I.J. Education and Management Engineering, **2017, 4, 29-40**
Published Online July 2017 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijeme.2017.04.04

Available online at http://www.mecs-press.net/ijeme

Evaluation of Voice & Ear Biometrics Authentication System

Safiia Mohammed [a], Michael Hegarty [b]

[a] *M.Sc Graduate, Institute of Technology Blanchardstown, Khartoum, Sudan*
[b] *Lecturer, Institute of Technology Blanchardstown, Dublin, Ireland*

Abstract

The core aim of biometrics authentication methods and technologies is to solve issues and concerns existing in traditional authentication methods like passwords, PIN numbers or identity cards. The Most important concern for business sectors and organizations is to authenticate individuals who interact with them and their services. By considering more than one biometric technology, the authentication process is expected to be more reliable and secure. The Ear and Voice Multimodal Biometrics System is evaluated to compare its performance with ear and voice unimodal systems; the multimodal system takes advantages of the permanence characteristic of ear biometric and voice biometric which is highly acceptable by users. According to the experiment, the ear and voice multimodal system provides better performance than the ear or voice unimodal system. In addition to that, the multimodal system makes a right balance between false rejection and false acceptance rates. This evaluation is intended to contribute to multimodal biometrics research by using behavioral biometric (voice print) and physiological biometric (ear-print) and makes advantage of using both of them in one system.

Index Terms: Multimodal Biometric System, Ear Biometric, Voice Biometric, Biometric Authentication.

1. Introduction

Biometrics authentication technologies are moving towards identification and verification of the individuals with something that describes the human physiologically or behaviorally, For instance: DNA, Face, Iris, Retina, Ear, Hand geometry and fingerprint are examples of physiological parts of the human whereas, voice, gait, signature and keystroke are measures of human behavior or action. Comparing with traditional authentication methods like passwords, PIN numbers (i.e. something that you know or remember) and identity cards (i.e. something that you have), Biometric authentication depends on asking a question like ‘who you are?' to identify the individual identity. Physiological and behavioral human biometrics should answer this question. As illustrated in Fig.1 bellow, the biometrics systems -in general- have four main components: (1) sensor (2) feature extraction (3) matching and (4) database. Sensors play the role of the user interface to collect raw

* Corresponding author.
E-mail address: Safiia.mohammed@yandex.com, Michael.Hegarty@itb.ie

biometric data from users, then the features of biometric traits are extracted from the raw data and stored in the databases as well as other personal information (e.g. Subject ID, Name ..., etc.). Depending on which biometrics technology uses, some enhancement steps are done to the raw biometrics data to reduce its noise and extract unique features. To verify individuals, their extracted features compared to data that is already stored in the databases and then the decision made depends on the result of the matching.

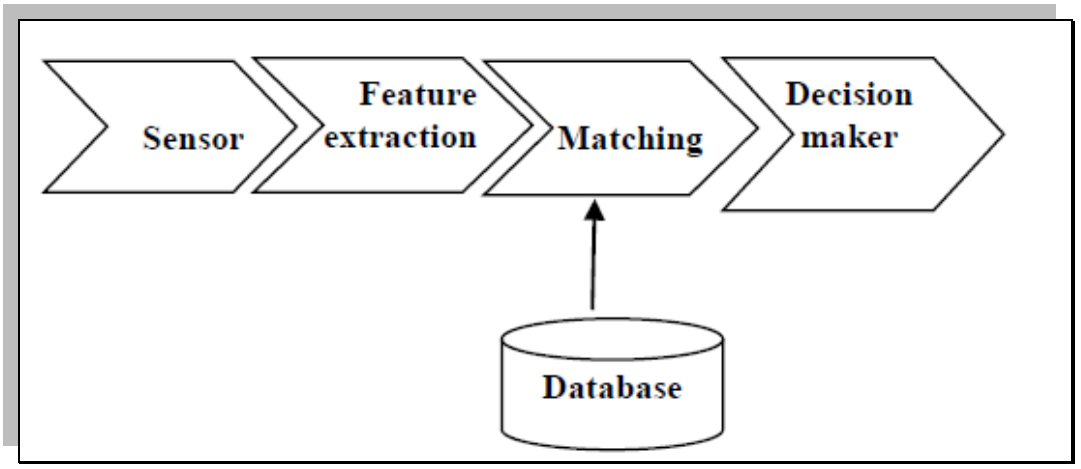

Fig.1. General Components of Biometrics System

1.1. Verification and Identification

The biometrics system has two main modes: verification and identification modes. In verification, the biometric system authenticates an individual who claims to be a particular person. The system performs a one-to-one comparison in the system database to verify the person. The system in verification attempts to answer the question "are you who you say you are?". On the other hand, identification mode identifies the person by conduct one-to-many comparisons to see whether the individual in the system database or not, identification answer the question "who are you?" [1].

2. Background

This section presents some background about unimodal and multimodal biometrics as well as ear and voice biometrics systems.

2.1. Unimodal Versus Multimodal biometrics systems

The unimodal or single biometric system is a system that depends on one biometric technology to identify and/or authenticate individuals. This kind of systems may face different challenges. From a security perspective, these systems are expected to be circumvented and exposed to spoof attacks more likely than a system that uses more than one biometric technology to authenticate the individuals (i.e. multimodal systems) as it is less challenging for imposters to bypass single biometric system. Another point to think about is the Intra-class variations which can be due to various uncontrolled factors during enrolment process; this causes a rejection of individuals even though they are genuine users. The level of variation, definitely, differs from biometric to another. However, it is better to use another biometrics to reduce these variations. By choosing multimodal biometrics, there will be an increase in population coverage, in particular, if one biometric has lower universality than the other [2]. Moreover, some single biometric systems have relatively high unacceptable

error rates, and that can be mitigated by using the multimodal systems too. Therefore multimodal biometrics systems can contribute to overcoming some limitations of unimodal biometric systems and to improve the performance of biometrics systems [3]. However, some issues should be taken into account when considering multimodal biometrics systems. Multimodal system storage requirements are higher compared to the unimodal systems as there are more than one biometrics traits to store, processing and computational times also expected to be longer [2]. Also, one of the important considerations either in unimodal or multimodal systems are the ethical and privacy issues. The person who consents to be authenticated by the biometric systems has to be confident that his / her biometrics data will be kept secure and processed in a lawful way.

2.2. Ear Biometrics

Identifying people using biometrics data becomes commonplace. However, the real challenge is to find biometrics data which is rich in distinctive features [4]. The ear biometric is a kind of image processing based biometrics technology, which has many unique features that can be extracted and used as a biometric trait to identify or/and verify people. The ear is one of a high permanence biometric characteristics, as well as it has a low cost of implementation (e.g. it is possible to use the mobile camera to capture user's ear image). However, the ear has a less acceptable rate compared to the voice or fingerprint. In addition to that, any occlusive part of the ear may affect the verification process.

2.3. Voice Biometrics

The voice biometrics defines as "a numerical representation of the sound, pattern, and rhythm of an individual's voice". Voice biometric is a type of signal based biometrics technology in which every human has a unique voiceprint and voice biometrics can be used to identify and authenticate people [5]. The human voice has many features that can be used to identify people. Different pitch, the tone of the voice which comes from the shape of the mouth, lip movement and vocal tract structure are unique features to identify individuals. Voice biometrics data can be collected and found quickly. It has a Low cost of implementation (i.e. any recorder device can do that) and it is easy to use and accepted by users. Also, it is possible to use voice biometrics to authenticate people remotely (e.g. during a telephone call). However, voice biometrics have some disadvantages e.g. the changes that happen to the voice of the individual during the time due to different factors not limited to the age, health, noise, etc.. Which may lead to the rejection of authorized people. Another disadvantage is the ability to bypass the system by replaying a pre-recorded voice of another genuine person.

2.4. Multimodal Authentication systems

Multimodal biometrics systems have two forms; a multimodal system can be synchronous when more than one biometrics are combined within one authorization process. The other form of multimodal system is known as the asynchronous system in which two or more biometric technologies process consecutively. To build a multimodal biometrics system, the level in which two or more Biometrics technologies are fused should be determined. There are four levels of fusion scheme:

- Sensor level: when a single or different combined sensor is used to get more than one biometrics data.
- Features level: extracted biometrics traits are fused on this level
- Matching score level: all extracted features are compared to features that are stored in templates database to calculate the matching scores. These scores are combined to end up with a single matching score.
- Decision level: it is also known as abstract fusion when the numbers of separate decisions are fused to form a final matching decision about the individual, various method like voting, AND/OR rules are used to take the last decision.).[6]

2.4.1. Ear and Voice Multimodal System:

When combining ear and voice biometrics, it is an opportunity to take advantage of the two biometrics traits to enhance the performance of biometrics systems and to reduce some of the drawbacks of using each biometric separately. To implement the multimodal system, open source voice SDK performs the extraction and verification functions, while for ear biometric; geometric ear features are extracted and then used to verify users.

2.5. Biometric System Performance

The performance of biometric systems is usually measured by false rejection rate, false acceptance rate and Failure to enroll rate:

- Failure to Enrol rate (FTE): represents the percentage of users who failed to enroll in the biometrics system.
- False Rejection Rate (FRR): it is the percentage of all genuine individuals who failed to pass the system threshold.
- False Acceptance Rate (FAR): the percentage of imposters who are Succeed to bypass the system's threshold.

3. Design and Implementation of Proposed System

This section discusses the technical part of the multimodal system; it describes how the multimodal biometrics system is designed and implemented.

3.1. System Components and Architecture

As in other biometric systems, there are four components for the multimodal biometric system which are the main functions of the system, namely: Sensors, feature extraction, verification and matching and decision-making.

Ear and Voice Enrolment: Built-in camera and microphone are playing the role of sensors to collect raw biometrics data from people. The camera will capture the image of the ear while the voice is recorded from the microphone, then they will be stored in the database.

Feature Extraction: to create a template from raw biometric data, unique features are extracted and stored in the database. This template is used in comparison with another template to authenticate the user.

Verification: To verify or authenticate people, they must pass the system's threshold when their enrolled biometrics data is comparing to their corresponding template in the system database. In this multimodal system, the verification for ear and voice is performed separately and their biometric scores are recorded in the database. The last decision will be made from the results obtained for the two scores.

Decision-making: To make the final decision about if the user is authenticated or not, the system uses the fusion-rank method. In this method each biometric is ranked equally, i.e. each ear and voice have a rank of 5 if the user succeeds to pass the set threshold (taking into account that the system has different thresholds) they will get 10 (full pass). If one person passes only one biometric test and fails in the other one, in this case, the ratio between the passing score (5) and the score that under threshold (<5) is normalized (to be from 5), computed and added to the first rank (which is 5), then if the summation of the two ranks is above or equals to specific rate, the user will authenticate successfully. Otherwise, he will not pass the multimode system. For more illustration of the rank approach, if a person is successfully authorized by his voice and at the same time failed to pass the threshold set for the ear biometric, he will then get 5 for voice as the first rank, while his ear

score will be scaled from 5, so if he got 4.2 as the second rank, then adding the two ranks will give 9.2 out of 10. If the rule says that any rank from 9-10 will be authorized, in that case, the user will pass the multimodal system. The benefit from this rank method is to reduce the intra-variations between the same user biometrics data.

3.2. System Design

The system designed to operate as a desktop based system. No specific hardware is required, the built-in laptop webcam camera is used to capture the ear image of the user and the built-in microphone is used to record user's voice. Some biometric software technology is used like Neuro Technology Biometric SDK (6.0 trial version) to extract features and to verify user's voice. To perform ear biometric, the open source Emgu CV is used to process ear images under Visual Basic.NET environment. [7].

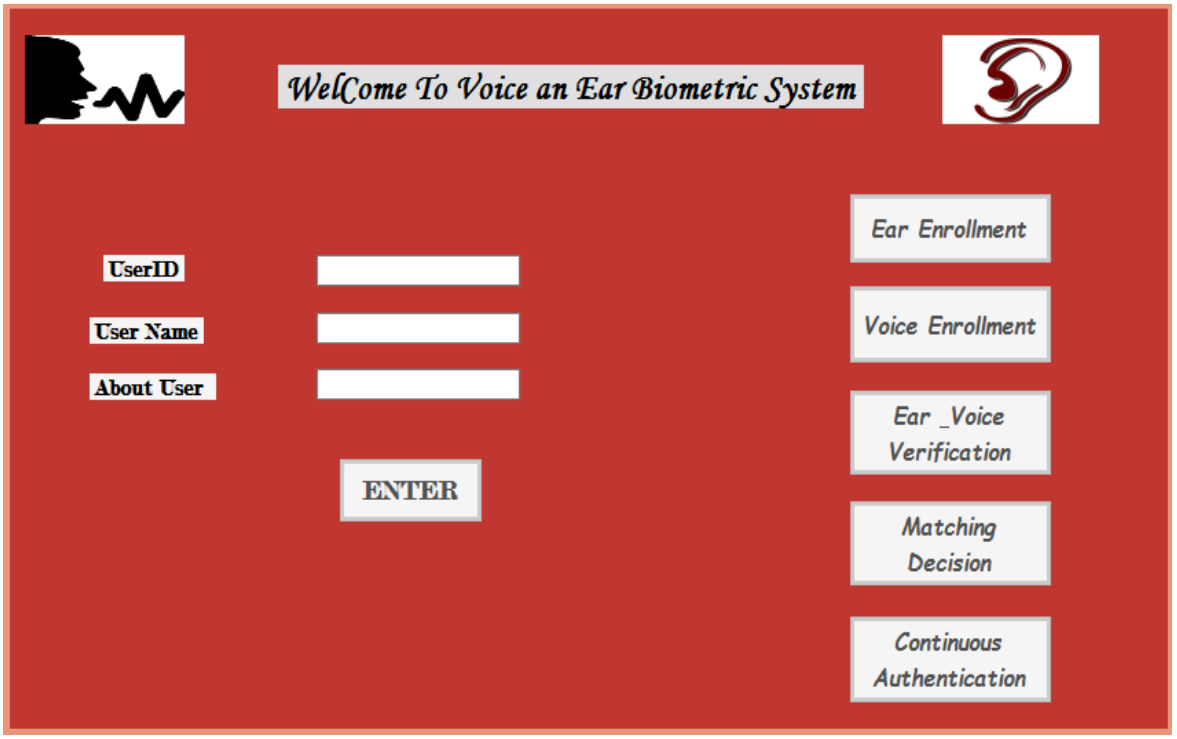

Fig.2. Multimodal Biometrics System Interface

3.3. Implementation of Ear Biometric System

Like other biometric systems, ear biometrics implemented to execute three main functions: ear enrolment, features extraction and ear verification. Firstly, ear image could be enrolled as an image file or captured by a webcam camera. The captured image usually contains the ear image and other surrounding parts like face or hair, so the ear itself will be selected manually and saved in the database. After being enrolled, the image is processed to extract its unique features. There are various algorithms or methods used to enhance the ear image before extracting the features. Canny edge detection algorithm is applied to ear image to detect the edge of the ear. Before applying the Canny algorithm, firstly the original image is converted into a grayscale image after

that Gaussian filter is used before the canny algorithm is finally applied and produces the final edge of the ear image. The enhancement process and edge detection are performed by Emgu CV library [8]. The geometrical extraction method is used to extract ear geometric features. After edge detection, the max and normal lines of the ear are defined. Max line is the longest line that can be drawn between two endpoints in the ear edge, while the normal lines are those connected between the centre of max line and the points on the outer helix of the ear edge (which are 12 points). These points come from dividing the area between the max line and the outer helix of the ear into 12 equal parts. After that, the ratio between normal and max lines is computed and their values are recorded and saved in the database together with the ear biometric score which is the sum of Y-axis values of the 12 points. Depending on the fact that the outer helix is unique for every ear the points on that outer helix has to be unique also.

To verify ear, firstly the number of thresholds are set. There are four different thresholds: 85%, 75%, 65% and 55% representing the ratio between the score of the ear and ratios values (between max and normal lines) which are already stored in the database (as a template) and the score and ratios values of another ear which need to be verified. If the ratio between two ears is less than the selected threshold, the ear will not match.

3.4. Implementation of Voice Biometric System

The functions of voice biometrics system are enrolment, features extraction, and verification. To enroll the voice of the user, there are two options: either from a microphone by recording the voice of the user or from a file (load voice or sound as a file). After the raw voice is enrolled, its corresponding feature is extracted, and the template is generated and stored in the database. The Neurotechnology's SDK has two options for features extraction, text-independent, and text-dependent features extraction. To verify voice, the enrolled and pre-stored templates are uploaded to test if the two templates are referring to the same user or not. There are two decisions for verification process which are either match or non-match, if the two subjects are matched, then there would be a match score that measures the similarity between the two voice subjects (bigger match score indicates higher similarity).

3.5. Multimodal System

The multimodal system has the same functions like ear and voice biometrics systems enrolment, feature extraction, verification and matching decision. The ear and voice enrolment will be conducted as normal enrolment process for ear and voice biometric systems, which is also true for features extraction and verification as described earlier. The final matching decision depends on the rank of each biometric, if two biometrics get the full rank (i.e. the person is authenticated in both ear and voice biometrics), then it will be authenticated in the multimodal system too. If he/she fails to pass the two of them, he/she will not be authenticated by the multimodal system. The third situation is when a person passed only one biometric test and failed to pass the other test. In such case the ratio between the rank score of the test he passed (5) and that he failed to pass (< 5) is normalized (to be from 5), computed and added to the first rank, then if the summation of the two ranks is above or equals to 9, the user will successfully be authenticated, otherwise he will not pass the multimode system.

4. System Test

After the implementation, biometrics system is tested to see how it works with different inputs. The outcomes will be evaluated in the next section. In this section, three tests are conducted. Firstly, voice and ear biometric systems are performed as two separate unimodal systems and then the multimodal system test will follow.

4.1. Voice Biometric System Test

To test Voice biometric system, there are four steps: enroll subjects, extract biometric traits, subject verification, and matching decision. Firstly To conduct the voice biometric test, a number of voice samples were prepared, while the system is expected to cover a relatively small number of users, about 25 subjects were selected. A total of 54 samples were considered in this experiment, representing a combination of ITB students' voice samples who gave their consent to use their voice samples (these samples were collected in April 2016) and the other samples were obtained from sampleswap.org and moviesoundclips websites which contain various voice samples for famous people. The duration for most of these samples varied from 1 to 6 minutes. However, the system can extract a voice template from less than ten seconds. The samples are chosen to simulate real situations as far as possible, yet some samples contain a noise which can affect the verification process later [9]. In the enrolment phase, 51 out of 54 voice samples were enrolled successfully. The next step is to extract the biometric features from enrolled samples. The features were extracted from the raw voices for each subject (two types of features were extracted, text independent and text dependent features.). The output is voice templates which store in templates database. The third step is the voice verification in which partial set of subjects were verified to test the performance of voice biometric system. The enrolled template is comparing to its corresponding template that is already stored in the system database (one to one comparison). The matching score resulting from this comparison will measure the similarity between two voice templates (bigger match score indicates high similarity).

4.2. Ear Biometric System Test

There are four phases during ear biometric system test: subject enrolment, extract biometric features from ear image, subject verification, and matching decision. Firstly, to conduct ear biometric system test a number of ear images were collected, while the system is targeting –relatively- a small number of users, ear images of 25 subjects are selected to be used in the experiment collected from ITB students who gave their consent to use their voice samples (samples were gathered in April 2016) while other images are a part of AMI Ear database, this database contains a number of ear images collected from 100 subjects selected from students and staff of the Computer Science Department at University of de Las Palmas de Gran Canaria (ULPGC), Las Palmas in Spain. Only right images are applied in the test. The samples were chosen to simulate real situations; different images are taken for the same ear in different positions (up, down, front, back) as well as a partially occluded ear with hair or jewellery [10]. Some of the ear images are enrolled directly in the system using webcam camera, while the other images were enrolled as a file from the computer. For each ear image, information like subject ID, subject name and subject description were enrolled in the system and store in the database. In the enrolment phase, 23 out of 25 images were enrolled successfully. The next step is to extract the biometric features from ear image. Firstly, the edge of the ear is detected using the Canny algorithm, after that the geometrical features were extracted using the concept of max lines and normal lines. The output is an ear template in the form of a group of ratios which are stored in the system database as well as ear biometric score. The third step is ear verification in which, partial set of ear images were verified to test the performance of ear biometric system. The enrolled template was compared to its corresponding template which is stored in the database (one to one comparison).

4.3. Ear and Voice Biometrics System Test

After testing the ear and voice biometric systems separately, the third part is to test the multimodal system, as in the previous tests there are four stages in multimodal system test. Firstly, ear image and voice sample of each subject is enrolled in the system, 30 subjects are selected to be used in the experiment each of them has 2 to 3 samples. This is the same data that previously used in ear and voice biometric tests. For each ear image and voice sample, information about the subject (subject ID, subject name and subject description) was enrolled in the system and store in the database. 25 out of 30 ear and voice samples were enrolled successfully. Secondly, the features are extracted from the ear image and voice sample as described in the ear and voice test in the

previous two sections, this results in generating voice and ear templates. The third step is the verification process for the two biometrics, where a partial set of ear images and voice samples are verified to measure the performance of the multimodal biometric system. Each enrolled template is comparing to the corresponding ear and voice template that already stored in the database (one to one comparison).

5. Result and Evaluation

Beginning with voice biometric system result demonstrated in Fig. 3. As the figure illustrates, the system has Failure to enroll rate (FTE) equals to 5.8%. The main reason for this failure is the too few features that could not be extracted from the voice sample as notified by the system. Referring to the previous section, the false rejection rate of the voice system increased when a high threshold is selected, i.e. when the threshold is set to be 1000, the FRR is about 26%, that means, more than a quarter of the samples are rejected because their similarity scores are below the threshold. This because the voice biometric system is very sensitive to any change that happens to the subject's voice. The level of similarity between the sample voice and its corresponding template decreases, resulting in a low degree of matching. By selecting a lower threshold, this rate is reduced as graph represents; when the threshold is 500, the FRR dropped to 20% and 13% when the threshold is 100. On the other hand, false acceptance rate measures the ability of the system to resist impostor's efforts to bypass the system. When the system has high FRR, it is expected to have low FAR. This happened when the system detects a number of simulated impostors' attempts (about 21 by replaying pre-record samples belong to authorized people) from unauthenticated people who none of them can fool the system when the threshold is 1000 or 500 (FAR = 0%); whereas one person succeeded to bypass the system using a pre-record voice of another genuine person (FAR = 4.7%).

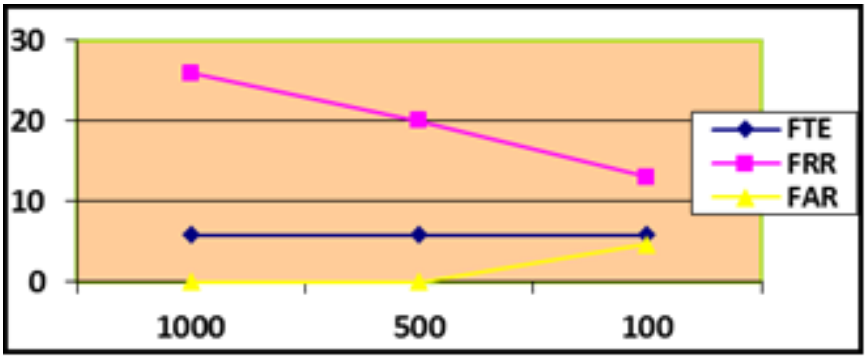

Fig.3. Voice Biometric System Performance Result

For ear biometric system result as demonstrated by Fig. 5, the failure to enroll rate (FTE) is 8%, this failure happened due to the poor detection of the edge of the ear image. This usually a result of a low ear quality image or semi-occlusive ear image. According to the previous section, the false rejection rate of the ear system increased when a high threshold is selected, i.e. when threshold equals 85%, the FRR is about 40% meaning that two-fifths of the ear images were rejected because of their similarity percentages below the selected threshold. By choosing a lesser percentage, the FRR rate is reduced as graph represents. When the threshold is 75%, the rejection rate dropped to 20% whereas the FRR dropped to 8% and 4% when the thresholds are 65% and 55% respectively. On the other hand, false accept rate measures the ability of the system to resist impostor's efforts to bypass the system. When the system has high rejection rate, it is expected to have low false acceptance rate, as they are opposite to each other, and that what happened when the system detected a number of simulated impostors' attempts (about 26 attempts which simulate imposters try to authorize themselves depending on a similarity between their ear images and other authorized people ear image). As

illustrated in Fig .5 when the threshold is 85%, 5% of the imposters will be able to fool the system. This percentage rises when a lower percentage is selected. With 75% and 65%, the FAR is 15% and 38% respectively, whereas this percentage is dramatically increased to 65% if the similarity percentage is 55%.

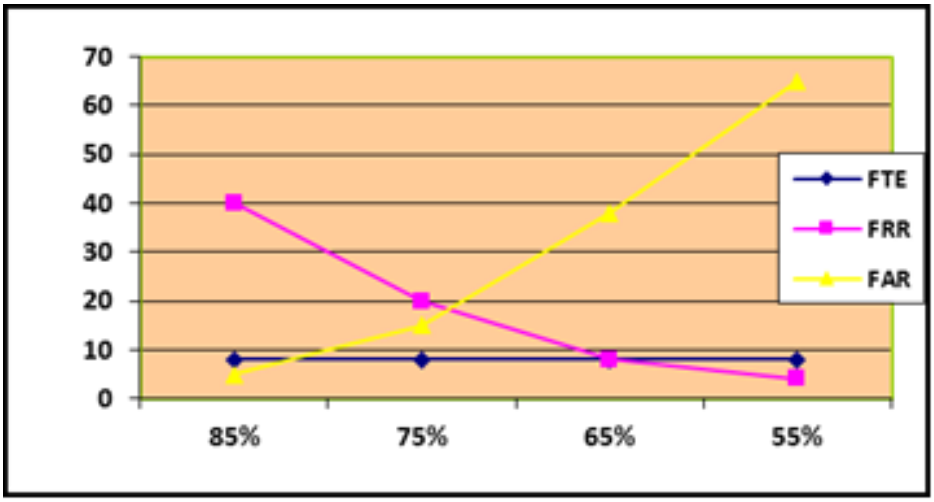

Fig.4. Ear Biometric System Performance Result

Fig. 5 and Fig. 6 illustrate the multimodal system results with different matching decision rules. Using AND rule or Rank approach as demonstrated by Fig. 5, the system Failure to enrol rate (FTE) equals to 16%, this failure is relatively high due to using AND rule, so if one biometric Failure to enrol, that means the multimodal has failed too, the person must successfully enrol in all biometrics, otherwise he/she will not be considered in the system, and this will raise the failure rate. On the other hand, when OR rule is used the failure rate is dropped to 3% as demonstrated by Fig. 6 ; that is because one successfully biometric enrolment is enough to enroll the person in the system and this will decrease the failure rate. The false rejection rate of the multimodal system is increased when a high threshold is selected, i.e. when the threshold is 85% for ear and 1000 for voice, the FRR is about 46.6%, taking into account that AND rule is applied. This indicates that, if there is any rejection for at least one biometric, it will regard as a false rejection for the multimodal system. However, if OR rule is considered, the FRR is rapidly declined to 10% because acceptance of at least one biometric is required to verify a person in the multimodal system. Selecting moderate thresholds like 500 for voice and 75% or 65% for ear will decrease the false rejection rate to 36.6% using AND rule, however, when OR rule is used it will be stable at 10%. Considering low threshold in the system as 100 for voice and 55% for the ear, the FRR equals to 6% for both rules. This expected since the low threshold leads to a decrease in false rejection rate. On the other hand, as illustrated in Fig. 5 and Fig. 6, 14 simulated impostors' attempts are performed to test the tolerances of multimodal system against any imposture attempt, all of the 14 attempts are failed to bypass the multimodal system when high and moderate thresholds are set (FAR = 0), while 6% of the attempts succeeded when low threshold is selected. This reflects one of the benefits when AND rule is considered because the imposters have to bypass all biometrics in the multimodal system. When using OR rule, the false accept rate is expected to have a higher rate. According to Fig. 6, the FAR is 0 when choosing high threshold while when applying moderate or low threshold the FAR will increase dramatically.

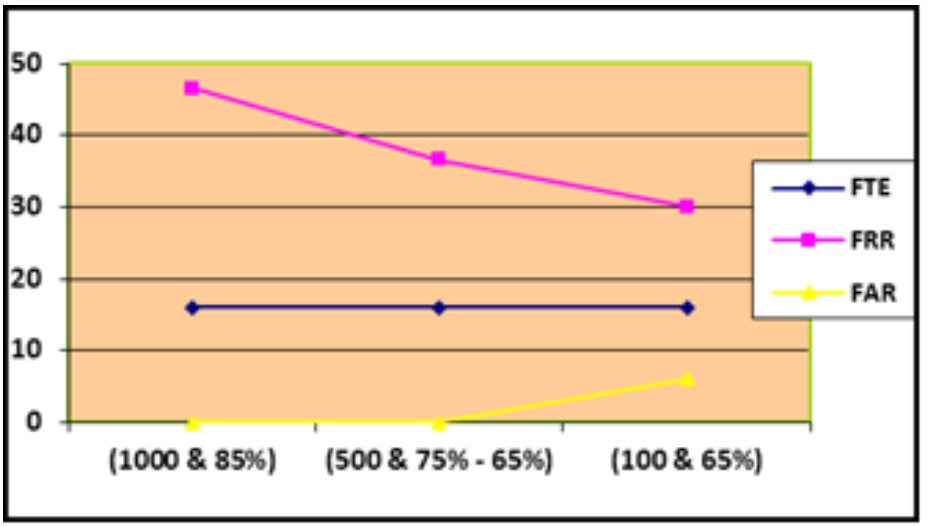

Fig.5. Ear and Voice Biometric System Performance Result (AND & Rank rules)

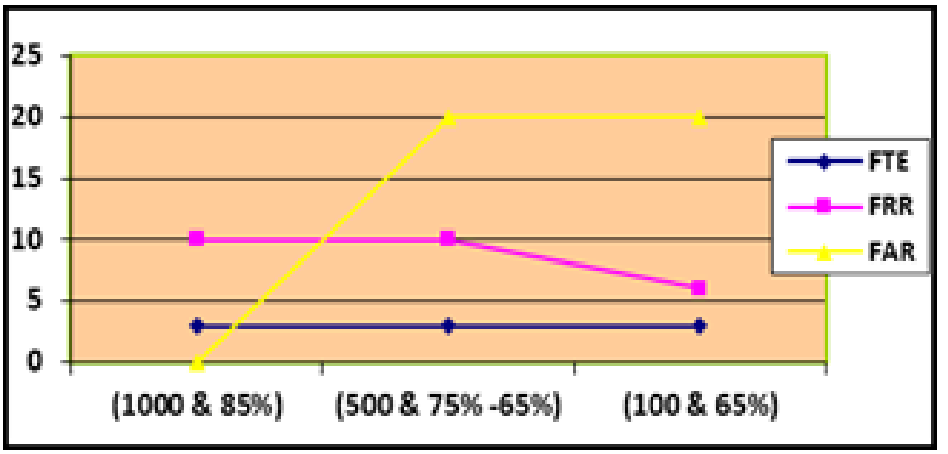

Fig.6. Ear and Voice Biometric System Performance Result (OR rules)

From above discussion, there is always a trade-off between achieving a high level of security, which means a high false rejection rate and authorizing more genuine people which mean a higher false accept rate. From these experiments, the multimodal system will decrease the false rejection rate and false accepting rate if at least one biometric is required to pass the multimodal system, this choice is helpful with ordinary companies and originations when a very high level of security is not a goal. However, if security is a significant issue, it would be better to consider AND or rank approach with a high threshold.

6. Conclusion

Multimodal biometric systems are one of the best ways to benefit from two or more different biometric technologies. Comparing to ear biometric unimodal and voice biometric unimodal, the multimodal biometrics of the ear and voice will provide better performance, especially if the authentication process depends on at least

one biometric authentication. By this way, the false rejection rate as well as failure to enroll rate will be reduced. Moreover, based on research findings the ear and the voice multimodal system can provide a better level of security, as it will be a big challenge for impostors to bypass more than one biometric at a time causing the false accept rate to drop down**.**

Acknowledgements

We would like to thank all people who help us to do this work, special thanks to ITB staff and students.

References

[1] Prabhakar, S., Pankanti, S. & Jain, A.K. 2003, "Biometric recognition: security and privacy concerns", IEEE Security & Privacy Magazine, vol. 99, no. 2, pp. 33-42.

[2] Monwar, M.M. & Gavrilova, M.L. 2009, "Multimodal Biometric System Using Rank-Level Fusion Approach", IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), vol. 39, no. 4, pp. 867-878.

[3] G. Amirthalingam, and G. Radhamani, "A Multimodal Approach for Face and Ear Biometric System," IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 5, No 2, September 2013.

[4] G. Amirthalingam, and G. Radhamani "Multimodal Biometric Cryptosystem for Face and Ear Recognition Based on Fuzzy Vault" Research Journal of Applied Sciences, Engineering, and Technology, November 2013.

[5] Authentify, "Voice Biometric Authentication" available at: < http://authentify.com/solutions/authentication-concepts/voice-biometric-authentication/ > [accessed: 2, 8, 2016].

[6] Ramadan Gad, Nawal El-Fishawy, Ayman El-Sayed, and M. Zorkany," Multi-Biometric Systems: A State of the Art Survey and Research Directions". International Journal of Advanced Computer Science and Applications Vol. 6, No. 6, 2015.

[7] Neuro Technology, "Neuro Technology Biometric SDK (6.0 trial version)" available at: <http://www.neurotechnology.com/ [accessed: 4, 8, 2016]>

[8] Emgu CV official page: < http://www.emgu.com/wiki/index.php/Main_Page> [accessed: 4, 8, 2016] sampleswap. web site, "VOCALS and SPOKEN WORD", available at <http://sampleswap.org/filebrowsernew.php?d=VOCALS+and+SPOKEN+WORD%2F>[accessed: 3, 8, 2016]

[9] Gonzalez, E., Alvarez, L. and Mazorra, L., AMI Ear Database, available at: <http://www.ctim.es/research_works/ami_ear_database/%23sample > [accessed: 4, 8, 2016].

Authors' Profiles

Safiia Mohammed is a master graduate student, She has got her B.Sc (honors) in Computer Sciences from University of Khartoum - faculty of mathematical science in 2012 and M.Sc in information security and digital forensics from ITB, Dublin, Ireland in 2016. She has a big interest in Biometrics field and this will be a field of her postgraduate researches in the future.

Michael Hegarty is a past student of Institute of Technology Blanchardstown (2000-2004) and a member of the lecturing team since 2012. Michael's area of research is Steganography with a focus on "The Development of Steganalysis tools to assess the impact of Steganography on electronic communications over insecure networks". Michael also has a keen interest in Biometrics, Digital Forensics, Business and Entrepreneurship.

How to cite this paper: Safiia Mohammed, Michael Hegarty,"Evaluation of Voice & Ear Biometrics Authentication System", International Journal of Education and Management Engineering(IJEME), Vol.7, No.4, pp.29-40, 2017.DOI: 10.5815/ijeme.2017.04.04