



Steganography-based healthcare model for safe handling of multimedia health care information using VR

Jeong Yoon-Su¹  · Shin Seung-Soo²

Received: 10 January 2019 / Revised: 25 March 2019 / Accepted: 23 May 2019 /

Published online: 6 July 2019

© Springer Science+Business Media, LLC, part of Springer Nature 2019

Abstract

Due to the development of the Internet of Things (IoT) in the medical field, special medical equipment such as CT and MRI, which are used in medical institutions, can be used for digital healthcare services by medical staff using VR. However, the integrity and confidentiality of multimedia health care information handled through special medical equipment using VR is still one of the major issues that cause many problems in the application sector of medical services. This paper proposes a steganography-based digital healthcare model to ensure the integrity of user multimedia image information processed through special medical equipment using VR. The proposed model aims to prevent illegal use by the medical team through VR of multimedia image information collected through special medical equipment without the consent of the user. The proposed model uses the user's signature and credentials in a hybrid cipher for multimedia health care information. The proposed model has features that ensure the integrity and confidentiality of the user's medical image information without disturbing the user's multimedia image quality filmed through special medical equipment. In addition, multimedia medical information viewed through VR is not exploited without the consent of users because the user's signature information was encrypted using steganography-based cryptography-based ciphering techniques. In particular, the proposed model provides real-time guidance related to users' health conditions and first-aid care in connection with the hospital health service to improve the management of medical image information for users in hospitals. As a result of the performance evaluation, the proposed model averaged 12.5% improvement in the management of the user's medical image information compared to the existing technique, and the user's accuracy in extracting medical image information was averaged 10.4% higher than that of the existing technique.

Keywords VR · Steganography · Medical information · Multimedia · MRI · CT

✉ Jeong Yoon-Su
bukmunro@mokwon.ac.kr

1 Introduction

With the recent advances in medical services and aging of the population becoming a major social issue, interest in elderly couples and single elderly households due to nuclear familyization has been growing [17]. While health care coverage for older people in the socially disadvantaged is not adequately responding to the timescale, the rate of medical burden at medical institutions is very difficult for the socially weak to bear. However, elderly couples and single elderly households who visit hospitals through medical insurance supported by the National Health Service are free to support expensive medical service equipment (CT, MRI etc.) provided by the medical institution [7].

Modern medical service equipment used in hospitals is widely used for medical surgery and medical education. Modern medical service equipment requires more sophisticated technologies to provide higher resolution and lower residual effects for equipment such as VR (Virtual Reality) [15]. To provide quality medical services to users, medical institutions are making various efforts to raise the quality of their medical image information by applying VR and AR (Augmented Reality) to CT (Computerized Tomographic) and MRI (magnetic resonance imaging).

The medical image information of a user whose medical staff is captured using VR and AR is stored in the personal information processing system or transmitted over the network. However, medical image information captured through special medical equipment is highly sensitive privacy information and should be managed so that information entered through VR and AR is not inconsistent [11, 12].

This paper proposes a digital medical image service management model that can efficiently manage medical image information of a user who is photographed by applying VR and AR to special medical equipment such as CT and MRI.

The purpose of the proposed model is to ensure the safe delivery of health care services to patients by reflecting the collected image information that is collected by the clinical workforce through hierarchical collection of patient demographics, patient status, and emergency care based on the AHP (Analytic Hierarchy Process). The proposed model used a paired contrast matrix to compensate for the ambiguity among information collected through medical equipment, and a steganography technique was used to reflect security image information collected in addition to the unique image information stored on the hospital server.

The proposed model has the following features: First, it ensures integrity of encryption and decryption for data confidentiality. Second, the medical imaging system ensures certification without disturbing the quality of medical images captured through special medical equipment. Third, steganography techniques are used to safely communicate medical image information.

Because the proposed model uses the user's signature and credentials in a hybrid cryptography for multimedia medical care information, it has features that ensure user integrity and confidentiality without disturbing the user's medical image quality captured through special medical equipment. In addition, medical image information viewed through VR is not exploited without consent because the user's signature information was encrypted using steganography-based encryption techniques. The proposed model provides the integrity of medical image information by maintaining synchronization at regular intervals between original medical image information and encrypted medical image information using anonymous keys to prevent exposing multimedia medical image information to third parties. The composition of this paper is as follows. Chapter 2 discusses medical information and existing research in virtual and augmented reality. Chapter 3 proposes a management model for steganography-based medical imaging information that improves the safety of medical

imaging information, while Chapter 4 carries out comparative evaluations of the proposed model and the existing model, and finally concludes in Chapter 5.

2 VR/AR and medical information

Health care information refers to data collected and analyzed to determine the need for medical provision. The medical information covers information about the health status of users collected throughout the course of medical activities, including diagnosis, treatment behavior, post-treatment observation, etc. Because health care information is highly sensitive privacy information, it must be fully confidential and responsive to the institution's unique and rapid processing needs. Personal information that should be treated by a medical institution is classified largely as the user's personal information and the employee's personal information within the institution. In particular, personal information from medical institutions is collected in large numbers of users' personal information and sensitive information during the course of care application, care process, and prescribing process. Key personal information (identifiable information, bio information, etc.) of users should be stored in the personal information processing system or transmitted over the network through secure protection measures such as encryption.

2.1 Current status of use of virtual reality in medical field

Applying virtual reality technology in the medical field requires verification of side effects as well as following ethical guidelines in clinical research. If clinical application is required during medical services, various countermeasures according to legal regulations should be implemented proactively. Table 1 is a study of the cases of applying virtual reality in health care so far in the medical field.






2.2 Previous works

Healthcare services are in the body to detect information or using information collected using all kinds of smart devices for use in health care services that can mean [2]. Recently, healthcare services have been used with IT technologies such as mobile devices to provide healthcare and disease prevention services to hospitals and medical staff located remotely [8, 20]. Health care services are subject to physical and time constraints and cannot provide health care urgently. E-care services are providing additional services that are better than those offered by existing health care services. m-healthcare provides security services that were not provided by healthcare [14, 18]. However, the security issues associated with user privacy still have issues to be addressed.

J. G. KO et al. analyzed information related to physical, behavioral, physiological, and cognitive data in relation to medical WSN [9]. In particular, the data used in most applications and projects used in hospitals is free for everyone to receive health-related information. S. C. Rathi et al. proposed a medical imaging method that incorporates watermarking techniques and systems used in hospitals to support the privacy of imaging medical information used in hospitals [13]. However, this method has security issues related to the transfer of medical data, which can be used immediately in hospital health care systems.

G. Virone et al. proposed a framework in which patients can receive medical assistance in a variety of ways, such as doctor availability, medical conditions, and hospitals, for patients in remote areas where medical services are not provided [16].

Table 1 Case study of applying virtual reality in healthcare field

| Field | Application | Example |
|---------------------------------|---|---|
| Medical training and simulation | It is used to use virtual reality for 3D structure without directly dissecting the body during anatomy training - External surgery exercise using virtual/enhanced reality technology |  |
| | Use Haptic Technology for Dental Education - Apply virtual reality to the training of dentists |  |
| | Introduction of 'Virtual Reality Education System' Hospital - Introduction of virtual reality education is the first in the field of surgery, which is highly restricted in field education. |  |
| Operation | a back-operative hologram lens - Surgery is performed by searching the exact location of surgery located inside the patient's body. |  |
| | Remote surgery - Using Haptics technology, surgery can be performed on patients at a distance. - Breaks down barriers between countries | |
| Patient care | Patient Care Using VR - Phobias script (Mental Health Department) - Applied to rehabilitation program |  |

Al Ameen et al. classified the risk categories associated with WSN's security and privacy issues for medical applications [1]. This paper covers issues related to security and privatization issues and legal, political, psychological, and economic health data. However, in order to safely process medical data in hospitals, algorithms related to encryption, authentication, and key management of medical data must be implemented [10, 19].

The Fan, R. He. technique proposed a user authentication technique that would make the wireless sensor network a two-tier authentication system that would make it resistant to DoS [3]. The technique was to perform the authentication through the user's unique identification to safely handle health care-related authentication information from DoS attacks. However, this technique performs validation and authentication on the server side at the request for user registration, but still has problems that are vulnerable to a variety of security attacks.

N. Gonzalez et al. proposed a model in which parameters can be accessed with ID and random values to protect medical data [5]. In addition, other models similar to this model allow users to use medical data through identification and control of access to patient-related medical data [4].

D.-Z. Sun et al. The technique proposed a technique to validate users who need to access medical data so that it can be shared by everyone [6]. However, this technique has a problem

with poor mutual authentication due to constraints related to memory, energy, and processing power in order for users to access.

3 Steganography-based user information management techniques that enhance the safety of medical image information

3.1 Overview

With the development of IT and Internet technologies, medical equipment used by medical institutions is also being introduced, such as VR. Additional up-to-date equipment such as VR is introduced to existing equipment used by medical institutions, and medical information (such as personal information, medical information, video information, etc.) of users visiting the medical institution is collected by a number of medical departments and stored in the medical institution's database. Many of the user's medical information stored in the database is changing from different care units to sharing it with one another to collaborate on patient care. However, the need to protect the user's medical information is increasing because it can be exploited through third-party illegal or malicious actions in the process of transmitting it over the Internet.

This paper proposes a steganography-based digital medical information service model to ensure the integrity of the user's medical image information using special medical equipment such as VR. The proposed model aims to prevent illegal use by the medical team through VR of multimedia image information collected through special medical equipment without the consent of the user. Because the proposed model uses users' signatures and credentials in a hybrid cryptographic manner for multimedia medical care information, it has the features that ensure the user's privacy and confidentiality without disturbing the user's multimedia image quality captured through special medical equipment. In addition, medical image information viewed through VR is not exploited without the consent of the user because the user's signature information was encrypted using steganography-based encryption techniques.

The proposed model aims to collect the user's medical information (temperature, blood pressure, heart rate, etc.) so that the doctor can efficiently process the patient/user's disease (heart disease, diabetes, etc.) while delivering the user's medical image information safely. Figure 1 shows the operational process of communicating user information to the clinical

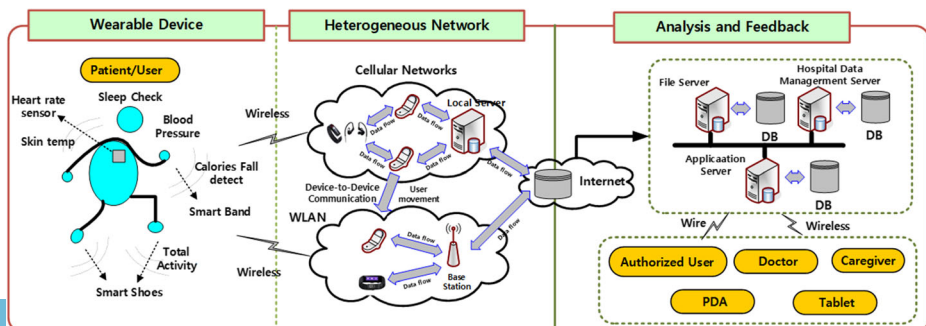


Fig. 1 Transmission process of multimedia information

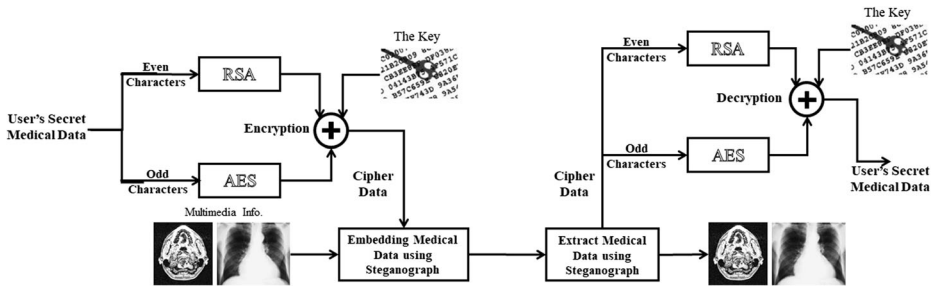


Fig. 2 Proposed scheme for securing the multimedia data transmission

workforce in the proposed model. The proposed model's operational processes are largely divided into three levels: wearable devices, the Heterogenous network, and the Analysis and Feedback. The Wearable Device process is a step in collecting patient/user information through advanced medical equipment such as VR. The Heterogenous Network process is a step in communicating the user's medical image information through Cellular Networks and WLANs. The Analysis and Feedback process is a step in which the user's medical image information is analyzed by authorized users or clinicians.

Figure 2 shows the cancer and recovery process for users' medical information in the proposed model. The proposed model in Fig. 2 ensures that the user's medical image information is analyzed and processed by authorized users or clinicians so that the medical service can be delivered quickly without additional patient/user actions/behavior. In particular, in the process of Fig. 2, medical image information is more appropriate for patients/users who need to ensure confidentiality than for general patients.

Table 2 shows a hybrid cancer and replication algorithm using steganography combining user medical information collected through special medical equipment such as VR. In Table 2, users' confidential medical information is given in binary probability information (Even Characters and Odd Characters). The user's secret medical information granted with binary probability information is converted to cryptographic data with shared keys using RSA and AES algorithms according to binary probability information. User-secured medical data encrypted by Table 2 can be safely protected by embedding via user's medical image information and steganography.

Table 2 Hybrid algorithm based on steganograph

Algorithm 1 Hybrid Algorithm

Inputs: User's Secret Medical Data, Multimedia Info.

Output: Embedding Medical Data

Begin

1. Divide plain message into two parts (Odd message, Even message)
2. Generate RSA Key, AES Key, Secrete Key
3. EncEven = RSA(Even Characters, RSA Key)
4. EncOdd = AES-128(Oven Characters, AES Key)
5. Encryption Cipher Data by inserting EncEven, EncOdd, Secret Key
6. Compress Cipher Data by convert to hashes
7. Embedding medical data = Concatenate (Multimedia Info., Cipher Data)

End

3.2 System model

The proposed model has four systems: user, storage server, special medical equipment, and key generation centers.

- User

The user is responsible for sending the user's personal information or data registered to the storage server. Users access storage servers through Internet communication channels using personal mobile devices (mobile devices, fixtures, etc.) and DMB. Users do not have the same location to access the storage server and may be victimized by third-party malicious activity during storage or transmission.

- Storage Server

The storage server stores both user multimedia information and user medical information collected through special medical devices. Storage servers can provide users' medical information in accordance with the requirements of the clinical workforce if they have the key to access the user's medical information. However, the personal or sensitive information of users stored on the storage server is exposed, allowing malicious users to acquire or expose their original medical information.

- Special medical equipment

Special medical equipment, such as VR, is responsible for generating medical image information for users. Special medical equipment, such as VR, is a trusted component to verify the integrity of a user's medical image information and delivers the user's medical image information to the server.

- Key generation center

The key generation center is responsible for generating cancer and replication keys and metadata to verify the integrity of the user's medical image information. The key-generation center divides the random number of people acting as private keys into random sizes to create random double-awareness for use by storage servers and medical teams. The key generation center then generates a key pair by creating a private key that corresponds to the user's public key to be used in the user's steganodrapy.

3.3 Generate medical information and keys

3.3.1 User medical information generation

The user's medical information generation process inserts the user's confidential information into an encrypted image pixel using the N-1th polynomial as shown in Expression (1) as a precursor to verify the integrity of the user's medical image information as a precursor to the clinical workforce and third parties as part of the verification of the integrity of the user's medical image information.

$$UI(x) = \begin{cases} s_1 + s_2x^1 + \dots + s_nx^{n-1} \bmod s & , \text{if } s, n > 1 \\ & , \text{otherwise} \end{cases} \quad (1)$$

Where n means the number of times the user's secret information has been inserted, and s refers to the size of the user's secret image.

The pixels of the user's medical image information with the user's secret information inserted create a steganographic image using the reference image pixel p to be camouflaged in each image and the size s of the user's secret image information as shown in expression (2).

$$s_n = p \bmod s \quad (2)$$

The steganographic images produced in Eq. (2) are identified after the differences in each pixel are calculated as shown in Expression (3) by referring to distributed encrypted images.

$$s'_n = s_n - p_n \quad (3)$$

The steganography-based secret image $\sum_{i=1}^n s_n$ is restored to zero by superimposing the identified hidden information $s_1 + s_2 + \dots + s_n$ for the reference pixel p .

3.3.2 Generate encryption/decryption key

The encryption and decryption keys used in the user's medical information are used to verify the integrity of the user's medical image information. Here, the private key is generated using two random numbers x_1^0 and x_1^1 , as shown in expression (4).

$$x_i^{\delta[i]} = \begin{cases} x_i^0 & , \text{if } \delta[i] = 0 \\ x_i^1 & , \text{if } \delta[i] = 1 \end{cases} \quad (4)$$

Where $\delta[i]$ means the binary value for creating the i -th selected private key (x_1^0, x_1^1).

The random number $x_i^{\delta[i]}$ generated by expression (4) depends on the number of lambdas generated by the binary value x_1^0, x_1^1 , and the public key is generated to correspond to the number of lambdas x_1^0, x_1^1 , as shown in expression (5).

$$PK_{i+1}^\delta = h(x_{i+1}^\delta) = \begin{cases} PK_{i+1}^\delta = h(x_{i+1}^\delta) & , \text{if } \delta = 0 \\ PK_{i+1}^\delta = h(x_{i+1}^\delta) & , \text{if } \delta = 1 \end{cases} \quad (5)$$

The reason for generating public keys according to two random numbers x_1^0, x_1^1 as shown in Eq. (5) is to ensure the integrity of the user's medical information and to prevent malicious behavior of third parties, including the medical staff.

3.4 Proxy signature-based protocol

This section divides the user's medical image information into three stages (initialization process, delegation process, verification process, etc.) for safe delivery of the user's medical image information through the user's proxy signer without their consent to the server.

3.4.1 Initialization process

The initialization process is the process of creating and communicating personal and public keys to the server to generate medical image information for the user.

- Step 1: Before transferring medical image information to the server, the user creates a public key, PK_{i+1}^δ , and private key $x_i^{\delta[i]}$ for cancer and replication of medical information, pairs it in pairs, and encrypts it with secret key K , and sends it to the server.

$$\text{Transfer } E_K\left(PK_{i+1}^\delta, x_i^{\delta[i]}\right) \quad (6)$$

Where, secret key K means shared key through secure channel between user and server in advance. At this time, K is calculated as $K=r^2$ by selecting the random number $r \in Z_N$, which is pre-generated by the server.

- Step 2: The server checks if the secret key K is a pre-shared key and stores the public key PK_{i+1}^δ and private key $x_i^{\delta[i]}$ on the server to encrypt the user's medical image information. In this case, the private key is applied to a secure hash function used by the user, such as expression (7) to expression (8) and the public key is stored on the server to be applied to a safe hash function used by the medical staff.

$$H_{x_i^{\delta[i]}} : \{0, 1\} \rightarrow Z_N \quad (7)$$

$$H_{PK_{i+1}^\delta} : \{0, 1\}^* \times Z_N \rightarrow Z_N \quad (8)$$

3.4.2 Delegation process

Delegation is a process in which the clinical workforce is delegated signatures to the user's clinical image information, consisting of three steps:

- Step 1: The user generates a delegation of information, pa_i , which includes information related to the user's signing rights or expiration date, as expression (9) for access to the user's medical image information.

$$\text{Generate } pa_i \quad (i \in Z^*) \quad (9)$$

- Step 2: Delegation information generated by the user creates a signature Sig on the delegated information pa_i as expression (10) to verify that the user agrees to access medical image information. At this time, the signature Sig uses the user's private key x_1^0, x_1^1 , delegation pa_i .

$$\text{Sig} = (-1)^{x_1^0} \cdot e^{x_1^1} \cdot H(pa_i, K) \bmod s \quad (10)$$

Where s is the size of the user's secret image information.

- Step 3: The user encrypts the proxy m_i and signature Sig with the private and shared keys, and the TPA checks the user's rights and ratings. In addition to the delegation m_i , Sig, T, x_i^0, x_i^1 are encrypted with the public key PK_{i+1}^δ as shown in formula (12).

$$\text{Transfer } E_{PK_{i+1}^\delta} (pa_i, \text{Sig}, K, x_i^0, x_i^1) \quad (11)$$

3.4.3 Verification process

The signing process is the process of using the user's signature information to the server to verify the integrity of the user's medical image information.

- Step 1: The server checks the user's secret information $UI(x)$ and calculates the steganographic image $ass_n = p \bmod s$ with the size of the randomly selected secret image information, $s \in Z_N$, with the reference image pixel p .
- Step 2: The server calculates the steganography image as $s'_n = s_n - p_n$ to identify the difference in each pixel by comparing it with the distributed encrypted image.
- Step 3: Create hidden information $s_1 + s_2 + \dots + s_n$ for secret images $\sum_{i=1}^n s_n$ based on steganography. If the steganography-based secret images do not match, the server asks the user again to sign on behalf.

4 Evaluation

In this section, when medical services are carried out through state-of-the-art equipment such as VR, medical teams surveyed 10 major hospitals using VR to process user medical information. The content of the survey was evaluated by calculating the importance of the efficiency of medical information and the accuracy of user medical information extraction. It also conducted a security assessment that could occur when using the user's medical information.

4.1 Performance evaluation

4.1.1 Efficiency in healthcare information management

Figure 3 illustrates the effectiveness of managing user medical image information that occurs when a medical team processes the user's medical image information through advanced medical equipment, such as VR. In order to assess the effectiveness of managing medical image information for users, the proposed model used the results of the user's medical image information collection and investigation analysis through VR, depending on the position of the medical team and access authority level. As a result of Fig. 3, the higher the level of clinical workforce and access authority, the more efficient the user's management of medical image information, the more efficient the user is to manage it. These results are due to the fact that clinicians with high levels of access to clinical workforce have smooth access to user medical image information management and ease of user care methods and treatment decisions.

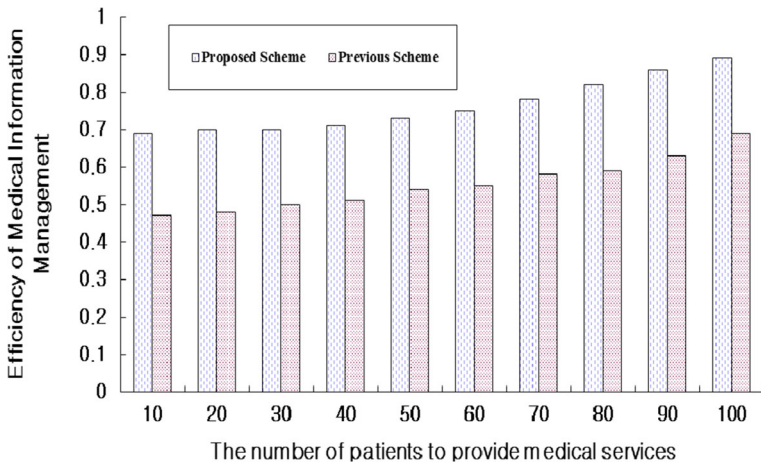


Fig. 3 Efficiency in healthcare information management

4.1.2 Accuracy of extracting user medical information

Figure 4 shows information extraction accuracy as to whether clinicians can accurately extract collected image information by collecting user personal information, user health status, and image information related to the user’s emergency care, which is collected through advanced medical imaging equipment such as VR. As Fig. 4 showed, on average, the rate at which medical teams analyze users’ medical image information accurately through medical imaging equipment is 10.4% higher than if not. These results are due to the use of paired contrast matrices to complement the ambiguity between the information collected through imaging medical equipment in the proposed technique, as well as adding steganography-based video information in addition to the unique image information. In addition, this is the result of the additional application of the medical team to the basic medical information of the user as well as the user’s treatment process and treatment methods for the purpose of image analysis by the medical team using VR.

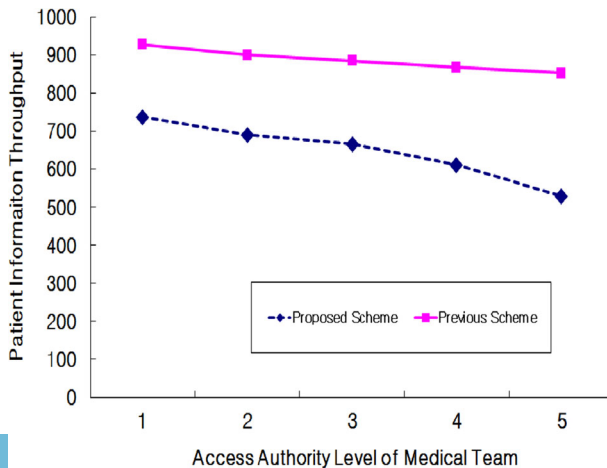


Fig. 4 Accuracy of extracting user medical information

Table 3 Comparisons of different remote data integrity schemes

| Scheme | Data dynamics | Public auditability | Server comp. complexity | Verifier comp. complexity | Encryption comp. complexity | Verifier storage complexity |
|------------|---------------|---------------------|-------------------------|---------------------------|-----------------------------|-----------------------------|
| [7] | No | Yes | O(1) | O(1) | O(1) | O(1) |
| [1] | Yes | No | O(1) | O(1) | O(1) | O(1) |
| [15] | Yes | Yes | O(logn) | (logn) | (logn) | O(1) |
| Our scheme | Yes | Yes | O(logn) | O(logn) | O(logn) | O(logn) |

4.1.3 Integrity assessment

Six items (Data dynamics, public audibility, Server comp. complexity) as shown in Table 3 to check the integrity of the proposed model and medical image information of the existing technique [1, 7, 15]. Verifier comp.complexity, Encryption com.complexity, and Verifier storage complexity) were compared. As shown in Table 3, the proposed model supported all items not provided by the existing technique, providing a high performance efficiency for the medical services of the clinical workforce using VR. In particular, because the proposed model is inserted so that the user's secret information is distributed by sampling the user's secret information in an encrypted image pixel using the N-1th polynomial, it is not possible to identify the encrypted images contained in a steganographic image without knowing exactly how many times the user's secret image is inserted and the size of the user's secret image size. The steganography-based secret image $\sum_{i=1}^n s_n$ is restored to zero by superimposing the hidden information $s_1 + s_2 + \dots + s_n$, which is identified for the reference pixel p, and thus server comp.complexity, encryption.complexity, and storage. Additionally, Verifier storage complexity such as O(logn) appears because the proposed model performs a merge treatment of critical medical information for each user in each layer.

4.2 Security evaluation

Table 4 shows the results of a non-interpreted review of six items: Data Confidence, Data Integrity, Precision, Free Riding Resistance, Dynamic Operations, and Batch Operation for different cloud perspective data integrity checks from the proposed model and traditional techniques [1, 7, 15]. As a result of Table 4, the proposed technique supports all the items provided in Table 4, because it used access controls that were not provided by the existing

Table 4 Comparisons of security evaluation

| Property | [7] | [15] | [1] | Our scheme |
|------------------------|-----|------|-----|------------|
| Data confidentiality | × | × | Δ | √ |
| Data integrity | × | × | × | √ |
| Privacy preservation | × | × | × | √ |
| Free riding resistance | √ | × | √ | √ |
| Dynamic operations | × | √ | √ | √ |
| Batch operation | × | × | √ | √ |

√: provide the corresponding property

Δ: partially provide the corresponding property

×: not process the corresponding property

techniques. In addition, the proposed technique provides the user's medical information integrity by generating the number of lambs x_1^0, x_1^1 , that act as a private key from $R\{0, 1\}^n$ during the process of generating cancer and reinstatement keys used in the user's medical information, so that public keys $PK_{i+1}^\delta = h(x_{i+1}^\delta)$ are created.

5 Conclusion

With the recent Westernization of diet, a variety of high-tech medical devices are being used depending on the disease of the users receiving medical services. In particular, medical information protection is required as advanced medical equipment such as VR and AR are used extensively for medical surgery and medical education. In this paper, the clinical workforce proposed a steganography-based digital healthcare information service model to ensure the integrity and confidentiality of user multimedia image information through special medical equipment such as VR. The proposed model ciphered the user's signature and credentials on a steganographic basis to ensure the integrity of user's multimedia image information collected through special medical equipment, such as VR, without the user's consent. Encrypted digital medical information can be provided in real time by connecting directly to a hospital server to address problems in existing studies, providing real-time guidance related to user health and first aid. As a result of the performance evaluation, the proposed model averaged 13.1% more efficient management of multimedia medical information than the existing model, and the user's accuracy in extracting multimedia medical information was averaged 10.4% higher than the existing techniques. In a future study, performance evaluation is planned to be carried out for hospitals planning to utilize VR according to the size of hospitals and the number of medical staff using the results derived from this paper.

Acknowledgements This work was supported by the BB21+ Project in 2018.

References

1. Al Ameen M, Liu J, Kwak K (2012) Security and privacy issues in wireless sensor networks for healthcare applications. *J Med Syst* 36(1):93–101
2. Bang DW, Jeong JS, Lee JH (2010) An implementation of privacy security for PHR framework supporting u-healthcare service. In: 2010 6th international conference on networked computing(INC), pp 1–4
3. Fan R, He DJ, Pan XZ, Ping LD (2011) An efficient and DoS-resistant user authentication scheme for two-tiered wireless sensor networks. *Journal of Zhejiang University-Science C(Computers & Electronics) (JZUS-C)* 12(7):550–560
4. Garkoti G, Peddoju SK, Balasubramanian R (2014) Detection of insider attacks in cloud based e-healthcare environment. In: Proceedings - 2014 13th international conference on information technology (ICIT 2014), pp 195–200
5. Gonzalez N, Miers C, Redigolo F, Carvalho T, Simplicio M, Naslund M, Pourzandi M (2011) A quantitative analysis of current security concerns and solutions for cloud computing. In: 2011 IEEE third international conference on cloud computing technology and science, pp 231–238
6. Kester QA, Nana L, Pascu AC, Gire S, Eghan JM, Quaynor NN (2015) A security technique for authentication and security of medical images in health information systems. In: Proceedings - 15th international conference on computational science and its applications (ICCSA 2015), pp 8–13

7. Khalil MI (2017) Medical image steganography: study of medical image quality degradation when embedding data in the frequency domain. *International Journal of Computer Network and Information Security(IJCNIS)* 9(2):22–22
8. Kim YH, Kook KH (2014) A study on the relative importance of the administrative and technical measures for the personal information protection. *The Journal of Society for e-Business Studies (JSEBS)* 19(4):614–624
9. Ko JG, Lu C, Srivastava MB, Stankovic JA, Terzis A, Welsh M (2010) Wireless sensor networks for healthcare. *Proc IEEE* 98(11):1947–1960
10. Liu D, Song T, Dai Y (2005) Isomorphism and generation of Montgomery-form elliptic curves suitable for cryptosystems. *Tsinghua Sci Technol* 10(2):145–151
11. Mohamed E, Gustavo RG, Osama MA, Shihab AS, Arunkumar N, Farouk A (2018) Secure medical data transmission model for IoT-based healthcare systems. *IEEE Access* 6:20596–20608
12. Rahimi F, Hossein R (2011) A dual adaptive watermarking scheme in contourlet domain for DICOM images. *Biomed Eng Online* 10(1):53–53
13. Rathi SC (2012) *Technology. I. : medical image authentication through watermarking preserving ROI*, vol 2, pp 292–295
14. Saaty TL (2008) Decision making with dependence and feedback : the analysis network process. *Int J Services Sciences (IJSSci)* 1(1):83–98
15. Seyyedi SA, Sadau V, Ivanov N (2016) A secure steganography method based on integer lifting wavelet transform. *International Journal of Network Security(IJNS)* 18(1):124–132
16. Virone G, Wood A, Selavo L, Cao Q, Fang L, Doan T, Stankovic JA (2006) An advanced wireless sensor network for health monitoring. *Transdisciplinary conference on distributed diagnosis and home healthcare (D2H2)*, pp 2–5
17. Walters W, Betz A (2009) Medical identity theft. *Journal of Consumer Education (JCE)* 15(10):1–5
18. Wu JHK, Ruey-Feng C, Chii-Jen C, Ching-Lin W, Ta-Hsun K, Woo KM, Dar-Ren C (2008) Tamper detection and recovery for medical images using near-lossless information hiding technique. *J Digit Imaging* 21(1):59–76
19. Yang T, D M, W H, Zhang H (2014) Energy-efficient border intrusion detection using wireless sensors network. *EURASIP J Wirel Commun Netw* 1:46
20. Yong CD (1996) Application of the extent analysis method on fuzzy AHP. *Eur J Oper Res* 95(3):649–655

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Jeong Yoon-Su was born in Cheong-Ju, Korea in 1975. He received the B.S. degree in the department of computer science, Cheongju National University in February 1998. He received the M.S. degree and Ph.D in the department of computer science, Chungbuk National University in February 2000 and 2008. He is currently working professor in the department of Information and Communication Convergence Engineering, Mokwon University. His research interests also include cryptography, network security, information security, healthcare service, bioinformatic, cloud service, wire/wireless communication security, Privacy, Big data. bukmunro@gmail.com.



Shin Seung-Soo was born in Cheong-Ju, Korea in 1966. He received the B.S. degree in the department of mathematic, Chungbuk National University in February 1988. He received the M.S. degree and Ph.D in the department of mathematic, Chungbuk National University in February 1993 and 2001. And He received the Ph.D in the department of computer engineering, Chungbuk National University in February 2004. He is currently working professor in the department of Information Security, Tongmyong University. His research interests also include cryptography, network security, information security. shinss@tu.ac.kr.

Affiliations

Jeong Yoon-Su¹ · Shin Seung-Soo²

Shin Seung-Soo
shinss@tu.ac.kr

- ¹ Department of Information and Communication Convergence Engineering, Mokwon University, Daejeon, South Korea
- ² Department of Information Security, Tongmyong University, Busan, South Korea

Multimedia Tools & Applications is a copyright of Springer, 2020. All Rights Reserved.