Journal of Computer Science

Original Research Paper

Secure Fingerprint Identification for Unconscious Personal Health Record Users During an Emergency Situation

[1]Pariwat Choosang, [1]Sangsuree Vasupongayya and [2]Kitsiri Chochiang

[1]*Department of Computer Engineering, Faculty of Engineering, Prince of Songkla University, Songkhla, Thailand*
[2]*Division of Computational Science, Faculty of Science, Prince of Songkla University, Songkhla, Thailand*

Article history
Received: 30-01-2024
Revised: 21-02-2024
Accepted: 12-03-2024

Corresponding Author:
Sangsuree Vasupongayya
Department of Computer Engineering, Faculty of Engineering, Prince of Songkla University, Songkhla, Thailand
Email: vsangsur@coe.psu.ac.th

Abstract: The Personal Health Record (PHR) system is a system that allows an individual to collect, store and share his/her health-related information. Such information about the victim during an emergency is critical, especially when the victim is unconscious. A privacy-preserved user identification method for a PHR system during an emergency was proposed in this study. Two cancelable biometrics were used with two fingerprints of the victim to identify the victim and return the victim's PHR information. The proposed method was evaluated against the previously proposed method using a synthesis fingerprint workload that was created to mimic the environment of an emergency. The two main measurements were the processing time and the identification accuracy. The proposed method was also evaluated against three attack scenarios including (1) Stealing the original fingerprints during the PHR user identification process, (2) Collecting the identity-related information during the identification process to perform illegal access to the PHRs and (3) The PHR identity exposure. The experimental results showed that the proposed approach had a higher potential to be used for identifying the PHR user during an emergency than the previous approach.

Keywords: Fingerprint, Identification, Cancelable Biometrics, Biometric Cryptosystems, Health Records

Introduction

Under the Personal Health Records (PHR) concept, the health-related information is maintained by the data owner (Tang *et al*., 2006; Park and Yoon, 2020). The health-related information can be stored on the system provided by the third party, but the policy to enforce access to the stored information must be defined by the data owner. Many PHR systems and related techniques were presented (Li *et al*., 2012; Huang *et al*., 2012; Wang *et al*., 2012; Fan *et al*., 2015; Alanazi *et al*., 2023; Song *et al*., 2015; Sieverink *et al*., 2019). Since the PHR owner has full control over his/her PHR data, the critical challenge in emergency situations is how the emergency staff can access the victim's PHR information, even when the PHR owner (i.e., the victim) is unable to give his/her consent (Thummavet and Vasupongayya, 2013). The emergency staff, who provides necessary first-aid treatments during an emergency, can access the health-related information immediately if the data owner, who is the victim, already set the policy for emergency situations. In order to provide the correct PHRs to the emergency staff, however, the PHP system requires the victim's identity.

The Secure Personal Health Record Framework (SPHRF) (Thummavet and Vasupongayya, 2015) assumed that the victim's identity was already known by the emergency staff. Figure 1, the Emergency Department (ED) must first register with the PHR system in order to verify the ED staff. An Emergency Server (EmS) handles the request for an emergency. During an emergency, the emergency staff performs an authentication to their corresponding ED to request authorization to interact with the victim's PHR system. When the emergency staff connects to the victim PHR system, the EmS can verify the emergency staff. Thus, only emergency staff that is already authenticated by the associated ED can interact with the EmS. Each PHR data must be assigned the access control level. There are three access control levels in the SPHRF. First, the secure level is accessed by the emergency staff during an emergency situation. Second, the restrict level is accessed by the emergency staff if and only if enough numbers of delegators of the PHR owner give their approvals. Third, the exclusive level could not be accessed by the emergency staff.

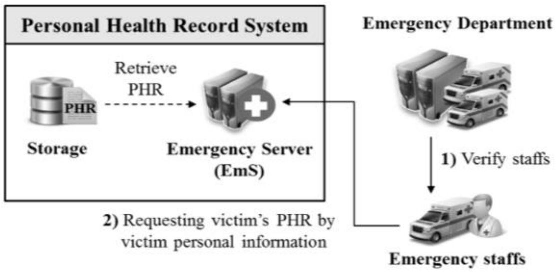

Fig. 1. Secure personal health record framework

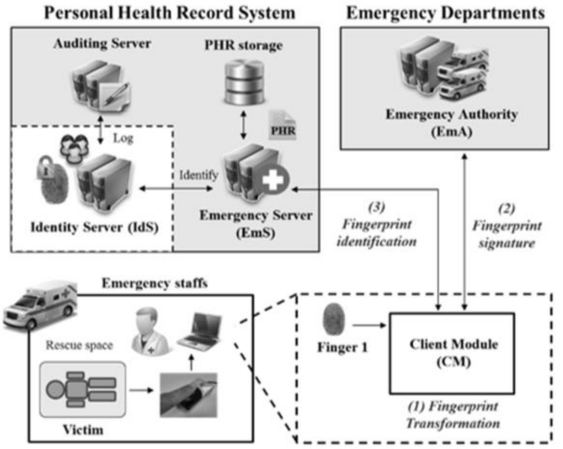

Fig. 2: Secure personal health record framework with the fingerprint identification module

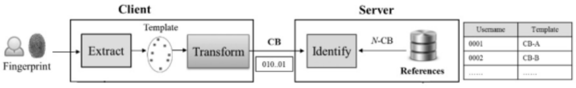

Fig. 3: The process of cancellable biometrics

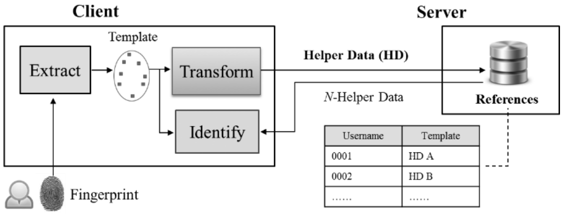

Fig. 4: The process of biometric cryptosystem

The access control requires an explicit and unique victim identity for retrieving the PHR data. The emergency staff needs to collect/search at least one identification of the victim in order to request the correct PHRs. Meanwhile, if the victim is unconscious or unable to provide his/her identity information, the PHR cannot be used. In the healthcare sector, biometrics was linked to the patient medical profile (Marohn, 2006; Flores Zuniga *et al*., 2010). The fingerprint is an obvious personal identity with a high possibility of remaining with the victim during an emergency. However, the security of the fingerprint must be considered because the fingerprint-related data used for the identification process can be reversed to reconstruct the original fingerprint image (Cappelli *et al*., 2007).

To be practical, the work in Choosang and Vasupongayya (2015) protected the fingerprints by proposing a fingerprint identification module using a protected fingerprint template in Figure 2. In comparison with the model in Figure 1, two new modules were created including Identity Server (IdS) and Client Module (CM). The IdS handles the management of the fingerprint identification process on the server side, while the CM contains all necessary transformation techniques on the client side. The fingerprint template will be modified and concealed by the CM. The emergency response unit personnel can interact securely with the PHR system via the CM. This way, the original fingerprint will not be transmitted over the Internet. This study aims to propose a method to overcome the time-consuming process of the previously proposed method.

Fingerprint Protection

The concept of Cancellable Biometrics (CB) (Patel *et al*., 2015) is to use a transform function to generate an irreversible form of the biometrics data. Roughly speaking, the CB is similar to a hashing function because the CB and the hashing function are based on the same concept that uses the irreversible transforms function. However, the important difference between the two is that the CB uses the fingerprint minutiae to generate the irreversible form while the traditional hashing function does not. Figure 3 shows the process of CB. During an identification process, the irreversible form is used for matching without the requirement of the fingerprint template. The CB can identify a fingerprint in the transformed domain. The fingerprint template is transformed by the client. Thus, the actual template cannot be seen by any party except the node that operates the transformation.

Tams and Rathgeb (2014) proposed a two-phase fingerprint identification process. Two fingerprints of a user are applied for the two phases. The first phase uses the CB to filter the whole reference database to produce a list of possible identities. The first fingerprint is used as an input and the output is a candidate list. The second phase uses the Biometric Cryptosystem (BCS) to select the final identity from the candidate list. The second fingerprint and the candidate list are used as input and the output is the final identity. The combination of CB and BCS can reduce the identification time under the traditional BCS system because the set of identities for the BCS process is optimized into a small set by the CB. Roughly speaking, BCS is equivalent to the encryption technique in primitive cryptography, where the secret is viewed as the data and the fingerprint minutiae is the encryption key. The procedure of the BCS is described in Fig. 4.

Materials

To evaluate the mechanism in this study, fingerprint data sets are used. There are two sets of fingerprint data in this study. The first fingerprint data set is the original data. The original fingerprint data sets used for evaluations are obtained from three available data sources including the Fingerprint Verification Competition (FVC) (Maltoni *et al*., 2001; 2002; 2003; Neurotechnology, 2024) and Institute of Automation, Chinese Academy of Sciences (CASIA) (BIT, 2010). The second data set is the modified fingerprint data set.

Original Fingerprint Data

The original fingerprints obtained from the FVC are free and available on the official website for FVC2000 (Maltoni *et al*., 2001), FVC2002 (Maltoni *et al*., 2002) and FVC2004 (Maltoni *et al*., 2003). Each data set contains 4 subsets including DB1, DB2, DB3 and DB4. Each subset contains 10 different fingerprints with 8 samples per fingerprint. The number of fingerprints collected from the FVC is 120 fingerprints. There are two fingerprint data sets available on the (Neurotechnology, 2024) official website. In the first set, the fingerprints are collected by the cross-match reader and there are 51 fingerprints with 8 samples per fingerprint. In the second set, the fingerprints are collected by a digital persona reader and there are 65 fingerprints with 8 samples per fingerprint. The number of fingerprints obtained from the Neurotechnology is 116 fingerprints. The CASIA provides a large and available free fingerprint data set. The fingerprints can be downloaded from its official website (BIT, 2010). The CASIA researchers collected the fingerprints from 500 volunteers. Each volunteer provides 8 fingerprints with 5 samples per fingerprint. The number of fingerprints obtained from the CASIA is 4,000 fingers. Therefore, the amount of fingerprint data that is obtained from the three sources is 4,236 different fingerprints.

Modified Fingerprint Data

In order to support the emergency situation, the fingerprint collecting conditions under the emergency situation are discussed. During an emergency, the fingerprint obtained from the fingerprint reader might be sensitive to the variation according to the ambient environment and human error. The emergency staff will identify the victim in the ambulance while delivering the victim to a medical facility such as a hospital. The emergency staff would collect the fingerprint, instead of the PHR user. As a result, the victim's finger might not be placed in a certain direction or tightly pressured on the fingerprint reader. To make our experiment realistic, a certain set of conditions derived from the emergency is constructed in this study. The fingerprints used in our experiment are modified by these conditions to ensure that the measurement results correspond with the emergency situation. For this reason, there are three conditions that are derived from the emergency as proposed by Mon *et al*. (2019).

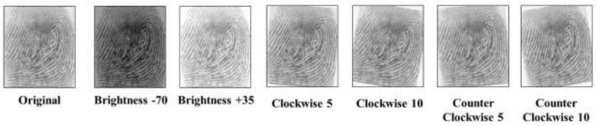

Fig. 5: The modified fingerprint images

The first condition represents the form of the fingerprint data when it is distorted in its quality by the contact surface of the reader or wet finger. To follow this condition, the fingerprint image should be decreased its brightness to blend the fingerprint descriptors. In this study, the darkness varies from 0-70%. The second condition represents the form of the fingerprint data when it cannot be tightly impressed or dry finger. Thus, the fingerprint detail can be blurred or almost invisible. Thus, to follow the condition, the sharpness of the fingerprint must be decreased. In this study, the brightness varies from 0-35%. The third condition represents the form of the fingerprint data when the victim's finger is rotated, in comparison with the orthogonal of the fingerprint reader. In this study, the rotation is done in two angles including 5 and 10°C and in two directions clockwise and counterclockwise. The fingerprint images are modified by three conditions into six data types including B-70 for the brightness of -70, B+35 for the brightness of +35, CW5 for the clockwise rotation of 5°C, CW10 for the clockwise rotation of 10°C, CC5 for the counterclockwise of 5°C and CC10 for the counterclockwise of 10°C as shown in Fig. 5.

Methods

To evaluate the potential uses of the protected fingerprint template in the SPHRF during an emergency, the SPHRF is modified by adding the proposed double-CBs fingerprint identification module. The proposed module is also evaluated against the previously proposed module (i.e., CB-BCS) in Choosang and Vasupongayya (2015).

Methodology

In this study, a cancelable biometric fingerprint protection template mechanism is used on two fingerprints in this study. Instead of constructing a single candidate list as proposed in Tams and Rathgeb (2014), two CBs are applied to generate two irreversible forms and both generated forms are identified in order to obtain two candidate lists. The lists are sorted and the correct identity may be placed at the top of the lists. This way, the speed of the identification process is increased because two fingerprints are identified simultaneously. Meanwhile, the use of two candidate lists can increase the identification accuracy because the correct identity can be placed on one of the two lists.

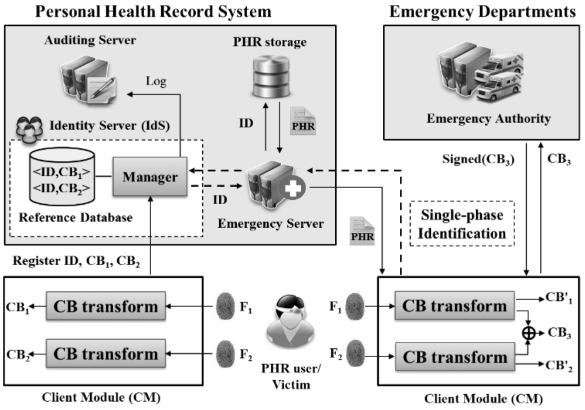

Fig. 6: Secure personal health record framework with the proposed double-CBs module

Figure 6 shows the proposed two CBs (denoted double-CBs). The CM contains two CBs for the fingerprint transformation process and the IdS must identify two irreversible forms generated by the CB in parallel. At the CM, two fingerprints are simultaneously transformed into two irreversible forms. Both forms are sent to the IdS for the identification process. If the identification process succeeds the victim PHR data will be returned to the CM.

To make the evaluation process similar to the real situation, the reference database contains all three fingerprint data sets. However, the measurement will be done on the two widely used data sets namely Neuro and FVC. Since the portion of the measured data set is very small while the portion of the CASIA data set is large. This picture mimics the real-world situation when the SPHRF is utilized in a real emergency situation.

Measurements

All original fingerprint images are evaluated on the developed prototypes. The results show that 5 fingerprint images (4.2%) from the FVC data set and 11 fingerprint images (9.5%) from the Neuro data set cannot be used with the prototypes. Therefore, these fingerprint images are removed from the reference database. Since the developed prototype requires two fingerprint images in the identification process, the remaining fingerprint images are randomly paired to simulate the identification information of the PHR users. As a result, the FVC data set contains 57 pairs of fingerprint images while the Neuro data set contains 52 pairs of fingerprint images. The two sets of fingerprint images will be used for evaluating the developed prototypes. However, the reference database also contains the CASIA data set to make the experiment realistic. The total data on the reference database is 2,054 pairs of fingerprint images including the two measured sets.

The two main measurements in this study are the processing time and the identification accuracy. The period at the step that the emergency staff uses the victim's fingers to impress on the fingerprint reader until the step that the PHR can be successfully retrieved is defined as the whole identification processing time. As the standard operation time defined by the World Health Organization (WHO) (Pons and Markovchick, 2002), the operation time from when the call is placed to report an emergency to when the victim arrives at the medical facility should take no more than 8 min. If the emergency department is assumed to be located at the medical facility, the operation time for the emergency response unit to reach the victim is approximately 4 min. Thus, only 4 min remain before the victim reaches the medical facility. However, the victim must receive first-aid treatment before he/she arrives at the medical facility. Thus, the identification process must finish before 4 min retrieving the victim PHR necessary for the first-aid treatment in the ambulance. The identification accuracy is measured as the rank of the correct identification returned by the identification process. The identification process will return a set of identities in a short order. The identity with the highest similarity score with the owner of the fingerprint in question will be ranked at the top of the list. The next identity on the list will have a similarity score less than that of the identity listed above.

Results and Discussion

First, the evaluation results of the CB-BCS identification processing time and accuracy are given. Next, the results of the double-CBs identification processing time and accuracy are presented. Last, a comparison of the two approaches is given.

CB-BCS Method

Table 1 shows the identification accuracy performance of the CB-BCS approach over all three conditions of the fingerprint images of the Neuro data set and the FVC data set. The identification accuracy is the ratio of the correct identity over the total number of identities to be measured. The result shows that the CB-BCS approach performs well on the Neuro data set in comparison with that of the FVC data set. The identification accuracy ranges from approximately 73-100%. The CB-BCS approach has problems with the rotation of the fingerprint images on both data sets, especially the FVC data set. The identification processing time of the CB-BCS approach is approximately 12.62 sec. Therefore, the identification processing time of the CB-BCS approach is still practical for the real emergency situation.

Table 1: The identification accuracy performance of the CB-BCS approach

	Identification accuracy (%)				
	FVC data set				
Data	Rank1	Rank2	Rank3	Rank4	Rank5
B-70	82.46	82.46	82.46	82.46	82.46
B+35	87.72	87.72	87.72	87.72	87.72
CW5	73.68	77.19	77.19	77.19	77.19
CW10	73.68	75.44	75.44	75.44	75.44
CC5	82.46	84.21	84.21	84.21	84.21
CC10	80.70	80.70	80.70	80.70	80.70
	Neuro data set				
Data	Rank1	Rank2	Rank3	Rank4	Rank5
B-70	100.00	100.00	100.00	100.00	100.00
B+35	98.08	98.08	98.08	98.08	98.08
CW5	90.38	90.38	90.38	90.38	90.38
CW10	88.46	88.46	88.46	88.46	88.46
CC5	84.62	84.62	84.62	84.62	84.62
CC10	84.62	84.62	84.62	84.62	86.54

Table 2: The identification accuracy performance of the double-CBs approach

	Identification accuracy (%)				
	FVC data set				
Data	Rank1	Rank2	Rank3	Rank4	Rank5
B-70	89.47	89.47	89.47	89.47	89.47
B+35	92.98	92.98	92.98	92.98	92.98
CW5	96.49	96.49	96.49	96.49	96.49
CW10	91.23	91.23	91.23	91.23	92.98
CC5	96.49	96.49	96.49	96.49	96.49
CC10	98.25	98.25	98.25	98.25	98.25
	Neuro data set				
Data	Rank1	Rank2	Rank3	Rank4	Rank5
B-70	100.00	100.00	100.00	100.00	100.00
B+35	100.00	100.00	100.00	100.00	100.00
CW5	100.00	100.00	100.00	100.00	100.00
CW10	100.00	100.00	100.00	100.00	100.00
CC5	100.00	100.00	100.00	100.00	100.00
CC10	100.00	100.00	100.00	100.00	100.00

Double-CBs Method

Table 2 shows the identification accuracy performance of the double-CBs approach over all three conditions of the fingerprint images of the Neuro data set and the FVC data set. The result shows that the Double-CBs approach performs well on the Neuro data set in comparison with that of the FVC data set. The identification accuracy ranges from approximately 89-96% for the FVC data set while the Double-CBs approach gets 100% identification accuracy on the Neuro data set. Unlike the CB-BCS approach, the Double-CBs approach has problems with the wet fingerprints (B-70) with an identification accuracy of 89.47% at rank 1 on the FVC data set. For the rotation of fingerprint images, the double-CBs approach provides an identification accuracy of 91-98% at rank 1 on the FVC data set. The identification processing time of the double-CBs approach is approximately 2.61 sec. Therefore, the processing time of the double-CBs approach is still practical for the real emergency.

Processing Time Comparison

The processing time of the two identification approaches is measured to investigate the use of both approaches under a real emergency situation. The overall identification times shown in this section are measured under the local network infrastructure. Figure 7 shows the identification processing time of both approaches on various ranks. The characteristic of CB-BCS identification time is growing up linearly to the numbers of candidates generated by the CB, while the double-CBs identification time is constant. A key factor to describe the significant difference is that the CB-BCS approach is based on the BCS. The BCS needs the fingerprint data as input for the identification process so it must be performed at the client side (CM).

Identification Accuracy Comparison

The identification accuracy of the double-CBs approach is higher than that of the CB-BCS approach on all conditions and all data sets. The CB-BCS approach provides a higher accuracy on the dry and wet fingerprints in comparison with that on the disoriented fingerprints. That means the victim's fingerprint that is rotated during the emergency staff collection time will affect the identification accuracy of the CB-BCS approach significantly. Unlike the CB-BCS approach, the double-CBS approach has an issue with the wet fingerprint image on the FVC data set. For the performance on the remaining conditions on the FVC data set, the double-CBs approach achieves the identification accuracy of 91-98% at rank 1 and the double-CBs approach performs well on the Neuro data set on all conditions.

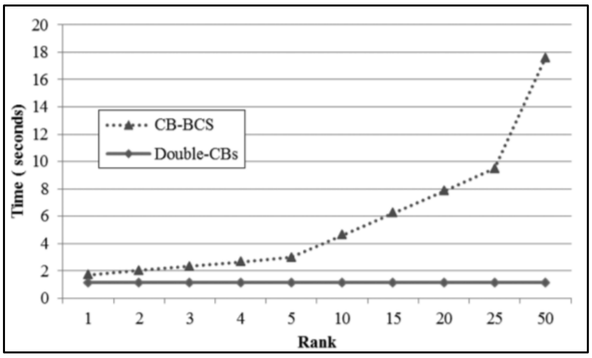

Fig. 7: The identification processing time of both approaches on various ranks

Security Concerns

The proposed method is evaluated against three attack scenarios including stealing the original fingerprints during the PHR user identification process, collecting the identity-related information during the identification process to perform illegal access to the PHRs and the PHR identity exposure.

The first attack scenario is related to the fingerprint stolen attack. There are two actions for an adversary to steal the original fingerprints. The first action is to grab the original fingerprints from the inner storage of the client machine. The emergency staff may be the adversary in this case and the staff may be authorized to access the inner storage when he/she is authorized to use CM. Under the double-CBs approach, the original fingerprints F1 and F2 are collected from a reader and instantly transformed into the irreversible form CB1 and CB2 by the CM without any caching of both F1 and F2. The adversary would get nothing from the client machine's inner storage. Meanwhile, the second action for getting the original fingerprint is to collect multiple irreversible forms to recover the original fingerprint. As the well-known attack, namely attack via record multiplicity (Patel *et al.*, 2015), the original fingerprint can be approximately reconstructed if the adversary knows the system parameter and collects multiple irreversible forms that are generated from a single fingerprint. As CB1 and CB2 are generated from different fingerprints, both irreversible forms are not colluded for performing the attack via record multiplicity. For these reasons, fingerprint-stolen attacks can be prevented.

In the second attack scenario, the identity-related information during the PHR user identification process may be collected to perform illegal access to the PHR later. An adversary can be the dishonest/fake staff so that two irreversible forms CB1 and CB2 can be collected by the adversary. The Double-CBs approach applies the access token issued from the ED to request the identification process from the EmS. The valid time of the token can enforce a period using CB1 and CB2. Moreover, the transaction logs in the auditing server record all activities. This way, illegal access to the PHRs is prevented.

In the third attack scenario, the CB-BCS approach suffers from identity exposure when an adversary collects the candidate list and then uses the CM to leverage the PHR user identifier. If the adversary is the emergency staff, the adversary can collect the candidate list. The adversary inputs the candidate list to the BCS module inside the CM twice. Then, the adversary obtains two identity lists. According to the BCS module, the correct identity is still the same when decoding the second time, while the incorrect identities are different. As a result, the adversary can see the same identity between both lists. This way, the PHR user identity is exposed. In contrast, the Double-CBs approach can manage the identity exposure issue. The CM generates two irreversible forms, sends both data to be identified by the IdS and obtains the victim PHRs. No identity-related information is returned from the IdS during the identification process.

Conclusion

According to the experimental results, it can be concluded that the proposed double-CBs approach has a higher potential to be used for identifying the PHR user during an emergency than the previously proposed CB-BCS approach. The identification processing time of the double-CBs approach takes approximately 5 times less than that of the CB-BCS approach, while the identification accuracy of the double-CBs approach on the Neuro data set is 100% on all conditions. For the FVC data set, both the CB-BCS approach and double-CBs approach cannot achieve 100% accuracy, but the Double-CBs approach achieves 89-98% accuracy while the CB-BCS approach achieves only 73-87% accuracy. The CB-BCS approach has issues in identifying the rotated fingerprint images while the double-CBs approach has issues in identifying the wet fingerprint images.

Acknowledgment

Authors would like to acknowledge the researchers (Maltoni *et al*., 2001; 2002; 2003; Neurotechnology, 2024; BIT, 2010). We collected the fingerprint images and made them available to the research community.

Funding Information

This study was supported by the higher education research promotion and national research university project of Thailand, office of the higher education commission under funding no. MED540548S at prince of Songkla University.

Author’s Contributions

Pariwat Choosang: Developed the code, conducted the experiments, analyzed the results, drafted the method section and produced the graphs and tables of the results.

Sangsuree Vasupongayya: Designed the experiments, analyzed the results and findings, drafted the introduction, result and discussion and conclusion sections, edited the method section and communicated with the publisher.

Kitsiri Chochiang: Analyzed the results, drafted and edited the material section.

Ethics

There is no ethical issue in this study because the prototype has not yet been tested on human subjects. The model is proposed based on the freely available fingerprint data sets.

References

Alanazi, A., Alanazi, M., & Aldosari, B. (2023). Personal Health Record (PHR) experience and recommendations for a transformation in Saudi Arabia. *Journal of Personalized Medicine*, *13*(8), 1275. https://doi.org/10.3390/jpm13081275

BIT. (2010). Institute of Automation, Chinese Academy of Sciences CASIA. Fingerprint Image Database Version 5.0" http://biometrics.idealtest.org

Cappelli, R., Maio, D., Lumini, A., & Maltoni, D. (2007). Fingerprint image reconstruction from standard templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *29*(9), 1489-1503. https://doi.org/10.1109/TPAMI.2007.1087

Choosang, P., & Vasupongayya, S. (2015, November). Using fingerprints to identify personal health record users in an emergency situation. *In 2015 International Computer Science and Engineering Conference (ICSEC)*, (pp. 1-6). IEEE. https://doi.org/10.1109/ICSEC.2015.7401421

Fan, K., Huang, N., Wang, Y., Li, H., & Yang, Y. (2015, November). Secure and efficient personal health record scheme using attribute-based encryption. *In 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing* (pp. 111-114). IEEE. https://doi.org/10.1109/CSCloud.2015.40

Flores Zuniga, A. E., Win, K. T., & Susilo, W. (2010). Biometrics for electronic health records. *Journal of Medical Systems*, *34*, 975-983. https://doi.org/10.1007/s10916-009-9313-6

Huang, J., Sharaf, M., & Huang, C. T. (2012, September). A hierarchical framework for secure and scalable EHR sharing and access control in multi-cloud. *In 2012 41st International Conference on Parallel Processing Workshops*, (pp. 279-287). IEEE. https://doi.org/10.1109/ICPPW.2012.42

Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2012). Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *IEEE Transactions on Parallel and Distributed Systems*, *24*(1), 131-143. https://doi.org/10.1109/TPDS.2012.97

Maltoni, D. Maio, D. Jain, A. K. & Prabhakar, S. (2001). FVC2000. Fingerprint Verification competition. http://bias.csr.unibo.it/fvc2000

Maltoni, D. Maio, D. Jain, A. K. & Prabhakar, S. (2002). FVC2002. Fingerprint Verification competition. http://bias.csr.unibo.it/fvc2002

Maltoni, D. Maio, D. Jain, A. K. & Prabhakar, S. (2003). FVC2004. Fingerprint Verification competition (811-814). http://bias.csr.unibo.it/fvc2004

Marohn, D. (2006). Biometrics in healthcare. *Biometric Technology Today*, *14*(9), 9-11. https://doi.org/10.1016/S0969-4765(06)70592-6

Mon, E. E., Vasupongayya, S., Karnjanadecha, M., & Angchuan, T. (2019). Evaluating biometrics fingerprint template protection for an emergency situation. *Tehnički glasnik*, *13*(4), 280-285. https://doi.org/10.31803/tg-20191104190328

Neurotechnology. (2024). Sample fingerprint databases. http://www.neurotechnology.com/download.html

Park, Y., & Yoon, H. J. (2020). Understanding personal health record and facilitating its market. *Healthcare Informatics Research*, *26*(3), 248. https://doi.org/10.4258/hir.2020.26.3.248

Patel, V. M., Ratha, N. K., & Chellappa, R. (2015). Cancelable biometrics: A review. *IEEE Signal processing Magazine*, *32*(5), 54-65. https://doi.org/10.1109/MSP.2015.2434151

Pons, P. T., & Markovchick, V. J. (2002). Eight minutes or less: Does the ambulance response time guideline impact trauma patient outcome?. *The Journal of Emergency Medicine*, *23*(1), 43-48. https://doi.org/10.1016/S0736-4679(02)00460-2

Sieverink, F., Kelders, S., Braakman-Jansen, A., & van Gemert-Pijnen, J. (2019). Evaluating the implementation of a personal health record for chronic primary and secondary care: A mixed methods approach. *BMC Medical Informatics and Decision Making*, *19*, 1-12. https://doi.org/10.1186/s12911-019-0969-7

Song, Y. T., Hong, S., & Pak, J. (2015, June). Empowering patients using cloud based personal health record system. *In 2015 IEEE/ACIS 16th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, (pp. 1-6). IEEE. https://doi.org/10.1109/SNPD.2015.7176216

Tams, B., & Rathgeb, C. (2014, September). Towards efficient privacy-preserving two-stage identification for fingerprint-based biometric cryptosystems. *In IEEE International Joint Conference on Biometrics*, (pp. 1-8). IEEE. https://doi.org/10.1109/BTAS.2014.6996241

Tang, P. C., Ash, J. S., Bates, D. W., Overhage, J. M., & Sands, D. Z. (2006). Personal health records: Definitions, benefits and strategies for overcoming barriers to adoption. *Journal of the American Medical Informatics Association*, *13*(2), 121-126. https://doi.org/10.1197/jamia.M2025

Thummavet, P., & Vasupongayya, S. (2013, September). A novel personal health record system for handling emergency situations. *In 2013 International Computer Science and Engineering Conference (ICSEC)*, (pp. 266-271). IEEE. https://doi.org/10.1109/ICSEC.2013.6694791

Thummavet, P., & Vasupongayya, S. (2015). Privacy-preserving emergency access control for personal health records. *Maejo International Journal of Science and Technology*, *9*(1). https://doi.org/10.14456/mijst.2015.7

Wang, C., Liu, X., & Li, W. (2012, September). Implementing a personal health record cloud platform using ciphertext-policy attribute-based encryption. *In 2012 4th International Conference on Intelligent Networking and Collaborative Systems*, (pp. 8-14). IEEE. https://doi.org/10.1109/iNCoS.2012.65