ISSN 2278-3091
Volume 8, No.4, July – August 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse48842019.pdf
https://doi.org/10.30534/ijatcse/2019/48842019

# Multi-Biometric Authentication Using Deep Learning Classifier for Securing of Healthcare Data

**Dr. Gandhimathi Amirthalingam[1], Harrin Thangavel[2]**
[1]Department of Computer Science, King Khalid University, Kingdom of Saudi Arabia, mathymca@yahoo.com
[2]Midun Technologies, India, midunthangavel@gmail.com

## ABSTRACT

Ensuring the security of healthcare data is becoming an increasingly important problem as modern technology is integrated into existing medical services. As a consequence of the adoption of healthcare data in the health care sector, it is becoming more and more common for a health professional to edit and view a patient's record using a tablet PC. To protect the patient's privacy, a secure authentication system to access patient records must be used. Yet, most Health apps used by consumers do not fall under federal or regional health privacy laws, even when the apps are used to manage a chronic illness. To solve this issue multi-biometric authentication is performed in this work via the use of deep learning classifier. This paper analyzes the performance of combining the use of on-line signature and fingerprint authentication to perform robust user authentication. Signatures are verified using the dynamic time warping (DTW) technique of string matching. The proposed minutiae-based matching algorithm, stores merely a small number of minutiae points, which greatly reduces the storage requirement with the help of phase correlation. Here, matching score level fusion is used by applying weighted sum rule for the biometric fusion process. To improve the authentication performance, deep learning classifier is proposed in this work for multi-biometrics authentication. When a biometric authentication request is submitted, the proposed authentication system uses deep learning to automatically select an appropriate matching image. In the experiment, biometric authentication was performed on healthcare in the UCI database. Multi -Biometric Authentication was used during the authentication stage.

**Keywords:** Unauthorized access, Information Security, Electronic Medical Record (EMR), Multi-Biometric Authentication, Deep Learning.

## 1. INTRODUCTION

The Health Care System has long been plagued by problems such as diagnoses being written illegibly on paper, doctors not being able to easily access patient information, and limitations on time, space, and personnel for monitoring patients. Information security and privacy in the healthcare sector is an issue of growing importance [1]. Health Care Institutions gather and store sensitive information from patients to provide the best care. The medical history of a patient is essential to guarantee that the right diagnosis is achieved and help the clinical staff act in the shortest time possible. This information is highly sensitive and must be kept private for the responsible staff only.

In such cases, a patient that wants to receive treatment in a different institution needs to ask his usual doctor to release his medical records and send them to his new doctor. This process is time consuming, complex and, in some cases, maybe impossible if the patient is unable to do this (for instance, if he is unconscious) [2]. It is complex to implement protocols that enable health care institutions to share patient's data due to heterogeneous systems, legacy systems, and legislation and software limitations. At the same time, the medical records should be accessible by any health care institution to ensure that a patient can be attended anywhere.

To guarantee data availability, health care institutions rely on data repositories accessible. It is also extremely difficult to manage access to data using standard access control mechanisms due to the vast amount of users, groups, and patients and the constant adjustment in privileges that must be done to maintain confidentiality. With advancements in technology, opportunities exist to improve the current state of health care to minimize some of these problems and provide more personalized service [3].

The adoption of digital patient records, increased regulation, provider consolidation and the information exchange between patients, providers, and payers, all point towards the need for better information security. "The terminology for EMR is evolving, beginning with the term "computer-stored medical records" followed by computerized patient record (CPR), computerized medical record (CMR), computer-based patient record system (CBPR), electronic health record (EHR), and automated medical record (AMR)." Electronic Health Records (EHR) are kept and managed by health care

institutions [4]. There is no control with the way records are kept and stored; it is extremely difficult to grant access to third parties or different health care institutions. This is a problem since EHRs contain essential information to treat patients, such as clinical history, allergies, blood type, genetic conditions and so on.

Some researchers had agreed to refer Electronic Medical Record (EMR) as a patient medical record from various sources related to patient treatment, diagnosis, lab test, history, prescription and allergies that can be accessed from various sites within the organization. The ultimate goal of an EMR is to have the ability to share the record, not merely with other facilities and physicians [5]. EMR composed of the clinical data repository, clinical decision support, controlled medical vocabulary, order entry, computerized provider order entry, pharmacy, and clinical documentation applications. By having a security plan, EMR can help to meet legal requirements to protect sensitive and privacy of patients' information. Therefore, access to patients' information is highly restricted and it allows only authorized users to access all patient information available within an organization.

In healthcare, biometric technology has been gradually introduced as a method to secure and restrict access to medical facilities and reduce fraud in healthcare programs. Using biometric to provide security services can be a noteworthy alternative considering the flow of sensitive information present in large software applications and the resources required to manage complex information systems that can be accessed by hundreds or thousands of local as well as remote users.

Biometric technology offers several security features such as fast and user-friendly authentication and access control as well as the ability to encrypt sensitive information. In this work, proposed Multi-Biometric Authentication is performed with the use of deep learning classifier for fingerprint biometrics authentication.

The rest of the paper is organized as follows. In Section I, explained the importance of Electronic Medical Record (EMR) and security plan for a patient's information. In section II, discuses about the review of the latest work on the biometric authentication technique for providing the security-based Electronic Medical Record. In Section III, presents the proposed methodology of multi-biometric authentication using deep learning classifier for securing the health care data. In Section IV, analyzed the experimental results for the given datasets and compared with the other algorithms. In Section V, explains the conclusions and future enhancements.

## 2. RELATED WORK

The Omotosho et. al [6] presented the development of privacy and security system for cryptography-based- Electronic Health Record (HER) by taking advantage of the uniqueness of fingerprint and iris characteristic features to secure cryptographic keys in a bio-cryptography framework. The results of the system evaluation showed significant improvements in terms of time efficiency of this approach to cryptographic-based-HER and also justifies the feasibility of implementing a fuzzy key binding scheme in real applications.

Díaz-Palacios et al [7] proposed to exploit biometric identification to access a central health record database featured by privacy policies. The experiments implement a real-world scenario in which an ambulance reaches an unconscious patient who needs pre-hospital medical care for which their health record is retrieved from the database and is modified to meet privacy policies. The results demonstrate an average response time of 19.8 seconds when over 200K patients are registered in the database.

Enaizan et al [8] studied a new Multi-Criteria Decision-Making (MCDM) framework. An integrated technique for order of preference by similarity (TOPSIS) and analytic hierarchy process (AHP) was used as bases in employing the MCDM approach to rank each group of factors. K-means clustering was also applied to identify the critical factors in each group.

Kiah et al [9] proposed a new hybrid method to be implemented on EMR systems. This method will enhance the robustness, security, and integration of EMR systems. The hybrid of simple object access protocol/extensible markup language (XML) with advanced encryption standard and secure hash algorithm version 1 has achieved the security requirements of an EMR system with the capability of integrating with other systems through the design of XML messages.

Pravinthraja et al [10] proposed the Multimodal Biometric system to establish the security in the organization and the matching process is performed by applying the Fuzzy based Reduced Coulomb Energy (FRCE) neural networks. In this work the biometric features like face, fingerprint and nail images are used to authenticate the patient details in the hospital application. Initially, the biometric images are preprocessed by using a Gaussian filter which removes the noise from the image and without affecting the quality. From the preprocessed image ROI region is segmented and the biometric significant key features are extracted by applying the Hermittan based Haar Wavelet technique.

## 3. PROPOSED METHODOLOGY

The proposed Multi Biometric systems increase the level of security by eliminating any chance of spoofing in Electronic Medical Record (EMR). It involves the use of a Multi Biometric Authentication system as an access-control manager to health records for patient's information that is

stored in Health care institutions as shown in figure 1. The proposed algorithm mainly consists of four stages: 1. Patient requisition, 2. Health professional verification process, 3. Multi-biometric Authentication system, and 4. Health Care Institutions.

Healthcare institutions have adopted computerization on a massive scale. Almost all healthcare providers maintain Electronic Medical Record (EMR) for the outpatient and inpatient treatments they provide. The Electronic Medical Records (EMR) of each patient from the Data Lake which is maintained by health care institutions only. Usually, hospitals use multiple identifiers to view the patient record. So there is a chance of spoofing while multiple identifiers access the patient's data. Also, if the records are in the wrong person's hand, it can lead to a great hazard to a patient's health. In health care institutions, the patient records play a vital role in patient care, but incomplete health records or misplaced information or mix-ups with another patient's record can result in wrong medication.

The Proposed system eliminates medical identity thefts. When a biometric requisition is submitted from the patient, the health professional presents himself for the biometric verification process. His biometrics such as fingerprints and signature structure is scanned. This scanned biometric is then analyzed digitally and converted to its equivalent biometric template. The biometric template obtained and checked for a match against all the patient records in the database. If a match is found, then the authentication system granted access for an authorized health professional to view the patient's data. If results in a match do not be found, then the authentication system does not provide access for an unauthorized user to avoid spoofing.

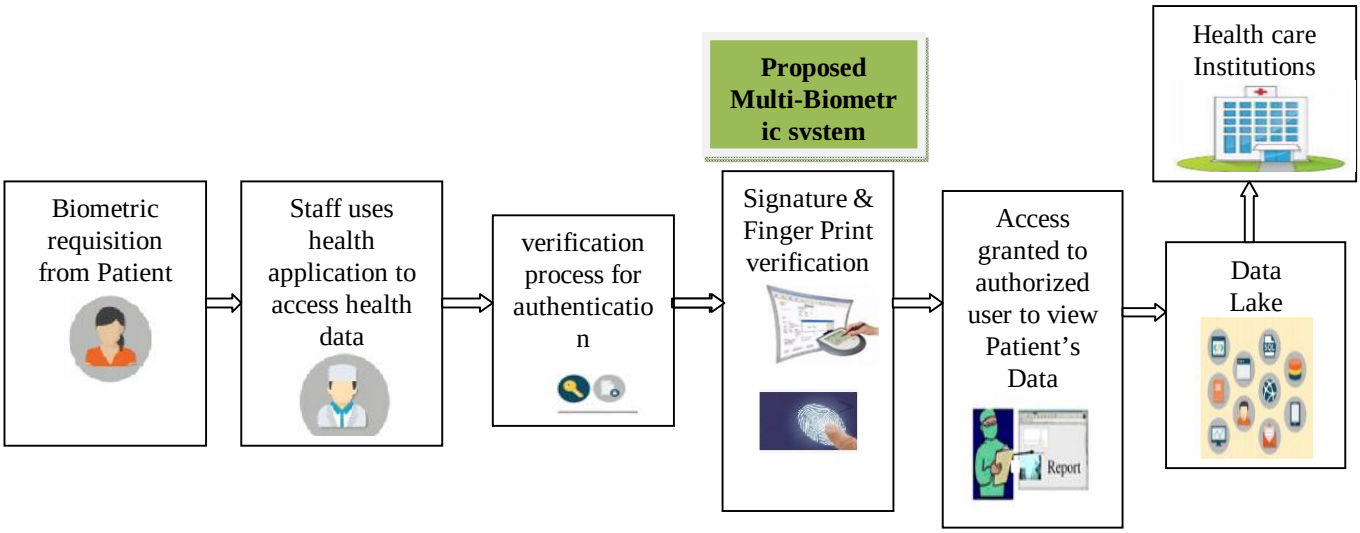


**Figure 1:** General process of proposed Multi biometric system for securing the healthcare data

The whole process from capture to authentication is digitized. There is no human element of error involved in matching the scanned biometric of a patient against the stored records and is fully automated. Overlays and duplicate medical records cannot happen with the proposed multi-biometric authentication. This results in high accuracy. The Flow chart for proposed Multi-biometric authentication system is shown in figure 2.

**Algorithm 1: Proposed multi-biometric authentication process**

**Signature recognition steps:**

**Step 1**: The Signature is scanned and stored as a digital image.

**Step 2**: Original digital image is converted into greyscale image.

**Step 3**: Then edge detection is applied on to the greyscale image. In this canny edge detection is applied on the image.

**Step 4:** Dynamic Time Wrapping (DTW) algorithm is applied to the previous output image. This DTW technique aims to minimize the effects of distortion and time-shift between two signatures collected in different sessions.

**Finger Print recognition steps:**

**Step 1:** The fingerprint is scanned and stored as a digital image.

**Step 2:** A grey scale conversion is applied to the digital input image, and then canny edge detection is applied to it.

**Step 3:** Then, binarization is applied to the image. It is done to highlight the foreground pattern from the background. It is the process of conversion of a grayscale image into a binary image.

**Step 4:** After this minutia extraction is applied on to the binarized image. In this method, minutiae points of one's fingers are matched with the other's minutiae points. Two thumbprint impressions are matched by comparing minutia matching points. The displacement coordinates are determined according to the location of the peak in the inverse cross-phase spectrum space using phase correlation.

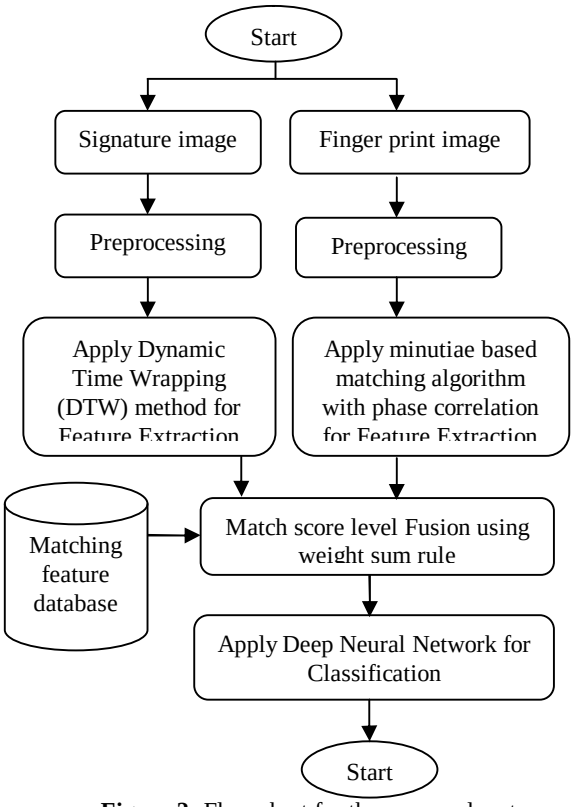


**Figure 2:** Flow chart for the proposed system

**The Fusion of finger and signature features**

The fingerprint feature vector ($x_m$) and signature feature vector ($y_m$) are fused to present a novel user authentication system. The sum of the feature vector ($F_m$) of fingerprint and signature is performed by as given below:-

$$F_m = x_m + y_m$$

**Matching**

Matching has been done by using a weighted sum rule-based. It gives the similar bits containing between two-bit patterns. A decision can be made whether template matches to the trained template image. A deep neural network has been applied for classification. Instead of using the threshold as the judgment rule, another method to measure the similarity between the feature vectors of the input fingerprint and signature with those of the templates is realized by a Convolutional Neural Network (CNN). Train Set function has been used for testing the original image with the trained image. Authentication is possible if they are matched otherwise not possible.

**3.1 Signature Recognition Process**

In this work, online signature verification is performed using Dynamic Time Warping (DTW) Algorithm. This section describes the main stages involved in the online signature verification algorithm. It can be divided into signature preprocessing, alignment between captured and template signatures based on DTW.

**i) Pre-Processing**

A preprocessing stage aims to reduce noise and normalize the signature stroke. The preprocessing stage is carried out following four steps:

1) Filtering: Signals acquired by the electronic device are smoothed by applying a low-pass filter that reduces noise introduced in the capturing process.

2) Equally-spacing: The average signals are transformed into an equally-spaced 256-point temporal sequence by using linear interpolation.

3) Location and time normalization: The temporal functions are normalized by centering the origin of coordinates at the signature centre of mass with a specific rotation.

4) Size normalization: The signature is normalized by using the norm of the 2 dimension vector [x,y]. Moreover, the dynamic characteristics such as pressure and inclination are also normalized by their maximum value.

**ii) Dynamic Time Warping (DTW)**

DTW technique aims to minimize the effects of distortion and time-shift between two signatures collected in different sessions [11]. Thus, the DTW shows a nonlinear elastic transformation that allows the optimal alignment (minimization of distance) of similar shapes even if they are out of phase in the time axis. A comprehensive analysis of this algorithm which basically can be summarized as follows:

1) Signatures are represented as a sequence of bi-dimensional points that represent the horizontal x and vertical y position:

$$\begin{cases} S = s_1,\ s_2, \ldots\ldots\ldots s_j, \ldots\ldots s_N; & with\ s_j = (s_x[j], s_y[j]) \\ T = t_1,\ t_2, \ldots\ldots\ldots t_i, \ldots\ldots t_N; & with\ t_i = (t_x[i], t_y[i]) \end{cases} \quad i,j\ \epsilon[1:N] \qquad (1)$$

S and T denote the captured and template signatures to be aligned, respectively. It is provided that signatures have been previously preprocessed.

2) From these two sequences, a distance matrix is built. This matrix represents the Euclidean distance between each pair of elements of S and T according to the following expression.

$$C(t_i, s_j) = \sqrt{(t_x[i] - s_x[j])^2 + (t_y[i] - s_y[j])^2};\ i,j\epsilon[1:N] \qquad (2)$$

3) The warping path P, which is built starting from matrix 'C', is defined as any sequence of points $P = (p_1, p_2, \ldots\ldots p_k)$ with

$P_m = C(t_i,s_j)$, m$\epsilon$ [1:K],$P_1=C(t_i,s_j)$ and $P_k=C(t_N,s_N)$

On the other hand, the cost function related to this warping path P is defined as follows

$$D_P(T,S) = \sum_{m=1}^{K} P_m \quad (3)$$

4) The optimal warping path $P_0$ is defined as the warping path which has a minimal cost function

$$P_0 = P|D_0(T,S) = \min\{D_P(T,S)\} \quad (4)$$

Note that the number of possible warping paths P is very high so that the assessment of covering all possibilities becomes a task of minimal efficiency. To reduce the calculation time, the dynamic programming algorithm is used. Besides, the number of operations needed by this algorithm for its resolution could be reduced by introducing some restrictions, represents the accumulative matrix that results after applying the programming algorithm for signature and its reference template. When two sequences are completely identical the optimal warping path is ideally placed on the diagonal of this matrix. Time misalignment between signatures is represented by small deviations of the optimal warping path from the diagonal line.

### 3.2 Finger Print Recognition Process

The proposed minutiae-based matching algorithm stores merely a small number of minutiae points, which greatly reduces the storage requirement. During fingerprint authentication, the identity of a new feature set is verified by matching it with the super-template of the subject's finger whose identity is claimed. Although any well known minutiae-based matching algorithm could be used for verification. It consists of Fingerprint Acquisition module, Feature Extraction module, Matching module, a Storage module, Decision module.

The Fingerprint Acquisition module contains an input device or a sensor that captures the finger print information from the user. It first refines, the finger print image against the image distortion obtained from the finger print sensor. A typical process consists of three stages. The binary conversion stage applies a low pass filter to smooth the high-frequency regions of the image and threshold to each sub-segment of the image. The thinning operation generates a one-pixel-width skeleton image by considering each pixel with its neighbors. In the positioning operation, the skeleton obtained is transformed and/or is rotated such that valid minutiae information can be extracted.

The Feature Extraction module refers to the extraction of features in the finger print image. After this step, some of the minutiae are detected and stored into a pattern file, which includes the position, the orientation, and the type (ridge ending or bifurcation) of the minutiae. The proposed fingerprint matching algorithm using phase correlation is based on minutiae points. Minutiae are prominent local ridge characteristics in fingerprint. This matching algorithm includes two stages: the alignment stage and the matching stage. In the alignment stage, transformations including rotation and translation between two minutiae sets are calculated and then the input minutia set is aligned to models for similarity measurement. In this work, assume there is no scaling different between two fingerprints as they are usually taken at the same resolution. The similarity between aligned input minutiae set and the template minutiae set is calculated in the matching stage.

**Phase Correlation**

The phase correlation (PC) method is a popular choice for image registration because of its robust performance and computational simplicity. It is based on the well-known Fourier shift theorem. Suppose two images $f_1$ and $f_2$, which differ only by a translation dx and dy and the relationship between these two images is given by

$$f_2(x,y) = f_1(x-dx, y-dy) \quad (5)$$

Their corresponding Fourier Transforms $F_1$, F2 are related by,

$$F_2(u,v) = e^{-j2\pi(udx/M+vdy/N)}F_1(u,v) \quad (6)$$

In other words, the Fourier magnitudes of the two images are the same while their phases are different. This phase difference is directly related to displacement. The cross-phase spectrum (or normalized cross-phase spectrum) P (u, v) is represented by

$$P(u,v) = \frac{F_1^*(u,v)F_2(u,v)}{|F_1^*(u,v)F_2(u,v)|} = e^{-j2\pi(udm/M+vdn/N)} \quad (7)$$

$F_1^*(u,v)$ denotes the complex conjugate of $F_1(u,v)$., the 2D inverse Fourier transform of cross-phase spectrum is given by

$$p(m,n) = \frac{1}{MN}\sum_{u,v} P(u,v)e^{j2\pi(um/M+vn/N)} \quad (8)$$

$p(m,n)$ is a delta function. The displacement coordinates are determined according to the location of the peak in the inverse cross-phase spectrum space.

**Minutiae Direction Map (MDM)**

Phase correlation cannot be used to align two-point sets directly. Here presents a new representation called Minutiae Direction Map (MDM) which is generated by converting minutiae point sets into a 2D image space. Alignment parameters are determined using a phase correlation between two MDMs [12].

Let $M = \{(x_1,y_1,\alpha_1),\ldots\ldots,(x_N,y_N,\alpha_N)\}$ denote the set of N minutiae in a fingerprint image. The image size is C × R and ($x_i$, $y_i$, $\alpha_i$) are the three features (spatial position and orientation) associated with the $i^{th}$ minutiae in set M. Define the MDM of set *M* as, $\mathfrak{M}^M(m,n), m \epsilon [0, R-1]$. It contains the angles of minutiae directions at the positions of minutiae points and 0 otherwise, which is written as

$$\mathfrak{M}^M(m,n) = \begin{cases} cos\alpha_i + j\ sin\alpha_i & m = x_i, n = y_i, \\ 0 & otherwise \end{cases} \quad (9)$$

where $(x_i, y_i, \alpha_i) \in M$. The size of the MDM $\mathfrak{M}^M$ is the same as that of the fingerprint image.

### 3.3 Fusion in Multi-Biometric System

The signature and fingerprint verification systems are combined in the proposed work. A new user authentication system which depends upon the joint acquisition of signature and fingerprint signals with elevated accuracy rate [13]. The feature set has richer data for the raw biometric data than the match score or the last decision. The procedure for weighted sum rule-based fusion is stated as follows.

After getting a set of normalized scores ($x_1$, $x_2$,…, $x_m$) from a particular person (here the index i=1,….,m indicates the biometric matcher), the fused score $f_s$ is evaluated using the formula, $f_s = w_1 x_1 + \cdots + w_m x_m$ (10)

The notation $w_i$ stands for the weight which is assigned to the matcher –i, for i=1,…, m. In the next step, the fused score $f_s$ will be compared to a pre-specified threshold t. If $f_s \geq t$, then a person declares as to be genuine otherwise an impostor.

### 3.4 Deep Neural Network (DNN) for Authentication

The classifier is needed after feature extraction to find the corresponding label for every test image. In this work, a Convolutional Neural Network (CNN) classifier has been used. A brief description of CNN is as follows: Assume to have the set of training data $(x_1,y_1),(x_2,y_2),\ldots(x_n,y_n)$ and want to classify the set into two classes where $x_i \in R^d$ is the feature vector and $y_i \in \{-1, +1\}$ is the label class. The two classes are linearly separable with a hyperplane w.x+b=0. With no other previous knowledge about the data, CNN can find the optimal hyperplane is the one with the maximum margin (which results in the minimum expected generalization error).

**Algorithm 2: Classification using Convolutional Neural Network (CNN)**

**Input**: The input images

**Output**: The recognition accuracy

**Step 1:** Load input featured images and its labels

**Step 2:** Split each category into a similar number of images

**Step 3:** Load pre-trained CNN

**Step 4:** Split the sets of the images into training and testing data.

**Step 5:** Extract Features from the deeper layers of CNN.

**Step 6:** Get training labels from the training set

**Step 7:** Extract features from the test set

**Step 8:** Use trained classifier to predict the label for test set

**Step 9:** Get the known labels for test set

**Step 10:** Display the recognition accuracy

The Convolutional Neural Network (CNN) can be implemented for a set of data with M classes, can train M binary classifiers that can distinguish each class against all other classes, and then select the class that classifies the test sample with the greatest accuracy margin [14].

## 4. RESULTS AND DISCUSSION

The experimental results of the proposed authentication system have been presented in this section. The proposed approach is implemented in MATLAB (Matlab7.4). Also tested this proposed system with different sets of fingerprint and Signature images of the corresponding individuals. Fingerprint verification competition 2006 (FVC2006) is used in this work for biometric authentication. Four different databases (DB1, DB2, DB3, and DB4) were collected by sensors/technologies. Each database is 150 fingers wide and 12 samples per finger in-depth (i.e., it consists of 1800 fingerprint images). Each database will be partitioned in two disjoint subsets A and B:

1. Subsets DB1-A, DB2-A, DB3-A, and DB4-A, which contain the first 140 fingers (1680 images) of DB1, DB2, DB3, and DB4, respectively, will be used for the algorithm performance evaluation.
2. Subsets DB1-B, DB2-B, DB3-B, and DB4-B, containing the last 10 fingers (120 images) of DB1, DB2, DB3 and DB4, respectively, will be made available to the participants as a development set to allow parameter tuning before the submission.

### Evaluation of the Multi-Biometrics

The evaluation of the proposed multi-biometric authentication system was implemented and fingerprint and signature images authentication were done using Deep Learning Approach.

#### *Recall*

Recall evaluates the percentage of actual positives which classifies the actual image as actual. The sensitivity is defined as below:

$$Recall = \frac{T_p}{T_p + F_n} \quad (11)$$

Where $T_p$ defines the face image correctly as a face image. $F_p$ defines the non-face image incorrectly as the non-face image. $F_n$ defines the non-face image incorrectly as the face. $T_n$ defines the non-face correctly as non-face.

#### *Precision*

Precision is defined as the proportion of the true positives against both true positives and false positives results for multimodal biometric images. It is defined as follows

$$Precision = \frac{T_p}{T_p + F_p} \quad (12)$$

#### *Accuracy*

Accuracy is defined as the overall correctness of the model and is calculated as the sum of actual classification parameters ($T_p + T_n$) separated by the total number of classification parameters ($T_p + T_n + F_p + F_n$)

$$Accuracy = \frac{T_p + T_n}{T_p + T_n + F_p + F_n} \quad (13)$$

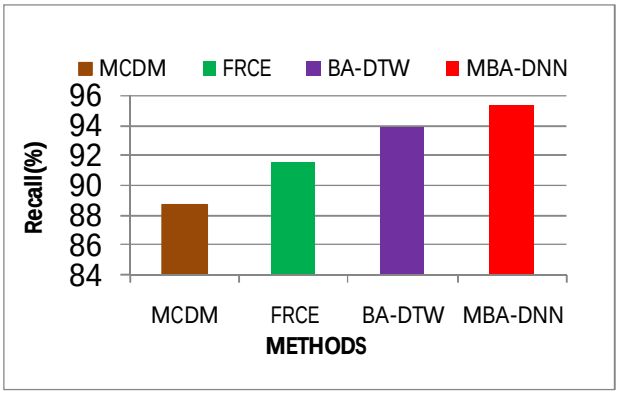


**Figure 3:** Recall comparison with Different Methods

The recall evaluation of the proposed MBA-DNN method is better than the existing methods. The proposed MBA-DNN produces higher recall results of 95.41%, whereas MCDM method metric is 88.72%, FRCE method metric is 91.56% and the BA-DTW is 93.87%. Figure 3 shows a better recall analysis compare than the other methods.

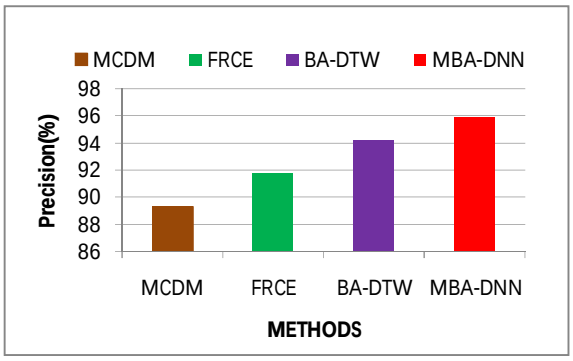


**Figure 4:** Precision comparison with Different Methods

The Precision comparison of the proposed MBA-DNN method is better than the existing methods. The proposed MBA-DNN produces higher Precision results of 95.97%, whereas MCDM method metric is 89.36 %, FRCE method metric is 91.74% and the BA-DTW is 94.21%. Figure 4 shows the better precision analysis compare than the other methods.

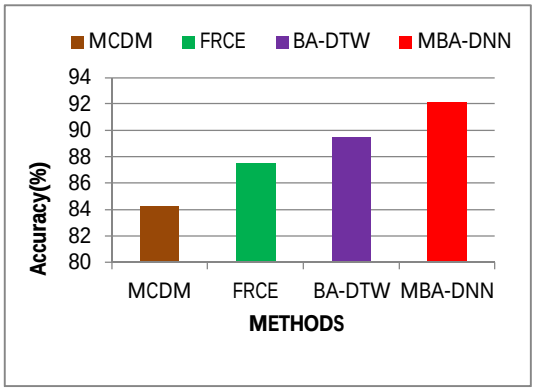


**Figure 5:** Performance Evaluation of Accuracy with Different Methods

The Performance Evaluation Accuracy of the proposed MBA-DNN method is better than the existing methods. The proposed MBA-DNN produces higher accuracy results of 92.13%, whereas the MCDM method metric is 84.26%, FRCE method metric is 87.54% and the BA-DTW method metric is 89.51%. Figure 5 shows better accuracy results compare than the other methods.

The performance evaluation is done using the FAR (false acceptance rate) and FRR (false rejection rate).

$$FAR = \frac{N_a}{N} \quad (14)$$

$$FRR = \frac{N_r}{N} \quad (15)$$

Where $N_a$ the number of imposters which were falsely is accepted i.e. scores of imposters match are more than T. $N_r$ is the number of a genuine sample which was false rejected i.e. score of genuine match T; N is the total number of match: T is the threshold.

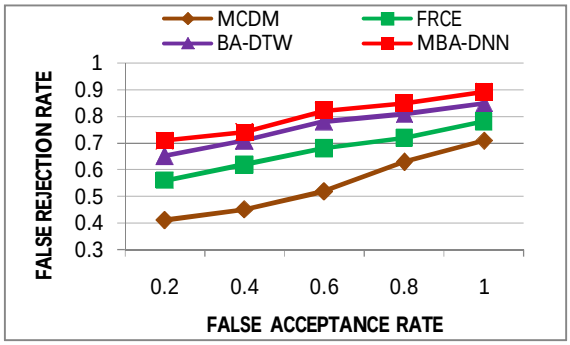


**Figure. 6**: Evaluation of the Proposed MBA-DNN

The above figure 6 shows that the Evaluation of the proposed MBA-DNN system. It can be seen that the MBA-DNN system has a better performance and also reduces the error rates (FAR and FRR) of the individual compare to other model systems.

## 5. CONCLUSION AND FUTURE WORK

The proposed multi-biometric authentication system provides security for Electronic Medical Record (EMR) to avoid the misplaced information from an unauthorized health professional that can able to edit and view a patient's record. In this work, it has been shown that if fingerprint and signature image of a health professional is given then the network can recognize a secure authentication system to access patient records. In this proposed Dynamic Time Wrapping (DTW) method has been used for feature extraction of signature samples. Minutia extraction method has been used for feature extraction of fingerprint samples. Here, matching score level fusion is used by applying weighted sum rule for the fusion process. Deep Learning classifier is used for classification while increasing the security level of the authentication system dramatically. This

proposed multi-biometric authentication system increases the system performance rate as compared to a single biometric authentication system and also increases the security level of the system. Future work could go in the direction to combine other modalities, other methods of classification, and other methods of fusion to accomplish a large comparative study in the multi-biometric domain and to develop a tool to automate some of the processes.

## REFERENCES


1. Noraziani, K., Nurul'Ain, A., Azhim, M. Z., Eslami, S. R., Drak, B., Sharifa Ezat, W., & Siti Nurul Akma, A. **An overview of electronic medical record implementation in healthcare system: Lesson to learn,** *World Applied Sciences Journal*, Vol. 25(2), pp. 323-332, 2013.
2. Matos, D. R., Pardal, M. L., Adão, P., Silva, A. R., & Correia, M. P. **Securing Electronic Health Records in the Cloud,** *In P2DS@ EuroSys*, pp. 1-6, 2018. https://doi.org/10.1145/3195258.3195259
3. Sood, S. P., Nwabueze, S. N., Mbarika, V. W., Prakash, N., Chatterjee, S., Ray, P., & Mishra, S. **Electronic medical records: A review comparing the challenges in developed and developing countries**,in *Proceedings of the 41st Annual* Hawaii *International Conference on System Sciences*, pp. 1-10, 2018.
4. Mane, R. R., & Kulkarni, R. V. **A Review: Electronic Medical Records (EMR) System for Clinical Data Storage at Health Centers**, *International Journal of Computer Technology and Applications*, Vol. *3*(5), pp.1837-1842, 2012.
5. Itumalla, R., & Acharyulu, G. V. R. K. **Indian healthcare and foreign direct investment: Challenges & opportunities**, *Asia Pacific Journal of Marketing & Management Review*, Vol. 1(2), pp.57-69, 2012.
6. Omotosho, A., Emuoyibofarhe, J., & Meinel, C. **Ensuring patients privacy in a cryptographic-based-electronic health records using bio-cryptography**, *Int. J. Electronic Healthcare, arXiv preprint arXiv:1708.01643*, pp.1-28, 2017. https://doi.org/10.1504/IJEH.2017.10003030
7. Díaz-Palacios, J. R., Romo-Aledo, V. J., & Chinaei, A. H. **Biometric access control for e-health records in pre-hospital care**. In *Proceedings of the joint EDBT/ICDT 2013 workshops*, pp. 169-173, 2013. https://doi.org/10.1145/2457317.2457345
8. Enaizan, O., Zaidan, A. A., Alwi, N. M., Zaidan, B. B., Alsalem, M. A., Albahri, O. S., & Albahri, A. S. **Electronic medical record systems: Decision support examination framework for individual, security and privacy concerns using multi-perspective analysis**, in *Health and Technology*, pp.1-28, 2018. https://doi.org/10.1007/s12553-018-0278-7
9. Kiah, M. M., Nabi, M. S., Zaidan, B. B., & Zaidan, A. A. **An enhanced security solution for electronic medical records based on AES hybrid technique with SOAP/XML and SHA-1**, *Journal of medical systems*, Vol. 37(5), pp. 1-18, 2013. https://doi.org/10.1007/s10916-013-9971-2
10. Pravinthraja, S., & Umamaheswari, K. **Multimodal Biometric System Recognition Using Fuzzy RCE Network**, *Journal of Medical Imaging and Health Informatics*, Vol. 6(3), pp.788-793, 2016. https://doi.org/10.1166/jmihi.2016.1761
11. Rajeswari, P., Raju, S. V., Ashour, A. S., & Dey, N. **Multi-fingerprint unimodel-based biometric authentication supporting cloud computing**, in *Intelligent techniques in signal processing for multimedia security*, pp. 469-485, 2017. https://doi.org/10.1007/978-3-319-44790-2_21
12. Thasiyabi, V. A., Koshy, R., & Satheesh, S. **Biometric fusion: Combining multimodal and multi algorithmic approach**, in *International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)*, pp. 618-620, 2016. https://doi.org/10.1109/SCOPES.2016.7955513
13. Kataria, S., & Goel, A. K. **A Hybrid Approach for Biometric Authentication using Fusion of Fingerprint and Signature**, *International Journal of Scientific Research Engineering & Technology (IJSRET)*, Vol. 5(1), pp.35-38, 2016.
14. Al-Waisy, A. S., Qahwaji, R., Ipson, S., Al-Fahdawi, S., & Nagem, T. A. **A multi-biometric iris recognition system based on a deep learning approach**, *Pattern Analysis and Applications*, Vol. 21(3), pp.783-802, 2018. https://doi.org/10.1007/s10044-017-0656-1