Authentication System

M. Rajya Lakshmi[1], B. Leela[2], B. Nikhila[3], A. Swarna[4], J. Sai Chandana[5]
1: Associate Professor, Department of Information Technology,
2,3,4: Student, Department of Information Technology,
Vasireddy Venkatadri Institute of Technology, Nambur, India

Abstract

Multi-biometrics refers to the use of multiple sources of biometric information in order to establish the identity of an individual. Multi-biometric systems combine the biometric evidence offered by multiple biometric sensors (e.g., 2D and 3D face sensors), algorithms (e.g., minutia-based and ridge-based fingerprint matchers), samples (e.g., frontal and profile face images), units (e.g., left and right irises), or traits (e.g., face and iris) to enhance the recognition accuracy of a biometric system. Information fusion can be accomplished at several different levels in a biometric system, including the sensor-level, feature- level, score-level, rank-level, or decision-level. The challenge is to design an effective fusion scheme to consolidate the multiple pieces of evidence to generate a decision about an individual's identity.

INTRODUCTION

Most biometric systems that are presently in use, typically use a single biometric trait to establish identity (i.e., they are uni-biometric systems). Some of the challenges commonly encountered the by biometric systems include:

1. **Noise in sensed data.** The biometric data being presented to the system may be contaminated by noise due to imperfect acquisition conditions or subtle variations in the biometric itself.
2. **Non-universality**. The biometric system may not be able to acquire meaningful biometric data from a subset of individuals resulting in a failure-to-en-roll (FTE) error.
3. **Upper bound on identification accuracy.** The matching performance of a uni-biometric system cannot be indefinitely improved by tuning the feature extraction and matching modules. There is an implicit upper bound on the number of distinguishable patterns (i.e., the number of distinct biometric feature sets) that can be represented using a template.
4. **Spoof attacks.** Traits such as voice and signature are vulnerable to spoof attacks by an impostor attempting to mimic the traits corresponding to legitimately enrolled subjects. Physical traits such as fingerprints can also be spoofed by inscribing ridge-like structures on synthetic material such as gelatine and play. Targeted spoof attacks can undermine the security afforded by the biometric system and, consequently, mitigate its benefits.

Some of the limitations of a uni-biometric system can be addressed by designing a system that console dates (or fuses) multiple sources of biometric information [1, 2]. This can be accomplished by fusing, for example, multiple traits of an individual, or multiple feature extraction and matching algorithms operating on the same biometric trait. Such systems, known as multi-biometric systems [3, 4], can improve the matching accuracy of a biometric system while increasing population coverage and deterring spoof attacks. Fusion in biometrics relies on the principles in the information fusion and multiple classifier system.

ADVANTAGES

1. Multi-biometric systems address the issue of non-universality (i.e., limited population coverage) encountered by uni-biometric systems. If a subject's dry finger prevents her from successfully enrolling into a fingerprint system, then the availability of another biometric trait, say iris, can aid in the inclusion of the individual in the biometric system. A certain degree of flexibility is achieved when a user into the system using several different traits (e.g., face, voice, fingerprint, iris, hand etc.) while only a subset of these traits (e.g., face and voice) is requested during authentication based on the nature of the application under consideration and the convenience of the user.
2. Multi-biometric systems can facilitate the filtering or indexing of large-scale biometric databases. For example, in a bimodal system consisting of face and fingerprint, the face feature set may be used to compute an index value for extracting a candidate list of potential identities from a large database of subjects. The fingerprint modality can then determine the final identity from this limited candidate list.

3. It becomes increasingly difficult (if not impossible) for an impostor to spoof multiple biometric traits of a legitimately enrolled individual. If each sub system indicates the probability that a particular trait is a ‘‘spoof’’, then appropriate fusion scheme can be employed to determine if the user, in fact, is an impostor. Furthermore, by asking the user to present a random subset of traits at the point of a multi-biometric system facilitates a challenge-response type of mechanism, thereby ensuring that the system is interacting with a live user. Note that a challenge-response mechanism can be initiated in uni-biometric systems also (e.g., system prompts ‘‘Please say 1-2-5-7’’, ‘‘Blink twice and move your eyes to the right’’, ‘‘Change your facial expression by smiling’’, etc.).

4. Multi-biometric systems also effectively address the problem of noisy data. When the biometric signal 968M Multi-biometrics acquired from a single trait is corrupted with noise, the availability of other (less noisy) traits may aid in the reliable determination of identity. Some systems take into account the quality of the individual biometric signals during the fusion process. This is especially important when recognition has to take place in adverse conditions where certain biometric traits cannot be reliably extracted. For example, in the presence of ambient acoustic noise, when an individual’s voice characteristics cannot be accurately measured, the facial characteristics may be used by the multi-biometric system to perform authentication. Estimating the quality of the acquired data is in itself a challenging problem but, when appropriately done, can reap significant benefits in a multi-biometric system.

5. A multi-biometric system may also be viewed as a fault tolerant system which continues to operate even when certain biometric sources become unreliable due to sensor or software malfunction, or deliberate user manipulation. The notion of fault tolerance is especially useful in large-scale authentication systems involving a large number of subjects (such as a border control application).

ALGORITHM

A Deep Neural Networks (DNN) is an artificial neural network that consists of more than three layers; it inherently fuses the process of feature extraction with classification into learning using FSVM and enables the decision making. Deep Neural Networks have become a promising solution to inject AI in our daily lives from self-driving cars, smartphones, games, drones, etc. In most cases, DNNs were accelerated by server equipped with numerous computing engines, e.g., GPU, but recent technology advance requires energy-efficient acceleration of DNNs as the modern applications moved down to mobile computing nodes. Therefore, Neural Processing Unit (NPU) architectures dedicated to energy-efficient DNN acceleration became essential. Despite the fact that training phase of DNN requires precise number representations, many researchers proved that utilizing smaller bit-precision is enough for inference with low-power consumption. This led hardware architects to investigate energy-efficient NPU architectures with diverse HW-SW co-optimization schemes for inference. This chapter provides a review of several design examples of latest NPU architecture for DNN, mainly about inference engines. It also provides a discussion on the new architectural researches of computers and processing-in-memory architecture, provides perspectives on the future research directions.

Step 1: Collecting data.

Step 2: Pre-paring the data

Step 3: Choosing the model

Step 4: Training the model

Step 5: Evaluating the model

Step 6: Parameter tuning

Step 7: Making predictions

EXISTING SYSTEM

Biometric combines the information collected from various sensors. Single biometric system has certain inherent problems such as noisy sensor data and error rates. Biometrics has been a concern from centuries providing once identity reliabily was done using several techniques. There are systems that required enrolment upstream of users.

Other identification systems do not require this phase. Authentication by biometric verification is becoming increasingly common in corporate and public security systems. In addition to security the driving force behind biometric verification has been convenience as there are no passwords to remember of security tokens to carry. Biometric data may be held in a centralized database. Biometric identifiers depend on the uniqueness of the factor being concerned.

PROPOSED SYSTEM

Multi-biometrics refers to the use of multiple sources of biometric information in order to establish the identity of an individual. Multi-biometric systems combine the biometric evidence offered by multiple biometric sensors (e.g., 2D and 3D face sensors), algorithms (e.g., minutia-based and ridge-based fingerprint matchers), samples (e.g., frontal and profile face images), units (e.g., left and right irises), or traits (e.g., face and iris) to enhance the recognition accuracy of a biometric system. Information fusion can be accomplished at several different levels in a biometric system, including the sensor-level, feature-level, score-level, rank-level, or decision-level. The challenge is to design an effective fusion scheme to consolidate the multiple pieces of evidence to generate a decision about an individual's identity.

ACTIVITY DIAGRAM

It shows the control flow from one activity to another. Activity diagram is another important diagram to describe dynamic behaviour. Activity diagram consists of activities, links, relationship .It models all types of flows like parallel, single, concurrent etc. Activity diagram describes the flow control from one activity to another without any messages. These diagrams are used to model high level view of business requirements

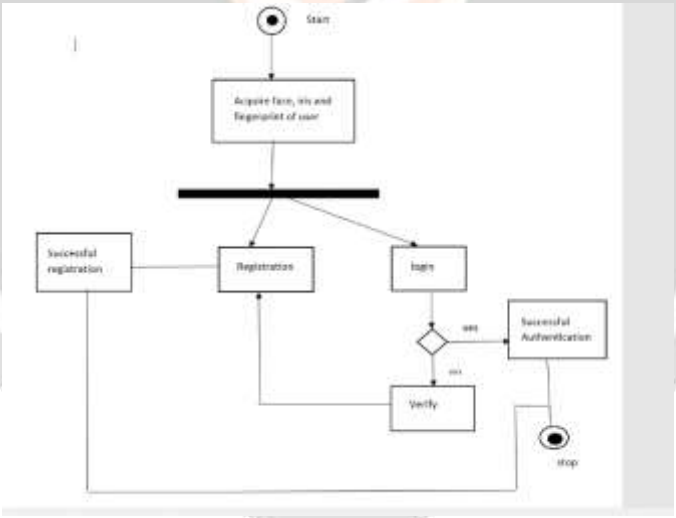

Figure**:** 1 Flow of Authentication System

LEVELS OF COMPARISON

As a basis for the definition of levels of combination in multi-biometric systems, Fig. 1 shows a single-biometric process. A biometric sample captured by a biometric sensor (e.g., a fingerprint image) is fed into the feature extraction module. Using signal processing methods, the feature extraction module converts a sample into features (e.g., fingerprint minutiae), which form a representation apt for matching. Usually, multiple features are collected into a feature vector. The matching module takes the feature vector as input and compares it to a stored template (a type of biometric reference, as defined in [2]). The result is a match score, which is used by the decision module to decide (e.g., by applying a threshold) whether the presented sample matches with the stored template. The outcome of this decision is a binary match or non-match. Generalizing the above process to a multi-biometric one, there are several

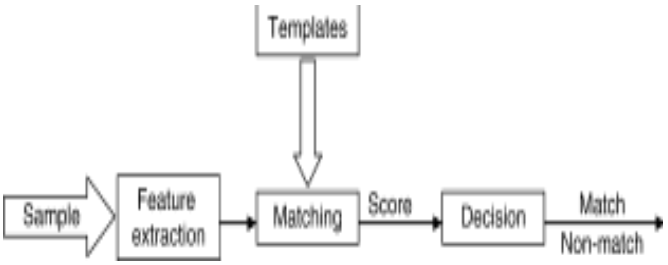

Figure: 2 Block diagram of authentication system

levels at which fusion can take place: (1) decision level (2) match score level (3) feature level and (4) sample level. Decision-level fusion takes place only after the results of matching from all biometric components are available. The decision module outputs match or non-match as a binary decision value. If a biometric system consists of a small number of biometric components, assigning logical values to match outcomes allows fusion rules to be formulated as logical functions. For two decision-level outputs, two most commonly used logical functions are logical AND & OR. For many decision-level outputs, various voting schemes can be used as fusion rules, the most common of which is majority voting. The logical AND & OR functions can be considered as voting schemes. In score-level fusion, each system provides matching scores indicating the proximity of the feature vector with the template vector. These scores can then be combined to improve the matching performance. The match score output by a matcher contains the richest information about the input biometric sample in the absence of feature-level or sensor-level information. Furthermore, it is relatively easy to access and combine the scores generated by several different matchers. Consequently, integration of information at the match score level is the most common approach in multimodal biometric systems. From a theoretical point of view, biometric processes can be combined reliably to give a guaranteed improvement in matching performance. Any number of suitably characterized biometric processes can have their matching scores combined in such a way that the multi-biometric combination is guaranteed (on average) to be no worse than the best of the individual biometric devices.

LEVELS OF FUSION

Based on the type of information available in a certain module, different levels of fusion may be defined. Sanderson and categorize the various levels of fusion into two broad categories: pre-classification or fusion before matching, and post-classification or fusion after matching (see Fig. 2). Such a categorization is necessary since the amount of information available for fusion reduces drastically once the matcher has been invoked. Pre-classification fusion schemes typically require the development of new matching techniques (since the matchers used by the individual sources may no longer be relevant) thereby introducing additional challenges. Pre-classification schemes include fusion at the sensor (or raw data) and the feature levels while post-classification schemes include fusion at the match score, rank and, decision levels.

1. Sensor-level fusion. The raw biometric data (e.g., a face image) acquired from an individual represents the richest source of information although it is expected to be contaminated by noise (e.g., non-uniform illumination, background clutter, etc.). Sensor-level fusion refers to the consolidation of (1) raw data obtained using multiple sensors, or (2) multiple snapshots of a biometric using a single sensor.
2. Feature-level fusion. In feature-level fusion, the feature sets originating from multiple biometric algorithms are consolidated into a single feature set by the application of appropriate feature normalization, transformation, and reduction schemes. The primary benefit of feature-level fusion is the detection of correlated feature values generated by different biometric algorithms and, in the process, identifying a salient set of features that can improve recognition accuracy. Eliciting this feature set typically requires the use of dimensionality reduction methods and, therefore, feature-level fusion assumes the availability of a large number of training data. Also, the features sets being fused are typically expected to reside in commensurate vector space in order to permit application of a suitable matching technique upon consolidating the feature sets.
3. Score-level fusion. In score-level fusion the match scores output by multiple biometric matchers are combined to generate a new match score (a scalar) that can be subsequently used by the verification or identification modules for rendering an identity decision. Fusion at this level is the most commonly discussed approach in the biometric literature primarily due to the ease of accessing and processing match scores (compared to the raw bio metric data or the feature set extracted from the data). Fusion methods at this level can be broadly classified into three categories: density-based schemes, transformation-based schemes, and classifier based schemas.

4. Rank-level fusion. When a biometric system operates in identification mode, the output of the system can be viewed a ranking of the enrolled identities. In this case, the output indicates the set of possible matching identities sorted in decreasing order of confidence. The goal of rank level fusion schemes is to consolidate the ranks output by the individual biometric subsystems to derive a consensus rank for each identity. Ranks provide more insight into the decision-making process of the matcher compared to just the identity of the best match, but they reveal less information than match scores. However, unlike match scores, the rankings output by multiple biometric systems are comparable. As a result, no normalization is needed and this makes rank level fusion schemes simpler to implement compared to the score level fusion techniques.
5. Decision-level fusion. Many commercial off-the-shelf (COTS) biometric matchers provide access only to the final recognition decision. When such COTS matchers are used to build a multi-biometric system, only decision level fusion is feasible. Methods proposed in the literature for decision level fusion include ‘‘AND’’ and ‘‘OR’’ rules, majority voting, weighted majority voting, Bayesian decision fusion, the theory of evidence, and knowledge space.

Figure: 3 Three biometric traits such as iris, face and finger are taken as the input.

A fusion of these three sample images is generated dynamically in the folder when we try to run the program.

Figure: 4 Fusion Image

SIMPLE FUSION

This type of fusion applies a rule to input opinions delivered by the experts. The rule is not obtained by 986M Multiple Classifiers training on expert opinions, but are decided by the designer of the supervisor. Assuming that the supervisor receives all expert inputs in parallel, common simple fusions

PROBABILISTIC FUSION

Experts can express opinions in various ways. The simplest is to give a strict decision on a claim of an identity, ‘‘1’’ (client) or ‘‘0’’ (impostor). A more common way is to give a graded opinion, usually a real number in [0, 1]. However, it turns out that machine experts can benefit from a more complex representation of an opinion, an array of real variables. This is not surprising to human experience because, a human opinion is seldom so simple or lacks variability that it can be described by what a single variable can afford. A richer representation of an opinion is therefore the use of the distribution of a score rather than a score. Bayes theory is the natural choice in this case because it is about how to update knowledge represented as distribution (prior) when new knowledge (likelihood) becomes available. Before describing a particular way o

f constructing a Bayesian supervisor let us illustrate the basic mechanism of Bayesian updating. Let two stochastic variables

X1, X2 represent these errors of two different measurement systems measuring the same physical quantity.

It is assumed that these errors are independent and are distributed normally as N (0, s12), N (0, s22), respectively. Then their weighted average

M = q1 X1 +q2 X2; where q1 +q2 = 1

is also normally distributed with N(0, q12s12 + q22s22).Given the variances s12, s22, if the weights q1,q2 are chosen inversely proportional to the respective variances, the variance of the new variable M (the weighted mean) will be smallest provided that where inverse-proportionality constants (the denominators) ensure q1 þ q2 1⁄4 1. Notice that the composite variable M is normally distributed always if the X1, X2 are independent but the variance is smallest only for a particular choice, (seen earlier) yielding

The fact that the composite variance never exceeds the smallest of the component variances, and that it converges to the smallest of the two when either becomes large, i.e. one distribution approaches the non-informative distribution N (0, 1), can be exploited to improve the precision of the aggregated measurements, Fig. 1.Appropriate weighting is the main mechanism on how knowledge as represented by distributions can be utilized to improve biometric decision making. Bayes comes handy at this point because it offers the powerful Bayes theorem to estimate the weights for the aggregation of the distributions, incrementally, or at one-go as new knowledge becomes available. We follow [4] to the fact that the composite variance never exceeds the smallest of the component variances, and that it converges to the smallest of
the two when either becomes large, i.e. one distribution approaches the non-informative distribution N(0, 1).

SAMPLE OUTPUT

The accuracy values are generated here

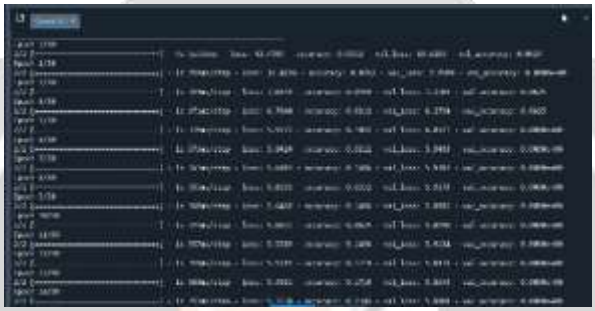

Figure: 5 Accuracy Values.

A graph which plots the accuracy values for training and validation.

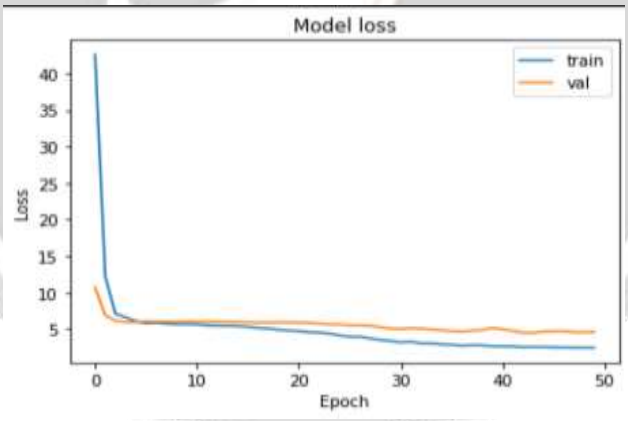

Figure: 6 Graph generated by plotting the accuracy values.

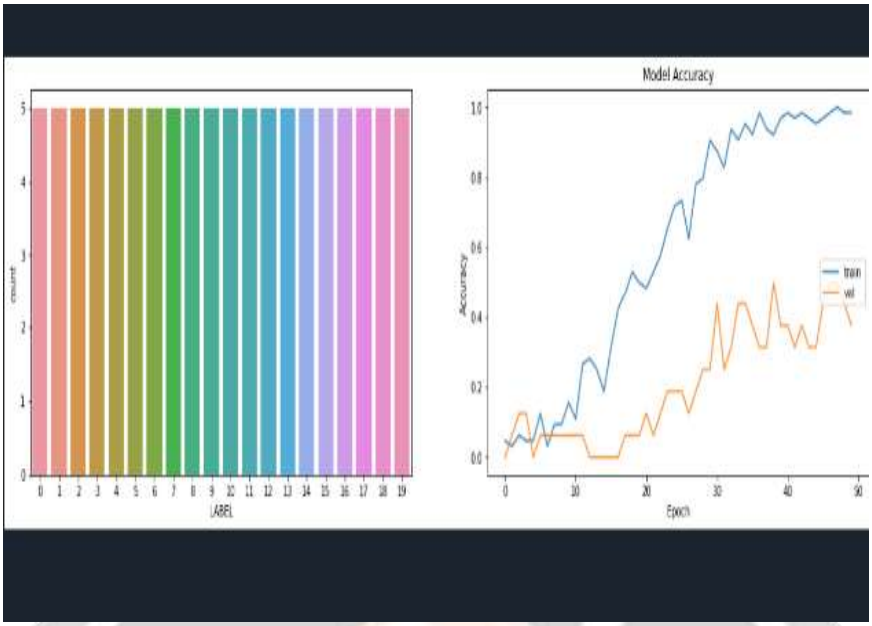

Figure: 7 The 20 labels for each sample are indicated here.

CONCLUSION

Multi-biometric systems are expected to enhance the recognition accuracy of a personal authentication system by reconciling the evidence presented by multiple sources of information. Early integration strategies (e.g., feature-level) are expected to result in better performance than late integration (e.g., score- level) strategies. However, it is difficult to predict the performance gain due to each of these strategies prior to invoking the fusion methodology. While the availability of multiple sources of biometric information (pertaining either to a single trait or to multiple traits) may present a compelling case for fusion, the correlation between the sources has to be examined before determining their suitability for fusion. Combining uncorrelated or negatively correlated sources is expected to result in a better improvement in matching performance than combining positively correlated sources. However, defining an appropriate diversity measure to predict fusion performance has been elusive thus far. Other topics of research in multi-biometrics include

(1) protecting multi-biometric templates;
(2) indexing multimodal databases;
(3) consolidating biometric sources in highly unconstrained non-ideal environments;
(4) designing dynamic fusion algorithms to address the problem of incomplete input data; and
(5) predicting the matching performance of a multi-biometric system.

REFERENCE

[1].Bigun, E.S., Bigun, J., Duc, B., Fischer, S.: Expert Conciliation for Multimodal Person Authentication Systems using Bayesian Statistics. In: Proceedings of First International Conference on Audio- and Video- N Based Biometric Person Authentication (AVBPA), pp. 291–300. Crane-Montana, Switzerland (1997)

[2].Hong, L., Jain, A.K., Pankanti, S.: Can Multi-biometrics Improve In: Proceedings of IEEE Workshop on Automatic Identification Advanced Technologies (AutoID), pp. 59–64. New Jersey, USA (1999)

[3].Ross, A., Nandakumar, K., Jain, A.K.: Handbook of Multibiometrics. 1st ed. Springer, New York, USA (2006)

[4].Jain, A.K., Ross, A.: Multibiometric Systems. Communications of the ACM, Special Issue on Multimodal Interfaces 47(1), 34–40 (2004)

[5].Kuncheva, L.I.: Combining Pattern Classifiers - Methods and Algorithms. Wiley (2004)

[6].Ho, T.K.: Multiple Classifier Combination: Lessons and Next Steps. In: 9392451551 H. Bunked, A. Kandel (eds.) Hybrid Methods in Pattern Recognition, Machine Perception and Artificial Intelligence, vol. 47, pp. 171–198. World Scientific (2002)

[7].Brielle, R., Falavigna, D.: Person Identification Using Multiple Cues IEEEChang, K.I., Bowyer, K.W., Flynn, P.J.: An Evaluation of Multimodal 2D+3D Face Biometrics. IEEE Transactions on Pattern Analysis and Machine Intelligence 27(4), 619–624 (2005) Transactions On Pattern Analysis and Machine Intelligence 17(10), 955–966 (1995)

[8].Sanderson, C., Paliwal, K.K.: Information Fusion and Person Verification Using Speech and Face Information. Research Paper IDIAP-RR 02-33, IDIAP (2002)

[9].Poh, N., Bengio, S.: How Do Correlation and Variance of Base Experts Affect Fusion in Biometric Authentication Tasks? IEEE Transactions on Signal Processing 53(11), 4384–4396 (2005)