Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 159 (2019) 1787–1794

Procedia Computer Science

www.elsevier.com/locate/procedia

23rd International Conference on Knowledge-Based and Intelligent Information & Engineering Systems

A Blockchain Based Proposal for Protecting Healthcare Systems through Formal Methods

Luca Brunese[a], Francesco Mercaldo[b,d,*], Alfonso Reginelli[c], Antonella Santone[d,*]

[a]*Department of Medicine and Health Sciences "Vincenzo Tiberio", University of Molise, Campobasso, Italy*
[b]*Institute for Informatics and Telematics, National Research Council of Italy (CNR), Pisa, Italy*
[c]*Department of Precision Medicine, University of Campania "Luigi Vanvitelli", Napoli, Italy*
[d]*Department of Bioscience and Territory, University of Molise, Pesche (IS), Italy*

Abstract

Blockchain technology is one of the most important and disruptive technologies in the world. Multiple industries are adopting the blockchain technology to innovate the way they work. One of the industries that are looking to adopt the blockchain is the healthcare industry. In fact, the protection of the private information stored in hospital database is a critical issue. In this paper we propose a method aimed to protect information exchanged in hospital networks, with particular regard to magnetic resonance images. As required from blockchain technology, each host network must validate the transiting data network: we exploit formal equivalence checking to perform this validation, by modeling magnetic resonance images in terms of automata by exploiting radiomic features.

Keywords: Formal Methods, Model Checking, Radiomic

1. Introduction and Motivation

Medical and healthcare services are one of the prominent and crucial services which need to be delivered on the required time and through secure and safer means.

The current healthcare systems are mostly based on centralized servers where multiple entities within the network require permission to access the medical information. This can cause delay in offering the medical services and also potential leakage of the information. In such kind of healthcare systems, patients are mostly unaware regarding which entities are storing and using their medical data without their consent. One of the challenges with the current healthcare systems is the secure accessibility of the medical data by various entities within the hospital network[5,7,3,6,4]. Many healthcare enterprises have legacy or antiquated devices that are running outdated software or operating systems. Furthermore, healthcare networks are usually designed to minimize cost and maximize efficiency, creating flat networks that are easy targets for attackers[33]. In fact, many healthcare networks and systems have been created to

* Francesco Mercaldo, Antonella Santone
E-mail address: francesco.mercaldo@iit.cnr.it, antonella.santone@unimol.it

1877-0509
10.1016/j.procs.2019.09.350

provide the greatest amount of connectivity across the organization and facilitate the ability to communicate across departments, and facilities. This makes it easier for an attacker to perform reconnaissance across the enterprise and pivot easily throughout the network[24,15,10,39], often providing network access to critical data[33]. Healthcare organizations are focused on their primary mission (i.e., helping patients) while cyber security[27,28,31,11] risks are not considered[8,21]. Furthermore, many healthcare enterprises leverage external third-party vendors to manage and run their systems, which can introduce a significant amount of risk. Instead of attacking large and well-funded organizations with advanced cyber capabilities directly[45,13], hostile actors often try to compromise a smaller third-party vendor that has access to the target organization, effectively bypassing all of the larger entitys security controls and providing direct access into their networks[41,38,36]. Often healthcare enterprises operate as decentralized organizations. Comprised of semi-autonomous provider groups and service locations, these organizations are decentralized in a way that makes it much more difficult to prioritize cyber security investments, establish standards, and enforce compliance[14]. As a result, the entire enterprise may be exposed by its most vulnerable component, with potentially dire consequences.

Blockchain can be utilized in these cases to achieve the secure accessibility and integrity of the healthcare data. In fact, blockchain as a decentralized and distributed technology can play a key role in providing such healthcare services. The concept of blockchain is being well-known for its use in bitcoin and crypto currencies. It has got widespread attention from various stakeholders due to its immense business potential and utilization in various applications such as banking, healthcare and supply chain management[42,26,47]. Blockchain technology promises to provide immense opportunities in the healthcare sector such as secure data storing and sharing among various stakeholders, nationwide data interoperability and flexible and quick billing and payment modes. From these considerations, in this paper we propose an architecture blockchain based aimed to guarantee the trustworthiness of MRIs passing through the hospital network. The proposed method basically considers a set of radiomic features to build automata from MRIs that each host must verify to confirm its authenticity, as required by blockchain technology, using equivalence checking.

2. Related Work

Zain and Fauzi developed a technique in 2006 to detect the tampered regions on medical images[49]. Their method uses a block-based approach and divides the image into non-overlapping 8 8 pixel blocks. Each block is then divided into 4 4 pixel subblocks, and a 9-bit watermark is generated. Watermark information is then embedded into least significant bits (LSBs) of the first nine pixels of the 4 4 pixel subblocks. Three-level hierarchical approach is used during tamper detection to detect the modified regions. Their results indicate that watermarked image has approximately 54 dB peak signal to noise ratio (PSNR).

Wu et al. developed a method based on robust watermarking and combined with modulo addition[46]. The method generates the joint photographic experts group (JPEG) bit string of the selected region of interest (ROI) and then divides them into fixed length segments. Medical image is divided into blocks by the method, and hash bits are calculated for each of them excluding the block with ROI.

Chiang et al. used symmetric key cryptography and modified difference expansion technique to propose block-based tamper detection methods[14]. Their work presents two different methods according to recovery capability. The first method divides the image into 4 4 pixel blocks. Average intensity values of all blocks are calculated and concatenated and then are encrypted with two symmetric keys. Smooth blocks are determined by the method by using Haar wavelet transform.

Al-Qershi and Khoo[1] developed a reversible ROI-based watermarking scheme. At senders end, the medical image is segmented into ROI and RONI. Later, data of patient and hash value of ROI are both embedded into ROI using the technique developed by Gou et al. Compressed form of ROI, average values of blocks inside ROI, embedding map of ROI, embedding map of RONI, and LSBs of pixels in a secret area of RONI are embedded into RONI using the technique of Tian. Finally, information of ROI is embedded into LSBs of pixels in a secret area. At receivers end, ROI information is extracted from a secret area and is used to identify ROI and RONI regions. From the identified RONI region compressed form of ROI, average values of blocks inside ROI, embedding map of ROI, embedding map of RONI, and LSB of pixels in secret area are extracted. Using the extracted location map of ROI, patients data and hash value of ROI are extracted from ROI. Then, hash value of ROI is calculated and compared with extracted hash value. If there is a mismatch between the two hash values then the ROI is divided into 16 16 blocks. For each block, the average value is calculated and compared with the corresponding average value in the extracted average values.

Al-Qershi and Khoo[2] proposed a scheme based on two-dimensional difference expansion (2D-DE). At senders end, the medical image is divided into three regions: ROI pixels, RONI pixels, and border pixels. Later, the concatenation of patients data, hash value of ROI, bits of pixels inside ROI, and LSBs of border pixels are compressed using Huffman coding and then embedded into RONI using 2D-DE technique. This embedding generates a location map which will be concatenated with information of ROI and then embedded into LSBs of border pixels. At receivers end, from border pixels in the watermarked medical image both information of ROI and location map are extracted. Using this ROI information, ROI and RONI are identified. The extracted location map is used to extract patients data, hash value of ROI, bits of pixels inside ROI, and LSBs of border pixels from RONI. Each tampered block is replaced by the corresponding block of pixels in the extracted ROI. The LSBs of border pixels are replaced using the extracted LSBs from RONI. A major drawback of this scheme is that it is applicable to only medical images whose ROI size is very less (up to 12

Researchers in[23] developed a region-based tampering detection and restoring scheme for authentication and integrity verification of images based on image homogeneity analysis. This method divides the image into variable-sized blocks using quadtree decomposition and then chooses the average value of each block as the recovery feature. Some of the drawbacks identified with this method are as follows: (1) the original image cannot be recovered exactly when the region with recovery information is tampered and (2) computational complexity of the algorithm is high.

Liew et al. proposed two block-based approaches in their work[25]. The medical image is separated into two regions in their first method: ROI and RONI. The method divides the ROI into 8 8 pixel blocks and RONI into 6 6 pixel blocks. A mapping between the ROI and RONI blocks is constituted, and LSBs of the ROI blocks are embedded into corresponding RONI blocks to realize the recovery. The method uses approach in[49] to detect the tampered regions. The second method in their work compresses LSBs of the ROI blocks with run length encoding scheme before embedding. PSNR for watermarked images is not reported in their work.

In 2011, Memon et al. embeds the watermark information into LSBs of the ROI portion by using fragile watermarking[29]. RONI portion of the image is divided into N N pixel blocks, and then, embeddable blocks are determined. Location map of these blocks and a robust watermark are embedded into blocks on the RONI using integer wavelet transform (IWT). LSB replacement is applied on the LL3 subband of the blocks to hide the location map for recovery purposes. After the embedding procedure, ROI and RONI portions are combined to form the watermarked image. Robust watermark in RONI is used for tamper detection. Their results indicate that WPSNR value of the watermarked image is approximately 59 dB.

Tan et al. construct the first layer watermark from source information and location information in encrypted form[43]. The second layer watermark accommodates the cyclic redundancy check (CRC) values of all blocks in the medical image. CRC values are used for tamper detection.

Deng et al. used reversible watermarking technique in their work[18]. Their method also takes the advantage of quadtree decomposition. The image is divided into blocks by using quadtree decomposition. Linear interpolation of pixels is embedded into the image via invertible integer transformation. The second watermark is constructed using quadtree information and embedded with LSB technique. At the receivers side, the embedded watermark is extracted and the original image is reconstructed because the technique has used reversible embedding approach during watermarking. Linear interpolation of the pixels is again calculated and compared with extracted ones. Thus, tampering detection and localization will be achieved.

Eswaraiah et al. segments the medical image into three parts: ROI, RONI, and border pixels in 2014[19]. Secure hash algorithm is used to extract the hash of ROI. ROI and RONI parts of the medical image are divided into 4 4 and 8 8 pixel blocks, respectively. A mapping scheme is constructed between ROI and RONI, and it collects ROI block pixels and embeds them into corresponding RONI block with LSB replacement technique. A key encrypts hash value and information of ROI. Border pixels are used for hiding the encrypted bits. Information of ROI and hash value are used for tamper detection. Watermarked medical image is divided into ROI and RONI portions using the extracted ROI information. Hash value of ROI is calculated and compared with extracted one. If there exists a mismatch, block-based search is realized. Each ROI block is consulted using the corresponding RONI block to detect the absence of any modification. PSNR of the watermarked medical images with different modalities is in [5055] decibel range.

The method explained in[44] exploits two watermarking approaches based on slantlet transform (SLT) to embed data. Their method used IWT coefficients to generate recovery information. ROI is divided into non-overlapping 16 16 pixel blocks. IWT is used to calculate average pixel intensities and recovery information from ROI blocks. These

values are embedded into RONI using a robust irreversible technique. Reversible technique is used to embed EPR information into ROI. Two drawbacks of this method are as follows: It uses average information from 16 16 blocks to detect the tampered regions, and it must send some side information with watermarked medical image.

Eswaraih et al. uses IWT to watermark a medical image[20]. The medical image is segmented into ROI and RONI regions. IWT is used to embed hash of ROI, recovery information, and EPR into RONI. The disadvantages of the method are as follows: The coordinates of ROI and the size of watermark are sent to the other side as side information; authentication of ROI depends on hash function, and it can be applied to only medical images whose ROI size does not exceed 20% of the whole image.

3. The Method

In this section, once provided background concepts about the blockchain technology and the equivalence checking, we describe the proposed method.

A blockchain is basically a growing list of records, called blocks, which are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data[35] (in this case the MRIs expressed in terms of automa).

A blockchain is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that any involved record cannot be altered retroactively, without the alteration of all subsequent blocks[48]. This allows the participants to verify and audit transactions independently and relatively inexpensively[30,9]. A blockchain database is managed autonomously using a peer-to-peer network and a distributed timestamping server[22]. They are authenticated by mass collaboration powered by collective self-interests. Such a design facilitates robust workflow where participants' uncertainty regarding data security is marginal. The use of a blockchain removes the characteristic of infinite reproducibility from a digital asset[37]. It confirms that each unit of value was transferred only once, solving the long-standing problem of double spending. A blockchain has been described as a value-exchange protocol[34,17,50]. A blockchain can maintain title rights because, when properly set up to detail the exchange agreement, it provides a record that compels offer and acceptance[16].

Equivalence checking[32] is the process of determining whether two systems, expressed using a process algebra, are equivalent to each other according to some mathematically-defined notion of equivalence. It is typically used to verify if a system design conforms to its high-level service specification. We propose a novel application of equivalence checking in an emerging field such as medical imaging security. In particular, once modeled MRIs as labelled transition systems, formal equivalence checking[40,12,31] is exploited to find relationships between the states of the generated automata. The states of the automata are build from a set of radiomic feature gathered from the MRIs.

Labelled transition systems can model a piece of software at various abstraction levels. The lower the abstraction level, the more implementation details are present. At high abstraction levels, such details are deliberately left unspecified. Binary relations between states are useful to compare labelled transition systems, possibly at different abstraction levels.

More specifically, formal equivalence checking takes as inputs two systems and an equivalence relation, namely two systems s_1 and s_2 and an equivalence relation $\sim_x$, and asks the question "is the model of s_1 equivalent to the model of s_2 with respect to $\sim_x$?". The answer of this question depends on the particular equivalence relation $\sim_x$ under consideration.

Many equivalence relations have been defined on Calculus of Communicating Systems of Milner (CCS)[32] processes (i.e., one of the most well known process algebras): they are based on the notion of bisimulation between states of the related transition systems. In the following we consider the well-known *weak equivalence*, which describes how processes (i.e., systems) match each other's behavior. In order to define the weak equivalence, we first introduce the following transition relation between processes.

Definition 3.1. *Let p and q be two CCS processes. We write $p \overset{\epsilon}{\Longrightarrow} q$ if and only if there is a (possibly empty) sequence of τ actions that leads from p to q. If the sequence is empty, then $p = q$. For each action α, we write $p \overset{\alpha}{\Longrightarrow} q$ iff there are processes p' and q' such that*

$$p \overset{\epsilon}{\Longrightarrow} p' \overset{\alpha}{\longrightarrow} q' \overset{\epsilon}{\Longrightarrow} q$$

For each action α, we use $\widehat{\alpha}$ to stand for ϵ if $\alpha = \tau$, and for α otherwise.

Thus $p \overset{\alpha}{\Longrightarrow} q$ holds if p can reach q by performing an α action, possibly preceded and followed by sequences of τ actions. For example $a.\tau.nil \overset{a}{\Longrightarrow} nil$ and $a.\tau.nil \overset{a}{\Longrightarrow} \tau.nil$.

The idea underlying the following definition of weak equivalence is that an action of a process can be matched by a sequence of actions from the other that has the same "observational content" (i.e., ignoring τ actions) and leads to a state that is equivalent to that reached by the first process.

Definition 3.2. *(weak bisimulation, weak equivalence). Let p and q be two CCS processes.*

- *A weak bisimulation, $\mathcal{B}$, is a binary relation on $\mathcal{P} \times \mathcal{P}$ such that $p\mathcal{B}q$ implies:*

  (i) if $p \overset{\alpha}{\longrightarrow} p'$ then $q \overset{\widehat{\alpha}}{\Longrightarrow} q'$ for some q' such that $p'\mathcal{B}q'$; and

  (ii) if $q \overset{\alpha}{\longrightarrow} q'$ then $p \overset{\widehat{\alpha}}{\Longrightarrow} p'$ for some p' such that $p'\mathcal{B}q'$

- *p and q are weak equivalent ($p \approx q$) iff there exists a weak bisimulation $\mathcal{B}$ containing the pair (p, q).*

The symbol τ, used in process algebra, states that hidden actions take place. Sometimes the τ actions must not be taken into account when reasoning on the equivalence of two processes.

Figure 1 shows the proposed method.

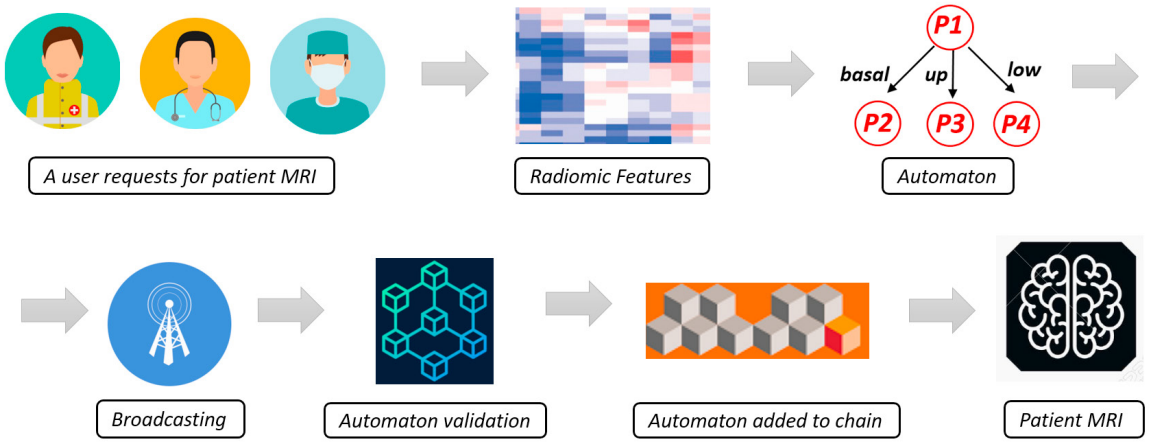

Fig. 1: Method.

The users of hospital networks are basically doctor, nursery and technicians which can request for patient magnetic resonance images (MRI). The proposed method is aimed to perform a distributed verification of the information transiting over the hospital network. In fact, when a new set of MRIs are generated, for instance by a MRI scanner, the radiologist from its host is reading the images. Once the MRIs are received from the radiologist host, a check is performed with the aim to guarantee the MRIs integrity. In fact, the MRIs stored in the sender side (in this case the medical equipment which generated the MRIs) and the ones in the receiver one are represented in terms of automata by means of radiomic features and then by exploiting formal equivalence the automata similarity is verified. We consider as radiomic features the so-called *shape features* i.e., features independent from the gray level intensity distribution in the cancer region of interest (i.e., ROI). Shape features are derived from the approximated shape defined by the triangle mesh. This mesh is generated using an adapted version marching cubes algorithm where a 2×2 square is moved through the mask space. For each position, the corners of the square are then marked "segmented" (1) or "not segmented" (0). Vertices (points) are first defined as points halfway on an edge between a voxel included in the ROI (i.e., Region Of Interest) and one outside the ROI[?]. By connecting these vertices a mesh of connected triangles is obtained, with each triangle defined by 3 adjacent vertices, which shares each side with exactly one other triangle. Once the radiologist has seen the MRIs its host represents a candidate for the verification and the automaton generated

from this host is added to the chain of verified automata. When a new host will ask for the same patient MRIs, the equivalence checker will perform the comparison between the medical equipment host, the radiologist one and the MRIs received from the new host. In case the equivalence checker outputs *true* for the related automata generated by the received MRIs, this host will represent a new node to perform the equivalence checking. In this way, for each host requiring the MRI data, the successfully equivalence checking verification will add a new automaton to the chain. The proposed method is distributed: in fact every equivalence checking computation is performed on the related host node that initially required the MRIs.

4. Conclusion and Future Work

In this paper a blockchain based architecture to protect sensitive information on hospital networks is presented. The proposed method exploits formal verification techniques: basically when an host is requiring the access to magnetic resonance images, an integrity check is performed by each host that required the same resource: in this way the proposed method ensures that the received information is not altered by an attacker. As future work we plan to evaluate the proposed blockchain based architecture in the context of a real hospital network.

References

1. Al-Qershi, O.M., Khoo, B.E., 2010. Roi-based tamper detection and recovery for medical images using reversible watermarking technique, in: 2010 IEEE International Conference on Information Theory and Information Security, IEEE. pp. 151–155.
2. Al-Qershi, O.M., Khoo, B.E., 2011. Authentication and data hiding using a hybrid roi-based watermarking scheme for dicom images. Journal of digital imaging 24, 114–125.
3. Amato, F., De Pietro, G., Esposito, M., Mazzocca, N., 2015. An integrated framework for securing semi-structured health records. Knowledge-Based Systems 79, 99–117. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84930540047&doi=10.1016%2fj.knosys.2015.02.004&partnerID=40&md5=1ca825bfefdeffa637cbebe1b8cb9eba, doi:10.1016/j.knosys.2015.02.004. cited By 9.
4. Amato, F., Mazzocca, N., Moscato, F., 2018a. Model driven design and evaluation of security level in orchestrated cloud services. Journal of Network and Computer Applications 106, 78–89. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85040120883&doi=10.1016%2fj.jnca.2017.12.006&partnerID=40&md5=b526ef9f3ec8bcf289698152399b76ab, doi:10.1016/j.jnca.2017.12.006. cited By 6.
5. Amato, F., Moscato, F., 2017. Model transformations of mapreduce design patterns for automatic development and verification. Journal of Parallel and Distributed Computing 110, 52–59. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85008485922&doi=10.1016%2fj.jpdc.2016.12.017&partnerID=40&md5=99a62a9496c65c537f35fe8be5672b0b, doi:10.1016/j.jpdc.2016.12.017. cited By 6.
6. Amato, F., Moscato, F., Moscato, V., Colace, F., 2018b. Improving security in cloud by formal modeling of iaas resources. Future Generation Computer Systems 87, 754–764. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85028364880&doi=10.1016%2fj.future.2017.08.016&partnerID=40&md5=08dcc27665a91c740861cedbe4020789, doi:10.1016/j.future.2017.08.016. cited By 7.
7. Amato, F., Moscato, F., Xhafa, F., 2019. Generation of game contents by social media analysis and mas planning. Computers in Human Behavior URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85062386729&doi=10.1016%2fj.chb.2019.02.030&partnerID=40&md5=884ab3d09c9483fee8d6efa2fcff7734, doi:10.1016/j.chb.2019.02.030. cited By 0.
8. Arumugham, S., Rajagopalan, S., Rayappan, J.B.B., Amirtharajan, R., 2019. Tamper-resistant secure medical image carrier: An iwt–svd–chaos–fpga combination. Arabian Journal for Science and Engineering , 1–20.
9. Brandenburger, M., Cachin, C., Kapitza, R., Sorniotti, A., 2018. Blockchain and trusted computing: Problems, pitfalls, and a solution for hyperledger fabric. arXiv preprint arXiv:1805.08541 .
10. Canfora, G., Martinelli, F., Mercaldo, F., Nardone, V., Santone, A., Visaggio, C.A., 2018. Leila: formal tool for identifying mobile malicious behaviour. IEEE Transactions on Software Engineering .
11. Canfora, G., Mercaldo, F., Moriano, G., Visaggio, C.A., 2015. Composition-malware: building android malware at run time, in: 2015 10th International Conference on Availability, Reliability and Security, IEEE. pp. 318–326.
12. Ceccarelli, M., Cerulo, L., Santone, A., 2014. De novo reconstruction of gene regulatory networks from time series data, an approach based on formal methods. Methods 69, 298–305. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84927158722&doi=10.1016%2fj.ymeth.2014.06.005&partnerID=40&md5=d48bdbbe7485ece91340da58bb0bd32a, doi:10.1016/j.ymeth.2014.06.005. cited By 12.
13. Chen, Y., Ding, S., Xu, Z., Zheng, H., Yang, S., 2019. Blockchain-based medical records secure storage and medical service framework. Journal of medical systems 43, 5.
14. Chiang, K.H., Chang-Chien, K.C., Chang, R.F., Yen, H.Y., 2008. Tamper detection and restoring system for medical images using wavelet-based reversible data embedding. Journal of Digital Imaging 21, 77–90.
15. Cimitile, A., Mercaldo, F., Nardone, V., Santone, A., Visaggio, C.A., 2018. Talos: no more ransomware victims with formal methods. International Journal of Information Security 17, 719–738.

16. Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V., et al., 2016. Blockchain technology: Beyond bitcoin. Applied Innovation 2, 71.
17. Dai, J., Vasarhelyi, M.A., 2017. Toward blockchain-based accounting and assurance. Journal of Information Systems 31, 5–21.
18. Deng, X., Chen, Z., Zeng, F., Zhang, Y., Mao, Y., 2013. Authentication and recovery of medical diagnostic image using dual reversible digital watermarking. Journal of nanoscience and nanotechnology 13, 2099–2107.
19. Eswaraiah, R., Reddy, E.S., 2014. Medical image watermarking technique for accurate tamper detection in roi and exact recovery of roi. International journal of telemedicine and applications 2014, 13.
20. Eswaraiah, R., Reddy, E.S., 2015. Robust medical image watermarking technique for accurate detection of tampers inside region of interest and recovering original region of interest. IET image Processing 9, 615–625.
21. Goléa, N.E.H., Melkemi, K.E., 2019. Roi-based fragile watermarking for medical image tamper detection. International Journal of High Performance Computing and Networking 13, 199–210.
22. Huh, S., Cho, S., Kim, S., 2017. Managing iot devices using blockchain platform, in: 2017 19th international conference on advanced communication technology (ICACT), IEEE. pp. 464–467.
23. Kim, K.S., Lee, M.J., Lee, J.W., Oh, T.W., Lee, H.Y., 2011. Region-based tampering detection and recovery using homogeneity analysis in quality-sensitive imaging. Computer Vision and Image Understanding 115, 1308–1323.
24. Lee, C.H., Lee, Y.K., 1999. An adaptive digital image watermarking technique for copyright protection. IEEE Transactions on Consumer Electronics 45, 1005–1015.
25. Liew, S.C., Zain, J.M., 2010. Reversible medical image watermarking for tamper detection and recovery, in: 2010 3rd International Conference on Computer Science and Information Technology, IEEE. pp. 417–420.
26. Liu, K.H., Chang, S.F., Huang, W.H., Lu, I.C., 2019. The framework of the integration of carbon footprint and blockchain: Using blockchain as a carbon emission management tool, in: Technologies and Eco-innovation towards Sustainability I. Springer, pp. 15–22.
27. Martinelli, F., Mercaldo, F., Nardone, V., Santone, A., 2017. Car hacking identification through fuzzy logic algorithms. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85030158556&doi=10.1109%2fFUZZ-IEEE.2017.8015464&partnerID=40&md5=a222bf64656a78632012fd8c9ebbe783, doi:10.1109/FUZZ-IEEE.2017.8015464. cited By 13.
28. Martinelli, F., Mercaldo, F., Orlando, A., Nardone, V., Santone, A., Sangaiah, A., 2018. Human behavior characterization for driving style recognition in vehicle system. Computers and Electrical Engineering URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85039902193&doi=10.1016%2fj.compeleceng.2017.12.050&partnerID=40&md5=6d879e263209893fd0f5ace3abac1539, doi:10.1016/j.compeleceng.2017.12.050. cited By 10; Article in Press.
29. Memon, N.A., Chaudhry, A., Ahmad, M., Keerio, Z.A., 2011. Hybrid watermarking of medical images for roi authentication and recovery. International Journal of Computer Mathematics 88, 2057–2071.
30. Meng, W., Tischhauser, E.W., Wang, Q., Wang, Y., Han, J., 2018. When intrusion detection meets blockchain technology: a review. Ieee Access 6, 10179–10188.
31. Mercaldo, F., Nardone, V., Santone, A., Visaggio, C., 2016. Hey malware, i can find you!, pp. 261–262. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84983803047&doi=10.1109%2fWETICE.2016.67&partnerID=40&md5=21b88831ed64d663142b799da7ac03b9, doi:10.1109/WETICE.2016.67. cited By 10.
32. Milner, R., 1989. Communication and concurrency. PHI Series in computer science, Prentice Hall.
33. Mirsky, Y., Mahler, T., Shelef, I., Elovici, Y., 2019. Ct-gan: Malicious tampering of 3d medical imagery using deep learning. arXiv preprint arXiv:1901.03597 .
34. Natoli, C., Gramoli, V., 2016. The blockchain anomaly, in: 2016 IEEE 15th International Symposium on Network Computing and Applications (NCA), IEEE. pp. 310–317.
35. Nofer, M., Gomber, P., Hinz, O., Schiereck, D., 2017. Blockchain. Business & Information Systems Engineering 59, 183–187.
36. Parah, S.A., Ahmad, I., Loan, N.A., Muhammad, K., Sheikh, J.A., Bhat, G., 2019. Realization of an adaptive data hiding system for electronic patient record, embedding in medical images, in: Security in smart cities: models, applications, and challenges. Springer, pp. 47–70.
37. Pilkington, M., 2016. 11 blockchain technology: principles and applications. Research handbook on digital transformations 225.
38. Rajagopalan, S., Janakiraman, S., Rengarajan, A., 2019. Medical image encryption: Microcontroller and fpga perspective, in: Medical Data Security for Bioengineers. IGI Global, pp. 278–304.
39. Rayachoti, E., Edara, S.R., 2014. Block based medical image watermarking technique for tamper detection and recovery. arXiv preprint arXiv:1412.6143 .
40. Santone, A., Vaglini, G., 2012. Abstract reduction in directed model checking ccs processes. Acta Informatica 49, 313–341. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84864389117&doi=10.1007%2fs00236-012-0161-3&partnerID=40&md5=4f4cceffa15f2e8012617372a7621561, doi:10.1007/s00236-012-0161-3. cited By 15.
41. Soualmi, A., Alti, A., Laouamer, L., Benyoucef, M., 2019. A blind fragile based medical image authentication using schur decomposition, in: International Conference on Advanced Machine Learning Technologies and Applications, Springer. pp. 623–632.
42. Swan, M., 2015. Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc.".
43. Tan, C.K., Ng, J.C., Xu, X.i., Poh, C.L., Guan, Y.L., Sheah, K., 2011. Security protection of dicom medical images using dual-layer reversible watermarking with tamper detection capability. Journal of Digital Imaging 24, 528–540.
44. Thabit, R., Khoo, B.E., 2017. Medical image authentication using slt and iwt schemes. Multimedia Tools and Applications 76, 309–332.
45. Thakur, S., Singh, A.K., Ghrera, S.P., Elhoseny, M., 2019. Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications. Multimedia tools and Applications 78, 3457–3470.
46. Wu, J.H., Chang, R.F., Chen, C.J., Wang, C.L., Kuo, T.H., Moon, W.K., Chen, D.R., 2008. Tamper detection and recovery for medical images using near-lossless information hiding technique. Journal of Digital Imaging 21, 59–76.
47. Xu, X., Weber, I., Staples, M., 2019. Blockchain patterns, in: Architecture for Blockchain Applications. Springer, pp. 113–148.
48. Yli-Huumo, J., Ko, D., Choi, S., Park, S., Smolander, K., 2016. Where is current research on blockchain technology?a systematic review. PloS one 11, e0163477.
49. Zain, J.M., Fauzi, A.R., 2006. Medical image watermarking with tamper detection and recovery, in: 2006 International Conference of the IEEE Engineering in Medicine and Biology Society, IEEE. pp. 3270–3273.

50. Zhang, Y., Wen, J., 2017. The iot electric business model: Using blockchain technology for the internet of things. Peer-to-Peer Networking and Applications 10, 983–994.