A Proposed Method of Biometric Authentication System using Multi-Modal Features

Dele W.S. Alausa, M.Sc.

Department of Computer Engineering, The Federal Polytechnic, Ilaro, Ogun State, Nigeria.

Email: dele.alausa@federalpolyilaro.edu.ng

ABSTRACT

The security challenges encountered in electronic transactions can be overcome by using a robust biometric authentication system to verify identities of users. This paper proposes a multimodal biometric authentication system that fuses decisions from two subsystems based on human physiological and behavioral traits. Feature level and Score level fusion is to be used with support vector machine and neural network classifiers. The output from the propose system will enhance level of security in electronic transaction.

(Keywords: biometric authentication system, multimodal, fusion, classifiers, trait, security)

INTRODUCTION

A method of identifying an individual using human physiological or behavioral features (e.g., iris, face, fingerprint, hand, to mention but a few) in an automatic way is known as biometrics. Applications including computer system security, entry (door) control, and many other uses (Kang et al, 2000). Biometric recognition is used to validate the individuality of a person, whether by behavioral or physiological description, and it is a dependable and widespread method. The recognition capability computes the effectiveness of a biometric system.

Multimodal biometrics is where two or more individual modalities are engaged to increase the recognition correctness and has been the focus of many researchers (Aravinth et al., 2016). A method used to capture a physical (e.g., face, thumb impression, iris, etc.) or behavioral (e.g., gait, signature pattern, key stroke pressure, etc.) parameters with an authentication job being performed and deriving the features from the parameter is the conventional biometric analysis. Measurements are combined from different biometric traits to enhance the performance using multimodal biometric fusion (Chakrabotty, et al., 2017). Multimodal biometric systems, when compared with a single-modal biometric systems, tend to improve system reliability, security, and recognition accuracy. However, biometric features are designed and processed independently without taking into account features in various modules in the existing multimodal biometric system (Yang et al., 2015).

Sensor levels, feature levels, matching score levels, and decision levels are some of the various levels of fusion in existence. Concatenation of two feature vectors is done by forming a new feature vector in feature level fusion extraction. Thus, a new feature vector handles large number of inputs. While in matching score levels, scores provided by the system for indicating proximity of the feature vector with the template vector are combined for identification. In decision level fusion, various weighting parameters are combined with the output from the individual classifiers. When sensor data are of different types or format, decision fusion is ideal for such cases (Chakraborty et al., 2017). The fusion or amalgamation of various biometric modes data by feature extraction, match score or decision level is the main objective of the procedure contained in the multimodal biometrics (Ross et al., 2001).

In this work, score level fusion is favored, since it includes enough data to make impostor and authentic cases obvious and simple to acquire. The combination of data acquired from each modality using score level fusion is classified into three types is the score fusion (e.g., identity-based score level fusion, transformation-based score level fusion and classifier-based score level fusion) (Chakraboty et al., 2017; Aravinth et al., 2016; Sharifi et al., 2016; Rokita et al., 2018; and

Cheng et al., 2016). The rest of this paper is organized into relevant state-of-the art methodologies in proposed areas of research, current research problems in the research area, and the problem statement the research work will address.

PROBLEM STATEMENT

Biometric authentication uses one or more of a person's attributes to validate the person's identity, the controlled and validated enrollment of the individual and that of individuals biometric is essential. This enrollment can only be conducted in a secure and controlled manner to guard against an imposter. Also, always contained in a biometric system is the low recognition error rates. But in a verification system, errors can be quantified using False Non-Match Rate (FNMR) and False Match Rate (FMR). While False Negative Identification Rate (FNIR) and False Positive Identification Rate (FPIR) are the error metrics used [2]. The major problems in biometric system are as follows:

(i) Weak/ Porous system which brings about the use of other people's credit card and password to purchase goods on-line and to impersonate.

(ii) The use of Unimodal biometric systems are not strong enough to detect skilled forgery.

(iii) Many biometric systems use weak feature extraction and weak matching systems using one tract.

It should be pointed out that biometric traits do not have a universally accepted matcher or representation scheme. The biometric characteristics of captured samples by the sensor and application requirements are taken into consideration by the extracted feature and matching algorithms.

RELATED WORKS

There is a great deal of literature on multimodal biometrics where various methods were used. In Wencheng et al. (2015) the authors designed a multimodal biometric system which includes two modules, namely, face module and finger print module. In the face module, images were collected, rotated and cropped into a standard size of 128 x 128 pixels accordingly to the eye coordinates. Then the Gabor Filter and linear discriminate analysis-based technique were used. For each face image, 99 real values were generated. In the finger module, finger print images were collected and preprocessed. Then feature extraction were carried out on both the face and finger print simultaneously. Then matching was carried out before they finally did the fusion. The performance of the designed multi-biometric system is evaluated by the false accept rate (FAR) and false reject rate (FRR). From the results it can be shown that the performance of the two cases are quite different. When the FRR is set to 0.1%, the FRR is 0.78% for case 1 and 1.66% for case 2. While case 3 may also happen in real life but it is more like a kind of attack. Thus, case 3 also shows performances different from case 2. When FAR=0.1%, the FRR is 0.73% in case 3, which is also quite different from FRR of 1.66% in case2.

Charkraborty et al. (2017) used a method whereby images were captured, preprocessed, fusion extracted, scores obtained were matched and fused and the decision were fused. Authors proposed a multimodal system using face and ECG signal. They collected side face imaged and ECG signals at the same time from 40 volunteers with age 32.5±12.5 years. Three sets of data patterns are taken for all subjects corresponding to different tilting positions. Average template of two different sets were used as stored patterns and the pattern of the remaining one is considered as new entry. Finally, the accuracy of classification was measured. It was found that face and ECG template as an individual modality acquires 95% accuracy whereas combined attributes with both face and ECG based templates provides 97.5% accuracy for all subjects. Results obtained were compared with some previously reported works. The proposed method presents a reliable system in the multimodal biometrics. Thus, multimodal methods are deemed to provide better performance over unimodal system.

According to according to Aravinth et al. (2016), they proposed weighted-based multiple classifier for score level fusion of multimodal biometrics. The modalities chosen were face, fingerprint, and iris. Images were captured accordingly. They, preprocessed, and feature extraction was done before feature matching and classifying and finally fusion recognition. The authors carried out score level fusion including three categories of classifiers like fuzzy rule classifier, lazy classifier (Naïve Bayes) and learning classifiers (ABC-NN). The combined results are used for biometric authentication. The hybridization is one of the key contributions of the technique. The scores are combined in the combination module using proposed formula to have the output as recognize or not. The technique is implemented using MATLAB and FRR, FAR and accuracy employed as the evaluation metrics. Comparative analysis with other prominent techniques were done while evaluation was carried out using accuracy value and ROC curves.

In Sharifi et al. (2016), the authors investigated the problem of combining different levels of fusion in a face-iris multimodal biometric system framework. Their aim was to implement different fusion schemes and then compare them with a scheme, including their complementary advantages in terms of performance. Authors proposed an optimal scheme for the fusion of face and iris biometrics. The scheme combines score level, feature level and decision level fusion to investigate the effect of combining different fusion levels in designing robust schemes for a face and iris multimodal system. The proposed scheme considers the combination of the face and left and right irises due to their complementary information.

The optimal subset of face and both iris features were first extracted at feature level fusion. The complementary details of both irises with face were fused as shown. Then the weighted sum rule fusion technique (WS) was applied to fuse the left and right iris scores separately with the face scores to achieve two optimal set of fused scores. The proposed scheme combines the decision using the OR rule in an optimal way and guarantees an improvement in the fused classifiers in terms of error rates. The produced scores from each modality and the produced scores at match score level fusion using WS are considered as six different sets of scores to fuse threshold-optimized ROCs. Thus, two ROCs are fused to generate a new optimal ROC and the computed threshold-optimized ROC is fused with the next arbitrary component ROC and so on.

Whereas according to Karmaka et al. (2014), the authors proposed generation of new points for training set and feature-level fusion in multimodal biometric identification. They carried out their integration at feature level since it provides better recognition performance than the other levels of fusions. The authors considered data on faces and iris only. Here new face and iris images are generated and are included in the training set.

The information from the two biometric is combined at feature level in which the resultant recognition rates are found to be significantly better than the existing recognition rates. The proposed system design was taken to be in parallel mode. It should be noted that once a face image of a person is concatenated to his left and right iris images, the concatenated images are termed usually represented as a column vector, “faris” (face + iris). Thus, reconstruction of an image from its feature space carries extra importance as it show cases the correctness of the applied feature reduction scheme. New face images were constructed and applied it to construct new faris images from existing faris points. The authors therefore considered several face and iris images for the same person. The number of classes is the same as the number of persons. Images are chosen to be more or less the same. Experiments were carried out upon the identifiers; face and iris. For inter- and intra-class feature sharing purpose, each dataset is divided into training and test parts. Assumptions were made and the research on the integration of multiple characteristics in biometrics is carried out in this way if the data of all the characteristics are not available for persons. Authors emphasized image generation, verification and reconstruction in their proposal. Thus the work uses simple MST approach along with convex combination to generate these new points.

But Ross et al. (2001), proposed an information fusion in verification systems where they use fingerprint, face, and hand geometry features of an individual for verification purposes. In this work, their experiments dealt with combining information at the representation and confidence levels, and not at the abstract level. Images of a subject’s face were obtained using a Panasonic video camera. Thus, an eigenface approach was used to extract features from the face image. Then the matching involves computing the Euclidean distance between the coefficients of the eigenface in the template and the eigenface for the detected face.

In fingerprint verification, images were acquired using a digital biometric sensor at a 500dpi. The features correspond to the position and orientation of certain critical points known as minutiae that are present in every fingerprint. The matching process involves comparing the two-dimensional minutiae patterns extracted from the user's print with those in the template.

Whilst in hand geometry verification, images of a subject's right hand were captured using a Pulnix TMC-7EX camera. The feature extraction system computes 14 features vales comprising of the lengths of the fingers, widths of the fingers and widths of the palms at various locations of the hand. The Euclidean distance metric was used to compare feature vectors and generate a matching score. The results show that the sum rule performs better than the decision tree and linear discriminant classifiers. Thus, all the three fusion schemes considered provided better verification performance than the individual biometrics.

In Imran et al. (2015), the authors proposed an online signature verification system using multi-section VQ. Since biometrics-based recognition has gained wide spread acceptance compared with the unreliable and inconvenient conventional methods that are used for security (i.e., comparison of the given signature to a reference signature with a naked eye). Although signatures vary for the same individual at different times, it appears to be possible for humans to discriminate visually the real signatures and the forge ones.

Moreover, the hardware used for on-line or off-line signatures verification is quite cheap as compared to the other biometric authentication techniques. For example, on-line signature verification requires only a tablet with good sampling rate and off-line signatures verification requires a pen, a paper, and a scanner. Nevertheless, signatures do get forged, most of the signature verification methods used by electronics devices to detect forgeries are complex. Thus, on-line signature verification system present more robust performance as compared to the off line system, but it requires the physical presence of the person during the acquisition of reference and verification data at registration and verification times, respectively, whereas, off-line signature verification process does not require such electronic devices other than a simple scanner. But it requires a more sophisticated and refined recognition process and a larger sized database. Thus, some difficulties are associated with online signature acquisition and verification. But the advancement in technology and availability of relatively cheaper data acquisition devices has triggered the use of online signature authentication in many real-world applications. But a signature belonging to one person may have different dynamic range and there might be insignificant intra-class variations in signature orientation.

Preprocessing was carried out for better recognition to remove the intra-class variation. Therefore, feature extraction was done where local features analyses the signature based on specific sample point (i.e., velocity, center of mass, etc.), whereas global feature are extracted from complete signature signal (i.e., average writing speed, pen up, signature duration). The feature matrix for each sub pattern was extracted and concatenated. In conclusion, signature recognition is one of the most important biometrics authentication method as it is a part of everyday life and is considered non-invasive and non-threatening process.

The proposed methodology utilized the temporal information and provided a significant improvement in terms of accuracy and speed. Multilevel fusion was carried out and experimental results on SVC and UESD databases provided 100% accuracy with 0.003 EER and 100% with 0.0046 EER, respectively, for skilled forgeries.

But in Jagadiswary et al. (2016) the authors presented fused multimodal system which includes two modules namely; enrollment module and verification module. In enrollment module, a suitable user interface incorporating the biometric sensor or reader is used to measure or record the raw biometric data of the user. The feature is extracted in the proposed biological tracts (e.g., finger print, retina, and finger vein). The feature extraction of these three biometric traits were fused using feature level fusion and encrypted using RSA and stored in a database for desired authentication and verification. Thus, this facilitates the next process of verification module where the user claim is genuine or imposter.

The captured traits are compared against the stored data and this is used to determine the user identity. The query is compared only to the template corresponding to the claimed identity after decryption. The security level of the proposed multimodal biometric system was designed using a GUI in MATLAB 2014. The three biometric traits finger print, retina, and finger vein are chosen for multimodal fusion and the required features of finger print, retina, and finger vein are extracted using various techniques like minutia extraction, blood vessel extraction and maximum curvature method respectively. The feature level fusion technique is used for the design of multimodal biometric traits such as fingerprint, retina and finger vein which protects the multiple templates using RSA and it was implemented using MATLAB R2014. The overall performance of multimodal systems has increased with GAR by 95.3% and reduced with FAR of 0.01% which was compared to unimodal biometric using RSA.

Whilst in Radhey et al. (2015), the authors presented a novel multimedia state-of-the-art biometric system for face recognition by combining the similarity scores of the unimodal modalities (e.g., texture based and appearance techniques of face recognition), catering for the decisive results at the matching score level. Thus, a multimodal biometric system combines more than one source of information for establishing human identity. Thus, the authors in their approach fuses the tested unimodal face recognition techniques in other to achieve a robust unimodal face recognition system.

METHODOLOGY

The synthesis of the various biometric mode data brought into operation the multimodal biometrics (Wayman, 2000). The fusion or amalgamation of different biometric data modes done by feature extraction, match score or decision level are the goals and processes followed in multimodal biometrics.

Therefore, the multimodal biometric recognition fusion technique based on the three images data provided are presented in this work. The combination module will then combine the scores using the formula to recognize the output or not as shown in the proposed framework of Figure 1.

SENSOR MODULE

Individual data can be acquired using a biometric hardware sensor which is the first step in a biometric system. For face images, the sensor is a camera the sensor for signature is a tablet, and the sensor for a fingerprint is a scanner. The system's performance depends on the quality of the acquisition module due to the sensitivity of the environmental conditions (i.e., variation in image's brightness), sensor quality (i.e., image's dpi), and the human factor (i.e. variation in pose).

In this work, the customer's facial image is captured and the pose acquisition of the face image is controlled by the user is put in a space. Several face images for the same person are acquired and considered (Karmaka et al., 2014). While the fingerprint features are extracted using an optical scanner taking from the fingerprint impressions done with distinct ridges. Accuracy of fingerprint recognition system mainly depend on effectiveness of the extracted features (Aravinth et al., 2016).

The system's accuracy is determined by the False Rejection Rate (FRR) and the False Acceptance rate (FAR) of the system. Whereas betwixt the first knuckle impression and the fingerprint's central area is captured by the rolled print, which will be used in this work (Daramola et al., 2011). Whilst signature recognition as important in pattern recognition field since it is accepted for personal identification by widely comparing it with other biometric traits such as; face, iris, voice, and fingerprint (Karmaka et al., 2014).

Generally, more robust performance is presented by signature recognition module, yet the person is present physically, while acquiring reference and verification of data at the registration and verification period respectively since his presence is required (Daramola et al., 2011). Therefore, online or dynamic signature is based on signature acquisition and verification procedure. The user is authenticated using the dynamic characteristics of the signature.

PRE-PROCESSING MODULE

The pre-processing stage is very important for identification in biometric systems. It is used to correct distortion and to get to the region of interest for feature extraction. For the input information to be extracted, raw input is processed and can be split into two different types: feature extraction and pre-processing. Noise from the raw input are removed or superimposed in the processing stage, while the feature extraction stage is where the unique biometric template for all subject is performed (Imran et al., 2015).

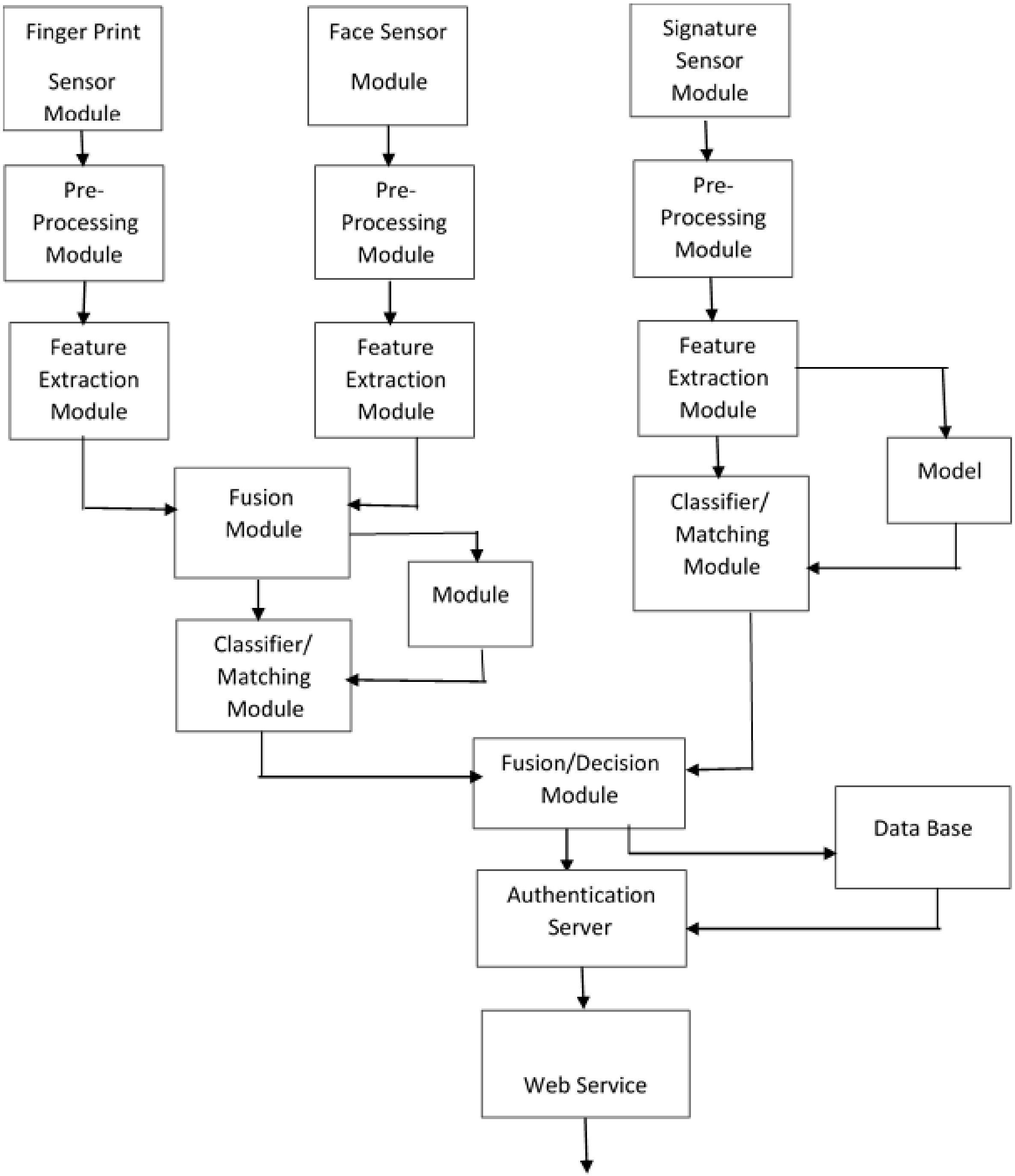

Figure 1: Proposed Framework for the Multimodal Biometric System.

FEATURE EXTRACTION MODULE

Another very important stage in the identification process of biometric system is the feature extraction stage. It involves a large set of data described by the amount of resources for simplification (Oloyede et al., 2016). Relevant information is selected and preserved from the original signal, for feature extraction process which is distinct from person to person. Feature extraction are done on the pre-processed images (Chakraborty et al., 2017). Ridge thinning algorithm will be used to extract features for fingerprint, while for face Local Gabor XOR Pattern (LGXP) will be used. Whereas, the signature is verified using the efficient text based directional signature recognition algorithm. The symbols and special unconstrained cursive characters (signature) are made up of signatures that are superimposed and embellished (www.mdpi.com).

FUSION/DECISION MODULE

The use of multiple types of biometric data or methods of processing is carried out by the improvement in the biometric system's performance is known as biometric fusion (www.itl.nist.gov). It can also be known as a special case of combining multiple classifiers in pattern recognition.

The decision stage is the stage where the match score generated in the matching/classifier module either reject or accept the user (www.noblis.org) The scores obtained above using the combination module formula in order for the output to be recognized or not. Also, this output is then combined with that of the signature at the score level as shown in Figure1. The technique is implemented using MATLAB and the evaluation metrics employed are False Rejection Rate (FRR), accuracy and False Acceptance Rate (FAR). Using other prominent techniques, comparative analysis will be carried out on them (Wayman, 2000). The accuracy values and ROC values will be used to carry out the evaluation.

CLASSIFIER/MATCHING MODULE

The comparation of the feature values with the present features in the template to generate a matching score is done in the matching/classifier stage. The test images features are compared to those in the data base using Euclidean distance to compute the score for each modality. Since the score level fusion is declared in the multimodal biometric systems, ample data to distinguish between real and bogus cases is encompassed by the matching scores and are accessible easily (Chakraborty et al., 2017). Therefore, the scores have to be adopted in an identical nature.

Amongst the notable instances of amalgamation procedures are classifier-based score level fusion, identity-based score level fusion and transformation-based score level fusion (Jagadiswary et al., 2016; Imran et al., 2015; Rokita et al., 2015). To be used in this work, for biometric modalities are; face, fingerprint and signature. In fingerprint recognition case it has the benefit of high uniqueness and worldwide. While the supportive subject is not necessarily to be close to any sensor, the face recognition is very submissive (Aravinth et al., 2000; Jagadiswary et al., 2016; Chang et al., 2006). Whereas in Online/Dynamic signature, the availability of relatively cheaper data acquisition devices and the technological advancement triggers the use of online signature authentication in many applications. Since detecting signature forgeries is the aim of any signature verification system (Karmaka et al., 2014).

BIOMETRIC ON-LINE LOG-IN MODULE

Features from the fusion/decision module is then sent to the authentication server to determine whether the person is who or what they declare themselves to be, which is done in the database. It should be noted that the authentication of an entity which tries to access the network is facilitated by an application called the authentication server. After the authentication, one can now log-on to the web services. This is known as biometric log-in, it provides more security, speed and ease of use than the traditional methods like passwords, and PIN's or small cards (Oloyede et al., 2016).

BREAK-DOWN OF THE PROBLEM STATEMENT

Presented in Table 1 is the breakdown of the problem statement.

Table 1: Summary of the Breakdown of the Problem Statement and Solution.

Problem Statements	Solution
Weak and porous system.	Development of a strong and virile system using physiological and behavioral features
Weak Uni-modal system to detect skilled forgery.	Development of a multimodal system that will eliminate all weaknesses
Weak feature extraction using one trait.	Development of a strong algorithm for feature extraction.
Weak Matching system.	The use of a suitable matching/classifier algorithm will be put in place.
Multimodal Biometric Platform	Development of authentication server for Web Service.

EXPECTED DELIVERABLES

(i) Development of biometric algorithm using both physiological and behavioral features and a multimodal system that will eliminate the weaknesses.

(ii) Development of Biometric authentication system for online transaction.

REQUIRED RESOURCES (TOOLS, EQUIPMENT/ SOFTWARE PACKAGES)

Amongst the tools, equipment/software packages required for this work are:

I. **Canon Ixus 190 Compact Camera:** Canon IXUS 190 compact camera has a 20-megapixel sensor and DIGIC 4+ processor that combines to give impressive images. It also has intelligent Optical Image Stabilization that keeps images sharp in any situation. It captures high quality images and video and has seamless connectivity with your smartphone or tablet. It also has an ultra-slim design with a point and shoot simplicity (www.currys.co.uk).

II. **FRO530 Optical Finger print Scanner:** Compact and powerful, FRO530 is ideal for applications deployed in limited space. With international standard including ISO and ANSI supported, FRO530 is applicable for authentication in different industries such as finance, health care, hospitality etc. Ruggedized and durable, FRO530 works perfectly with its Seamless Aratek Trust Link platform access (www.aratek.co/ptoducts/arafr530).

III. **Intuos3 Wide A6 USB Tablet PTZ-431W-E:** The Intuos3 Wide A6 has an area of 158x98 mm that is active and has the same format used for modern wide-screen computer displays that is accurate and small. It also has Corel Painter Essentials 3 software which fulfils all the Intuos3 input needs on its small footprint; portable use and perfect for crowded desk spaces. It also has Intuos3 Grip Pen (including the Stroke and Felt Pen nib) and the 5-button Intuos3 Mouse. Located on the left-hand side of the tablet are the Express Keys and the Touch Strip (www.intuos3wideA6usbtablet).

IV. **HP Laptop: Intel® Core(TM) i3-2350M CPU:** The HP laptop contains the following features: product collection - Legacy Intel Core Processor, processor base frequency: 2.30GHZ, maximum memory 16GB, processor number: i3-2350M, and Windows 7 (32 and 64 bit).

V. **MACROMEDIA DREAMWEAVER 8:** The leading web development tool that is used for efficiently designing, developing and maintaining standards-based websites and applications is the Macromedia® Dreamweaver® 8. It also gives a powerful combination of visual layout tools, application development features, and code editing support (www.macromediadreamweaver8).

VI. **MATLAB:** A high-performance language that is used for technical computing. Its environment incorporates programming, visualization and computation. It contains an in-built editing, debugging tools and supports object-oriented programming and sophisticated data structures. It also contains a powerful built-in routines which enable a very wide variety of computations with easy to use graphics commands that make the visualization of results available. It also has symbolic computation, simulation, optimization, control theory, toolboxes for signal processing, and other fields of applied science and engineering. The software to carry out this function will be developed using MATLAB (www.matlab.com).

VII. **Microsoft Visual C# Language:** It is a programming language used to build a wide range of enterprise applications that can run on .NET Framework. It is the combination of Microsoft C and Microsoft C++, it is simple, safe, object oriented and modern. Its code is compiled as managed code because it benefits from the services of the language routine, which includes; enhanced security, language interoperability, improved version support and garbage collection (www.msdn.microsoft.com).

VIII. **MySql Server 5.1:** This is the most popular open source database. It has become a leading data base choice for web-based applications, due to its performance reliability and it's ease of use. MySql server is used to update images when new MySql server releases are published (www.mysql.com)

IX. **Galaxy S6 Default Web Browser:** Default browser is one that other programs will open web pages in. it is the browser the operating system looks to first (www.verizowireless.com).

CONCLUSIONS

In this work, a multimodal biometrics System suitable for accessing electronic transaction is proposed. The system is based on two physiological features and one behavioral feature. The finger print, face, and the dynamic signatures are extracted from lots of activities performed by the user. Two levels of fusion shall be engaged.

At feature extraction level, the physiological features shall be combined and output from this subsystem shall be fused with output from the second subsystem based on behavioral signature feature. The two classifiers proposed to be used for matching are Support Vector Machine (SVM) and Artificial Neural Network (ANN). The proposed work will improve security level for electronic transaction technique. The proposed framework will be done experimentally in order to provide a promising recognition and verification rates. But one of the major technique's contributions is hybridization, thus, the research work will develop a unique method for the biometric authentication system using multimodal features.

REFERENCES

1. Aravinth, J. and S. Valarmathy. 2016. "Multiclassifier Based Score Level Fusion of Multi-Modal Biometric Recognition and its Application to Remote Biometrics Authentication". *The Imaging Science Journal*. 6(1).

2. Assaad, F.S. and G. Serpen. 2015. "Transformation Based Score Fusion Algorithm for Multi-modal Biometric User Authentication through Ensemble Classification". Conference Organized by Missouri University of science and Technology, San Jose CA, Complex Adaptive Systems Publication 5. Science Direct.

3. Chakraborty, S., M. Mitra, and S. Pal. 2017. "Biometric Analysis using Fused Feature Set from Side Face Texture and Electrocardiogram". *IET Science Measurement Technology*. 11(2): 226-233.

4. Cheng, Y. and K.V. Larin. 2006. "Artificial Finger Print Recognition by Using Optical Coherence Tomography with Autocorrelation Analysis". *Journal of Applied Optics*. 45(36).

5. Daramola, S.A. and T.S. Ibiyemi. 2010. "Dynamic Signature Verification System using Statistics Analysis". *International Journal in Computer Science and Engineering.* 02(07): 2466-2470.

6. Daramola, S.A. and C.N. Nwankwo. 2011. "Algorithm for Fingerprint Verification System". *Journal of Emerging Trends in Engineering and Applied Sciences (JETEAS)*. 2(2):355-359.

7. Jagadiswary, D.A. and D. Saraswady. 2016. "Biometric Authentication using Fused Multimodal Biometric". International conference on computational Modeling and security (CMS). Science Direct.

8. Jain, A.K. K. Nandakumar, and A. Ross. 2016. "50 Years of Biometric Research: Accomplishments, Challenges and Opportunities". *Pattern Recognition Letters*. 79:80-105.

9. Kang, B.J. and K.R. Park. 2010. "Multi-Modal Biometric Method based on Vein and Geometry of a Single Finger". *IET Computer Vision*. 4(3):209-217.

10. Karmakar, D. and C.A. Murthy. 2014. "Generation of New Points for Training Set and Feature-Level Fusion in Multimodal Biometric Identification". *Journal of machine vision and Application*. 25:477-487.

11. Lumini, A. and L. Nanni. 2017. "Overview of the Combination of Biometric Matchers". *Information Fusion.* 33:71-85.

12. Mai, G., M.H. Lim, and P.C. Yuen. 2016. "Binary Feature Fusion for Discriminative and Secure Multi-Biometric Cryptosystems". *Journal of image and Vision Computing*. Science Direct.

13. Oloyede, M.O. and G.P. Hancke. 2016. "Unimodal and Multimodal Biometric Sensing Systems: A Review". *IEEE Access*, Doi 10.1109/ACCESS2016.2614720

14. Razak, M.I. and B. Alhaqbani. 2015. "Multilevel Fusion for Fast Online Signature Recognition using Multi-Section VQ and Time Modelling". *Journal of Neural Computing and Application.* 26: 1117-1127.

15. Rokita, J., A. Krzyzak, and C.Y. Seun. 2008. “Multimodal Bometrics by Face and Hand Images taken by a Cell Phone”. *International Journal of Pattern Recognition and Artificial Intelligence*. 22(3):411- 429.

16. Ross, A., A. Jain, and J.Z. Qlan. 2001. “Information Fusion in Biometrics”. Proc. of 3rd International Conference on Audio and Video-Based Person Authentication (AVBPA). 354 – 359 Stockholm, Sweden.

17. Sharifi, O. and M. Eskandari. 2016. “Optimal Face Iris Multimodal Fusion Scheme”. *Symmetry*. 8(48).

18. Singh, R. and Y.N. Singh. 2015. “Identifying Individuals using Multimodal Face Recognition Techniques”. *Procedia Computer Science*. 48:666-672.

19. Viriri, S. and J.R. Tapamo. 2012. “Integrating Iris and Signature Traits for Personal Authentication using User-Specific Weighting”. *Journal of Sensors*.12:4324 – 4338.

20. Wayman, J.L. 2000. “The Scientific Development of Biometrics Over the Last 40 Years”. In: *The History of Information Security: A Comprehensive Handbook*. Elsevier: Amsterdam, The Netherlands. 263–274.

21. Yang, W., J.H.S. Wang, and C. Chen. 2015. “Mutual Dependency of Features in Multimodal Biometric System”. *Electronics Letters*. 51(3):234-235.

SUGGESTED CITATION

Alausa, D.W.S. 2018. “A Proposed Method of Biometric Authentication System using Multi-Modal Features”. *Pacific Journal of Science and Technology*. 19(2):86-95.

Pacific Journal of Science and Technology