applied sciences

MDPI

Concept Paper

False Image Injection Prevention Using *i*Chain

Mohiuddin Ahmed

Academic Centre of Cyber Security Excellence, School of Science, Edith Cowan University, WA 6027, Australia; mohiuddin.ahmed@ecu.edu.au; Tel.: +618-6304-5121

Received: 31 August 2019; Accepted: 10 October 2019; Published: 15 October 2019

Abstract: The advances in information and communication technology are consistently beneficial for the healthcare sector. A trend in the healthcare sector is the progressive shift in how data are acquired and the storage of such data in different facilities, such as in the cloud, due to the efficiency and effectiveness offered. Digital images related to healthcare are sensitive in nature and require maximum security and privacy. A malicious entity can tamper with such stored digital images to mislead healthcare personnel and the consequences of wrong diagnosis are harmful for both parties. A new type of cyber attack, a false image injection attack (FIIA) is introduced in this paper. Existing image tampering detection measures are unable to guarantee tamper-proof medical data in real time. Inspired by the effectiveness of emerging blockchain technology, a security framework, image chain (*i*Chain) is proposed in this paper to ensure the security and privacy of the sensitive healthcare images. The practical challenges associated with the proposed framework and further research that is required are also highlighted.

Keywords: blockchain; cyber attacks; false data injection; healthcare; image; tampering

1. Introduction

The advancement of information technology has both positive and negative impacts on our daily lives, wellbeing, economy, privacy, and more [1–3]. Therefore, mitigating the negative impacts have become an important task. In today's age, cyber security has become an integral part of fighting criminals in cyber space. The proliferation of the internet has given rise to threats such as zero-day vulnerabilities which have detrimental consequences [3–5]. Despite the tremendous amount of research efforts continuing in the area of cyber security, cyber criminals are not at rest. Healthcare is a lucrative target for cyber criminals as it contains sensitive information that can be used to gain monetary benefits quickly.

False data injection is an emerging type of cyber attack in the area of smart grid, power systems, control systems, and supervisory control and data acquisition (SCADA) networks etc. [5]. In simple terms, it is a type of cyber attack where the attacker manipulates the data in compromised networked devices. For example, the compromised sensors in smart grid will reflect manipulated events. The smart grid networks are used for monitoring and controlling critical infrastructures, including the energy system, transportation system, gas and water systems, and so on [6]. Hence, the impact of false data injection attacks in such smart systems has attracted a great deal of attention in recent years [5]. Unlike SCADA systems, the healthcare domain has become one of the prime targets for cyber attackers due to the unprecedented impact and potential for profitable crime [5]. The impact of false data injection attacks have been investigated recently in [5] and are still at its early stage in terms of research contributions from the practitioners. Due to the incorporation of wireless sensor based medical devices such as pacemakers, and cardiac re-synchronization therapy devices, the hackers are more interested in such attacks as they can demand ransoms from helpless patients or their families. Successful attacks of such a genre will mislead physicians and healthcare personnel. In this scenario, we are

interested in focusing on a specific type of healthcare data, specifically medical images. According to [7], it is estimated that by 2020, the healthcare domain will have 1021 zettabytes of information stored (1 zettabyte = 1 trillion gigabytes). According to the Stanford Medicine Health Trend Report 2018 [8], the healthcare domain faces a high number of breaches each year and a majority (52%) are caused by cyber attacks, whereas system and human errors cause the remaining breaches (48%).

As stated earlier, the advances in wireless sensor technology, miniaturisation and computing power are accelerating innovation in the healthcare sector. These advances facilitate the development of networked medical devices capable of generating, collecting, analyzing and transmitting data. Therefore, a healthcare focused version of the Internet of Things (IoT) is termed the Internet of Medical Things (IoMT). In simple words, the IoMT is a connected infrastructure of medical devices, software applications, health systems, and services. The connectivity between sensors and medical devices is improving patient care by smooth clinical operations and workflow management. However, due to the availability of cyber attack tools, people with malicious intent are continuously creating chaos (False Data/Image Injection in the context of this paper) in such connected environments. Figure 1 below reflects a basic IoMT architecture and how hackers can exploit such an environment. The sensors or the smart medical devices use short-range networking protocols such as bluetooth, or ZigBee etc. to transmit the data to a gateway, and the gateway is connected to the data repository in the cloud from where other parties can access.

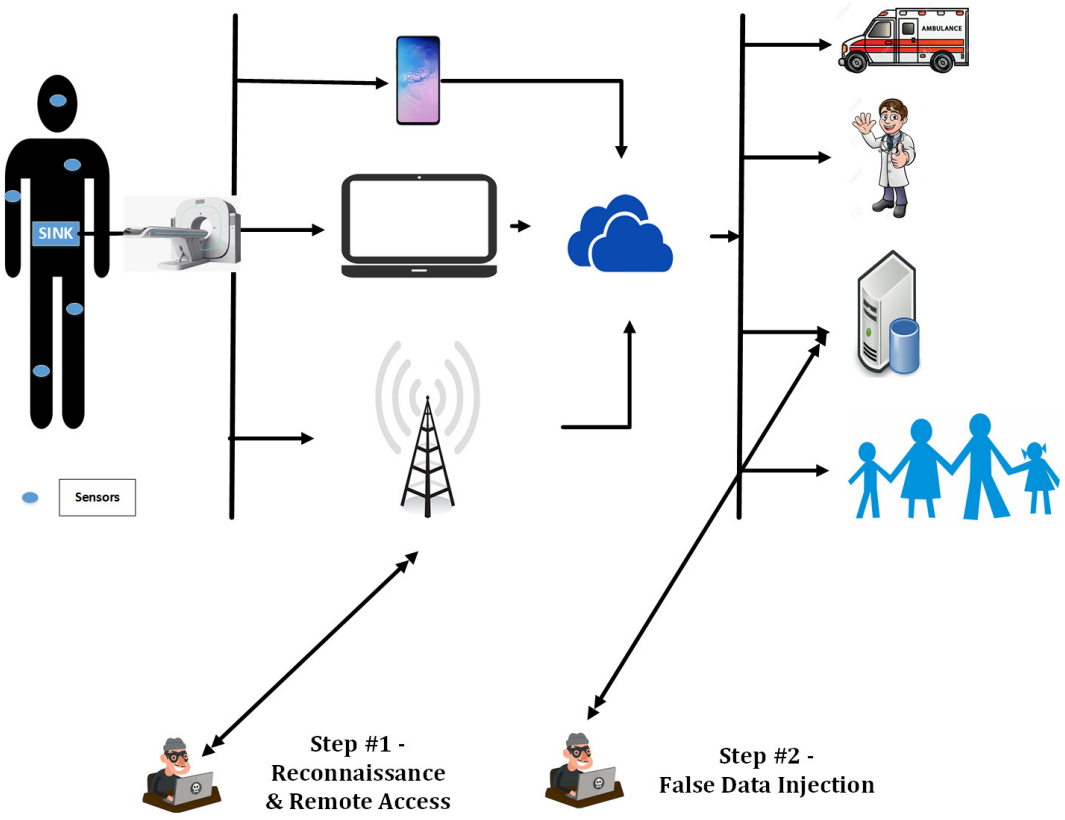


Figure 1. Conceptual view of False Data/Image Injection in the Internet of Medical Things (IoMT).

In this paper, a variant of false data injection attack based on the medical imaging is proposed. The attack is termed as a false image injection attack (FIIA), where the attacker gains access to the medical imaging repositories and injects a false image to manipulate the original image, the decision or diagnosis based on these manipulated images will put the patient in jeopardy and in the worst case, might cause death. This is highly probable as attackers have already tried to assassinate political figures by compromising implanted medical devices [9,10]. Therefore, in this paper, a countermeasure is proposed for such attacks, *i*Chain. The proposed countermeasure framework exploits the effectiveness

of blockchain technology [11] to ensure the security and privacy of the medical images. The recent literature [12] reflects that existing image tampering detection techniques fail to provide real time results. These techniques need to be applied on the suspicious images, which results in high false positive rates and is not effective in real time diagnosis. The key contributions of this paper are listed below:

- Introduction of false image injection attack (**FIIA**);
- Critical analysis of image tampering detection techniques; and
- Blockchain-based security framework, ***i*Chain** to prevent **FIIA**.

In summary, the key objective of this paper is to raise awareness of considering preventive measures for **FIIA** in healthcare in the hope of saving lives. The rest of the paper is organized as follows. Section 2 describes the false image injection attacks followed by critical analysis of existing security measures on image tampering in Section 3. The backbone of the proposed framework to fight false image injection attacks, blockchain is discussed in Section 4 and the proposed security framework, ***i*Chain** is showcased in Section 5. Evaluation of the existing techniques for image tampering detection and blockchain based frameworks are presented in Section 6. The paper is concluded with future research directions in Section 7.

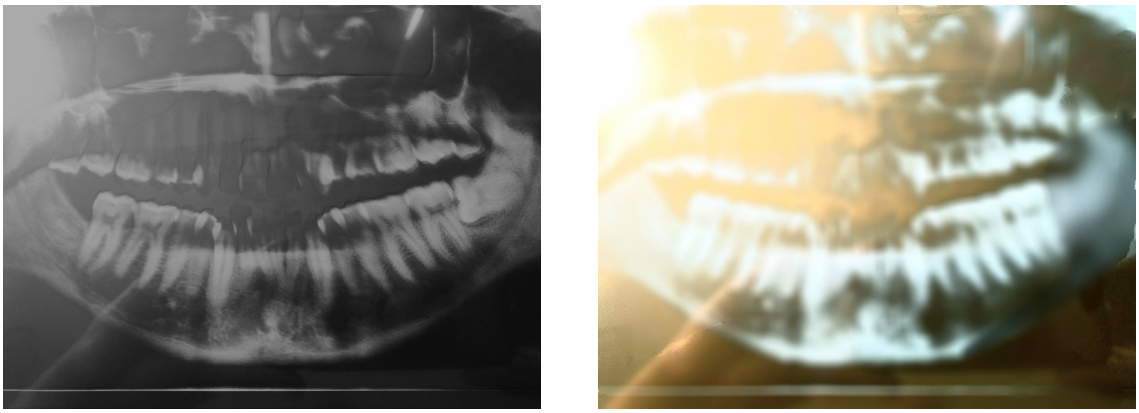
2. False Image Injection Attacks

The idea behind false image injection attacks originates from the original false data injection attack [7]. In [7] the mathematical representation is provided and this holds true for the false image injection attacks.

- Original image vector, $I\{i_1, i_2, \ldots\ldots, i_n\}$
- Observed image vector, $I_a\{i_{a_1}, i_{a_2}, \ldots, i_{a_n}\}$
- False image vector, $a\{a_1, a_2, \ldots, a_n\}$
- $I_a = I + a$; when $a \neq 0$.

When there is a false image injection attack, $a \neq 0$. Though, this definition is originally devised for smart grid, it can be seen from the healthcare perspective as long as the healthcare domain is now heavily dependent on sensor networks [7]. Figure 2 reflects the false image injection attacks in a dental scan. Figure 2a shows the original image and Figure 2b reflects the false image injection attack on the original image. The false image hides one of the wisdom teeth which is in horizontal position. Consider a patient going to their dentist with dental pain but the false image will mislead the dentist and result in a subsequent wrong treatment for the patient. The example of this dental scan is quite simple, the consequences will be much more dangerous if the images are related to more sensitive organs, such as CT scans of the brain, lungs etc. We highlight a few scenarios where **FIIA** leads to dangerous consequences:

- **Misleading patient diagnosis**: In an unexpected case when the medical equipment which is part of a sensor network is compromised, the injected false image will mislead the physicians [7]. For example, refer to Figure 2.
- **Counterfeit insurance claim**: Injecting false imaging records may cause the insurance provider to pay unnecessarily as the patient data is not legitimate [7]. For example, if a cyber attacker, injects a false image for a surgery which is supposed to be covered by insurance, then the beneficiary will get paid without having any surgery.
- **Emergency situations**: While a complicated tele-surgery is going on and the physicians are dependent on the real time images, even a slight variation of these images (as a consequence of **FIIA**) can lead to loss of life [7].



a. Original dental scan **b**. False image injected dental scan

Figure 2. An example of a false image injection attack.

3. Critical Analysis of Image Tampering Detection Techniques

A recent survey covers all of the state-of-the-art image tampering detection techniques [12]. Figure 3 showcases the current practices of image tampering. Due to the free availability of a plethora of photo editing applications and software, image tampering has become easy, but dangerous when in the wrong hands. Cyber criminals have been enjoying the full privileges of such image tampering techniques to commit false image injection attacks after compromising imaging repositories. The survey states that there is a very high probability of not being able to differentiate between tampered images and original images leading to confusion.

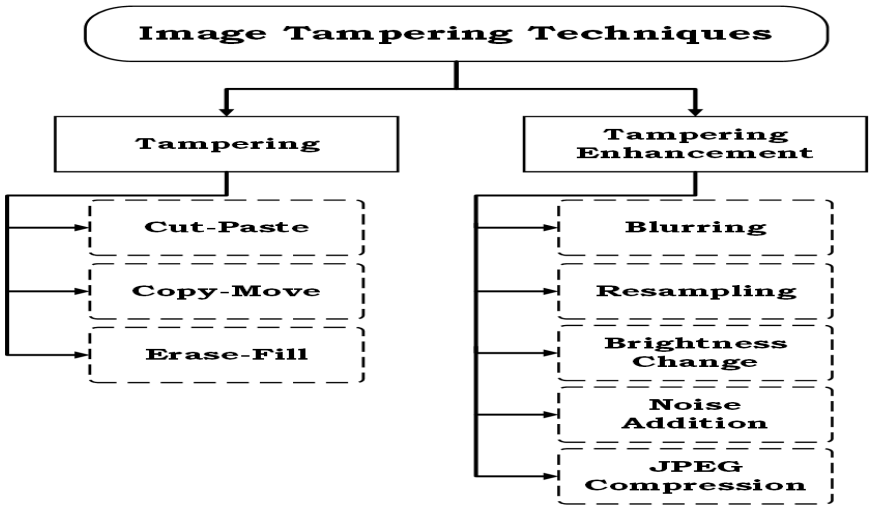


Figure 3. A taxonomy of image tampering techniques, adapted from [12].

Figure 4 reflects a generic framework for detecting tampered images. In the context of false image injection attacks, it is imperative to identify the tampered images in real time. It is practically infeasible for healthcare personnel or physicians to apply tampering identification techniques before analyzing medical images every time. Therefore, the existing image tampering detection techniques are inadequate to secure the privacy of sensitive medical images.

Deep learning is considered the most popular algorithm in recent times in the field of artificial intelligence [13]. The mechanism of deep learning can efficiently capture the complex architecture of data. The algorithm has been welcomed and adopted by technology giants such as Google, Facebook etc. Unlike neural networks, deep learning has the capability to provide stability, scalability and the generalization to deal with big data [14]. It is becoming a popular algorithm for showing the highest predictive accuracy in a wide range of applications. In [15], a convolutional neural network (CNN)

is utilized to detect image forgery. However, the method requires labeled data to extract features for forgery identification. Considering the nature of false image injection attacks, deep learning based solutions are not suitable when prevention of the healthcare images are prioritized more than detection after the suspected compromise. The issue remains the same for all other supervised learning based image forgery or tampering identification. Although, the deep learning approaches can be customized for unsupervised learning and subsequent forgery detection, the performance might not be same as supervised learning. Next, the backbone of the proposed approach, blockchain technology, is discussed.

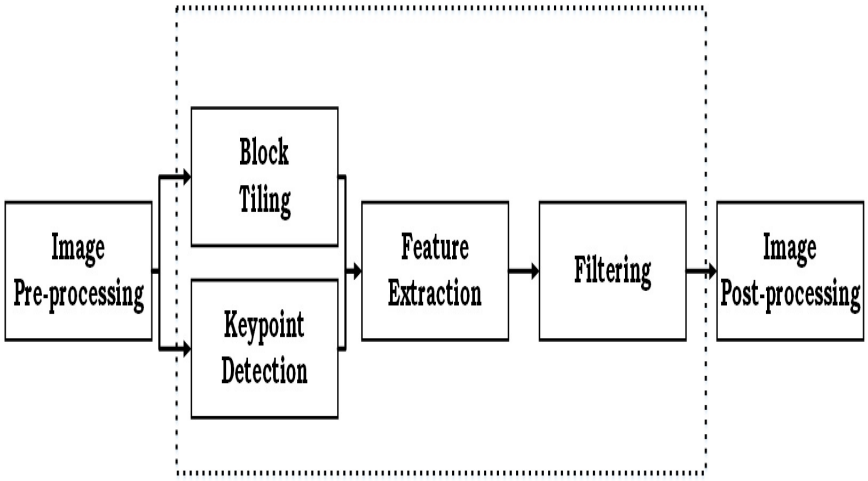


Figure 4. A generic framework to identify tampered images, adapted from [12].

4. Blockchain: Panacea to Cyber Crime

A blockchain is the collection of a series of blocks, where each block stores data involved in a transaction. When the transaction occurs, it is stored in a block and added to the chain [16]. These blocks form a distributed database to store valuable information and thus form a blockchain. Blockchain contains shared databases, i.e., each of the participants in the blockchain have access to the same database. These databases are cryptographically secure to protect the integrity of the data and to add any new block in the chain, each of the participants needs to approve and therefore, the data in the blockchain would be immutable. Any malicious entity will not be able to tamper any data from the blockchain. In terms of data security, the cyber attacks where data manipulation is carried out such as false data injection [5] and many others [1–3] do not have any significant effect if the data are stored using blockchain. Therefore, this technology is being embraced at a rapid pace across a number of application domains and to secure sensitive medical images, it is an appropriate technology. Next, the important components of blockchain, which make it promising, are briefly discussed.

- **Hash**: A hash algorithm changes arbitrary data into a definite length hash. Any change in the original data results in a different hash value. Therefore, it makes falsification difficult in blockchain. Every new block creation utilizes the calculation of a hash value for creating a new block or transactions as well. Blockchain adopts this security mechanism to generate random hash values for data storage and authentication [17].
- **Block**: A block is the data storage facilitator of a transaction. A block is thus a permanent store of records, which, once written, cannot be altered or removed. If we make a comparison with a common record keeping style it is a page of a ledger, we only go to the next page of a ledger when it finishes. Similarly, a block indicates a current transaction and when the next block is created that one becomes the latest one. Each time a block is 'completed', it gives way to the next block in the blockchain. There is no maximum number of blocks, it will continue to grow as long as people use it for transactions. It has three parts: header, transaction counter, and block content [17].

- **Digital signature**: The digital signature was first used by D Johnson [18]. A digital signature is a procedure to prove the authenticity of the blockchain transmission. It mainly contains a public and private key to provide a double layer protection of transaction information. Signing phase and verification phase are two steps needed for this verification. The private key is reserved for personal transactions, and the public key is shared globally. In the signing part, one encrypts data with the private key and sends the original data with encryption. In the verification part, the receiver can easily check the validity of the received data with the sender's public key. When the sender sends the data and hash value, on the other hand,the receiver can verify that the information was actually generated from the hash and the private key of the sender [17].

Next, we discuss the proposed approach, ***i*Chain** to prevent false image injection attacks.

5. Image Chain (*i*Chain) to Prevent False Image Injection Attacks

In recent times, blockchain has been investigated by a number of researchers [19–22]. The common finding is that blockchain is helpful for healthcare domain security and privacy along with other applications. However, specific attacks such as false image injection attacks have never been addressed. Therefore, inspired by the effectiveness of this emerging technology, in this paper, a blockchain based remedy for false image injection attacks is proposed. Figure 5 reflects the conceptual framework of the proposed ***i*Chain** approach to prevent false image injection attacks. The fundamental idea behind this approach is to use the blockchain technology as discussed in the previous section. Since, this paper is trying to establish the concept of false image injection attack prevention using blockchain technology, the classification of the blockchain is treated as part of future works. Blockchains are classified into three major categories [23] as follows: public, private and hybrid. All parties can read, and write in public blockchains. In private blockchains, specific individuals are allowed to participate in the verification process. Hybrid blockchains can be customized based on the combination of private and public chains.

Sensitive medical images should be stored in a blockchain network to avoid any consequences of false image injection attack. Once the images are stored using blockchain, if an attacker tries to inject false images, all the parties in the blockchain network must agree otherwise it is impossible to make any changes. In case of the example shown in Figure 5, there are three parties in the network, doctor, patient and family members who all should agree to approve any changes in the medical images stored in the blockchain based medical image repository. The ***i*Chain** framework (Algorithm 1) reflects the backbone of the proposed framework. Additionally, blockchain saves data in hash functions with time stamps, it is highly unlikely to be tampered with or to have any chance of being misled by false image injection attacks. Unlike other cryptographic techniques to secure data, such as AES, DES, and RSA algorithms, blockchain requires a validation stage, i.e., agreement among all parties involved. This unique characteristics enforces the integrity and effectiveness of the data being stored in a blockchain framework.

Algorithm 1: *i*Chain Algorithm

Begin
A new image needs to be added/modified in the repository
The image is broadcasted to all parties
if *All parties agree* **then**
  Add the image or approve the modification;
else
  Ignore the change
end
End

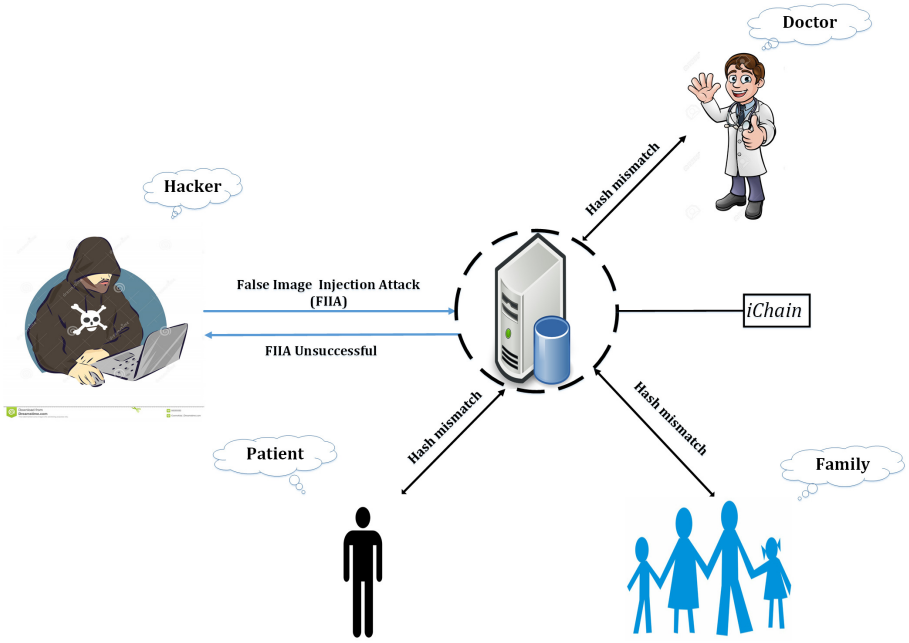


Figure 5. Conceptual framework of ***i*Chain**.

Figure 6 reflects the underlying mechanism of the proposed framework. The first part of the figure shows a sample of **N** blocks in the image chain. It is shown that the hash values are stored in each block for both the current and previous blocks. Let us assume that an attacker injects a false image in Block 2. Once the image data is changed, the corresponding hash value will also change. However, Block 3 in this blockchain contains the original hash of Block 2. At this stage, due to the mismatch of hash values in the ***i*Chain**, all the associated blocks are considered tampered with for not having the correct hash of the previous block. Thus the false image injection attacks can be prevented by the proposed framework. In terms of the usage of hash algorithms, based on the computational efficiency of MD5, SHA-1, SHA256, or SHA512. can be chosen.

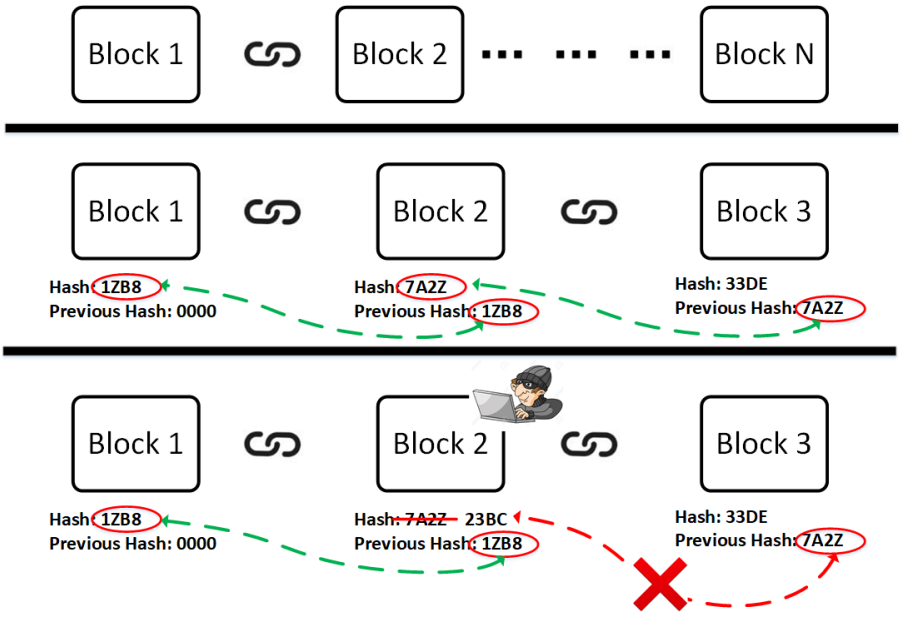


Figure 6. Underlying mechanism of ***i*Chain**.

Although, blockchain based solutions are widely accepted for a variety of applications, they are still struggling to ensure security despite their promising characteristics [24]. Blockchain systems can

be found vulnerable and there is a trade-off between scalability and security. Since blockchain based systems are quite new, there is a significant lack of research to address the scalability issues in an blockchain environment. As the blockchain enabled system grows, i.e., the number of users increases, so to facilitate services, the security is overlooked as shown in Figure 7.

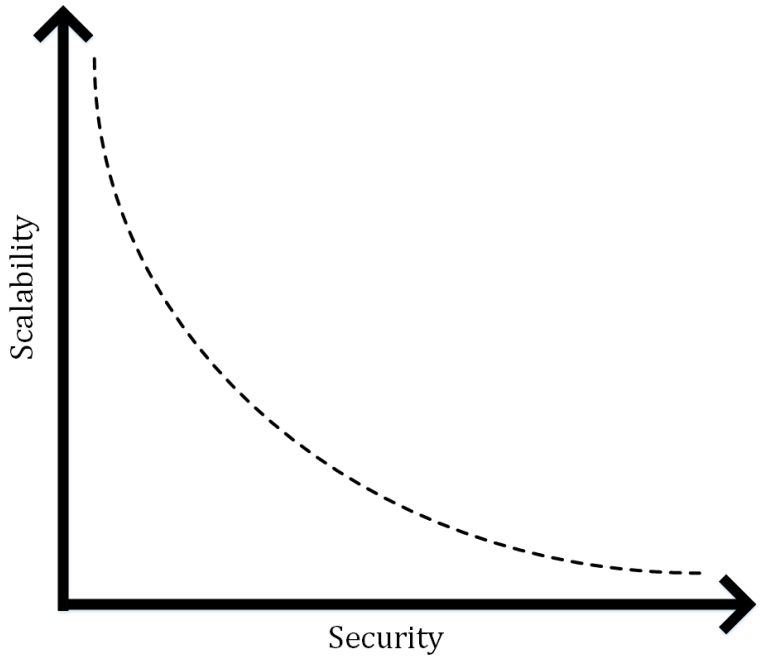


Figure 7. Security vs. scalability in blockchain based frameworks.

6. Evaluation

This section covers the comparison of existing image tampering detection techniques with the proposed approach, and from a blockchain perspective, compares with the existing approaches, which used blockchain based information processing. Although none of these techniques have addressed the issues associated with false data/image injection attacks, the comparison is not straightforward.

Table 1 reflects a comparison among image tampering techniques [12,25–28]. The metrics used for comparison are focused on learning method, complexity, privacy, and the ability to handle false image injection attacks. No existing techniques have addressed the issue of false image injection attacks and the image tampering detection techniques are based on supervised learning. Therefore, any new tampering approaches have high chances of being successful. Also, the privacy and complexity issues are overlooked in the existing techniques whereas the proposed method is focused on security and privacy of the images along with reduction in the complexity of processing.

Table 1. Comparison among image tampering techniques [12].

Technique	FIIA Countermeasure	Privacy	Complexity	Learning
Deep Learning [15]	×	×	High	Supervised
Keypoint Features [25,26]	×	×	High	Supervised
Support Vector Machine [27]	×	×	High	Supervised
Pixel Feature [28]	×	×	High	Supervised
***i*Chain**	✓	✓	Medium	Unsupervised

The blockchain based systems [29–33] are primarily designed for electronic health record keeping and not focussed on cyber security i.e., they are not designed for false image injection attack countermeasures. Therefore, the proposed approach can be customized for different types of blockchains used in the background, such as private, public and hybrid blockchains etc. It is

reflected in Table 2 that the security and privacy of the private and public type of blockchains are both high. Since ***i*Chain** is focused on both security and privacy of medical images, the other factors should be considered when choosing between a private or public version of blockchain to be used. The optimized version of ***i*Chain** should take the architecture, cost and end users into account when choosing between private or public types of blockchain as an underlying mechanism. A simplified version of the proposed ***i*Chain** method is implemented using the python platform for creating chains and adding transactions. Figure 8 showcases the computational performances while using different hash functions such as MD5, SHA-1, SHA256, SHA512. It is evident that, the incorporation of the SHA512 hash function requires the lowest possible time with a simple transaction to process. Therefore, for preventing false image injection attacks, SHA512 hash function usage is computationally more effective than others.

Table 2. Comparison among different blockchains [23].

Type	User	Cost	Security	Architecture	Privacy
Public	Crypto Traders	High	High	Decentralized	Medium
Private	Government	Medium	Medium	Partially Decentralized	High
Hybrid	Private Sector	Low	Medium	Partially Decentralized	High

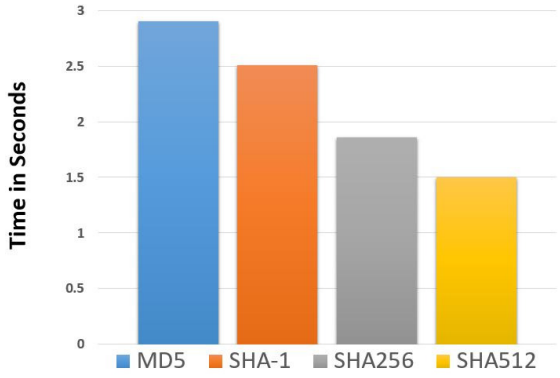


Figure 8. Computational time comparison for different hash functions. .

7. Conclusions and Future Research

This paper introduces a new type of cyber attack, false image injection attack (**FIIA**), specific to the healthcare domain and more importantly related to sensitive medical images. This type of attack is not being handled well in real time by the existing image tampering detection techniques. To ensure security and privacy of such images, a blockchain based medical image storage solution, ***i*Chain** is proposed. The proposed framework is designed to ensure that the medical images have not been tampered with and can provide support to the correct diagnosis for patients. Although, this framework is expected to be ideal, there is still scope to improve blockchain based systems, particularly the scalability issue which will be addressed in future works. The specific research questions that future research will try to answer are the following:

- How ethical hacking tools can be utilised to identify vulnerabilities of blockchain based frameworks?
- How to inject software vulnerabilities or malware into blockchains?
- How to address the scalability of the blockchain based security framework used in implanted medical devices such as pacemakers, CRT-D (Cardiac resynchronization therapy devices) etc.?

Funding: This work was supported in part by the Edith Cowan University Early Career Research Scheme for project: Securing Internet of Medical Things against False Data Injection Attacks using Blockchain, Chief Investigator: Mohiuddin Ahmed. The article processing charge is funded by Edith Cowan University Open Access Funding Support Scheme.

Acknowledgments: The author would like to thank the reviewers for the valuable feedback to enhance the quality of the manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ahmed, M.; Mahmood, A.N.; Hu, J. Outlier Detection. In *The State of the Art in Intrusion Prevention and Detection*; Pathan, A.-S.K., Ed.; CRC Press: New York, NY, USA, 2014; Chapter 1, pp. 3–21.
2. Ahmed, M.; Mahmood, A.N.; Hu, J. A survey of network anomaly detection techniques. *J. Netw. Comput. Appl.* **2016**, *60*, 19–31. [CrossRef]
3. Ahmed, M.; Mahmood, A.N.; Islam, M.R. A survey of anomaly detection techniques in financial domain. *Future Gen. Comput. Syst.* **2016**, *55*, 278–288. [CrossRef]
4. Ahmed, M. Thwarting dos attacks: A framework for detection based on collective anomalies and clustering. *Computer* **2017**, *50*, 76–82. [CrossRef]
5. Ahmed, M.; Ullah, A.S.S.M.B. False data injection attacks in healthcare, In *Australasian Conference on Data Mining 2017*; Boo, Y.L., Stirling, D., Chi, L., Liu, L., Ong, K.-L., Williams, G., Eds.; Springer: Singapore, 2018; pp. 192–202.
6. Ahmed, M.; Anwar, A.; Mahmood, A.N.; Shah, Z.; Maher, M.J. An investigation of performance analysis of anomaly detection techniques for big data in scada systems. *EAI Endorsed Trans. Ind. Netw. Intell. Syst.* **2015**, *15*, 5. [CrossRef]
7. Aiello, M.; Cavaliere, C.; D'Albore, A.; Salvatore, M. The challenges of diagnostic imaging in the era of big data. *J. Clin. Med.* **2019**, *8*, 316. [CrossRef]
8. *Stanford Medicine 2018 Health Trends Report*; Stanford School of Medicince: Stanford, CA, USA, 2018.
9. Klonoff, D.C. Cybersecurity for connected diabetes devices. *J. Diabetes Sci. Technol.* **2015**, *9*, 1143–1147. [CrossRef]
10. Pycroft, L.; Aziz, T.Z. Security of implantable medical devices with wireless connections: The dangers of cyber-attacks. *Expert Rev. Med. Dev.* **2018**, *15*, 403–406. [CrossRef]
11. Fernández-Caramés, T.M.; Fraga-Lamas, P. A review on the use of blockchain for the internet of things. *IEEE Access* **2018**, *6*, 32979–33001. [CrossRef]
12. Zheng, L.; Zhang, Y.; Thing, V.L. A survey on image tampering and its detection in real-world photos. *J. Vis. Commun. Image Represent.* **2019**, *58*, 380–399. [CrossRef]
13. Pouyanfar, S.; Sadiq, S.; Yan, Y.; Tian, H.; Tao, Y.; Reyes, M.P.; Shyu, M.-L.; Chen, S.-C.; Iyengar, S.S. A survey on deep learning: Algorithms, techniques, and applications. *ACM Comput. Surv.* **2018**, *51*, 92. [CrossRef]
14. Ahmed, M.; Pathan, A.S.K. Investigating deep learning for collective anomaly detection—An experimental study. In Proceedings of the Sixth International Symposium on Security in Computing and Communications (SSCC 2018), Bangalore, India, 19–22 September 2018; Volume 969.
15. Rao, Y.; Ni, J. A deep learning approach to detection of splicing and copy-move forgeries in images. In Proceedings of the 2016 IEEE International Workshop on Information Forensics and Security (WIFS), Abu Dhabi, United Arab Emirates, 4–7 December 2016; pp.1–6.
16. Ali, M.S.; Vecchio, M.; Pincheira, M.; Dolui, K.; Antonelli, F.; Rehmani, M.H. Applications of blockchains in the internet of things: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2018**, *21*, 1676-1717. [CrossRef]
17. Hassan, M.; Ahmed, M. Blockchain in the era of Industry 4.0. In *Data Analytics: Concepts, Techniques, and Applications*; Ahmed, M., Pathan, A.S.K., Eds.; CRC Press: New York, NY, USA, 2018; Chapter 10, pp. 235–273
18. Johnson, D.; Menezes, A.; Vanstone, S. The elliptic curve digital signature algorithm (ecdsa). *Int. J. Inf. Secur.* **2001**, *1*, 36–63. [CrossRef]
19. Siyal, A.A.; Junejo, A.Z.; Zawish, M.; Ahmed, K.; Khalil, A.; Soursou, G. Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. *Cryptography* **2019**, *3*, 3. [CrossRef]
20. Esposito, C.; De Santis, A.; Tortora, G.; Chang, H.; Choo, K.R. Blockchain: A panacea for healthcare cloud-based data security and privacy? *IEEE Cloud Comput.* **2018**, *5*, 31–37. [CrossRef]
21. Aggarwal, S.; Chaudhary, R.; Aujla, G.S.; Kumar, N.; Choo, K.-K.R.; Zomaya, A.Y. Blockchain for smart communities: Applications, challenges and opportunities, *J. Netw. Comput. Appl.* **2019**, *144*, 13–48. [CrossRef]
22. Banerjee, M.; Lee, J.; Choo, K.-K.R. A blockchain future for internet of things security: A position paper. *Digit. Commun. Netw.* **2018**, *4*, 149–160. [CrossRef]

23. Yang, J.; Hassan, M.; Lee, N.-Y.; Ahmed, M.; Kim, C.-S. Proof-of-Familiarity: A Privacy-Preserved Blockchain Scheme for Collaborative Medical Decision-Making. *Appl. Sci.* **2019**, *9*, 1370. [CrossRef]
24. Ye, C.; Li, G.; Cai, H.; Gu, Y.; Fukuda, A. Analysis of Security in Blockchain: Case Study in 51%-Attack Detecting. In Proceedings of the 2018 5th International Conference on Dependable Systems and Their Applications (DSA), Dalian, China, 22–23 September 2018; Volume 4, pp. 15–24.
25. Christlein, V.; Riess, C.; Jordan, J.; Riess, C.; Angelopoulou, E. An evaluation of popular copy-move forgery detection approaches. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 1841–1854. [CrossRef]
26. Al-Qershi, O.M.; Khoo, B.E. Passive detection of copy-move forgery in digital images: State-of-the-art. *Forensic Sci. Int.* **2013**, *231*, 284–295. [CrossRef]
27. Ng, T.-T.; Chang, S.-F.; Sun, Q. Blind detection of photomontage using higher order statistics. *IEEE Int. Symp. Circuits Syst. (ISCAS)* **2004**, *5*, V.
28. Cozzolino, D.; Gragnaniello, D.; Verdoliva, L. Image forgery localization through the fusion of camera-based, feature-based and pixel-based techniques. In Proceedings of the 2014 IEEE International Conference on Image Processing (ICIP), Paris, France, 27–30 October 2014; pp. 5302–5306.
29. Zhang, P.; White, J.; Schmidt, D.C.; Lenz, G.; Rosenbloom, S.T. Fhirchain: Applying blockchain to securely and scalably share clinical data. *Comput. Struct. Biotechnol. J.* **2018**, *16*, 267–278. [CrossRef] [PubMed]
30. Fan, K.; Wang, S.; Ren, Y.; Li, H.; Yang, Y. Medblock: Efficient and secure medical data sharing via blockchain. *J. Med. Syst.* **2018**, *42*, 136. [CrossRef] [PubMed]
31. Tseng, J.-H.; Liao, Y-C.; Chong, B.; Liao, S.-W. Governance on the drug supply chain via gcoin blockchain. *Int. J. Environ. Res. Public Health* **2018**, *15*, 1055. [CrossRef]
32. Esmaeilzadeh, P.; Mirzaei, T. The potential of blockchain technology for health information exchange: Experimental study from patients' perspectives. *J. Med. Internet Res.* **2019**, *21*, e14184. [CrossRef] [PubMed]
33. Dubovitskaya, A.; Xu, Z.; Ryu, S.; Schumacher, M.; Wang, F. Secure and trustable electronic medical records sharing using blockchain. *AMIA Annu. Symp. Proc.* **2017**, *2017*, 650–659. [PubMed]