IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-7, Special Issue-15, May 2019 E-ISSN: 2347-2693

Improved Sequential Fusion of Heart-signal and Fingerprint for Anti-spoofing

Radha N[1*], Kavya N[2], Harsha A C[3]

[1,2,3]Department of Computer Science and Engineering, East West Institute Of Technology, Bangalore, India.

DOI: https://doi.org/10.26438/ijcse/v7si15.226231 | Available online at: www.ijcseonline.org

Abstract— Biometrics is one of the most encouraging authentication systems in the recent years. However, spoof attack is one of the main problems with a biometric system. Spoof attack falls within a subset of what is called presentation attack. The heart is an emerging biometric modality which is getting attention for its robustness against presentation attacks. Introducing heart-signal into a fingerprint biometric system can yield promising results showing its robustness against spoof attacks with increasing the authentication accuracy. In this work, a sequential fusion method is improved for anti-spoofing capability. The idea behind the proposed system is the utilization of the natural liveness property of heart-biometrics in addition to boosting the heart-signal scores to increase the anti-spoofing of a multimodal biometric system. We have evaluated our proposed method with public databases of fingerprint biometric and heart-signal (ECG signal). The obtained results are very encouraging for the development of a robust anti-spoofing multimodal authentication system.

Keywords—Component, Formatting, Style, Styling, Insert (key words)

I. Introduction

Fingerprint is one of the most common biometric modalities used in practical applications. Extensive researches are done on fingerprint show that its authentication accuracy is very high [1, 2]. Fingerprint biometrics is widely used in many applications because of the availability of accurate, cheap and compact fingerprint scanners. One of the limitations of fingerprint biometric is its high vulnerability to presentation attacks [3], mainly in remote authentication applications [4]. Recently, it has been discovered that the heart-signal possesses essential biometric characteristics such as universality, permanence, and uniqueness, etc. [5-7].

Heart-signal is a description of the heart's electrical activity and can be captured in a non-invasive way from body's surface (e.g. fingers) for biometric applications [8, 9]. Heart-signal has additional biometric characteristics like liveness detection, robustness to spoof attacks, and continuous authentication over time [7]. These characteristics give the preference for using heart-signal biometric over traditional biometrics. Furthermore, due to the crucial location of the heart in the structure of the body, it has a very high potentiality to be used as a secured biometric modality. Several researchers worked on the fusion of heart-signal with other biometrics mainly fingerprint as a mean to improve the performance and security (robustness against presentation attacks) of the biometric system [10-15].

Many advantages can be gained by introducing heart-signal into a multimodal biometric system. As we mentioned before, heart biometrics provides natural property for liveness detection and robustness against presentation attacks. Hence, fingerprint scanner and heart-signal reader that are integrated into one compact device would be a secure and accurate authentication system [16]. This integration between fingerprint and heart-signal can have a major impact on the improvement of the remote authentication systems [4].

Presentation attack is the presentation of an artefact or of human characteristics to a biometric capture subsystem in a fashion intended to interfere with system policy [17]. When artificial or synthetic materials are used to forge a fake biometric characteristic, it has been more commonly called spoof attack. A spoof attack is one of the most common attacks on the biometric authentication systems [18]. The automated process for determining a presentation attack is called presentation attack detection (PAD) [17], it can be also called anti-spoofing. In another word, anti-spoofing in the multimodal biometric system is the ability to protect the system from hacking by detecting and discarding the spoof attacks against one or more biometric modalities [19]. In this work, a multimodal biometric system is described combining heart-signal with fingerprint biometrics. We have proposed a method for improving sequential fusion method based on score level fusion. We have evaluated our proposed method with existing databases of fingerprint and heart-signal and observed that this system could improve the anti-spoofing of a multimodal biometric system together with maintaining a high authentication accuracy. This paper is organized as follows. In the next section, we outlined the related works. The proposed method is presented in the third section. Then the experiments are explained in the fourth section. The results are shown and discussed in the fifth section. Finally, the conclusions and future works are highlighted.

II. RELATED WORK

Many works focus on studying the security of the multimodal biometric systems against different kinds of attacks. These attacks can be grouped into two main classes: Indirect attacks and direct attacks (spoof attacks). Indirect attacks need the attacker to have knowledge about the internal system design and processes, which is out of our focus in this paper. While the direct attacks or spoof attacks can be made without such knowledge. There is a common belief that the multimodal biometric systems are intrinsically more robust against spoof attacks due to the assumption that in order to hack the system it is needed to spoof all the fused biometric modalities [20-22]. Many recent works have proved that this belief is incorrect [23-27]. They provided evidence that the multimodal biometric system can be hacked by successfully spoofing only one biometric modality; even the system has more than two fused biometric modalities. Thus, there is no benefit of fusing many biometric traits if this makes such system weaker especially if a very secure trait is fused with a weak trait. That will encourage the impostor to spoof the weak traits, which is enough to hack the whole system [23-26].

The authors in literature who studied the anti-spoofing in multimodal systems considered systems that fuse many different biometric modalities. They focused mainly on score level fusion methods, which is considered as one of the most common fusion methods because of the ease of access and combination of multiple modalities with preserving rich information about fused modalities [22]. They used different matching score fusion methods: weighted sum, likelihood ratio, and fuzzy logic. In [23, 24],a modification of an exciting score fusion methods is done, where the authors suggested an extension to LLR by utilizing an auxiliary information about the security of each fused modality. A new way for choosing the operating point is proposed in [25]. In [27], the authors integrated liveness detection algorithm with the fusion mechanism. Although most of these works focused on parallel score fusion methods (e.g. weighted sum), sequential fusion methods are also studied [11, 28].

The author of [11] proposed a score fusion algorithm for the multimodal system that fuses heart-signal with fingerprint biometrics modalities in a sequential way. They put heart-signal matcher as a first stage, and the authenticated subjects by heart-signal were asked to provide their fingerprint to be authenticated by fingerprint matcher. In the final stage, parallel score fusion was applied, where user-weighting score fusion method was used. Figure 1 illustrates the block diagram of this sequential fusion method.

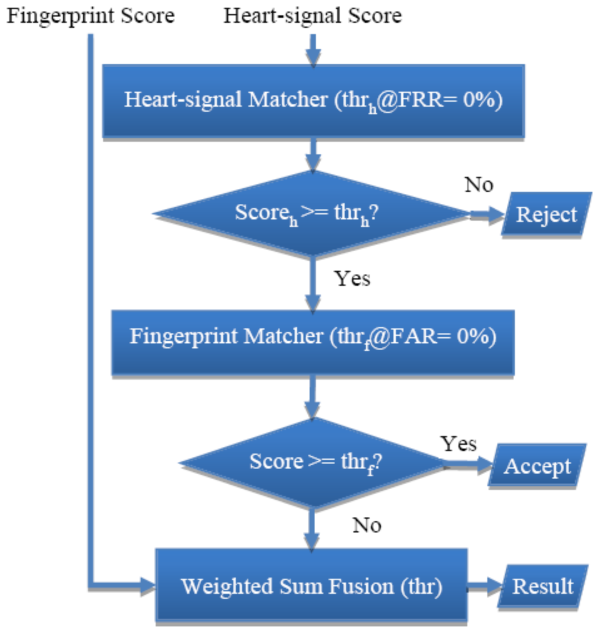

Fingerprint Score
Heart-signal Score
Heart-signal Matcher (thr_h@FRR= 0%)
$Score_h >= thr_h$?
No
Reject
Yes
Fingerprint Matcher (thr_f@FAR= 0%)
Score >= thr_f?
Yes
Accept
No
Weighted Sum Fusion (thr)
Result

Figure 1: Block diagram of sequential method

The results of this system show good authentication performance i.e. *EER* (*equal error rate*) is less than 1%. The authors of this work supposed that their method can be considered as good anti-spoofing measure, but they did not test it under spoof attacks scenario. However, consider the spoof attacks scenario, i.e. fingerprint modality is spoofed, which leads to increase the chance of falsely accepting spoofed subjects by fingerprint matcher. Therefore, this method is not robust against spoof attacks as will be shown later in this paper.

- **The improved sequential fusion method**

In this work, we present a multimodal biometric system by using sequential fusion method of heart-signal and fingerprint. The fusion is aimed to improve the anti-spoofing of the multimodal biometric system with preserving high authentication accuracy. In the proposed system, we use the liveness property of heart-signal to increase the anti-spoofing of the multimodal biometric system, in addition to limiting the fingerprint modality from having a significant role in falsely authorizing spoofed subjects. This is achieved in three main steps. First, we use heart-signal as a primary matcher to ensure that the accepted score is coming from alive subject, which means it has a bigger chance to be genuine. Second, applying a boosting process on the accepted heart-signal scores, where the heart-signal score is increased before fusing it with fingerprint score. Last, we used weighted sum fusion rule in a way that gives higher weight to heart-signal scores and lower weight to fingerprint score. We discard fingerprint as independent matcher in the sequential method [11], in order to limit its impact of falsely accepting spoofed subjects, instead, we only use it in the weighted sum fusion rule. In this way, we ensure that most attempts to hack the multimodal by spoofing the fingerprint will be detected and rejected. Figure 2 shows the different steps of our proposed method.

A. Authentication with heart-signal

In the first stage of our proposed method, heart-signaL matcher is applied with a specific threshold 1 *thr* . This threshold is at *zeroFRR* of heart-signal (@ 0% *h FRR*). Thus we are sure that no genuine subject will be rejected as an impostor. In this stage, we are implicitly utilizing the liveness property of heart-signal to guarantee that the accepted subjects are alive.

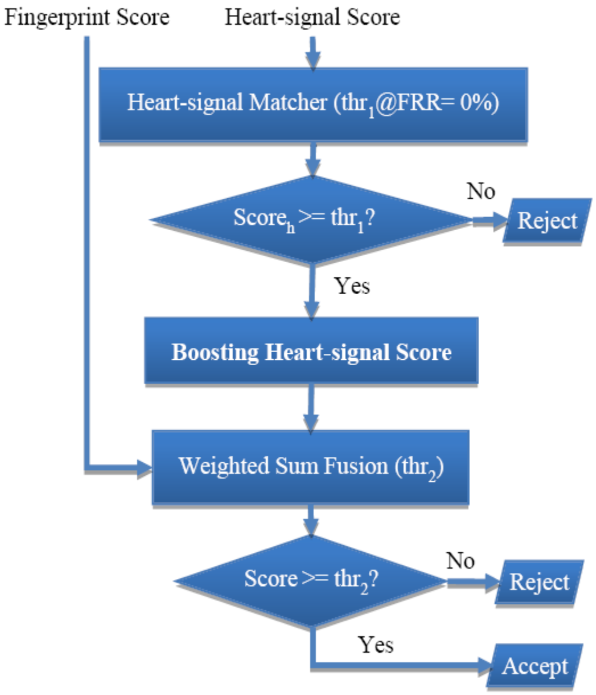


Figure 2: The proposed method

B. Heart-signal score boosting

In the boosting stage, the heart-signal scores are increased proportionally with its difference of the *zeroFRR* threshold 1 *thr* of heart-signal matcher according to (1). The increased amount of heart-signal score is a score-dependent value.

$$s_h^{new} = s_h(1 + s_h - thr_1) \qquad (1)$$

Where s_h and s_h^{new} are the values of the heart-signal score before and after boosting respectively, 1 *thr* is the threshold of heart-signal matcher at which there is no genuine score is wrongly rejected. The idea behind the boosting process of the heart-signal score is to increase its share in the weighted sum fusion rule.

C. Parallel score fusion

The parallel score fusion is based on weighted sum fusion rule. The fusion of scores required that these scores are normalized. We used a common normalization technique called min-max normalization, where all scores are transferred in the range [0, 1]. Equation (2) shows the formula of weighted sum fusion rule.

$$s = w_h s_h + w_f s_f \qquad (2)$$

Where *h s* and *f s* are the scores for heart-signal and fingerprint modalities, and *h w* and *f w* are their weights respectively. In the literature, several techniques are used to calculate these weights of fused matching score in the weighted sum fusion method. One of the common methods to compute these weights is using d-prime measure also known as decidability measure. The d-prime measure is used to compute how much two different distributions are separated [29]. The formula of d-prime measure is shown in (3).

$$d' = \frac{|\mu_1 - \mu_2|}{\sqrt{\frac{1}{2}\left(\delta_1^2 - \delta_2^2\right)}} \qquad (3)$$

For a multimodal biometric system with N biometric modality (in our experiments N=2), the d-prime weight for the *th k* modality is shown in (4). We consider that the weights are proportional to the d-prime value for the respective modality.

$$W_k = \frac{d'_k}{\sum_{i=1}^{2} d'_i} \qquad (4)$$

The threshold 2 *thr* at which weighted sum rule will be applied is calculated during the training phase. This threshold can be calculated under many training scenarios (e.g. spoofed training scenario).

- **Datasets and experiments**

In this section, we explain the datasets and the experimental procedure we used to test and evaluate the proposed improved-sequential method. In this research, a virtual multimodal dataset is constructed and used for evaluation. The virtual dataset is composed of two public-domain datasets for fingerprint and heart-signal. The fingerprint dataset is DB1_A which is provided by FVC2004 [30]. This dataset consists of 100 subjects with eight samples for each subject. Therefore, there are in total 800 fingerprint samples.

In the literature, there are many researches on fingerprint regarding features extraction and matching algorithms [2]. In our work, we used an algorithm proposed by [31-34], which based on Minutiae Cylinder-Code (MCC). This algorithm is considered as one of the most accurate algorithms in the state-of-the-art. For heart-signal dataset, we used 100 ECG records of sixty-seconds each obtained from one hundred different persons selected from PTB (Physikalisch-Technische Bundesanstalt) dataset [35] as listed in [36]. Authors in [37] divided each record into four segments and extracted heartbeat shape (HBS) feature. During this work we are interested in developing a robust matching score method against spoof attacks, thus we do not focus about the details of the matching algorithms for both heart-signal and fingerprint.

A. Virtual multimodal dataset

The heart-signal dataset has only four samples for each subject; thus we consider only four samples for each subject in the fingerprint dataset (the first four samples). In the virtual multimodal dataset, we randomly assigned one subject from the heart-signal dataset to a subject from the fingerprint dataset. Subsequently, a virtual multimodal dataset composed of 100 virtual subjects is formed, each has four heart-signal samples and four fingerprint samples.

B. Spoofed multimodal dataset

As mentioned earlier, that fingerprint modality is much vulnerable to spoof attacks, in contrast to heart-signal modality. For that, our experiments aimed to test the anti-spoofing of the proposed system under spoof attacks against fingerprint modality. We simulated the spoof attacks by considering that the distribution of spoof attack scores is identical to the genuine scores distribution. Thus we replace each fingerprint impostor score in the virtual subject by genuine score of the same subject. This protocol is the same protocol followed in many works in the literature [23-25, 27].

C. Experiment procedure

Our experimental protocol is composed of two phases: training and test. Cross validation method will be used to achieve the training and testing, and the average results will be reported. During the experiments, we considered that one sample of each subject is a gallery template and the other three samples are probe templates. Then we compared each gallery template with the 300 (100□3) probe templates. That means we have in total 30000 matching scores (300 genuine scores and 29700 impostor scores). These scores were divided into three sets, one for the training and two for the test.

□ Training phase: In this phase, the scores resultant from comparing the gallery template with only one probe template (100 genuine scores and 9900 impostor scores) are considered. We did the training phase using spoofed multimodal dataset (spoofed training scenario). In this phase, we calculated the threshold 2 *thr* that is used in the weighted sum stage during the test phase. This threshold was computed based on *spoof equal error rate EERspoof* of weighted sum fusion rule, which is calculated using spoofed multimodal dataset. *EERspoof* is the value where *false rejection rate FRR* equals *Impostor Attack Presentation match rate IAPMR.*

□ Test phase: In this phase, we considered the other two probe templates (different from that used in training) for each test set. Thus there are two training sets with 100 genuine scores and 9900 impostor scores in each. We did the test phase under two scenarios; under spoof attacks scenario, where spoofed multimodal dataset are applied and without spoof attacks scenario (licit scenario) [38]. In the first scenario the anti-spoofing performace is measurced by calculating *IAPMR* and *FRR*, while in the later scenario the authentication accuracy are measured by calculating *False accept rate FAR* and *FRR*.

This experiment was repeated three rounds, in each a different probe is used for training. Then the average of the performance measures is calculated.

D. Performance measure

Evaluating a biometric authentication system with considering presentation attacks detection involves measuring three main metrics: *False accept rate FAR, False reject rate FRR, and Impostor Attack Presentation match rate IAPMR* [39, 40]. *Impostor Attack Presentation match rate* is the proportion of impostor attack presentations in which the target reference is matched, in another word, the proportion of the wrongly authenticating spoof attacks. We evaluated the performance of the improved-sequential system using a measure called *half total error rate HTER* .

$$HTER = \frac{FRR + FAR}{2} \qquad (5)$$

The idea behind using *HTER* is that in such sequential systems, it is hard to calculate *EER* for the whole system, Where we can get only one value for each error rate (*FAR* and *FRR*). When we are testing under spoof attacks scenario, then we use the *HTERspoof* which gives the relation between *FRR* and *IAPMR.*

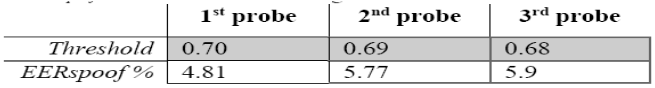
$$HTER_{spoof} = \frac{FRR + IAPMR}{2} \qquad (6)$$

III. RESULTS & ANALYSIS

As mentioned in the previous section, we trained the system using spoofed multimodal dataset. The training phase aims to

compute the threshold 2 *thr* , which is used in the last stage of the improved-sequential system (weighted sum stage). This threshold is computed based on the best *E Rspoof* achieved when applying weighted sum fusion rule (directly without applying heart-signal as a first stage) to fuse heart-signal scores with spoofed fingerprint scores.
Table 1 shows the thresholds for different training rounds.

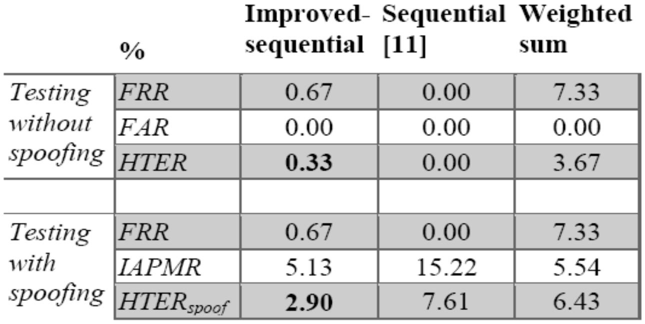
Table 1. Training results: The thresholds that achieve best *ERRspoof* for each round of training.



	1st probe	2nd probe	3rd probe
Threshold	0.70	0.69	0.68
EERspoof %	4.81	5.77	5.9

In the testing phase, we applied the thresholds we got from training phase as listed in Table 1, on the last stage in the proposed system. In Table 2, the average values of *FRR*, *IAPMR*/*FAR*, and *HTER* are listed for the proposed system vs. the other two existing systems: the sequential method [11] and weighted sum method. The testing phase is done with two scenarios, licit scenario and under spoof attacks against fingerprint biometric scenario. The presented results in Table 2, shows that the improved-sequential system is more robust against spoofing fingerprint compared to the sequential method [11] and weighted sum method. Our system achieves the best *IAPMR* =5.13% which can be considered as significant improvement comparing to 15.22% for sequential method [11]. Although *IAPMR* in the proposed is similar to what achieved in the weighted sum, however in the weighted sum method, *FRR* is very high. The proposed method gives good anti-spoofing performance, and in the same time, it gives high performance in case of absence of spoof attacks. Even though the method in [11] is more accurate if there are no spoof attacks, but it failed under spoof attacks scenario, when our system successes.

Table 2. Test Results: Performance measures *FRR* vs. *IAPMR*/*FAR* vs. *HTERspoof* /*HTER*.
Comparing the improved-sequential method with other methods.



	%	Improved-sequential	Sequential [11]	Weighted sum
Testing without spoofing	*FRR*	0.67	0.00	7.33
	FAR	0.00	0.00	0.00
	HTER	**0.33**	0.00	3.67
Testing with spoofing	*FRR*	0.67	0.00	7.33
	IAPMR	5.13	15.22	5.54
	HTER$_{spoof}$	**2.90**	7.61	6.43

The results of *HTER* in our proposed system compared with the other method are shown in Figure 3. This measure gives a clear indication that the proposed system outperforms the other under spoof attacks, *HTERspoof* =2.9% while it is 7.6% and 6.43% in sequential and weighted sum methods respectively. Although in case there are no spoof attacks, the improved sequential system achieves very high authentication accuracy *HTER* =0.3% which is a little bit worse than sequential method *HTER* =0%.

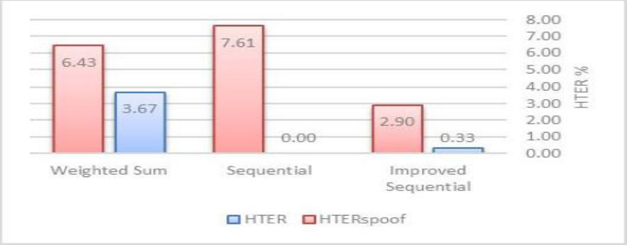


Figure 3: Test results: Comparing *HTERspoof* /*HTER* between the three methods under the two test scenarios

IV. CONCLUSION

Our contribution in this research is proposing a robust anti-spoofing multimodal biometric system. The proposed system is based on the assumption that heart-signal is secure and difficult to be spoofed in contrast with the vulnerability of fingerprint. The proposed system shows higher performance against spoofing of the fingerprint modality, and it outperforms the other compared methods. Also, it gives high authentication accuracy in case of there is no spoof attacks.
The obtained results encourage the idea of developing an integrated heart-signal and fingerprint-based biometric system, which can be very accurate and very robust against spoof attacks, taking the advantage of liveness property of Figure 3: Test results: Comparing *HTERspoof /HTER* between the three methods under the two test scenarios heart-signal biometrics and the high accuracy of the fingerprint biometrics. Moreover, this integrated system can be user-friendly and acceptable, since this two biometrics can be captured from fingers simultaneously. Many works to be done as future improvements for the proposed system. First, improving the way of choosing the weighted sum threshold. Second, adding new criteria to choose the heart-signal threshold in the first stage instead of using fixed threshold (*zeroFRR* threshold). Third, improving the criteria of boosting heart-signal scores. These improvements aim to reduce both *IAPMR/FAR* and *FRR* for the system and therefore to improve *HTERspoof*/*HTER*. Other aspects for future improvements is implementing multimodal system consisting of more than two modalities or using a different fusion method in the last stage of the system instead of weighted sum.

REFERENCES

[1] A. K. Jain and A. Kumar, "Biometric Recognition: An Overview," in *Second Generation Biometrics: The Ethical, Legal and Social*

Context, E. Mordini and D. Tzovaras, Eds., ed: Springer Netherlands, 2012, pp. 49-79.

[2] F. Alonso-Fernandez, J. Bigun, J. Fierrez, H.Fronthaler, K. Kollreider, and J. Ortega-Garcia, "Fingerprint recognition," in *Guide to biometric reference systems and performance evaluation*, ed: Springer, 2009, pp. 51-88.

[3] E. Marasco and A. Ross, "A survey on antispoofing schemes for fingerprint recognition systems," *ACM Computing Surveys (CSUR)*, vol. 47, p. 28, 2015.

[4] M. S. Islam, "Heartbeat Biometrics for Remote Authentication Using Sensor Embedded Computing Devices," *International Journal of Distributed Sensor Networks*, vol. 2015, p. e549134, 2015/01/29/ 2015.

[5] L. Biel, O. Pettersson, L. Philipson, and P. Wide, "ECG analysis: a new approach in human identification," *Instrumentation and Measurement, IEEE Transactions on*, vol. 50, pp. 808-812, 2001 2001.

[6] S. A. Israel, J. M. Irvine, B. K. Wiederhold, and M. D. Wiederhold, *The heartbeat: the living biometric*: Wiley-IEEE Press, New York, NY, USA, 2009.

[7] F. Agrafioti, D. Hatzinakos, and J. Gao, *Heart biometrics: Theory, methods and applications*: INTECH Open Access Publisher, 2011.

[8] M. S. Islam and N. Alajlan, "Biometric template extraction from a heartbeat signal captured from fingers," *Multimedia Tools and Applications*, vol. doi: 10.1007/s11042-016-3694-6, 2016.

[9] A. Lourenço, H. Silva, and A. Fred, "Unveiling the biometric potential of Finger-Based ECG signals,"*Computational intelligence and neuroscience*, vol. 2011, p. 5, 2011 2011.

[10] R. M. Jomaa, M. S. Islam, and H. Mathkour, "Enhancing the information content of fingerprint biometrics with heartbeat signal," in *Computer Networks and Information Security (WSCNIS), 2015 World Symposium on*, 2015, pp. 1-5.

[11] S. Pouryayevali, "ECG Biometrics: New Algorithm and Multimodal Biometric System," Master Thesis, Graduate Department of Electrical and Computer Engineering, University of Toronto, 2015.

[12] N. Alajlan, M. S. Islam, and N. Ammour, "Fusion of fingerprint and heartbeat biometrics using fuzzy adaptive genetic algorithm," 2013, pp. 76-81.

[13] S. A. Israel, W. T. Scruggs, W. J. Worek, and J. M. Irvine, "Fusing face and ECG for personal identifica ion," 2003, pp. 226-231.

[14] Y. N. Singh, S. K. Singh, and P. Gupta, "Fusion of electrocardiogram with unobtrusive biometrics: An efficient individual authentication system," *Pattern Recognition Letters*, vol. 33, pp. 1932-1941, 2012 2012.

[15] M. D. Bugdol and A. W. Mitas, "Multimodal biometric system combining ECG and sound signals," *Pattern Recognition Letters*, vol. 38, pp. 107-112, 2014 2014.

[16] C. Zhao, T. Wysocki, F. Agrafioti, and D. Hatzinakos, "Securing handheld devices and fingerprint readers with ECG biometrics," 2012, pp. 150-155.

[17] I. I. Standard, "Information technology – Biometric presentation attack detection -- Part 1: Framework," ed, 2016.

[18] A. K. Jain, K. Nandakumar, and A. Ross, "50 years of biometric research: Accomplishments, challenges, and opportunities," *Pattern Recognition Letters*, vol. 79, pp. 80-105, 2016.

[19] G. Fumera, G. L. Marcialis, B. Biggio, F. Roli, and S. C. Schuckers, "Multimodal Anti-spoofing in Biometric Recognition Systems," in *Handbook of Biometric Anti-Spoofing: Trusted Biometrics under Spoofing Attacks*, S. Marcel, M. S. Nixon, and S. Z. Li, Eds., ed London: Springer London, 2014, pp. 165-184.

[20] C. A. Shoniregun and S. Crosier, *Securing biometrics applications*: Springer, 2008.

[21] M. Tistarelli, S. Z. Li, and R. Chellappa, *Handbook of remote biometrics* vol. 1: Springer, 2009.

[22] A. A. Ross, K. Nandakumar, and A. K. Jain, *Handbook of multibiometrics* vol. 6: Springer, 2006.

[23] R. N. Rodrigues, N. Kamat, and V. Govindaraju, "Evaluation of biometric spoofing in a multimodal system," 2010, pp. 1-5.

[24] R. N. Rodrigues, L. L. Ling, and V. Govindaraju, "Robustness of multimodal biometric fusion methods against spoof attacks," *Journal of Visual Languages & Computing*, vol. 20, pp. 169-179, 2009 2009.

[25] P. A. Johnson, B. Tan, and S. Schuckers, "Multimodal fusion vulnerability to non-zero effort (spoof) imposters," in *2010 IEEE International Workshop on Information Forensics and Security*, 2010, pp. 1-5.

Authors Profile

Mr. C T Lin pursed Bachelor of Science from University of Taiwan, Taiwan in 2006 and Master of Science from Osmania University in year 2009. He is currently pursuing Ph.D. and currently working as Assistant Professor in Department of Computational Sciences, Department of Electronic and Communication, University of Taiwan, Taiwan since 2012. He is a member of IEEE & IEEE computer society since 2013, a life member of the ISROSET since 2013, ACM since 2011. He has published more than 20 research papers in reputed international journals including Thomson Reuters (SCI & Web of Science) and conferences including IEEE and it's also available online. His main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy, Big Data Analytics, Data Mining, IoT and Computational Intelligence based education. He has 5 years of teaching experience and 4 years of Research Experience.

Mr C H Lin pursed Bachelor of Science and Master of Science from University of New York, USA in year 2009. He is currently pursuing Ph.D. and currently working as Assistant Professor in Department of Telecommunication, University of New York, USA since 2012. He is a member of IEEE & IEEE computer society since 2013, a life member of the ISROSET since 2013 and ACM since 2011. He has published more than 20 research papers in reputed international journals including Thomson Reuters (SCI & Web of Science) and conferences including IEEE and it's also available online. His main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy, Big Data Analytics, Data Mining, IoT and Computational Intelligence based education. He has 5 years of teaching experience and 4 years of Research Experience.