Jurnal
Teknologi

Full Paper

MATCH SCORE FUSION OF FINGERPRINT AND FACE BIOMETRICS FOR VERIFICATION

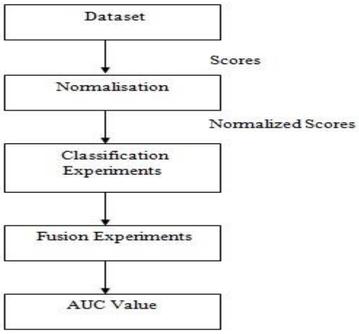
Chiung Ching Ho*, Mufaddal Ali Hussin, Hu Ng

Data Science SIG, Multimedia University, Cyberjaya, Malaysia

Article history
Received
15 May 2015
Received in revised form
1 July 2015
Accepted
11 August 2015

*Corresponding author
ccho@mmu.edu.my

Graphical abstract



Abstract

In recent years, attacks on password databases have been carried out at an increasing rate, with significant success. Thus, a new approach is needed to prove one's claim to identity instead of relying on a password. In this paper, we investigate the use of biometric match scores for the purpose of *verification*. Our work was performed using the BSSR1 multimodal match score biometric dataset, which contains match scores from face and fingerprint biometric systems. We investigated the use of match scores as a feature vector, and performed Simple Sum and Product Rule fusion of match scores. The results we obtained demonstrated that the use of match scores for *verification* purposes can be achieved to give a result that is highly accurate.

Keywords: Multimodal biometric fusion, match score fusion, verification, face, fingerprint, BSSR1

1.0 INTRODUCTION

Incidences of stolen passwords have been increasing of late. In 2015, companies as diverse as Uber, Toys "R" Us and Twitch reported that users' password were compromised [1], [2], [3]. The number of passwords compromised are in the millions [4], and recently a list of 10 million compromised passwords were shared in the public domain for educational purposes [5], [6]. These incidences have proven that passwords are becoming increasingly unreliable, and that a new solution for securing personal identity is needed.

Biometrics have been proposed as an alternative to passwords for securing personal identity. Biometrics are physical or physiological attributes of a person that can be used for proving one's claim to identity. Biometrics have been used to secure national identity cards and travel documents for up to 15 countries, and have been applied on smart-cards for identification and verification purposes [7]. A recent trend has seen biometrics being used in consumer electronic devices such as smartphones, tablets, laptops, fitness bands and even socks [8]. Although adoption of biometrics as proof of identity is a step in the right direction, it is by no means foolproof. There have been proven attacks on a single modality biometric systems [9], [10], [11], with high-profile attacks succeeding on premium consumer electronics such as the Iphone 6 [12].

A solution for the vulnerability caused by using a single biometric modality is the usage of more than one biometric modality as proof of identity, or also known as multimodal biometrics. Multimodal biometrics are becoming increasingly viable due to the increasing number of built in sensors (image, audio, accelerometers, fingerprint) found in many devices.

Such devices, however, will eventually lead to interoperability problems as there is a lack of standardization in terms of biometric sensors used, biometric data interchange, biometric sensor resolution, and biometric data revocation.

In our work, we present a solution to the problem of heterogeneous biometric sensors by examining multimodal biometric fusion which occurs at the match-score level. Match-score biometric fusion is independent of sensor type, sensor resolution and sensor data type as this approach uses the match score output from biometric recognition systems. While match-score fusion of biometric modalities has been attempted in the past, much of the efforts have been focused on the problem of *identification*, while the work done in this paper focuses on the task of *verification*. In this paper, we focus on match-score fusion of the biometric modalities of *fingerprint* and *face*

2.0 LITERATURE REVIEW

2.1 Biometric

Recognition and identification of a person in the natural world depends heavily on the recognition of physical, physiological and behavioural characteristics of a person. This can be seen in the behaviour of sentries at a guard post, who allows access past the post based on who they recognise. The earliest formal application of biometric as a proof of identity occurred when fingerprints were used in contracts to deter forgery. Bertilion [13] made use of fingerprint as a biometric in his anthropometry framework for person identification. Bertilion's approach was cumbersome, and did not ensure uniqueness for individuals. Advancement in fingerprint examination proved to be the eventual successor to Bertilion's system.

A number of different definitions have been given to the term "biometrics", dating back decades when [14] described biometrics as the scientific study of life measure. The modern day definition describes biometrics as a way of measurement of physical and physiological traits of a person for the purpose of recognition [15]. In order to facilitate effective person recognition, a biometric trait needs to exhibit the properties of being unique across individual, universally exhibited in all human person, and invariant over time [14].

Biometric as proof of identity have several advantages [16] when compared to the usage of passwords or tokens as proof of identity. Password and token based systems faces attacks such as client attacks (the guessing of password or the stealing of a token), host attacks (assessing files containing passwords), eavesdropping (observation of passwords being entered), repudiation (bogus claims that tokens were misplaced), trojan horse attacks (key loggers which captures password as they are keyed-in) and denial of service (locking out a system due to deliberate wrong entry of password). Biometrics are superior to password as biometrics are hard to be stolen or shared, and also offers negative recognition and non-repudiation. Negative recognition [17] excludes users who do not belong to a privileged set (e.g. list of users who are entitled to welfare payment), while non-repudiation prevents users who have used a biometric-authenticated system from falsely denying that they accessed said system.

Biometric systems can work in one of two ways [18], either *identification*, or *verification*. During *identification*, the biometric system aims to recognize a person by searching all the available biometric templates within a biometric system. Identification essentially is a one-to-many problem, to establish a person's identity without a claim to identity. Identification prevents a person from *assuming multiple identities* (a key aspect of negative identification), and also is used for convenience's sake. During *verification,* the biometric system the claim to identity by performing a one-to-one check to establish whether a claim is true or not, in order to prevent multiple people from assuming the same identity. Biometric verification is often solved by assuming that it is a two-class classification problem.

Unlike non-biometric systems, e.g. passwords, a perfect match between features from two sample of the same biometric trait belonging to the same person is rare. This is due various reasons, either attributed to the biometric sensor (noise in the sensor or occlusion), or the biometric system's user (changes due to illness, or ambient conditions or even changes in the manner of interaction with the biometric device). Due to these reasons, performance measures of a biometric system are many and varied [19]. The most commonly used measures includes Accuracy, False-Accept-Rate (FAR), Area Under ROC curve (AUC), False-Reject-Rate (FRR) and F-Measure. FAR is the rate at which an *impostor* user is mistakenly recognised as a *genuine* user, while FAR is the rate at which a *genuine* user is wrongly recognized as an *impostor*. Other measures related to FAR and FRR is the Genuine-Accept-Rate (GAR). Plotting FRR against FAR will result in two curves, the Detection Error Tradeoff (DET) and the Receiver Operator Characteristic (ROC), both of which will give the FRR and FAR at various threshold values. The performance of biometric systems may also be measured using the Equal Error Rate (EER), where FRR equals FAR on the DET curve. Another single measure performance measure for biometric system is the F-ratio, which is associated to the EER. Biometric systems may also be measured from a sensor and user perspective. Failure to Acquire (FTA) measures the rate at which the biometric sensor fails to acquire the biometric of a user (due to sensor wear and tear), while Failure to Enroll (FTE) measures the rate at which a user's biometric is non-readable, due to either natural causes (e.g. users without readable fingerprint) or failure in interaction.

A key consideration for choosing a biometric trait is that it must fulfil the following criteria:

- Universality – every user should posses this biometric trait
- Uniqueness – the trait can be told apart for members of a human population
- Permanence – the trait should be a invariant across time

- Measurability – the trait should be able to be acquired by a digital sensor without inconveniencing the user
- Performance - the chosen trait should be able to meet the biometric application's requirements
- Acceptability – users should be comfortable is providing this biometric trait
- Circumvention – the chosen biometric trait must be robust versus imitation via artifacts (e.g. silicone fingerprints), and mimicry

2.2 Multimodal Biometric Systems

Multimodal biometric systems can be defined as a biometric system which relies on more than one biometric trait for personal identification. Multimodal biometric systems can significantly overcome the limitations of a unimodal biometric system [20]. Unimodal biometric systems are limited, as the *d*-dimensional biometric feature set for an individual is often overlapping with that of another individual in the subspace manifold. Other factors, both operational and non-universality, further restrict the number of unique users. The usage of multimodal biometric solves this problem, by fusing different biometric traits, which expands the feature space, and results in more users being able to be enrolled in such a system. Multimodal biometric traits are also harder for imposters to forge as compared to a system relying on unimodal biometric characteristics. According to Hong and Jain [21], a greater level of assurance of a proper match in verification and identification modes are provided by multimodal biometric systems. Assurances offered by multimodal biometric system include:

- The addressing of the issue of non-universality encountered by unimodal biometric system
- Ability to facilitate the search and filter of large-scale biometric databases.

Multimodal biometric system have four modules, namely:

- Data-sensor module: Data from multiple sources are fused together
- Feature-extraction module: Computation of feature vector is done using data obtained from each sensor and two vectors are linked into a new vector, which in turn creates a higher dimensionality.
- Matching-score module: Scores which are generated by multiple classifiers pertaining to different modalities are combined.
- Decision module: The consolidation of final output of multiple classifiers is done.

A number of different fusion methods have been evaluated and reported in previous works. As discussed above, biometric fusion could involve more than one biometrics modality, which may involve a combination of physical biometrics and behavioural biometrics.

2.3 Fingerprint Biometric

Since the 20th century, fingerprints have been widely used and accepted as a form of valid authentication and have since become an effective measure for authentication procedure in various agencies worldwide. It has been reported that the Federal Bureau of Investigation (FBI) alone possesses 400 million fingerprints in their database [22]. Although technological advancement has brought in new biometric models such as iris and retina scans, the fingerprint is still considered as one of the most usable biometrics due to its uniqueness and consistency. Biometrics such as iris and retina scan offers similar characteristics such as uniqueness and consistency, but suffers from drawback such as high-cost of implementation and its usage is perceived by users as intrusive. Similarly, although behavioural biometric systems such as voice recognition are non-intrusive, but these tend to be affected by factors such as background noise and can be easily compromised by impostors. The advantages offered by fingerprint biometric are as follows:

- Performance - One of the main advantages offered by fingerprint biometric is the fact that it offers high level of accuracy. Studies in the past have proven that fingerprint recognition technology has the probability of reaching recognition of near 100% depending on the quality of image.
- High Distinctiveness - Fingerprints are unique for each and every individual, to the extent that even identical twins have different fingerprints. This advantage is further enhanced by the fact that fingerprint biometric may enrol multiple samples ,which means if one finger shows some problem ,there are still nine fingers which may be used. In addition, use of multiple fingers for recognition has proved to provide improvisation in a biometric system.
- Acceptability - Fingerprints have always been seen as a biometric measure which is widely accepted by the general public and can be easily obtained

The main limitations of a fingerprint as a biometric are:

- Some of the limitations encountered in a fingerprint are that in some cases, it may fail to enrol a fraction of the population. It has been reported that some two percents of the entire population posses fingerprints which are poor in quality and are not usable as a biometric.
- Degradation of fingerprint is considered as another drawback of fingerprint biometric. It has been reported that fingerprint's performance tend to deteriorate over time. This disadvantage has often been linked to factors such as the aging process where the fingerprint may suffer from some small

changes over a time period and therefore, affects the performance of a whole system.

2.3.1 Fingerprint Features

The scientific establishment of distinctive fingerprints features can be traced back to 1872, when the anthropologist Francis Galton [23] discovered a fingerprint characteristic known as a "minutiae" that are usually used to determine whether two fingerprints match.

Fingerprint features include the ridge, furrows, and minutiae points, orientation of minutiae points, distances between minutiae points, whorl and curves of fingerprints [24]

Ridges flow are considered as unique for each and every individual, however, past work have suggested that fingerprints are actually distinguished by abnormal points on the ridges known as "minutiae" .These minutiae features consist of a number of patters as follows:

- Crossover - A short ridge that runs between two parallel ridges
- Core - Inner point, normally in the middle of the print, around which swirls, loops, or arches center. Normally categorised by ridge ending and several acutely curved ridges.
- Bifurcation - a single ridge that divides into two ridges
- Ridge ending – single ridge which divides into two ridges
- Island - An independent ridge with approximately equal length and width
- Delta - Points ,normally at the lower left and right hand of the fingerprint , around which a triangular series of ridges center

These are the features that are usually extracted from the fingerprint in order to find a match in a database.

2.4 Overview of Face Biometric

Facial biometric can be considered as one of the fastest growing form of biometrics. In term of personal identification, face recognition refers to static, controlled full-frontal portrait recognition. Face recognition is considered as the automated computer recognition of an individual, which is based on geometric or statistical features derived from a captured face image. A survey by Chellappa *et al*. [25], has shown that face recognition have a number of strengths compared to other biometric modalities, however it is pegged back by few other weaknesses which has made it inappropriate for other applications. Some of the advantages offered by a Face Biometric are:

- Universality - Being ubiquitous and being universal compared to other biometric
- Acceptability - It is considered as non-intrusive and easy-to-use method, which means face recognition can be done in a passive way without participation of particular individuals.

However, as discussed previously, face biometric is pegged by some weaknesses and some of the main challenges faced are in terms of lighting changes and changes in the individual's appearance. The limitations of using face recognition are as follows:

- Pose and lighting variances, as well as imitation attacks (using photos or face masks) are still difficult problems to solve

2.4.1 Face Features

In the face verification process, the feature set from the image of the user's face is extracted and is compared with templates which are stored in the appropriate data structure. Before the feature extraction is executed, the face detection process is done whereby the position and space of the face is determined in the given image [26]. The process is particularly difficult considering to some factors that are involved.

One of the main factor is the human face itself, with the high degree of variability on color, texture, expression and pose found on human faces. Other external factors such as backgrounds and variable lighting conditions also affect the detection of the face.

Spatial coordinates of a face within an image have been reported to be useful in solving the variances mentioned above[27]. After the perimeter of the face is detected and established, Eigenface features can be extracted successfully.

In the eigenface approach, a set of orthonormal vectors that span a lower dimensional subspace is first computed using the Principal Components Analysis (PCA) technique. Feature vector of face image is the projection of the image on the eigenface. For the matching phase, computing the eigenface coefficients of the template and the detected face can be done using techniques such as Euclidean Distance.

2.5 Face and Fingerprint Multimodal Systems

Face and fingerprint biometrics formed the earliest multimodal biometric system that were developed by researchers [28], [29], [30], [31].

The reasons that both face and fingerprint biometrics were chosen were primarily linked to the factors of utility and user acceptance. In terms of utility, many official documents incorporates face biometric and fingerprint biometric (for instance, Malaysia's national identification card MyKad and passport [32], [22]), and as such the practical application of fusing face and fingerprint biometrics is not in doubt. In terms of user acceptance, most people are used to the concept of using photographs and thumb or fingerprints as proof of identity. A third reason that encouraged initial research into face and fingerprint multimodal biometric systems was the ready availability of sensors that could be used to capture and digitize face and fingerprint biometric samples. The individual advantages of face and fingerprint biometric modalities were discussed at length in Sections 2.3 and 2.4. For researchers, the abundance of bench-marked multimodal datasets [33] incorporating both face and fingerprint modalities undoubtedly encouraged research in this area.

Recent lines of research pertaining to face and fingerprint multimodal biometric systems include investigation into image quality of related systems (palm print and face)[34], [35], privacy preservation [36] and the issue of mutual dependency between face and fingerprint biometric features and its effect on accuracy [37].

2.6 Different Level of Fusion

Various levels of fusion can be implemented when combining multimodal biometric systems [38]. The most notable fusions are: (a) Feature extraction level (b) Match score level and (c) Decision level.

Fusion can be defined as the use of multiple types of biometric data or methods of processing in order to improve the performance of the biometrics. In general, fusion can be done on the different levels mentioned previously. Match-score fusion is a very popular method as there is easy access to the data which is to be fused and match-score fusion is relatively easy to be implemented. However, one of the drawbacks in match-score level fusion is that information obtained at a match-score level might be limited and may result in inferior performance. This is due to loss of information that might occur within the individual biometric scoring system.

2.6.1 Fusion at Feature Extraction Level

Despite extensive research conducted on multimodal biometrics' fusion in the past, fusion of multimodal biometrics at feature level haven't been given a vast amount of attention compared to fusion at a match-score level. Feature level fusion is implemented by concatenating the feature points gathered from different sources of information. Fusion at feature extraction level is considered hard to achieve due to the fact that multiple modalities tend to have incompatible feature sets and the correlation among different features are largely unknown. Moreover, Ross [39] in his literature reported that "concatenated feature set may lead to the problem of curse dimensionality; a very complex matcher may be required and the concatenated feature vector may contain noisy or redundant data, thus leading to a decrease in the performance of the classifier". However, researchers who have conducted fusion at feature level have reported significant results. Gyavoura *et al*. [40], reported that experiment conducted on the fusion of IR-based face recognition with visible based face recognition at a feature level showed a substantial improvement in recognition performance as compared to matching individual sensor modalities. There are more advantages in the feature level fusion since most of the information is available and the salient set of feature is able to be identified to improve recognition accuracy compared to the other levels. However, fusion at feature level is still considered to be more difficult due to the fact that features of different modalities have different dimensions.

2.6.2 Fusion at Match-Score Level

Match-score fusing is commonly preferred by researchers due to the fact that sufficient information can be obtained from the match scores which can easily distinguish genuine and impostor case. One of the advantages of the match score level is that match-scores can be used even without extensive knowledge of the feature extraction and matching algorithms that were deployed in the individual biometric system. This leads to combining information obtained from individual modalities using match-score level fusion both feasible and practical.

Generally, score level fusion techniques can be divided into three categories:

- Transformation-based score level fusion
- Classifier-based Fusion
- Density-based score level fusion

For the purpose of this paper, multiple biometric fusions which include face and fingerprint will be adopted and experiments will be done on a match-score level using a classifier-based approach.

2.7 Normalization

2.7.1 Min-Max

Min-Max normalisation is considered as one of the simplest form of normalisation techniques. Jain A. *et al* [38], reported that when bounds (maximum and minimum values) are available for a dataset, min-max normalisation technique is best suited for the dataset. This is the case for the BSSR1 dataset, where the bounds of the match-scores are known a priori.

In this paper, the first normalisation technique which is used for the experimental work is the Min-Max normalisation technique. Since the maximum and minimum scores of the dataset are available, it is assumed that the min-max normalisation technique will work very well. Apart from that, min-max normalisation technique is considered to be really efficient. Before the min-max technique can be applied, maximum and minimum values from the dataset are extracted.

However, the min-max normalisation method is considered as highly sensitive to outliers in the data used for estimation and this is one of the factors why it is considered as not robust [41]. Min-Max normalisation technique is used to transform the scores into a common range of between zero and one [0, 1].

2.7.2 Z – Score

Another commonly used method for normalisation for biometric dataset is the Z – Score normalisation technique. Z-Score normalisation is computed using the mean and standard deviation of the given data. Using Z-Score normalisation technique, normalized scores are calculated using arithmetic means and standard deviation of the given dataset. Z-Score normalisation technique usually works well when average score and variations of the matcher are available. Similar to min-max normalisation technique, Z-score normalisation technique is considered as not robust since standard deviation and mean are sensitive to outliers of the data.

2.7.3 Median and Median Absolute Deviation (MAD)

The third normalisation technique used in the work performed is the median and MAD normalisation technique. Median and MAD technique is considered as relatively robust as it is not sensitive to the outliers of the data. A Median and MAD normalisation technique has a high efficiency, however the scores cannot be transformed into a common numerical range.

2.7.4 Tanh-Estimator

The last normalisation technique which is used in this paper is the Tanh-Estimator normalisation technique. Tanh-Estimator normalisation technique is considered as highly effective and robust.

3.0 METHODOLOGY

3.1 Biometric Score Set Release 1 (BSSR1)

In this paper, we performed match score fusion of fingerprint and face biometrics for *verification*, using the Biometric Scores Set Release 1 (BSSR1) [42]. BSSR1 is a set of output similarity scores one fingerprint system and two face recognition systems, operating on left and right index live-scan fingerprints, and frontal faces respectively. The release includes true multimodal score data, i.e. similarity scores from comparisons of faces and fingerprints of the same people. In our work we made use of Set 1 from BSSR1, which contains face and fingerprint scores from the same 517 subjects. For each subject, the set contains one score from the comparison of two right index fingers (RI), one score for comparison of two left index fingers(LI), and two scores from two different matchers (known as Face C and Face G respectively). For each subjects, the set contains one score from the comparison of two right index fingers (RI), one score for comparison of two left index fingers(LI), and two scores from two different matchers (Called Face C and Face G). The total number of scores (Genuine and Impostors) 4 x 517 x 517 = 1069159.

3.2 Experimental workflow

The experimental workflow used in our work is shown in Figure 1.

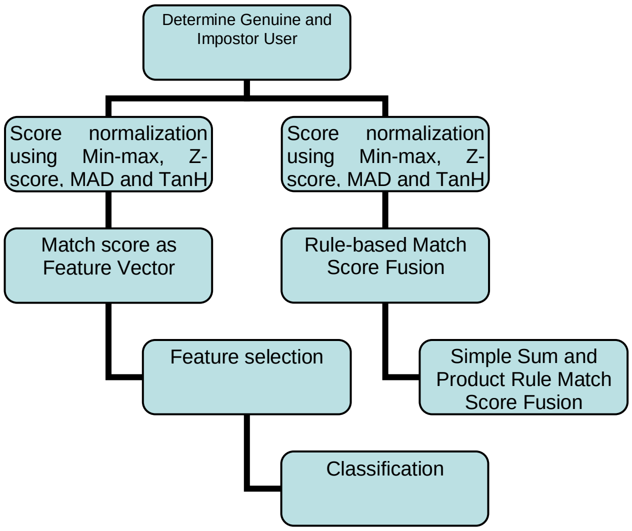

Determine Genuine and Impostor User
Score normalization using Min-max, Z-score, MAD and TanH
Score normalization using Min-max, Z-score, MAD and TanH
Match score as Feature Vector
Rule-based Match Score Fusion
Feature selection
Simple Sum and Product Rule Match Score Fusion
Classification

Figure 1 Experimental workflow

3.2.1 Determination of identity of Users and Enrollees

The data provided in BSSR1 is made up of similarity scores for the 517 subjects in a one-versus-all comparison (each of the 517 subject's face or fingerprint will be tested against the other users) for the face and fingerprint systems. At the same time, a list of users in the Users and Enrollees group is given (Users are people who were authenticated using the biometric systems, while Enrollees were people whose biometric traits were recorded using the biometric systems). The identity of an User and an Enrollee is determined by comparing the "name" against the "subject_id".

3.2.2 Partitioning of BSSR1 into Multimodal Biometric Datasets

Table 1 shows how the BSSR1 dataset is organized, in terms of biometric scores and biometric system types. Systems C, G, Li and Ri are unimodal biometric systems representing the face scores and index finger scores. These scores were combined to create 4 multimodal biometric scores dataset as shown in Table 2.

3.2.3 Match Scores as a Feature Vector and Feature Selection

One technique for fusing match scores is to concatenate match scores from different biometric modalities to form a new feature vector. In our work, we concatenated the match scores from different systems (G, G and V) for Users and Enrollees to form a new feature vector of match scores. This resulted in a feature vector which has a length of 1034 (there were 517 scores for the face modality and 517 scores for the fingerprint modality). As the concatenated feature vector length is long, we subsequently performed feature selection using a gain ratio feature selection technique.

Table 1 Composition of Biometric Systems in BSSR1

BSSR-1 Dataset (Partition One)		Labelled as	System Type
Face Scores	System C	C	Unimodal System
Face Scores	System G	G	Unimodal System
Left Index Finger Scores	System V	Li	Unimodal System
Right Index Finger Scores	System V	Ri	Unimodal System

3.2.4 Match Scores Normalization using Min-max, Z-score, MAD and TanH

The match scores for each biometric system had values on non-uniform scales. Values for the match scores ranged from decimal values less than one, up to decimal values of 100. Failure to normalize the scores will result in uneven weightage for biometric modalities

3.2.5 Simple Sum and Product Rule Match Score Fusion

The Simple Sum and Product rules match score fusion aggregates match scores from biometric systems to result in a new aggregated score.

For the Simple Sum rule, the match score for each biometric modality is summed up, while the Product rule multiplied the match score for each biometric modality. Subsequently, a threshold value was chosen to evaluate whether to a score belonged to a Enrollee or to a User. In the work we performed, the threshold value was set at 1.25 (using normalized scores as described in Section 2.7) after examining the statistical distribution of scores after application of the Simple Sum and Product Rule. The TPR and FPR rates were calculated, and subsequently the Area Under ROC curve were calculated as the effective measure.

4.0 RESULTS AND DISCUSSION

4.1 Match scores as a feature vector

The four datasets partitioned from BSSR-1 (namely CLi, CRi, GLi and GRi) were normalized using the Min-max, Z-score, MAD and TanH normalization techniques and were subsequently concatenated into a 1034 length feature vector. Each dataset has 224 Enrollees and 293 Users. Experiments were conducted using 10-fold cross validation, and were performed using the Weka data mining tool[43].

A total of 48 experiments were carried out using permutations of four datasets normalized using four normalization techniques, and evaluated using the following classifiers:

1. Bayes Network
2. k-Nearest Neighbour
3. Support Vector Machines (SVM)

In the interest of brevity, a summary of the most interesting results are presented in this section.

Tables 3-5 shows the effect of normalization techniques that were applied on face-and-fingerprint datasets using different classifiers. The Min-Max technique shows good results across different classifiers as compared to Z-Score, MAD and TanH.

As it is clear that the Min-Max normalization technique produces the best results in terms of area under ROC curve (which is a measure of the ability of the classifiers to distinguish between the Enrollee and User classes), the next line of investigation undertook was to investigate the performance of the match score feature vectors using different classifiers.

Table 2 Partitions of BSSR1 as multimodal biometric datasets

Dataset labels	System Type
C + Li = CLi	Multimodal System
C + Ri = CRi	Multimodal System
G + Li = GLi	Multimodal System
G + Ri = GRi	Multimodal System

Table 6 shows the accuracy, TPR, FPR and F-Measure for the four datasets using the Bayes Network, k-Nearest Neighbor and Support Vector Machine classifiers post Min-Max Normalization.

The SVM classifier performed very well in terms of accuracy, TPR and FPR and F-Measure across all the four datasets. This result is in line with SVM's ability to perform well in a two-class problem, particularly when the feature vector has been normalized.

The Bayes Network classifier performs well across all four datastes in terms of accuracy, TPR and F-Measure. False positives are prevented only in the GLi and GRi datasets using the Bayes Network classifier.

K-nearest neighbor was the least suitable classifier for use across the four datasets. It performed poorly compared to Support Vector Machine and Bayes Network in terms of all the effective measures.

Table 3 Area under ROC curve using Bayes Network

Normalization Technique	Area under ROC curve			
	CLi	CRi	GLi	GRi
Z-Score	0.99	0.99	0.99	0.99
Min-Max	1	0.99	0.88	0.97
Tan-H Estimator	0.99	0.97	0.99	0.99
Median Absolute Deviation	0.48	0.52	0.47	0.46

Normalization Technique	Area under ROC curve			
	CLi	CRi	GLi	GRi
Z-Score	0.53	0.54	0.54	0.51
Min-Max	0.87	0.51	0.89	0.53
Tan-H Estimator	0.48	0.52	0.51	0.51
Median Absolute Deviation	0.52	0.55	0.53	0.53

Table 4 Area under ROC curve using k-Nearest Neighbour

Table 5 Area under ROC curve using SVM

Normalization Technique	Area under ROC curve			
	CLi	CRi	GLi	GRi
Z-Score	0.57	0.50	0.57	0.57
Min-Max	0.98	0.99	0.96	0.96
Tan-H Estimator	0.50	0.57	0.50	0.57
Median Absolute Deviation	0.50	0.50	0.53	0.50

4.2 Simple Sum and Product Rule

As described in Section 3.2.5, we performed Simple Sum and Product Rule fusion for match scores as a complement to our approach to using the match scores as a feature vector.

Table 7 shows the Area Under AUC Curve using the Simple Sum and Product Rule. The Simple Sum Rule did not perform as well as the Product Rule in our experiment. Overall, once the scores have been normalized using the Min-Max normalization technique, it tends to result in better performance as compared to the other normalization technique.

Although the best result of using both Simple Sum and Product rule is not as good as compared to the best result of the match-score feature vector approach, it is worth to take note that the Simple Sum and Product Rule outperformed all the classifiers except for the Support Vector Machine. As such, the choice of using Simple Sum and Product Rule might be valid in circumstances when time constraints prevents extensive testing of classifiers.

Table 6 Accuracy rate, TPR, FPR and F-Measure for different classifiers

	Accuracy rate for Bayes Network	Accuracy rate for K-nearest neighbor	Accuracy rate for SVM
CLi	100	86.27	98.45
CRi	100	50.87	98.45
GLi	99.23	88.2	95.5
GRi	97.29	54.16	95.36
	TPR for Bayes Network	**TPR for K-nearest neighbor**	**TPR for SVM**
CLi	1	1	1
CRi	1	0.585	1
GLi	0.987	0.991	0.973
GRi	0.938	0.567	0.973
	FPR for Bayes Network	**FPR for K-nearest neighbor**	**FPR for SVM**
CLi	1	0.242	0.027
CRi	1	0.549	0.027
GLi	0.003	0.201	0.058
GRi	0	0.478	0.061
	F-Measure for Bayes Network	**F-Measure for K-Nearest neighbour**	**F-Measure for SVM**
CLi	1	0.863	0.982
CRi	1	0.508	0.982
GLi	0.991	0.879	0.95
GRi	0.968	0.517	0.948

5.0 CONCLUSION

In an age where incidences of password being stolen are on the rise, a new approach towards proof of identity is needed. In this paper, we investigate the use of face and fingerprint biometric scores as proof of identity in a *verification* setting.

We investigated the use of biometric scores as a feature vector, and achieved this by combining face and fingerprint scores from the BRR1 dataset to form a new feature vector, to be used in a classification task to classify Enrollees and Users. We complemented this approach by investigating the use of Simple Sum and Product Rule for *verification* purposes.

Table 7 Area Under AUC Curve using the Simple Sum and Product Rule

	Area Under ROC Curve Using Simple Sum Rule			
Normalisation Techniques	**CLi**	**CRi**	**GLi**	**GRi**
Z- Score	0.62	0.58	0.53	0.51
Min-Max	0.68	0.64	0.71	0.61
Tan-H	0.64	0.70	0.62	0.63
Median Absolute Deviation	0.66	0.59	0.68	0.62
	Area Under ROC Curve Using Product Rule			
Normalisation Techniques	**CLi**	**CRi**	**GLi**	**GRi**
Z- Score	0.65	0.70	0.68	0.74
Min-Max	0.81	0.68	0.76	0.72
Tan-H	0.56	0.60	0.56	0.58
Median Absolute Deviation	0.61	0.80	0.77	0.76

The result of our work demonstrates that using face and fingerprint match scores as a feature work performs well in a verification setting, particularly when Support Vector Machines are used as the classifier, after Min-Max normalization. Simple Sum and Product Rule fusion did not perform as well, although it's performance is comparable to that achieved by using the Bayes Network and k-nearest neighbor classifiers.

For future work, we aim to use different normalisation techniques, different classification techniques and different databases to evaluate the performance of fusion of multimodal biometrics.

References

[1] S. Murphy Kelly. 2015. Uber Passwords from Hacked Accounts Reportedly Selling Online for $1. *Mashable*, 30-Mar-2015. [Online]. Available: http://mashable.com/2015/03/29/hacked-uber-passwords-selling/. [Accessed: 27-Apr-2015].

[2] K. Ellison. 2015. Toys 'R' Us Resets User Passwords Following Stolen Rewards. *Welivesecurity*, 03-Mar-2015. [Online]. Available: http://www.welivesecurity.com/2015/03/03/toys-r-us-resets-account-passwords-counter-stolen-reward-points/. [Accessed: 27-Apr-2015].

[3] T. For-Brewster. 2015. Amazon's Twitch Hacked, Caves to Angry User Demands for Less Secure Passwords - Forbes. *Forbes*, 24-Mar-2015. [Online]. Available: http://www.forbes.com/sites/thomasbrewster/2015/03/24/amazon-twitch-hacked-passwords-nabbed/. [Accessed: 27-Apr-2015].

[4] J. Condliffe. 2015. The 25 Most Popular Passwords of 2014: We're All Doomed. *Gizmodo*, 20-Jan-2015. [Online]. Available: http://gizmodo.com/the-25-most-popular-passwords-of-2014-were-all-doomed-1680596951. [Accessed: 27-Apr-2015].

[5] L. Rehmann. 2015. Search Mark Burnett's 10 Million Usernames/Passwords. *rehmann.co*, 2015. [Online]. Available: https://rehmann.co/projects/10mil/. [Accessed: 27-Apr-2015].

[6] Z. Epstein. 2015. 10 Million Passwords Leaked: How to check if yours is one of them | BGR. *BGR*, 12-Feb-2015. [Online]. Available: http://bgr.com/2015/02/12/10-million-passwords-leaked-hack-check/. [Accessed: 27-Apr-2015].

[7] S. Alliance. 2011. Smart Cards and Biometrics. *Available www Smartcardalliance Org*.

[8] C. Kang. 2014. Consumer Electronics Show Will Highlight New Ways to Collect Biometric Data-The Washington Post. *The Washington Post*, 05-Jan-2014. [Online]. Available: http://www.washingtonpost.com/business/technology/consumer-electronics-show-will-highlight-new-ways-to-collect-biometric-data/2014/01/05/e8eac584-74c4-11e3-8def-a33011492df2_story.html. [Accessed: 27-Apr-2015].

[9] U. Uludag and A. K. Jain. 2004. Attacks on Biometric Systems: A Case Study in Fingerprints. In *Electronic Imaging 2004*. 622-633.

[10] A. Obied. 2009. How to Attack Biometric Systems in Your Spare Time. *Non Refereed Pap.*

[11] C. Rathgeb and A. Uhl. 2011. Statistical Attack Against Iris-Biometric Fuzzy Commitment Schemes. In *2011 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*. 23-30.

[12] R. Lemos. 2015. Fake Fingerprint Fools iPhone 6 Touch ID | Ars Technica. *arstechnica*, 25-Sep-2014. [Online]. Available: http://arstechnica.com/security/2014/09/25/fake-fingerprint-fools-iphone-6-touch-id-why-its-not-so-serious/. [Accessed: 27-Apr-2015].

[13] C. Chapman. 1993. Alphonse M. Bertillon: His Life and the Science of Fingerprints. *J. Forensic Identif.* 43(6): 585-602.

[14] A. K. Jain, P. Flynn, and A. Ross. 2008. *Handbook of Biometrics*. Boston, MA: Springer Science Business Media, LLC.

[15] J. D. Woodward. 1997. Biometrics: Privacy's Foe or Privacy's Friend? *Proc. IEEE*. 85(9): 1480-1492.

[16] A. K. Jain. 1999. *Biometrics: Personal Identification in Networked Society*. Boston: Kluwer.

[17] S. Prabhakar, S. Pankanti, and A. K. Jain. 2003. Biometric Recognition: Security and Privacy Concerns. *IEEE Secur. Priv.* 2: 33-42.

[18] A. Ross and A. Jain. 2003. Information Fusion in Biometrics. *Pattern Recognit. Lett.* 24(13): 2115-2125.

[19] P. J. Phillips, A. Martin, C. L. Wilson, and M. Przybocki. 2000. An Introduction Evaluating Biometric Systems. *Computer*. 33(2): 56-63.

[20] V. C. Subbarayudu and M. V. N. K. Prasad. 2008. Multimodal Biometric System. In *First International Conference on Emerging Trends in Engineering and Technology, 2008. ICETET '08*. 635-640.

[21] L. Hong, A. K. Jain, and S. Pankanti. 1999. Can Multi-biometrics Improve Performance. In *Proc. 1999 IEEE Workshop on Automatic Identification Advanced Technologies (WAIAT-99)*, Morristown NJ. 59-64.

[22] C. C. Ho and C. Eswaran. 2011. Consodilation of Fingerprint Databases: A Malaysian Case Study. In *In the*

Proceedings of the 2011 11th International Conference on Hybrid Intelligent Systems (HIS). 455-462.

[23] K. Pearson. 2011. *The Life, Letters and Labours of Francis Galton*. Cambridge University Press.

[24] Y. Chen and A. K. Jain. 2009. Beyond Minutiae: A Fingerprint Individuality Model with Pattern, Ridge and Pore Features. In *Advances in Biometrics*, vol. 5558, M. Tistarelli and M. S. Nixon, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg. 523-533.

[25] R. Chellappa, C. L. Wilson, and S. Sirohey. 1995. Human and Machine Recognition of Faces: A Survey. *Proc. IEEE*. 83(5): 705-741.

[26] A. K. Jain and A. Ross. 2004. Multibiometric Systems. *Commun. ACM*. 47: 34.

[27] Y. M. Lui, D. Bolme, P. J. Phillips, J. R. Beveridge, and B. A. Draper. 2012. Preliminary Studies on the Good, the Bad, and the Ugly Face Recognition Challenge Problem. In *2012 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*. 9-16.

[28] A. K. Jain, L. Hong, and Y. Kulkarni. 1999. A Multimodal Biometric System Using Fingerprint, Face and Speech. In *Proceedings of 2nd Int'l Conference on Audio-and Video-based Biometric Person Authentication, Washington DC*, 182-187.

[29] A. K. Jain, A. Ross, and S. Prabhakar. 2004. An Introduction to Biometric Recognition. *IEEE Trans. Circuits Syst. Video Technol.* 14: 4-20.

[30] L. C. Jain, U. Halici, I. Hayashi, S. Lee, and S. Tsutsui. 1999. *Intelligent Biometric Techniques in Fingerprint and Face Recognition*. Vol. 10. CRC Press.

[31] L. Hong and A. Jain. 1998. Integrating Faces and Fingerprints for Personal Identification. *Pattern Anal. Mach. Intell. IEEE Trans. On*. 20(12): 1295-1307.

[32] C. C. Ho and C. Eswaran. 2013. Consolidation of Fingerprint Databases: Challenges and Solutions in the Malaysian context. *Int. J. Comput. Inf. Syst. Ind. Manag. Appl.* 5: 373-382.

[33] M. Gomez-Barrero and J. Fierrez. 2015. "ATVS-Biometric Recognition Group » Databases. [Online]. Available: http://atvs.ii.uam.es/databases.jsp. [Accessed: 27-Jun-2015].

[34] J. Galbally, S. Marcel, and J. Fierrez. 2014. Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition. *IEEE Trans. Image Process.* 23(2): 710-724.

[35] N. Mohamad, M. I. Ahmad, R. Ngadiran, M. Z. Ilyas, M. N. M. Isa, and P. Saad. 2014. Investigation of Information Fusion in Face and Palmprint Multimodal Biometrics. In *2014 2nd International Conference on Electronic Design (ICED)*. 347-350.

[36] K. Gunasekaran, S. A. Priya, D. Saravanan, and P. Akilan. 2014. Privacy Preserving Multimodal Biometrics in Online Passport Recognition. *Biom. Bioinforma*. 6(3): 94-98.

[37] S. Wang, C. Chen, W. Yang, and J. Hu. 2015. Mutual Dependency of Features in Multimodal Biometric Systems. *Electron. Lett.* 51(3): 234–235.

[38] A. Jain, K. Nandakumar, and A. Ross. 2005. Score Normalization in Multimodal Biometric Systems. *Pattern Recognit.* 38(12): 2270-2285.

[39] A. Ross. 2005. *Multimodal Biometrics: Human Recognition Systems*. New York, London: Springe.

[40] A. Gyaourova, G. Bebis, and I. Pavlidis. 2004. Fusion of Infrared and Visible Images for Face Recognition. In *Computer Vision-ECCV 2004*, vol. 3024, T. Pajdla and J. Matas, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg. 456-468.

[41] K. Nandakumar, Yi Chen, S. C. Dass, and A. K. Jain. 2008. Likelihood Ratio-Based Biometric Score Fusion. *IEEE Trans. Pattern Anal. Mach. Intell.* 30: 342-347.

[42] NIST. 2015. NIST Biometric Scores Set. 2006. [Online]. Available: http://www.nist.gov/itl/iad/ig/biometricscores.cfm. [Accessed: 10-May-2015].

[43] M. Hall, E. Frank, G. Holmes, B. Pfahringer, P. Reutemann, and I. H. Witten. 2009. The WEKA data mining software. *ACM SIGKDD Explor. Newsl.* 11(1): 10.