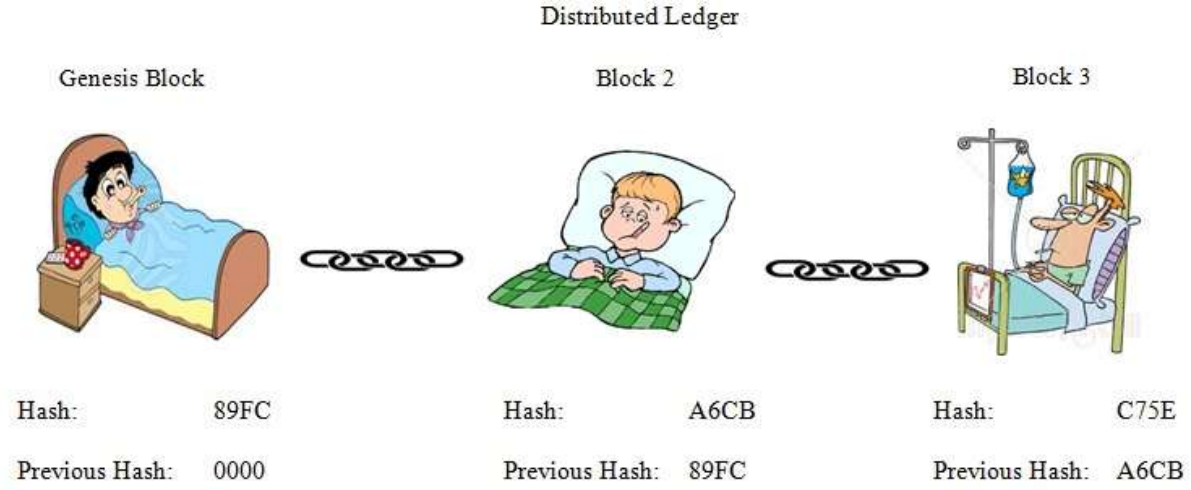

Figure. 7. Overview of Healthcare system using Blockchain technology

5. Experimental results and discussion

The performance of the various scenarios in healthcare system using the Blockchain technology and a number of experiments, performed on different patient images of size 512×512, are shown in Fig. 8. The logos of size 48×48, used as two different physician images, are shown in Fig. 9.

Patient 1 Patient 2 Patient 3

Figure. 8. Original images

Physician 1 Physician 2

Figure. 9. Watermarks

The image quality of each block is measured by finding the Peak Signal to Noise Ratio (PSNR) values of primary care, cross-disciplinary referral, multidisciplinary approach and the patient details. The PSNR is the logarithmic value of the ratio between the signal and the noise. It is expressed in decibels as

$$PSNR(dB) = 10\log_{10}\frac{255^2}{MSE} \qquad (3)$$

Where, the MSE = Mean square error

Normalized Correlation (NC) is used to measure the quality of the physician information after the recovery. The NC values are found between the embedded physician information W (i, j) and the extracted physician information W'(i, j) is given by

$$NC = \frac{\sum_{i=1}^{H}\sum_{j=1}^{L} W(i,j)\times W'(i,j)}{\sum_{i=1}^{H}\sum_{j=1}^{L}[W(i,j)]^2} \qquad (4)$$

Table 1 and Fig. 10 show the PSNR and NC values on various blocks of with and without attacks. To prove the robustness, primary care, cross-disciplinary referral and multidisciplinary approach, the images are tested with selected attacks such as salt and pepper noise, median filtering, cropping, rotation, JPEG compression, smoothing and row-column copying of the healthcare system using the Blockchain technology.

Journal of Engineering Technology
Volume 6, Issue 2, July. 2018, PP. 42-54
RESEARCH ARTICLE -ENGINEERNG TECHNOLOGY

Each block is corrupted with salt and pepper noise at the density of 3%, For median filtering, 3×3 mask consisting of 0.03 intensity values, is used to reduce the noise in the block. In cropping attack, a small portion of the block is cut or removed. Rotation is tested by rotating the block in 60 degrees direction and then brought back to the original position through bilinear interpolation. Each block is compressed with quality factor 20. In row-column copy attack, a set of rows and columns are copied to the adjacent or random locations. In this attack, from 151 to 200 rows are copied to 251 to 300 and 251 to 300 rows are copied to 151 to 200.

A fruitful Blockchain technology solution also needs to be sustainable. The proposed method utilizes a private Blockchain built using the distributed ledger for backend functions, such as keeping a ledger of embedded information and storing the records of permits. This is done for a tiny motive. First and foremost, it grants permission which is core to the EMRs vision. Second, there are no gas costs connected with private Blockchain as they utilize predefined verified nodes. With this method, each time, a medical record is accessed or updated, as it is cost-free. Third, it allows the platform to confirm the transactions at superior speeds.

Table 1. PSNR and NC values on various blocks without attacks

	Primary care		Extracted Physician 1	
Genesis Block				
	PSNR = 46.4387		NC = 1	
	Cross-disciplinary referral 1	Cross-disciplinary referral 2	Extracted Physician 1	Extracted Physician 2
Block 2				
	PSNR1 = 44.6303	PSNR2 = 38.3726	NC1 = 1	NC2 = 1
	Multidisciplinary approach		Extracted Physician 1	Extracted Physician 2
Block 3				
	PSNR = 40.6243		NC1 = 1	NC2 = 1

Journal of Engineering Technology
Volume 6, Issue 2, July. 2018, PP. 42-54
RESEARCH ARTICLE -ENGINEERNG TECHNOLOGY

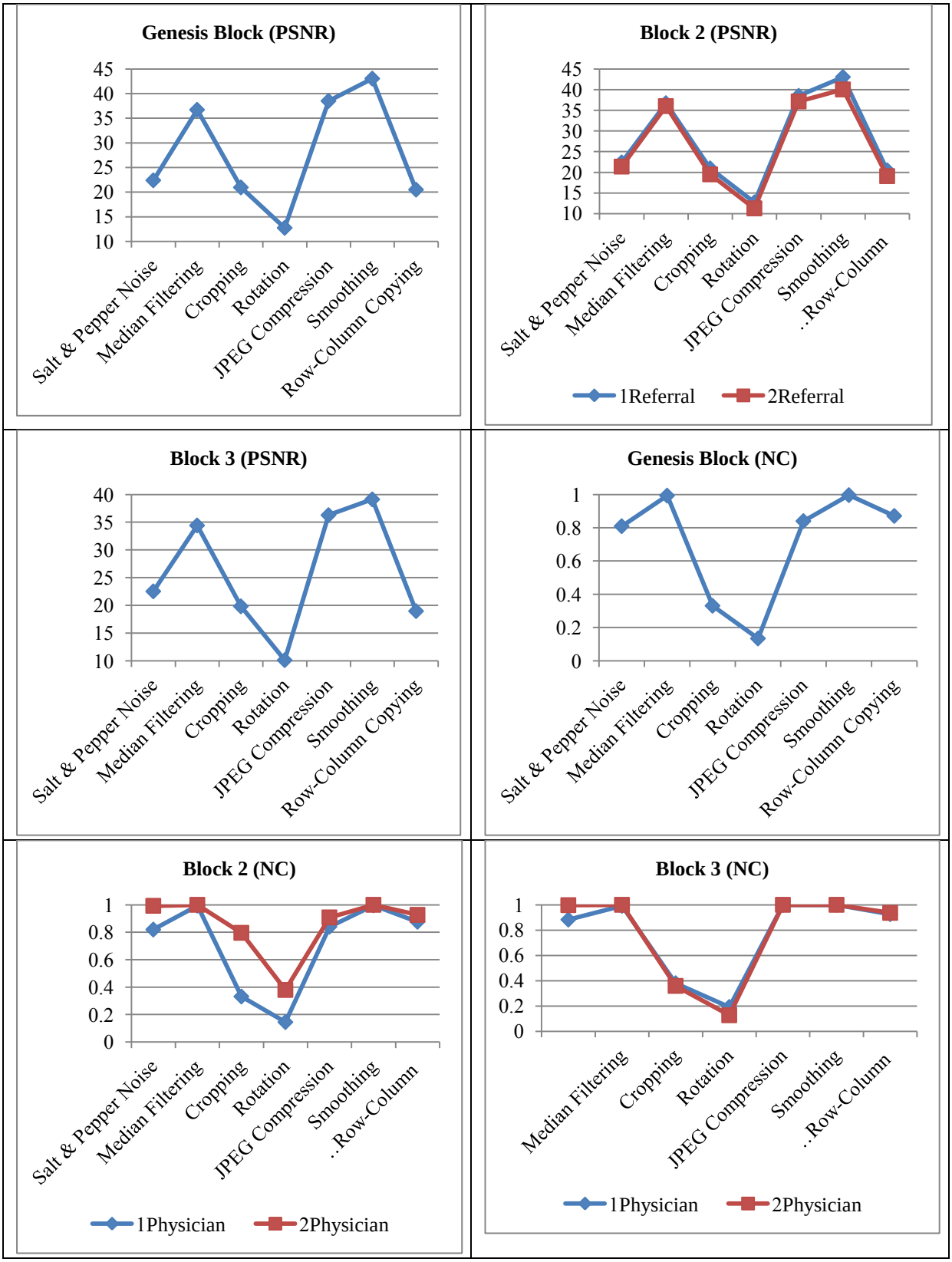

Figure. 10. PSNR and NC values on various blocks with attacks

6. Conclusion

The challenges of EMRs sharing within the healthcare system domain are significant. Simply sharing the records is not enough. The proposed method, using the private Blockchain technology, can play an essential role in enabling the records immutable, secure and share within a decentralized network. In this work, the blocks are defined as high level three-scenarios and their protocols are essential to apply this new technology in the healthcare system. Finally, the performance of imperceptibility and robustness values on each block of the distributed ledger are measured. Each suggestion provides some information and the motives behind the technical direction. It is hoped that this paper will stimulate further research and development to help the patients as well as the general healthcare system.

References

[1]. Medicalchain,https://medicalchain.com / Medicalchain – Whitepaper - EN.pdf/,2017.
[2]. Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system", (2008).
[3]. Edureka, Blockchain Tutorial Series, https://www.edureka.co/blog/blockchain-tutorial/, 2017.
[4]. Yli-Huumo J, Ko D, Choi S, Park S, Smolander K, "Where Is Current Research on Blockchain Technology?—A Systematic Review", PLoS ONE. 11, 2016, 1-27.
[5]. William Gordon, Adam Landman, "Blockchain in Health Care: Decoding the Hype", https://catalyst.nejm.org/decoding-blockchain-technology-health/, 2017.
[6]. Brodersen C, Kalis B, Leong C, Mitchell E, Pupo E, Truscott A , "Blockchain: Securing a New Health Interoperability Experience", https://newsroom. accenture.com/industries/healthpublic-service/accenture-finds-infor mationgoverna nce-framework-needed-to-guide-e-healthinvestments-and-strategy.htm /, 2016.
[7]. Ariel Ekblaw, Asaph Azaria, John D. Halamka, MD, Andrew Lippman, "A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data", IEEE Conference, 2016.
[8]. Xiao Yue, Huiju Wang, Dawei Jin, Mingqiang Li, Wei Jiang, "Healthcare Data Gateways : Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control", Journal of Medical Systems, 2016, 40 (10).
[9]. Arijit Chakrabarti, Ashesh Kumar Chaudhuri, "Blockchain and its Scope in Retail", International Research Journal of Engineering and Technology, 2017, 04 (07), 3053-3056.
[10]. Deepayan Bhowmik, Tian Feng, "The multimedia blockchain: A distributed and tamper-proof media transaction framework", IEEE international conference on Digital Signal Processing, 2017.
[11]. Alevtina Dubovitskaya MS, Zhigang Xu MD, Samuel Ryu MD, Michael Schumacher, Fusheng Wang, "Secure and Trustable Electronic Medical Records Sharing using Blockchain", AMIA Annual Symposium Proceedings, 2017.
[12]. Savjee, Blockchain, https://www.youtube.com/watch?v=SSoEIwHSd4/, 2017.
[13]. Loo P, Kingsbury N, "Digital watermarking using complex wavelets", IEEE International Conference on Image Processing, 2000, 29-32.
[14]. Venkateshappa, Cyril Prasanna Raj, "Fast Algorithm for Multimodal Image Registration with DTCWT", Indian Journal of Science and Technology, 2017, 10, 1-8.
[15]. Rich Wareham, Nick Kingsbury, Cian Shaffrey, DTCWT Documentation, https://media.readthedocs.org/pdf/dtcwt/latest/dtcwt.pdf/, 2017.

[16]. Hari Jyothula, KoteswaraRao S , ValliKumari V, "Image Segmentation Applying Adaptive Kernel Possibilistic C-Means with Level Set Method - A Cluster Center Initialization Approach Grounded on Cuckoo Based Search", Journal of Engineering Technology, 2017, 6, 19-34.

[17]. Sayantani Ghosh, Samir Kumar Bandyopadhyay, "Analysis of golden face based on semantic annotation of image", Journal of Engineering Technology, 2018, 6, 245-257.

[18]. A. Suganthi, M. SenthilMurugan, "An efficient image inpainting using patch sparsity with geodesic distance", Journal of Engineering Technology, 2017, 6 (2), 185-198.

[19]. Ananth C, Karthikeyan M, Mohananthini N, "Literature Survey on multiple image watermarking Techniques with Genetic Algorithm", Advanced Natural and Applied Sciences, 2017, 11, 237-257.

[20]. Mohananthini N, Yamuna G, "Performance Optimization of Multiple Watermarking Using Genetic Algorithms", International Journal of Enterprise Network Management, 2016, 7, 237-249.

[21]. Amit Kumar Singh, "Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images", Multimedia Tools and Application, 2016, 76 (6), 8881–8900.