Secured Different Disciplinaries in Electronic Medical Record based on Watermarking and Consortium Blockchain Technology

N. Mohananthini[1*], C. Ananth[2] and M.Y. Mohamed Parvees[3]
[1]Department of E.E.E., Muthayammal Engg. College (Autonomous),
Rasipuram-637408, Tamilnadu, India.
[e-mail: mohananthini@yahoo.co.in]
[2, 3]Department of Computer and Information Science, Annamalai University,
Annamalainagar-608002, Tamilnadu, India.
[e-mail: [2]ananth.prog@gmail.com, [3]yparvees@gmail.com]
*Corresponding author: N. Mohananthini

Received April 21, 2021; accepted February 22, 2022; published March 31, 2022

Abstract

The Electronic Medical Record (EMR) is a valuable source of medical data intelligence in e-health systems. The watermarking techniques have been used to authenticate the owner and protect the EMR from illegal copying. The existing distributive strategies, successfully operated to secure the EMR, are found to be inadequate. Blockchain technology, mainly, is employed by a sharing database that allows the digital crypto-currency. It rapidly leads to the magnified expectations acme. In this excitement, the use of consortium adopting the technology based on Blockchain, in the EMR structure, is found improving. This type of consortium adds an immutable share with a translucent record of the entire business and it is accomplished with responsibility, along with faith and transparency. The combination of watermarking and Blockchain technology provides a singular chance to promote a secured, trustworthy electronic documents administration to share with the e-records system. The authors, in this article, present their views on consortium Blockchain technology which is incorporated in the EMR system. The ledger, used for the distribution of the block structure, has team healthcare models based on dissimilar multiple image watermarking techniques.

Keywords: Consortium blockchain technology, electronic medical record, cryptography, image encryption, cipher watermark, team healthcare

http://doi.org/10.3837/tiis.2022.03.011 **ISSN : 1976-7277**

1. Introduction

Being an important part of electronic information technology, the EMR is a general methodical way to store the patients' information and biomedical images in the hospitals. The Information, related to a particular patient, is kept in the records of the hospitals. Hence, a complex effort is required to create a complete summary of each patient's records and make it available in the hospital since it involves great level of security and privacy issues. In the interim, the present EMR systems require a regular sharing policy in managing the data, which, otherwise can create complex problems for the scientists in the fields of pharmaceutical and mediate supported with the accurate medication data collected from applications [1].

The EMR, within the e-health system, generally, provide common information such as personal information about a patient, biomedical images, Physician details, and treatment history, as it is composed of the entity's medical data preparation. There is a necessity for the EMR to develop fool-proof methods of transferring information to several places.

The authors show that almost twelve million patients' blood tests records, obtained through Quest Diagnostics as hacked, and the major data stolen ever [2]. In fact, the e-health structure have more of data breaches than the erstwhile sectors and more than 95% of the agencies, included in the survey, suffered from the attacks of networks. The electronic records, thus, stolen were sold in black market as they are 10 fold expensive in the open networks, when compared to the credit card records [3]. Since the e-health systems suffer from huge threat, there is a need for an intelligent and viable strategy to analyse, fabricate, and frame a secured and well maintained system of storage facility of the records, related to the patients, along with the assurance of preserving the privacy of the individuals.

So, the author suggests viable methods to solve the issues of security and reliability in multiple watermarking by using Discrete Wavelet Transform (DWT) along with Singular Value Decomposition (SVD) for healthcare images. Their digital healthcare image watermarking scheme has been produced with higher quality watermarked images and the extraction watermarks have good perceptions as described in [4].

The revealed challenges will be solved with the Blockchain technology presented in [5]. This technology has become extraordinarily popular, in the present time, as it specifies a series of blocks filled with the details of a particular person or concept. This technology, originated in 1991, has been incorporated in time stamps digitized records. It is insufferable and never gets corrupt like a notary. However, it has been initially presented by Satoshi Nakamoto in 2008 [6] to make digital e-currency. The Blockchain could be an open system of ledger which everyone can have access [7]. Once the block is formed, the records can never be altered or erased as the result of each and every transaction can be confirmed by the entire members.

Jesse *et al*. [8] concludes that the applications of Blockchain have specialized more than 80% of the research articles in Bitcoin method and the remaining 20% arrangements have different applications like, e-health, law-enforcement, smart contracts, on-line music and voting system. This is necessary to know about the current applications enlarged with the technology. It is necessary to recognize the different applications, since it will be easy to appreciate erstwhile guidelines and traditions to use the Blockchain technology. The Blockchain technology increases its holds on security and privacy considerations, currently, because it presents a novel thought of sharing the records [9]. When the Blockchain's latent are used within the healthcare model, it can really evaluate these limitations. Thus, the planned-effort explores how this technology is useful for an e-health model. Thakur *et al.* [10] present a novel watermarking technique utilizing the transform domains for e-health systems. For superior privacy, the authors apply the chaos supported watermarking encryption algorithm for the images used with a fewer complex methods. The results of the investigation show the present method as being greatly robust with adequate security against different forms of attacks exclusive of any major distortions among the original and watermarked image.

1.1 Problem definition

- Many researchers could have studied and proposed the Blockchain technology as suitable for resolving the cryptocurrency application problems. However, it is essential to discover the erstwhile applications based on Blockchain technology. Thus, this technology, considered to be safe to the e-health model, is implemented.
- The methodology for the construction of the each block, within the Blockchain technology, is similar. But, the needs of e-health models, measured and planned by the methodology for the formation of the each block, are formed dissimilar and applied through single and various multiple image watermarking techniques.
- Generally, the EMRs are swapped, from one area to the needed area, via unsecured open-networks. In such cases, it may create a risk and the results indicate undesirable results. Considering this reality, the EMRs are employed in planned Blockchain technology with multiple image watermarking techniques. It is essential to avoid various problems such as, transparency, higher security and maintenance of the privacy of the patients.
- Although researchers have studied the e-healthcare systems based on Blockchain technology, their works may not have included in different disciplinaries [11].

The Blockchain execution principle is shown in **Fig. 1**.

2. Related Works

In several types of businesses, a novel model is employed that enables quicker, more professional and extremely protected business with consumer dealings. People employed in healthcare system expect similar distributed database technologies, which adopt this new method to preserve the related results inside the business. The formation of portable, secured, confidential information need to have a higher level of fidelity and integrity and must be confidential over the healthcare system continuum [12]. The authors proposed a new and decentralized data managing scheme to hold the e-healthcare system, via Blockchain technology. Their method provides the patients a complete, unalterable log with simple access to their record over the suppliers and healing locations [13].

Yue *et al.* [14] discuss centrical access method to ensure the patients in managing the health record by themselves. Being easy and united, the indicator – centrical scheme – can help arrange all types of personal healthcare records practically and simply. Their method, besides printing the Secure Multi-Party Computing (MPC), is helpful in allowing the untrusted third-party to perform computation across patient records, exclusively, by violating the privacy rules.

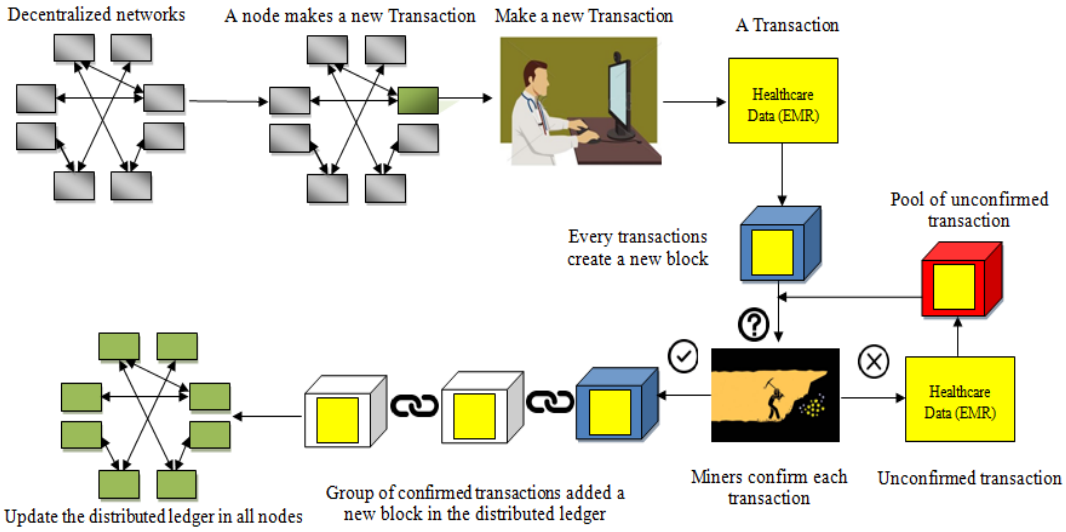

Decentralized networks
A node makes a new Transaction
Make a new Transaction
A Transaction
Healthcare Data (EMR)
Pool of unconfirmed transaction
Every transactions create a new block
Healthcare Data (EMR)
Update the distributed ledger in all nodes
Group of confirmed transactions added a new block in the distributed ledger
Miners confirm each transaction
Unconfirmed transaction

Fig. 1. Outline of Blockchain implementation principle

This technology's various benefits and important features are discussed in [15]. This technology, even now developing with major scope for various industries and field, is going to modify the globe. However, it isn't liberated from the difficulties; a little of them have been highlighted. While the technology is at the back of Bitcoin, its employability is not restricted only to the economic area. In 2016, Blockchain was introduced as the major modern technology in the trade industry than in any former industry. In 2017, Blockchain became the governing excitement expression for the trade industry.

Deepayan and Tian [16] present new watermarking supported multimedia Blockchain-based framework which can concentrate on several problems. The sole watermark symbol has two parts of data - the cryptographic hash contains the operation histories and the image hash conserves the retrievable cover-media. Once the watermark symbol is extracted, the initial part of the watermark symbol can be approved by a distributed ledger to regain the past transaction check and the final part can be utilized to recognize the tampered or edited sections.

Alevtina *et al.* [17] propose the perspectives for Blockchain supported electronic health records administration, in exacting the Electronic Medical Records distribution among the healthcare contributors with research studies. This agenda assists in managing and distributing the Electronic Medical Records for the cancer patients' history. Their works make easy the revolving time for the Electronic Medical Records, furthermore, to develop the decision creation for the healthcare professionals so as to decrease the general expenditure.

Ananth *et al*. [12] present a secured healthcare system based on private blockchain technology. The distributed ledger blocks, from various schemes like, primary care, multidisciplinary approach and cross-disciplinary referral utilizing dissimilar watermarking methods and its protocols, are found important to apply the Blockchain technology in healthcare model. The presentation of their method achieves the imperceptibility and also the robust values of every block of the distributed ledger which can be measured. However, the author has covered the partial disciplinaries of team healthcare models. Hongyu Li *et al*. [18] implemented a model of the DPS which is supported on the real world blockchain-based platform Ethereum. The performance assessment grades show the fact that their proposed systems are effective and efficient.

HaoWang *et al*. [19] proposed Electronic Health Record (EHR) system which is supported by attribute-based cryptosystem with Blockchain technology. Their system- Attribute Based Encryption (ABE) along with the Identity Based Encryption (IBE) - helps in encrypting the healthcare data and the Identity Based Signature (IBS) helps in implementing the digital signatures. In accretion, the Blockchain technology ensures the honesty and traceability of healthcare data.

3. Material and Models

3.1 Digital Image Watermarking Technique

The watermarking technique presents authentication and copyright production of digital images. It has been divided into two types [20],

Single watermarking: The only one watermark image which can be inserted into the novel image.

Multiple watermarking: It is an extension of single watermarking. Being greater than the single watermark image, it can be inserted into the novel image.

3.2 The Hash Algorithm

Every block has a unique ID like a finger-print. The unique ID is generated on the basis of the data using the hash-algorithm. A hash-algorithm is a kind of mathematical function which turns the data into a fingerprint of the data known as hash. It’s like a formula which takes the input of the data and turns it into an output of a fixed length data, which stands for the fingerprint of the data.

Always, a hash-algorithm gives the same hash for the same input data. Fascinatingly, if even one character, within the input data, is altered, the output hash value will be changed. In addition, a hash-algorithm is a one-way function; hence it is not possible to generate back the input data from its hash value. Therefore, we can go from the input data towards the hash, but not from the hash towards the input data [21]. The NIST (National Institute of Standards and Technology) recommended cryptographic-secured hash algorithm (SHA – 256) has been used to secure the proposed system. [22].

3.3 Blockchain Technology

This technology gives an immutable, transparent, and shared record of the entire connections to make the applications accountable, transparent and also trustful. It presents an exclusive opportunity to expand the trustable, secured record supervision and the sharing method [23].

The Blockchain technology has 3 types as mentioned below [24].

Private: It permits merely particular persons in the group to confirm and insert the business blocks, although each individual of the group can usually approve the vision.

Consortium: It permits merely a group of societies which can confirm and insert transaction blocks, although the ledger can be open or accessible only to certain groups.

Public: It perceives every person on the open-network and any person can confirm and insert a transaction block to the Blockchain.

For the above three types, the consortium Blockchain technology excitements are appropriate in the proposed method. Thus, we can utilize the consortium Blockchain technology.

3.4 Team Healthcare Models: Disciplinaries

Alexander [25] presented five different disciplinaries in healthcare as shown in **Fig. 2**:

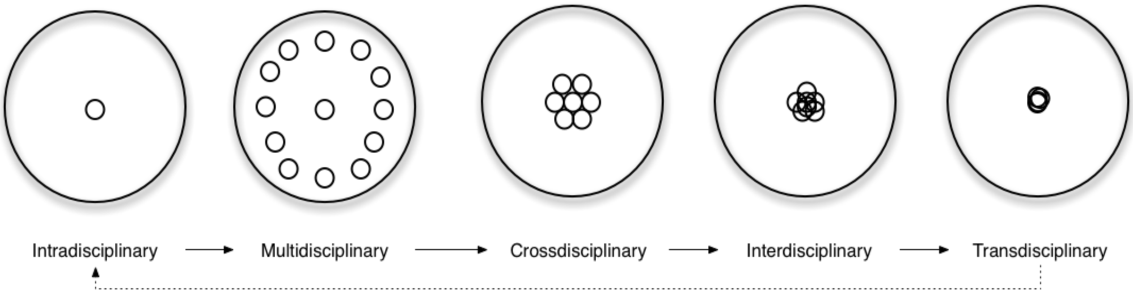


Fig. 2. Types of Disciplinaries

1. Intradisciplinary: dealing with the concept found in a homogeneous frame.
2. Crossdisciplinary: approaching a totally different field with the notions of another field.
3. Multidisciplinary: it is a mixture of many disciplinaries in which many work to gain the knowledge required for them.

4. Interdisciplinary: using the approach common to many disciplinaries and draw the necessary knowledge.
5. Transdisciplinary: crossing the borders of a particular field and integrating all the concepts and knowledge related to the base concept.

The difference between inter-disciplinary and multi-disciplinary care: the interdisciplinary care involves the panel members from dissimilar disciplines functioning collaboratively, with a general reason, to set the goals, create assessments, divide the resources and the responsibilities. Whereas, the multidisciplinary care engages the panel members functioning independently to make the discipline follow the specific-care procedure that are executed concurrently, although without explicit regard to their communication discussed in [26]. Nandiwada *et al.* [27] discussed the transdisciplinary healthcare which is vital among the underserved populations since these patients not only carry the major burden of chronic disease or infection, but also subject to economic, environmental and social determinants of health that contribute to make worse the results than in other groups.

4. The Proposed Method

The proposed method has a grouping of watermarking as well as Blockchain technology, initially; the single or multiple watermarks are embedded into EMR and, finally, store the embedded EMR in the distributed ledger using the blockchain technology.

The embedding process develops the quality of the embedded- image along with more robustness of the extracted watermark symbols utilizing the DWT and the SVD. The novel image and the containing the Patient’s information and the watermark image containing the Doctor’s information, as mentioned in the block diagram of the embedding method, are represented in **Fig. 3**. All the team healthcare models are examined below:

4.1 Structure of the Proposed Block

The structure of the proposed block has three parts as seen in **Fig. 4**. It includes the header, body and footer.

The header of the block has two components: Hash value of the present block and the Block Id.

The body of the block has four components: The identity of the block owner (Patient); the Identity of block generator (Doctor); and the embedded information (watermarked information) and its keywords.

The footer of the block has three components: Date and Time-stamp (generation date and time of the block), Size of the Block in addition to the hash value of the previous block.

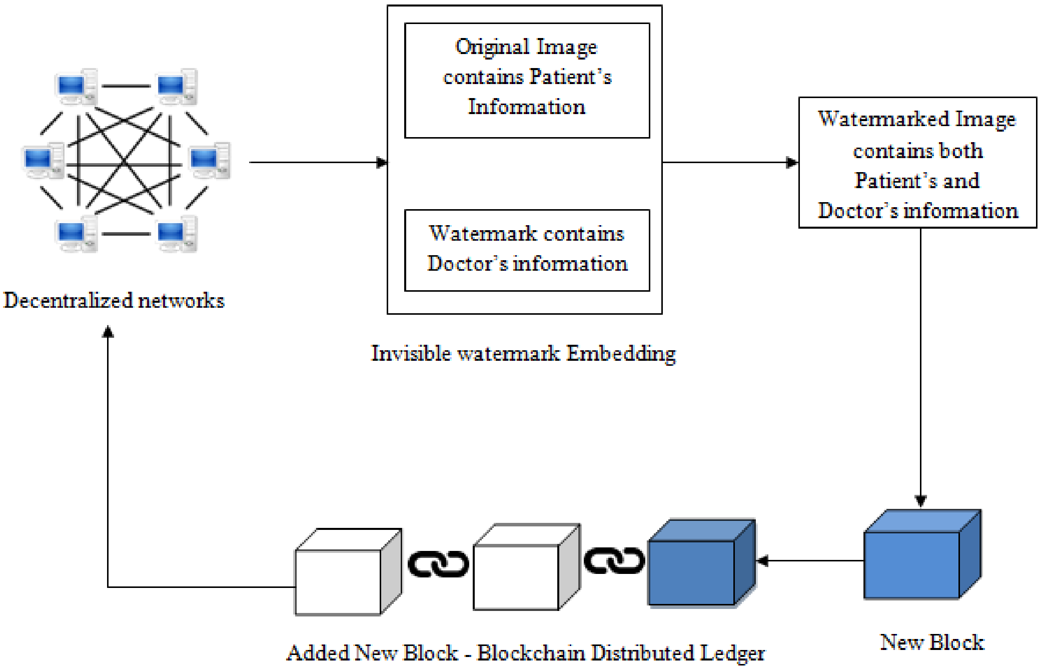

Decentralized networks
Original Image contains Patient's Information
Watermark contains Doctor's information
Invisible watermark Embedding
Watermarked Image contains both Patient's and Doctor's information
Added New Block - Blockchain Distributed Ledger
New Block

Fig. 3. The embedding process diagram

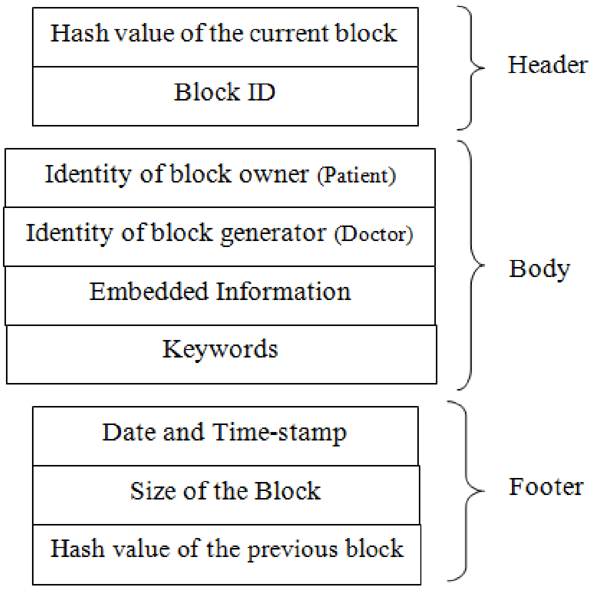

Hash value of the current block
Block ID
Header
Identity of block owner (Patient)
Identity of block generator (Doctor)
Embedded Information
Keywords
Body
Date and Time-stamp
Size of the Block
Hash value of the previous block
Footer

Fig. 4. Structure of the proposed block

4.2 Intradisciplinary Care

The preparation of the abilities and scope of instruction, which classify the primary-care of single discipline physician, contains the factors like the elementary examination, the treatment of fundamental diseases along with the medical condition. Diagnostic procedures help interview the patients to collect information regarding the current symptoms, prior medical history and erstwhile healthcare information, which may be followed by a physical assessment. **Fig. 5** displays the creation of block 1 (genesis block) as Intradisciplinary care:

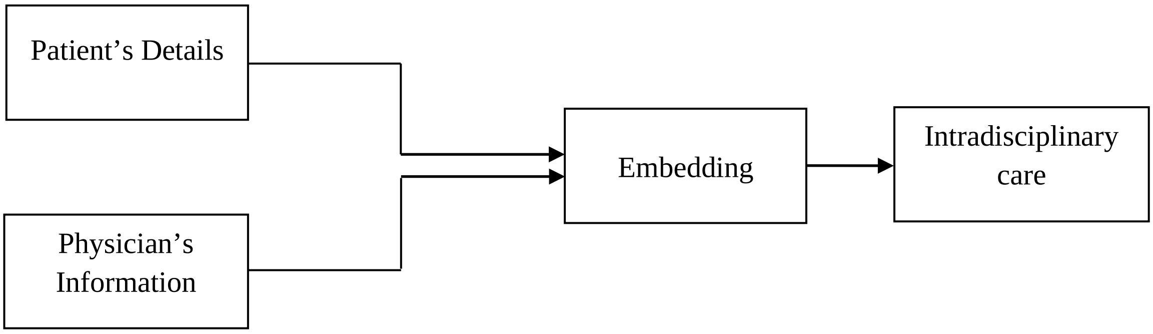


Fig. 5. Creation of genesis block as Intradisciplinary care

Algorithm - Intradisciplinary block

Input: User Instructions
Output: Encrypted Intradisciplinary block

Initialization: Hash value of the previous block and the Id of the block

```
if the user confirms the conservation then
    $P_{(i,j)}$ ← Identity of the block owner (Patient)
    $Q_{(i,j)}$ ← Identity of the block generator (Doctor)
    Embedded Image ← $S_{(i,j)} \leftarrow P_{(i,j)} + \alpha \times Q_{(i,j)}$
    $Tw$ ← Block's Keywords
    $Pub_{Key}$ ← generate the public key
    Stores the file in the block
else
    deletes the temporary storage of data conservation
end if
Stores the size of the block
Stores the date and time-stamps
Stores the hash value of the current block
```

4.3 Interdisciplinary Care

An inter-disciplinary care engages the panel members from dissimilar disciplines functioning collaboratively, through a common principle, to set the targets, create assessments and share the resources and the tasks. A panel of physicians, from dissimilar disciplines, jointly with the patient, develops a care plan, diagnoses, undertakes assessment, sets the goal and intervenes. Every one of the health-care physicians, who belongs to different disciplines, can suggest particular treatment procedure to the patient. **Fig. 6** exhibits the creation of block 2 as Interdisciplinary care:

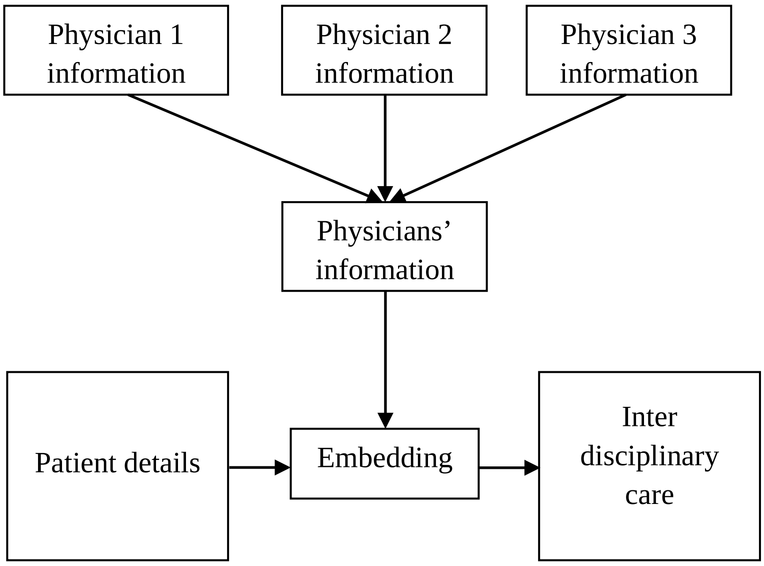


Fig. 6. Creation of block 2 as Interdisciplinary care

Algorithm - Interdisciplinary block

Input: User Instructions
Output: Encrypted Interdisciplinary block

Initialization: Hash value of the previous block and the Id of the block

```
if the user confirms the conservation then
    $P_{(i,j)}$ ← Identity of the block owner (Patient)
    $Q_{1(i,j)}$ ← Identity of the block generator (Doctor 1)
    $Q_{2(i,j)}$ ← Identity of the block generator (Doctor 2)
    $Q_{(i,j)} \leftarrow Q_{1(i,j)} + Q_{2(i,j)}$
    Embedded Image ← $S_{(i,j)} \leftarrow P_{(i,j)} + \alpha \times Q_{(i,j)}$
    $Tw$ ← Block's Keywords
    $Pub_{Key}$ ← generate the public key
    Stores the file in the block
else
```

```
        deletes the temporary storage of data conservation
    end if
    Stores the size of the block
    Stores the date and time-stamps
    Stores the hash value of the current block
```

4.4 Crossdisciplinary Care

In electronic healthcare model, a recommendation, effected for the transfer of care for a patient from one hospital or physician to another is necessary. The main objective is to develop and modernize the communication with basic-care physicians, specialists and any erstwhile health providers concerned with a patient's care. Fig. 7 shows the formation of block 3 as a cross-disciplinary care. The embedding steps are observed, rolled back and re-applied with the DWT. It permits the system to find out the order in which the physician's information is inserted. In this scenario, the EMR, when recommended, may be embedding the information equally between the physician and the patient. Lest, one more recommendation can occur, and on each occasion, the corresponding physician's information can be embedded.

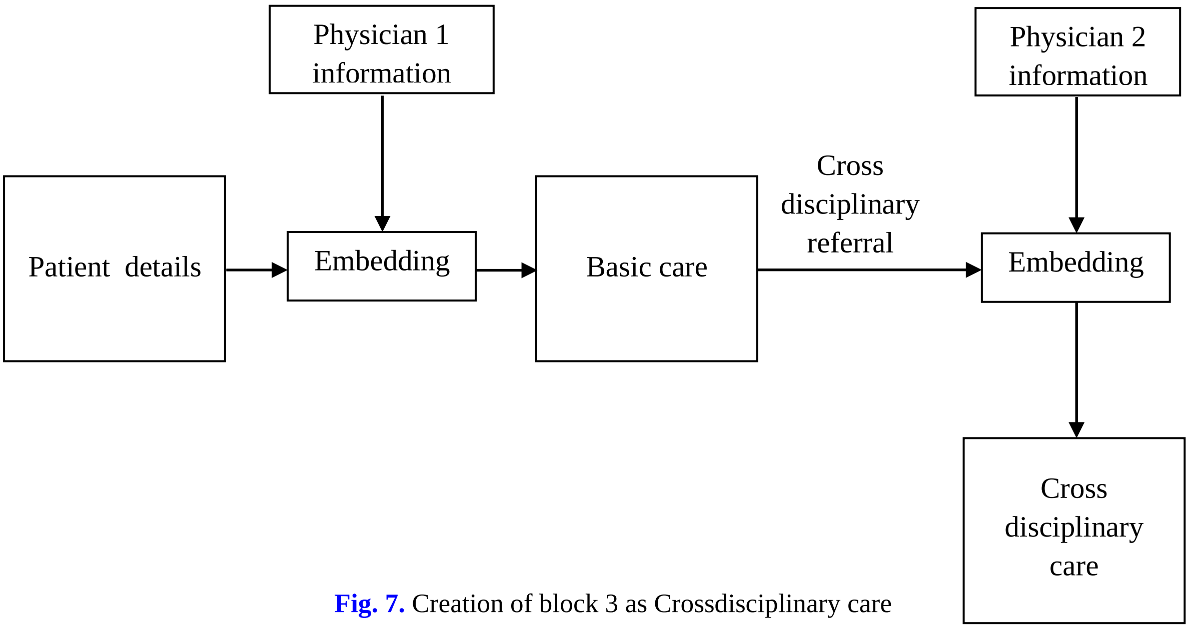


Fig. 7. Creation of block 3 as Crossdisciplinary care

Algorithm - Crossdisciplinary block

Input: User Instructions
Output: Encrypted Crossdisciplinary block

Initialization: Hash value of the previous block and the Id of the block

```
if the user confirms the conservation then
    $P_{(i,j)}$ ← Identity of the block owner (Patient)
    $Q_{1(i,j)}$ ← Identity of the block generator (Doctor 1)
    $Q_{2(i,j)}$ ← Identity of the block generator (Doctor 2)
    $S_{1(i,j)} \leftarrow P_{(i,j)} + \alpha \times Q_{1(i,j)}$
    Embedded Image ← $S_{2(i,j)} \leftarrow S_{1(i,j)} + \alpha \times Q_{2(i,j)}$
    $Tw$ ← Block's Keywords
    $Pub_{Key}$ ← generate the public key
    Stores the file in the block
else
    deletes the temporary storage of data conservation
end if
Stores the size of the block
Stores the date and time-stamps
Stores the hash value of the current block
```

4.5 Multidisciplinary Care

Multi-disciplinary care is an integrated team-heed extended to a patient. The team members, working independently on discipline-specific care procedure, can execute simultaneously, but with no explicit regard to their communication. This strategy coordinates their treatments and obtains the group functioning jointly to achieve a particular set of objectives. Fig. 8 shows the formation of block 4 as a multi-disciplinary care.

Algorithm - Multidisciplinary block

Input: User Instructions
Output: Encrypted Multidisciplinary block

Initialization: Hash value of the previous block and the Id of the block

```
if the user confirms the conservation then
    $P_{(i,j)}$ ← Identity of the block owner (Patient)
    $Q_{1(i,j)}$ ← Identity of the block generator (Doctor 1)
    $Q_{2(i,j)}$ ← Identity of the block generator (Doctor 2)
    Sliced_A-Image and Sliced_B-Image ←Sliced into two parts←$P_{(i,j)}$
    $S_{1(i,j)} \leftarrow Sliced\_A\text{-}Image + \alpha \times Q_{1(i,j)}$
    $S_{2(i,j)} \leftarrow Sliced\_B\text{-}Image + \alpha \times Q_{2(i,j)}$
    Embedded Image ← $S_{2(i,j)} + S_{1(i,j))}$
    $Tw$ ← Block's Keywords
    $Pub_{Key}$ ← generate the public key
    Stores the file in the block
else
    deletes the temporary storage of data conservation
```

```
end if
Stores the size of the block
Stores the date and time-stamps
Stores the hash value of the current block
```

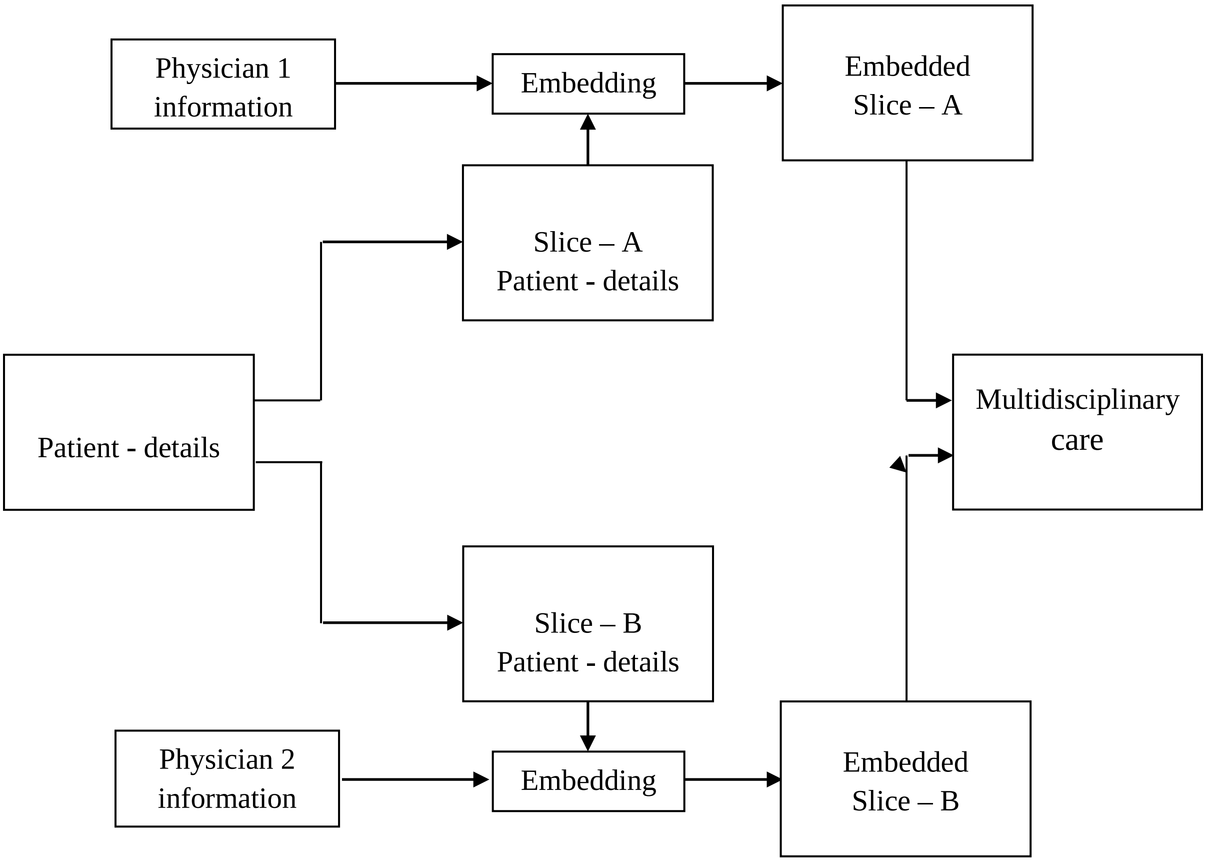


Fig. 8. Creation of block 4 as multidisciplinary care

4.6 Transdisciplinary Care

Transdisciplinary healthcare is engaged on the spaces among the disciplines to generate optimistic healthcare results during teamwork. This representation of care efficiently integrates the clinicians like, physicians, physician assistants, nurses, physical therapists, community health workers, complementary and alternative medicine practitioners and other healthcare providers to make a team that gives comprehensive precautionary primary healthcare. **Fig. 9** shows the formation of block 5 as a transdisciplinary care.

Algorithm - Transdisciplinary block

Input: User Instructions

Output: Encrypted Transdisciplinary block

Initialization: Hash value of the previous block and the Id of the block

```
    **if** the user confirms the conservation **then**
    $P_{(i,j)}$ ← Identity of the block owner (Patient)
    $Q_{1(i,j)}$ ← Identity of the block generator (Doctor)
    $Q_{2(i,j)}$ ← Identity of the block generator (Nurse)
    Embedded Image ← $S_{(i,j)}$ ← $P_{(i,j)} + \alpha \times Q_{1(i,j)} + \beta \times Q_{2(i,j)})$
    $Tw$ ← Block's Keywords
    $Pub_{Key}$ ← generate the public key
    Stores the file in the block
**else**
    deletes the temporary storage of data conservation
**end if**
Stores the size of the block
Stores the date and time-stamps
Stores the hash value of the current block
```

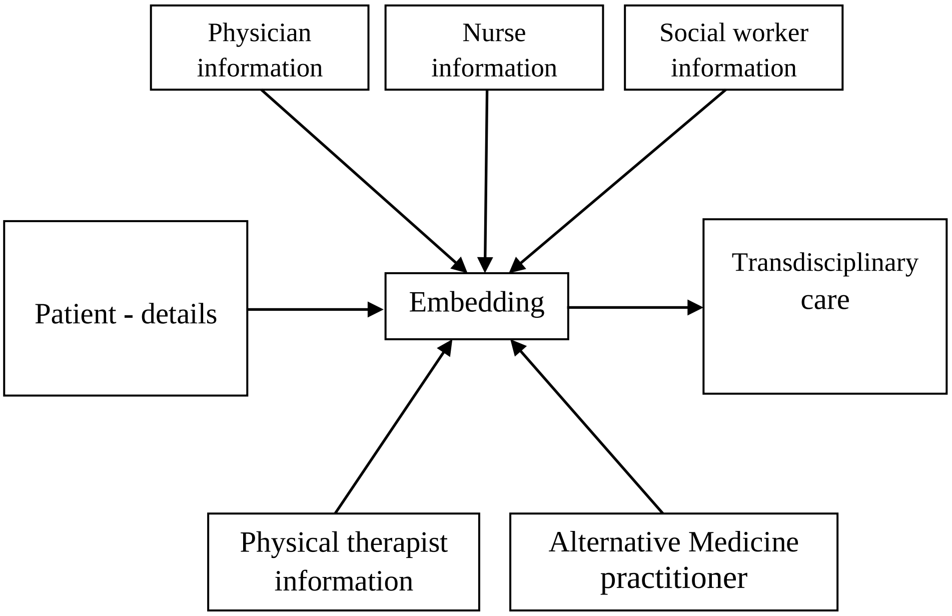
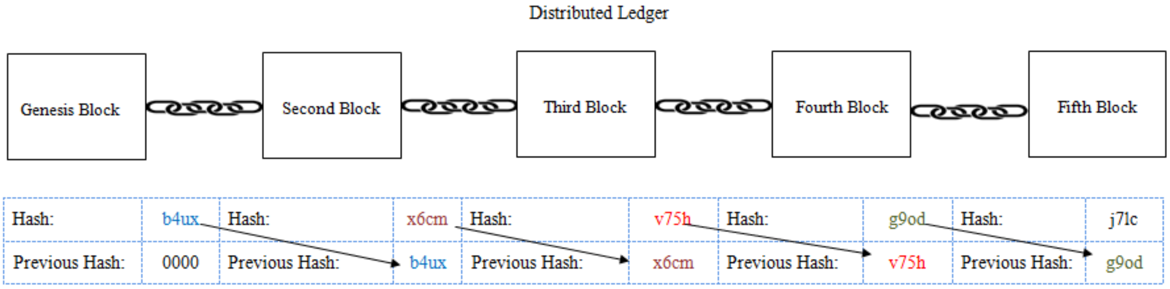

Physician information
Nurse information
Social worker information
Patient - details
Embedding
Transdisciplinary care
Physical therapist information
Alternative Medicine practitioner

Fig. 9. Creation of block 5 as trans-disciplinary care

4.7 Healthcare Model utilizing Blockchain Technology

In the proposed healthcare model, using the Secure Hash Algorithm (SHA-256), every encrypted image has 64 characters with unique hash value. **Fig. 10** shows the summary of electronic healthcare model utilizing the Blockchain technology. It has five different types of blocks; each block has separate own hash value and the hash value of the prior block. Consequently, block 5 is pointed towards the block 4 and the block 4 is pointed towards the block 3 and all the remaining blocks are pointed in this order. The opening block is an unusual one; this block cannot be pointed towards the prior block as it is the opening block. Thus, the opening block is called genesis block.

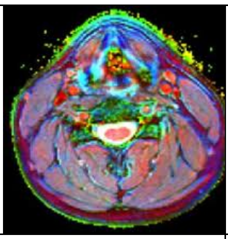
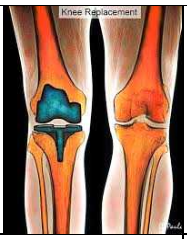
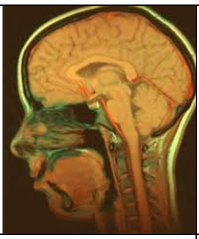


Hash:	b4ux	Hash:	x6cm	Hash:	v75h	Hash:	g9od	Hash:	j7lc
Previous Hash:	0000	Previous Hash:	b4ux	Previous Hash:	x6cm	Previous Hash:	v75h	Previous Hash:	g9od

Fig. 10. Summary of Healthcare model utilizing Blockchain technology

5. Results and Discussion

The presentation of the different scenarios within the e-healthcare model utilizing the watermarking, hash algorithm, Blockchain technology, and several trials, are presented with the original images of dimension 512×512 and the watermarks dimension 48×48, used as two dissimilar physician's information (watermark) images, are shown in **Fig. 11**.

				
Patient Image	Biomedical Image - 1	Biomedical Image - 2	Biomedical Image - 3	Lena Image
Original Images				

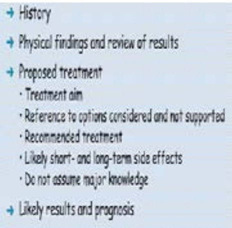
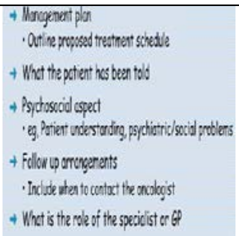
 History Physical findings and review of results Proposed treatment · Treatment aim · Reference to options considered and not supported · Recommended treatment · Likely short- and long-term side effects · Do not assume major knowledge Likely results and prognosis	 Management plan · Outline proposed treatment schedule What the patient has been told Psychosocial aspect · eg, Patient understanding, psychiatric/social problems Follow up arrangements · Include when to contact the oncologist What is the role of the specialist or GP
Physician1 Informations	Physician2 Informations
Watermark Images	

Fig. 11. Original and watermark images

5.1 Performance analysis

In this section, we discuss the security and efficiency of the proposed system.

5.1.1 Performance analysis of watermarking techniques

The advent of communication and information technology boosts the potential of digital information. At the same time, these benefits introduce parallel risks to unauthorized users. To overcome this problem, digital watermarking is a useful technique for preventing the misuse of an image and protecting the copyright of digital information. The embedding process is carried out for tetra-furcating the watermark and gets embedded into the subbands of the original image.

The image quality of every watermarked image can be calculated by finding the Peak Signal to Noise Ratio (PSNR) values of five different blocks and the patient's particulars. The PSNR assessment of ratio, among the signal and the noise and the articulation, in decibels, are given below:

$$PSNR(dB) = 10\log_{10}\frac{255^2}{MSE} \tag{1}$$

Where,

MSE = Mean square error

Normalized Correlation (NC) finds the worth of the watermark after recovery. It is a difference between the inserted watermark *W (i, j)* and the recovered watermark *W' (i, j)* as given by

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

Table 1 and **Table 2** demonstrate the point that the PSNR and NC values of different disciplinaries (without attacks).

Table 1. PSNR values on various disciplinaries (Without Attacks)

Disciplinaries	**Patient Image**	**Biomedical Image - 1**	**Biomedical Image - 2**	**Biomedical Image - 3**	**Lena Image**
	PSNR (dB)	**PSNR (dB)**	**PSNR (dB)**	**PSNR (dB)**	**PSNR (dB)**
Intradisciplinary care	43.1276	42.5452	43.9452	43.1364	43.5782
Cross-disciplinary referral	41.8651	40.6830	41.7694	40.9691	41.8892
Multidisciplinary approach	40.1523	38.2629	39.4901	38.9921	39.0215
Interdisciplinary	42.8726	41.6667	42.6721	41.3489	41.8793
Transdisciplinary	39.6271	40.0985	40.1874	39.4167	40.0184

Table 2. NC values of Extracted Physician Informations on various disciplinaries (Without Attacks)

Disciplinaries	**Patient Image**		**Biomedical Image - 1**		**Biomedical Image - 2**		**Biomedical Image - 3**		**Lena Image**	
	Image 1 NC	**Image 2 NC**	**Image 1 NC**	**Image 2 NC**	**Image 1 NC**	**Image 2 NC**	**Image 1 NC**	**Image 2 NC**	**Image 1 NC**	**Image 2 NC**
Intradisciplinary care	0.9887		0.9958		0.9828		0.9974		0.9853	
Cross-disciplinary referral	1	1	1	1	1	1	1	1	1	1
Multidisciplinary approach	1	1	1	1	1	1	1	1	1	1
Interdisciplinary	1	1	1	1	1	1	1	1	1	1
Transdisciplinary	1	1	1	1	1	1	1	1	1	1

The performance of the watermarking technique achieved only after withstanding a variety of attacks. **Table 3** and **Table 4** show the values of PSNR and NC about various disciplinaries for patient image and biomedical image against the attacks. To confirm the robustness, the watermarked image is tested with particular attacks. The watermarked images are corrupted with speckle noise variance of 0.005. The median filtering intensity value is 0.03 and it is used to decrease noise in the image. The cropping attack on the small portion of the embedded image can be cut or removed. The rotation can be tested by rotating 60 degrees direction of the image. The compression attack and the embedded images are compressed by quality factor 20.

The performance analysis of the PSNR and the NC values are found only after the first layer protection of the watermarking encryption is employed.

The imperceptibility of encrypted image quality is indicated with the PSNR values. The robustness of extracted watermark quality is indicated with the NC values. After applying various attacks, simulation result demonstrates that the proposed watermarking techniques have good imperceptibility on the encrypted image and good robustness on the extracted watermark.

5.2 Security Analysis of the Proposed System

The proposed system has three layers of protection based on watermarking techniques, secure hash algorithm and Blockchain technology. The uses of the proposed watermarking techniques are secured as discussed earlier. However, the image encryption with the addition of the secure hash algorithm (SHA – 256) is more secured. The hash value contains hexadecimal representation (0-9, a-f) and the hash value is like a figure print that each and every encrypted images has a unique hash value. A hash is not ‘encryption’ – it cannot be decrypted back to the original text (it is a ‘one-way’ cryptographic function having a fixed size for any size of source data).

Table 3. PSNR values on various disciplinaries (With Attacks)

Disciplinaries	**Attacks**	**Patient Image**	**Biomedical Image - 1**	**Biomedical Image - 2**	**Biomedical Image - 3**	**Lena Image**
		PSNR (dB)	**PSNR (dB)**	**PSNR (dB)**	**PSNR (dB)**	**PSNR (dB)**
Intradisciplinary care	Speckle Noise	28.9425	27.1463	29.0025	28.3587	29.2455
	Median Filtering	36.9266	34.8216	35.5762	34.9143	35.8203
	Cropping	19.8929	18.7822	19.6399	19.2023	19.6327
	Rotation	13.2057	11.1751	12.7075	11.8943	12.8632
	JPEG Compression	37.3449	36.9689	37.4509	36.9937	36.7935
Cross-disciplinary referral	Speckle Noise	28.1624	27.6206	27.8934	28.0698	28.0264
	Median Filtering	33.4385	33.4053	33.8532	32.9533	33.2642
	Cropping	18.7931	18.7839	17.8912	18.3969	18.1423
	Rotation	9.8156	9.8067	9.8061	9.7860	9.7043
	JPEG Compression	35.4331	35.3364	34.9932	35.2841	34.9621
Multidisciplinary approach	Speckle Noise	27.0765	27.0607	27.1852	26.9504	26.8281
	Median Filtering	33.5638	33.4184	33.3848	33.7895	32.9937
	Cropping	18.3673	18.2312	17.9629	18.0152	18.4027
	Rotation	8.7019	8.6891	9.0199	8.9811	9.1121
	JPEG Compression	35.3451	35.1999	35.0037	34.9959	35.2859
Interdisciplinary	Speckle Noise	34.6807	34.6705	33.8975	34.5734	34.7593
	Median Filtering	20.5123	20.5082	20.3574	20.5267	20.4831
	Cropping	19.0125	19.0015	18.8251	19.1353	19.0531
	Rotation	9.8221	9.8129	9.9132	9.8212	9.7223
	JPEG Compression	36.3684	36.3543	36.6448	36.5393	36.7581
Transdisciplinary	Speckle Noise	29.9224	28.8206	28.7234	29.0045	29.1245
	Median Filtering	32.8590	31.9853	32.4932	31.8528	32.2353
	Cropping	19.9831	18.8839	19.7219	18.9297	18.7943
	Rotation	9.1076	9.0637	9.1296	9.2783	9.1021
	JPEG Compression	35.9831	36.0624	36.1052	36.2034	36.0438

Table 4. NC values of Extracted Physician Informations on various disciplinaries (With Attacks)

Disciplinaries	**Attacks**	**Patient Image**		**Biomedical Image - 1**		**Biomedical Image - 2**		**Biomedical Image - 3**		**Lena Image**	
		Image 1 NC	**Image 2 NC**	**Image 1 NC**	**Image 2 NC**	**Image 1 NC**	**Image 2 NC**	**Image 1 NC**	**Image 2 NC**	**Image 1 NC**	**Image 2 NC**
Intradisciplinary care	Speckle Noise	0.9861		0.9978		0.9862		0.9902		0.9846	
	Median Filtering	0.9723		0.9923		0.9835		0.9846		0.9903	
	Cropping	0.4356		0.3371		0.4175		0.3631		0.4193	
	Rotation	0.3388		0.1352		0.2285		0.3087		0.1984	
	JPEG Compression	0.8693		0.8769		0.8630		0.8593		0.8641	
Cross-disciplinary referral	Speckle Noise	0.9970	1	0.9980	1	0.9963	1	0.9953	1	0.9957	1
	Median Filtering	0.9964	1	0.9950	1	0.9972	1	0.9953	1	0.9924	1
	Cropping	0.5301	0.9931	0.5130	0.9991	0.5421	0.9842	0.4958	0.9937	0.5288	0.9865
	Rotation	0.3654	0.9561	0.3664	0.9739	0.3598	0.9553	0.3686	0.9632	0.3598	0.9598
	JPEG Compression	1	0.9745	1	0.9834	1	0.9845	1	0.9732	1	0.9821
Multidisciplinary approach	Speckle Noise	0.9954	0.9992	0.9967	0.9981	0.9946	0.9963	0.9984	0.9961	0.9966	0.9971
	Median Filtering	0.9997	1	0.9992	1	0.9991	1	0.9983	1	0.9986	1
	Cropping	0.5891	0.5341	0.5833	0.5441	0.5882	0.5439	0.5901	0.5398	0.5893	0.5421
	Rotation	0.3240	0.3174	0.3240	0.3187	0.3189	0.3067	0.3238	0.3185	0.3295	0.3185
	JPEG Compression	1	1	1	1	1	1	1	1	1	1
Interdisciplinary	Speckle Noise	0.9991	0.9989	1	1	0.9934	0.9925	0.9972	0.9968	1	1
	Median Filtering	0.9982	1	0.9982	1	0.9981	1	0.9979	1	0.9974	1
	Cropping	0.5610	0.5245	0.5615	0.5245	0.5691	0.5254	0.5598	0.5178	0.5632	0.5235
	Rotation	0.3231	0.3883	0.3235	0.3883	0.3341	0.3985	0.3432	0.3998	0.3385	0.3856
	JPEG Compression	1	1	1	1	1	1	1	1	1	1
Transdisciplinary	Speckle Noise	0.9900	0.9990	0.9970	1	0.9992	0.9994	0.9999	1	0.9987	1
	Median Filtering	0.9841	1	0.9990	1	0.9974	1	0.9894	1	0.9863	1
	Cropping	0.5726	0.9867	0.5514	1	0.5843	0.9743	0.5784	0.9699	0.5832	0.9853
	Rotation	0.4684	0.9671	0.3184	0.9692	0.4958	0.9532	0.3945	0.9486	0.4328	0.9521
	JPEG Compression	0.9981	0.9825	1	0.9794	0.9979	0.9923	0.9957	0.9932	1	0.9982

Assume that an attacker can tamper or steal any information before the blockchain created from the communication network between the image encryption and the mining process at any time. An attacker can change even a single bit, in such a situation the hash value of the transaction also gets changed. The minors confirm each transaction with the hash value, in the mining process, and it can be identified by the miners. The proposed system, in this section, before the blockchain is created, provides an authoritative platform, for confirming the integrity of encrypted image combined with the hash value, which can effectively resolve the tampering attacks on the encrypted images.

We can check the similarity of the compared hash values of the images in the following algorithm,

Algorithm – Similarity measure of hash values of the images

Input: User Instructions
Output: Similarity checks whether same image or not

Initialization: Calling hashfile( ) function to obtain hashes of the images

```
Read the image – 1
Read the image – 2
f1_hash = hashfile (image – 1)
f2_hash = hashfile (image – 2)
if f1_hash == f2_hash then
    print ("Both files are same")
    print (f"Hash: {f1_hash}")
else
     print ("Files are different!")
    print (f"Hash of File 1: {f1_hash}")
    print (f"Hash of File 2: {f2_hash}")
end if
```

The uses of the proposed watermarking techniques and secure-hash algorithm are more secured. However, the image encryption and the secure hash algorithm with the addition of Blockchain technology are the most secured.

Every block is tied with the chain (hash value) of the previous block and the next block as shown in **Fig. 10**. No attacker can tamper or steal any information after the blockchain is created from the distributed ledger of the decentralized networks at any time.

When facing such an attacker, if some modification happens in any block, it will craft all the subsequent blocks as invalid, because it no longer has the ability to store the suitable hash value of the prior block. Therefore, it is not possible to modify any of the block in the distributed ledger on the Blockchain technology. The five color test images are used to verify the tamper detection ability of the proposed system. Assume that each encrypted image has been tampered with varying degrees, during the transmission (the number of pixels being changed is 1, 25, 50 and 100 respectively), the minor extracts the 256-bit hash code in the transaction and compares it with the 256-bit hash code of the received encrypted image to determine whether the encrypted image has been tampered with during the transmission. The test results confirm that the proposed system can successfully detect the illegal tampering encountered when the encrypted images are transmitted on untrusted channels.

If a user desires to access the information effectively, the user should meet the access control protocol and decrypt the information. In our scenario, we presume that the user never exposes his identity credential to others and so the key cannot be recovered by the attacker. We assume that *X* is a user, *Y* is a distributed ledger, *Z* is an attacker and *A* is an authentication node. *K* is defined as a public-private key, $E_{k_a^{-1}}(m)$ is defined as a watermark, $E_{k_a}(m)$ is an image, encrypted by *Ka. Z(X),* indicates the *Z* is disguised as *X* to send a message.

Attacks on security protocols.

Scenario – 1:

$$Z \to Y:\ E_{\left(K_z^{(-1)}\right)}(E_{K_y}(N_x, Z)); \tag{3}$$

If the attacker, without identity credential, tries to access the ledger, he cannot see the watermark collection and encrypted summary. It is of no benefit to the attacker.

Scenario – 2:

$$X \to Z(Y):\ E_{\left(K_x^{(-1)}\right)}(E_{K_y}(N_x, X)); \tag{4}$$

$$Z(X) \to Y:\ E_{\left(K_x^{(-1)}\right)}(E_{K_y}(N_x, X)); \tag{5}$$

$$Y \to Z(X):\ E_{\left(K_y^{(-1)}\right)}(E_{K_x}(M)); \tag{6}$$

We permit the attackers to interrupt the messages sent by the users and execute reply attacks. And we suppose that Z can successfully deceive Y, which leads Y to regard Z as X. Also, they can query the information on the Blockchain. But, as an outcome, they can only get a piece of encrypted information without using the decryption method.

$$X \to Z(A):\ X, Y, N_x; \tag{7}$$

$$Z(X) \to A:\ X, Z, N_x; \tag{8}$$

$$A \to Z(X):\ A, E_{\left(K_A^{(-1)}\right)}(A, X, N_x, Z, K_z); \tag{9}$$

$$Z(A) \to X:\ A, E_{\left(K_A^{(-1)}\right)}(A, X, N_x, Z, K_z); \tag{10}$$

It is presumed that the public key of *Y* is *Ky,* and the public key of the attacker *Z* is *Kz.* And the attacker needs the user *X* to believe that the public key of *Y* is *Kz,* hence, the binding attack is executed. Though the returned information contains the Z identity information, the X can find the target as inconsistent and avoid the binding attacks.

Scenario – 3:

$$X \to Z(Y):\ E_{\left(K_x^{(-1)}\right)}(E_{K_y}(N_x, X)); \tag{11}$$

$$Z \to Y:\ E_{\left(K_x^{(-1)}\right)}(E_{K_y}(N_x, X)); \tag{12}$$

$$Y \to Z(X):\ E_{\left(K_y^{(-1)}\right)}(E_{K_x}(M)); \tag{13}$$

$$Z(Y) \rightarrow X : E_{\left(K_z^{(-1)}\right)}(E_{K_x}(M')); \tag{14}$$

Even if the attacker wants to send false information to the patient, it can be judged as false information due to the absence of authentication information of the distributed ledger.

Analyzing the overall security of the proposed system, we can start with two parts.

The *X* is a user, *Y* is a distributed ledger, *K* is defined as the public-private key and *m* is defined as a watermark.

Authentication stage:

$$\frac{Y\,\mathrm{Re}ceived\ \ m_1\ \ SignedWith\ \ K_x^{-1}, x\ \ in\ \ m_1, Y\ \ IsTrustedOn\ \ K_x}{Y\,Can\,\mathrm{Pr}\,ove\,(X\ Says\,x)} \tag{15}$$

Reception stage:

$$\frac{X\,\mathrm{Re}ceived\ \ m_2\ \ SignedWith\ \ K_y^{-1}, X\ \ Can\,\mathrm{Pr}\,ove\ (K\,Authenticates\ \ Y)}{X\ Can\,\mathrm{Pr}\,ove\,(Y\,Says\,m_2)} \tag{16}$$

Table 5 indicates that the proposed system as resisting the tamper detection, identity disguise, reply attack and binding attack.

Table 5. List of system resistance attack

Scheme	Tamper Detection	Identity Disguise	Reply Attack	Binding Attack
Electronic Medical Records (EMR)	✓	✓	✓	✓

A successful Blockchain technology result wants to be sustainable. The presented scheme exploits a consortium Blockchain, constructed by the distributed ledger for backend functions of different disciplinaries, for instance the maintenance a ledger of embedded data with the storing of the authorized records.

The first and foremost, it approves the authorization of the EMR vision. Second, there is no gas expenses attached with consortium Blockchain as they employ predefined verified nodes. Through this method, every time, a stored EMR can be read or updated, as it is cost free. Third, it permits the stand to verify the communication at higher speeds.

5.3 Comparison with Related Works

This part evaluates the proposed system with the existing system.

Table 6. Comparison with existing works

Properties	**Thakur [10]**	**Fan [1]**	**Yue [14]**	**Wang [19]**	**Ananth [11]**	**Proposed system**
Blockchain-based	×	✓	✓	✓	✓	✓
Unforgeablity	×	✓	✓	✓	✓	✓
Access control	×	✓	✓	✓	✓	✓
Privacy preservation	✓	✓	✓	✓	✓	✓
Partial Disciplinaries	×	×	×	×	✓	✓
Complete Disciplinaries	×	×	×	×	×	✓

Table 6 evaluates the properties of the present model with the Blockchain supported methods Fan [1], Yue [14], Ananth [11] and Wang [19], and non-Blockchain based method Thakur [10]. The table contains the proposed method to achieve and cover all the properties in e-health system.

6. Conclusion

The challenges of sharing the EMR within the e-healthcare domain are important. Mere sharing of the information or records is not adequate. The important role of this method enables the medical records immutable, keeps them protected and shares them inside a decentralized network using the consortium Blockchain technology. The proposed build blocks are distinct and the higher ranking team healthcare models and their protocols have the necessity to apply this novel technology in the electronic healthcare system. In this work, we have discussed all the possibilities of working in the healthcare system such as, intradisciplinary, interdisciplinary, crossdisciplinary, multidisciplinary and transdisciplinary. Ultimately, we evaluated the performance of imperceptibility values on all the blocks of the distributed ledger.

References

[1] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, "MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain," *J. Med. Syst.*, vol. 42, no. 8, Art. no. 136, Jun. 2018. Article (CrossRef Link)

[2] Erin Elizabeth, "Electronic medical records fail again, as 12 million patient records at Quest Diagnostics get hacked," Jun. 07, 2019. [Online] Available: https://www.healthnutnews.com/major-data-breach-shows-dangers-of-online-records-storage/ (accessed Jul. 10, 2019).

[3] "Medicalchain-Whitepaper-EN.pdf" Accessed: Sep. 05, 2018. [Online]. Available: https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf.

[4] Mohananthini N and Yamuna G, "A Study of DWT-SVD based Multiple Watermarking Scheme for Medical Images," *Int. J. Network Security*, vol. 17, no. 5, pp. 558–568, Jan. 2015.

[5] Y. Ji, J. Zhang, J. Ma, C. Yang, and X. Yao, "BMPLS: Blockchain-Based Multi-level Privacy-Preserving Location Sharing Scheme for Telecare Medical Information Systems," *J. Med. Syst.*, vol. 42, no. 8, Jun. 2018, Art. no. 147. Article (CrossRef Link)

[6] "Bitcoin: A Peer-to-Peer Electronic Cash System" [Online] Available: https://bitcoin.org/en/bitcoin-paper (accessed Sep. 05, 2018).

[7] "Blockchain Tutorial - A Beginner's Guide to Blockchain Technology | Edureka," *Edureka Blog*, Sep. 06, 2017. [Online] Available: https://www.edureka.co/blog/blockchain-tutorial/ (accessed Sep. 05, 2018).

[8] Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park, and Kari Smolander, "Where Is Current Research on Blockchain Technology?—A Systematic Review," *PLoS ONE*, vol. 11, no. 10, 2016. Article (CrossRef Link)

[9] "Blockchain Technology in Health Care: Decoding the Hype," *NEJM Catalyst*, Feb. 09, 2017. [Online] Available: https://catalyst.nejm.org/decoding-blockchain-technology-health/ (accessed Sep. 05, 2018).

[10] S. Thakur, A. K. Singh, S. P. Ghrera, and M. Elhoseny, "Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications," *Multimed. Tools Appl.*, vol. 78, pp. 3457–3470, 2019. Article (CrossRef Link)

[11] C. Ananth, M. Karthikeyan, and N. Mohananthini, "A secured healthcare system using private blockchain technology," *J. Eng. Technol.*, vol. 6, no. 2, pp. 42-54, July 2018.

[12] A. Zhang and X. Lin, "Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain," *J. Med. Syst.*, vol. 42, no. 8, Jun. 2018, Art. no. 140. Article (CrossRef Link)

[13] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data" [Online] Available: https://www.healthit.gov/sites/default/files/5-56-onc_blockchainchallenge_mitwhitepaper.pdf (accessed Sep. 05, 2018).

[14] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control," *J. Med. Syst.*, vol. 40, no. 10, Aug. 2016, Art. no. 218. Article (CrossRef Link)

[15] Brodersen, "Blockchain: Securing a New Health Interoperability Experience," 2016. [Online] Available: https://www.healthit.gov/sites/default/files/2-49-accenture_onc_blockchain_challenge_response_august8_final.pdf (accessed Sep. 05, 2018).

[16] D. Bhowmik and T. Feng, "The multimedia blockchain: A distributed and tamper-proof media transaction framework," in *Proc. of 2017 22nd International Conference on Digital Signal Processing (DSP)*, pp. 1–5, Aug. 2017. Article (CrossRef Link)

[17] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and Trustable Electronic Medical Records Sharing using Blockchain," *AMIA. Annu. Symp. Proc.*, vol. 2017, pp. 650–659, Apr. 2018.

[18] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, and S. Liu, "Blockchain-Based Data Preservation System for Medical Data," *J. Med. Syst.*, vol. 42, no. 8, Art. no. 141, Jun. 2018. Article (CrossRef Link)

[19] H. Wang and Y. Song, "Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain," *J. Med. Syst.*, vol. 42, no. 8, Jul. 2018, Art. no. 152. Article (CrossRef Link)

[20] M. Natarajan and Y. Govindarajan, "Performance Comparison of single and multiple watermarking techniques," *Int. J. Comput. Netw. Inf. Secur.*, vol. 6, no. 7, pp. 28–34, Jun. 2014. Article (CrossRef Link)

[21] A. L. Selvakumar and C. S. Ganadhas, "The Evaluation Report of SHA-256 Crypt Analysis Hash Function," in *Proc. of 2009 International Conference on Communication Software and Networks*, pp. 588–592, Feb. 2009. Article (CrossRef Link)

[22] "What are NIST Encryption Standards?," *Hashed Out by The SSL Store^{TM}*, Dec. 11, 2017. [Online] Available: https://www.thesslstore.com/blog/what-are-nist-encryption-standards/ (accessed Apr. 18, 2021).

[23] Z. Feixiang, L. Mingzhe, W. Kun, and Z. Hong, "Color image encryption via Hénon-zigzag map and chaotic restricted Boltzmann machine over Blockchain," *Opt. Laser Technol.*, vol. 135, p. 106610, Mar. 2021, Article (CrossRef Link)

[24] Simply Explained - Savjee, *How does a blockchain work - Simply Explained*. [Online] Available: https://www.youtube.com/watch?v=SSo_EIwHSd4.

[25] Alexander Refsum Jensenius, "Disciplinarities: intra, cross, multi, inter, trans" [Online] Available: http://www.arj.no/2012/03/12/disciplinarities-2/ (accessed Sep. 05, 2018).

[26] D. of H. & H. Services, "Interdisciplinary approach to caring for older people in hospital fact sheet" [Online] Available: https://www2.health.vic.gov.au:443/hospitals-and-health-services/patient-care/older-people/resources/improving-access/ia-interdisciplinary (accessed Sep. 11, 2018).

[27] D. R. Nandiwada and C. Dang-Vu, "Transdisciplinary health care education: training team players," *J. Health Care Poor Underserved*, vol. 21, no. 1, pp. 26–34, Feb. 2010. Article (CrossRef Link)

Mohananthini Natarajan received her B.E. (Electrical and Electronics) Degree from Annai Mathammal Sheela Engineering College, Namakkal, Tamil Nadu, India in 2007. She received her M.E. (Applied Electronics) Degree from Anna University, Chennai, Tamilnadu, India in 2009. She received her Ph.D. Degree in Electrical Engineering from the Annamalai University in the year 2017. She has published many technical papers in national and international conferences and journals. Currently, she is working as Assistant Professor in the Department of Electrical and Electronics Engineering, Muthayammal Engineering College, Rasipuram, Tamil Nadu, India. Her current research areas are blockchain technology, digital image processing, information security and optimization.

Ananth Chidambaram received his Bachelor Degree from Bharathidasan University, Tamilnadu, India in 2001. He received his Master Degree from Bharathidasan University, Tamilnadu, India in 2004. He received his Ph.D. Degree in Computer Science from the Annamalai University in the year 2020. He has published many technical papers in national and international conferences and journals. He is working as Assistant Professor/Programmer in the Department of Computer and Information Science, Annamalai University from the year of 2004. His current research areas are blockchain technology, digital image processing, information security and optimization.

M. Y. Mohamed Parvees received his M.Sc. (Information Technology) in 2002 from Gandhigram Rural Institute - Deemed University and completed M.Phil. (Computer Science) in 2004 from Annamalai University, India. Presently, he is a faculty in Department of Computer and Information Science, Annamalai University. He completed Ph.D. degree in Bharathiar University. He has many international and national publications. His research interests include cryptography, multimedia security and medical information systems.