RESEARCH ARTICLE OPEN ACCESS

A Survey of Security of Multimodal Biometric Systems

Suvarnsing G. Bhable
Research Student Dept of CS & IT Dr. B. A. M. University, Aurangabad

ABSTRACT
A biometric system is essentially a pattern recognition system being used in adversarial environment. Since, biometric system like any conventional security system is exposed to malicious adversaries, who can manipulate data to make the system ineffective by compromising its integrity. Current theory and design methods of biometric systems do not take into account the vulnerability to such adversary attacks. Therefore, evaluation of classical design methods is an open problem to investigate whether they lead to design secure systems. In order to make biometric systems secure it is necessary to understand and evaluate the threats and to thus develop effective countermeasures and robust system designs, both technical and procedural, if necessary. Accordingly, the extension of theory and design methods of biometric systems is mandatory to safeguard the security and reliability of biometric systems in adversarial environments.
Keywords: Face, Fingerprint, Unimodal Biometrics & Multimodal Biometrics

I. INTRODUCTION

We human beings have an innate ability to recognize, identify, and categorize objects in a seemingly efficient, fast and effortless fashion. For instance, a child can recognize easily his best friend in a picture without experiencing any problem. Since the recognition process occurs subliminally, hence it is hard even for the computer scientists in conventional research paradigms to translate this process into a computer algorithm as accurate as human being. In other words, it is neither possible to explain nor to perceive meticulously how the recognition process works. However, Alan Turing (1912-1954), who is widely considered to be the father of modern computer science and artificial intelligence, thought that future had already arrived and in a couple of years machines would be able to think and act automatically such as understanding verbal languages or reading handwritten character (letter or number) and so forth. In a point of fact, these are still open research issues and very challenging tasks for researchers and computer scientists in the areas of pattern recognition and machine learning.

Pattern recognition or pattern classification can be defined as "the act of taking in raw data and taking an action based on the category of the pattern" [1]. Pattern recognition techniques are currently used in several security applications such as biometrics based person recognition, spam filtering, and intrusion detection in computer networks, with the goal to discriminate between a 'legitimate' and a 'malicious' pattern class. For example, genuine or impostor users in biometric systems. However, these tasks are different from classical pattern recognition tasks, since intelligent and adaptive adversaries (human beings) can manipulate their samples to defeat the system. For instance, biometric spoof attack using fake fingerprints. Since, classical pattern recognition techniques do not take into account the adversarial nature of classification problems like the one mentioned above, they therefore exhibit significant performance degradation when used in adversarial settings, namely under attacks.

II. ADVERSARIAL PATTERN CLASSIFICATION

Pattern classification is the scientific discipline whose goal is to classify the objects (samples) into a number of classes or categories. Depending on the type of application, these objects (commonly referred as patterns) may be any type of measurements, images or signal waveforms that need to be classified. In pattern classification, typically a set of patterns (the raw data), whose class is unknown, is given. The objective is then to devise an algorithm that assigns such patterns to one of the (possibly predetermined) classes, using some prior information. In addition, proper actions can be taken based on the outcome of the pattern classification. For instance, in fingerprint based high security access control system, when the impostor is detected, the system may decide to ring the alarm bell. A wide variety of pattern recognition, typically known as classification algorithms or classifiers, has been proposed for many classification tasks.

Traditionally, a classifier is designed by training it on a set of patterns (samples or feature vectors) whose true class is known– referred also as training set or design set, to find a classification function. When a pattern has to be classified, the classifier utilizes the acquired knowledge to assign the class to

a given input pattern. The capability of the classifier, designed using the training data set, to operate satisfactorily with data outside training set is known as classifier's generalization capability.

The classification function can be estimated by either supervised (classification) learning or unsupervised (clustering) learning, the first one involves only labeled data (training patterns with known class labels) while the latter involves

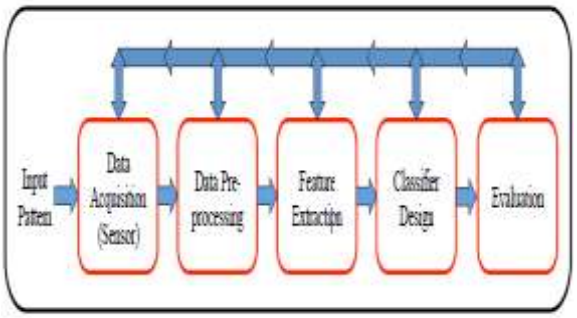

Fig 1: The basic stages involved in the design of a pattern classification system.

Only unlabeled data. To date, many classification algorithms have been proposed in the literature, such as Bayesian classifiers, neural networks, support vector machines (SVMs), decision trees and k-nearest neighbor classifiers, just to name a few. Indeed, it is clear from the literature that there is no best classifier for all types of problem. However, the simplest strategy could be to select the best performing classifier on the task at hand.

Figure 1shows the various stages followed for the design of a pattern classification system. The first step is to collect a pre-processed set of training samples. The role of data pre-processing module is therefore to segment the pattern of interest from the background, remove noise and any other operation which will contribute in defining a compact representation of the pattern. Features are then extracted from each training sample. In practice, a larger than necessary number of feature candidates is generated and then the best of them is adopted. The classifier, which is chosen among different algorithms, is trained on appropriate features. Finally, once the classifier has been designed (trained), one can evaluate the performance of the designed classifier (i.e., what is the classification error rate) on test set, namely prediction of classifier's behavior on the unseen samples that were not present in the training set, and whose class labels are unknown as well. The feedback path allows one to go back, depending on the results, to redesign the preceding stages in order to improve the overall performance.

We have already pointed out that pattern classification techniques have been greatly implicated in several security application (e.g. biometrics) to overcome the shortcomings of classical security systems. The current surge of interest in pattern classification for security applications, however, raises a vital issue: "are pattern classification techniques themselves secure?". Pattern classification systems themselves in principle can be circumvented by a malicious adversary. In particular, attacks can be devised at any stage of the system (see Figure 2). For instance, a biometric recognition system can be attacked by an accurate

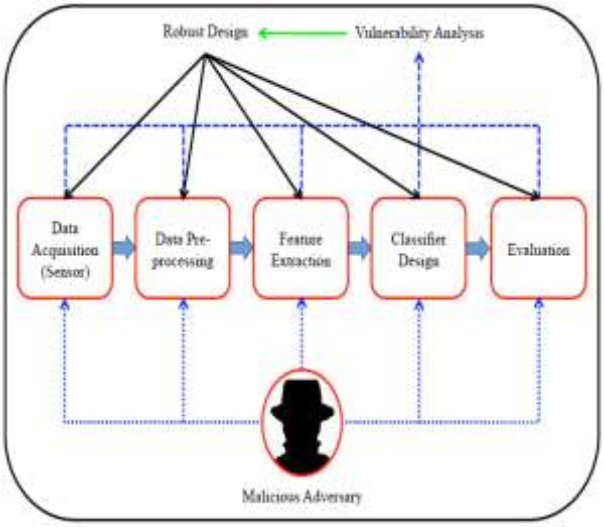

Fig 2: Adversaries may exploit different vulnerabilities at any stage of a pattern recognition system (adapted from [2]). Thus, the system designers should look for such vulnerabilities in advance, and propose specific countermeasures.

Three-dimensional model of a fake fingerprint belonging to a legitimate user. In general, it is necessary to identify and understand the threat (attack) points of a pattern classification system when used in adversarial environments, so that effective technical and procedural countermeasures can be proposed.

III. LIMITATIONS OF UNIMODAL BIOMETRIC SYSTEM

Some of the main factors affecting the accuracy of the unimodal biometric systems are as follows:

3.1 Noise in sensed data:

Noise in the acquired biometric sample may result from defective and improperly maintained sensors or unfavorable ambient conditions. For instance, accumulation of dirt or the residual remains on a fingerprint sensor may result in a noisy fingerprint image. Noisy biometric sample may not be successfully matched, for genuine users, with their respective templates in the database or may be incorrectly matched with the impostors, thus leading

to a significant reduction in the performance of the system [3, 4].

3.2 Intra-class variations:

Intra-class variations in biometric samples are typically produced by the user's inappropriate interaction with the changes in the environmental conditions (e.g., illumination changes), use of different sensors during enrollment and verification, or temporal variation in the biometric traits such as aging [5]. Large intra-class variations usually decrease the genuine acceptance rate (GAR) of a biometric system.

3.3 Inter-class similarities:

Inter-class similarity is defined as the overlap of the biometric samples, in the feature space, corresponding to multiple classes or individuals. The lack of uniqueness in the biometric feature set leads to an increase in the false acceptance rate (FAR) of the system. Hence, there is an upper bound on the number of unique individuals that can be accommodated by the biometric system.

3.4 Non-universality:

Universality means that every person using a biometric system is able to present the respective biometric trait. The biometric system may not be able to extract meaningful biometric data from a subset of users. For example, the National Institute of Standards and Technology (NIST) has reported that it is not possible to extract correct minutia features from the fingerprints of two percent of the population (manual workers with many cuts and bruises on their fingertips, people with hand related disabilities etc.), due to the poor quality of the ridges [6]. This contributes to an increase in the failure to enroll (FTE) rate. Hence, no biometric trait is truly universal.

3.5 Interoperability issues:

Most biometric systems are designed and operated under the assumption that the biometric sample to be compared are obtained using the same sensor and, hence, are restricted in their ability to match or compare biometric samples originating from different sensors.

3.6 Spoof attacks:

Biometric spoof attack is the deliberate attempt to manipulate one's biometric traits in order to avoid recognition, or the creation of physical biometric artifacts in order to take on the identity of another person.

IV. MULTIMODAL BIOMETRIC SYSTEMS

One of the fundamental issues in designing of a multimodal biometric system is to determine the type of information that should be fused. The information fusion can be carried at various levels: sensor level, feature level, score level, rank level and decision level, as described below. Conventionally, the availability of the information content decreases from the sensor level to the decision level [18].

4.1 Sensor level:

The raw data acquired from multiple sensors are combined in sensor level fusion before they are subjected to feature extraction [7]. In this type of fusion, the multiple cues must be compatible; hence usually fusion of the same biometric trait, obtained either using a single sensor or different compatible sensors, is carried out. For example, the fingerprint impressions obtained from optical and solid state sensors can be combined to form a single image to be input to the feature extraction and matching modules.

4.2 Feature level:

Feature level fusion refers to consolidating the evidence presented by two biometric feature sets of the same individual. The two feature sets are concatenated to form a single feature set to compare with the enrollment template in the system database, which itself is a concatenated feature set.

4.3 Score level:

In score level fusion, feature sets are extracted independently by each subsystem, which are later compared with separately stored respective templates. Depending on the proximity of feature set and the template, each subsystem computes its own match score. The individual scores are finally fused to produce a single match score for decisionmaking process.

4.4 Rank level:

This type of fusion is conducted in identification mode, where each subsystem associates a rank with each enrolled identity. Thus, the rank level fusion schemes consolidate the ranks produced by the individual subsystems in order to derive a consensus rank for each identity in order to establish the final decision [17].

4.5 Decision level:

A decision level, also known as abstract level, fusion is carried out by combining the authentication decision made by individual biometric matchers. Fusion at the decision level is too rigid, since only limited information is available at this level.

As mentioned above one of the most fundamental issues in the multimodal biometric

systems is to determine the type of information that should be consolidated by the fusion module. Since, the amount of informations goes on decreasing as one proceeds from sensor level to decision level, therefore multimodal biometric systems that fuse information at at early stages of processing are expected to yield more promising results than the systems that fuse the information at later stage. There has been a proliferation of works discussing different fusion schemes to integrate multiple sources of biometric information at different levels. Usually, the benefits of fusion technique are exploited when individual sources of information show complementary nature. Large performance disparity between component sources may dilute the performance of the "stronger" source [8].

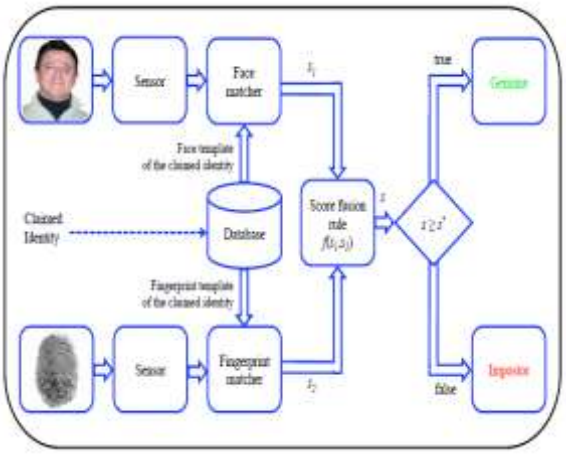

Fig 3: A multimodal biometric system made up of a fingerprint and a face sensor, whose match scores are combined through a fusion rule.

Figure 3 illustrates the architecture of a multimodal biometric system, with reference to the one considered in this thesis, namely a multimodal system composed of a face and a fingerprint matcher. Such systems operates as follows: At the design phase, genuine users are enrolled into the system, by storing their biometric traits (templates) in a database together with the corresponding identities. At authentication phase, the user provides his face and fingerprint to the respective sensors, and claims his identity.

V. ATTACKS AGAINST BIOMETRIC SYSTEMS

Adversary attacks exploit the system vulnerabilities generally at one or more modules or interfaces. Eight possible different points where security of biometric systems can be compromised have been identified in [9] as described below:

- A fake biometric trait may be presented at the sensor such as a fake finger, a copy of a signature, or a face mask.
- Digitally stored biometric data may be resubmitted to the system. In this kind of attack, a previously recorded biometric data is replayed into the system bypassing the sensor, thus also called as "replay attack". For instance, presenting a digital copy of fingerprint image or recorded audio signal of a speaker.
- The feature extractor may be attacked with a Trojan horse program that produces predetermined feature sets.
- Legitimate feature sets extracted from the biometric input may be replaced with synthetic feature sets. For example, if minutiae of a fingerprint are transmitted to a remote matcher (say over the Internet) than this threat is very real.
- The matcher may be attacked with a Trojan horse program that always directly produces a specified result - match, no match, or a score.
- The enrolled templates in the database may be modified or removed, or new templates may be introduced in the database, which could result in authorization for a fraudulent individual, or at least denial of service for the person associated with the corrupted template.
- The enrolled templates in the stored database are sent to the matcher through a communication channel which could be attacked to change the contents of the templates before they reach the matcher.
- The final decision output by the biometric system may be overridden with the choice of result from the hacker. Even if the feature extraction and matching modules had excellent performance characteristics, it has been rendered useless by the simple exercise of overriding the result.

VI. SPOOF ATTACKS

Among the potential attacks discussed in the literature, the one with the greatest practical relevance is "spoof attack", which consists in submitting a stolen, copied or synthetically replicated biometric trait to the sensor to defeat the biometric system security in order to gain unauthorized access. Recently, it has been shown that spoof attacks can be carried against many types of biometrics, like fingerprint, face, and iris [10, 11, 12, 13, 14, 15]. This kind of attack is also known as "direct attack", since it is carried out directly on the biometric sensor. The feasibility of a spoof attack is much higher than other types of attacks against biometric systems, as it does not require any knowledge on the system, such as the feature extraction or matching algorithm used. Digital protection techniques like hashing, encryption, and digital signature, are not useful due to the nature of spoofing attacks, which are done in

the analogical domain, outside the digital limits of the system.

4.6 Fingerprint spoofing

- The user presses his finger on a soft material such as wax, play doh, dental impression material, or plaster;
- The negative impression of the fingerprint is fixed on the surface to form a mold;
- A casting material such as liquid silicon, wax, gelatin, moldable plastic, plaster or clay, is poured in the mould;
- When the liquid is hardened, the fake/spooed fingerprint is formed.

4.7 Face spoofing

In spite of the fair amount of advancement in biometric face recognition systems, face spoofing, also known as "copy attack", still poses a serious threat to the system security. Face spoofing methods may vary according to the targeted face recognition system. Face recognition systems can be broadly classified into two groups: 2D (two-dimensional) and 3D (three-dimensional) systems. A biometric 2D face recognition system takes into consideration only the two dimensional image of the face. 3D systems are clearly more complex, and recognize faces on the basis of features extracted from the 3D shape of the whole face, using methods such as paraxial viewing, or patterned illumination light [16]. Conventionally, face recognition systems can be spoofed by presenting (i) a photograph, (ii) a video, or (iii) a 3D face model/mask of a legitimate user.

VII. CONCLUSIONS

In particular, we proposed two models of the match score distribution of fake biometric traits, that accounts for different possible realistic scenarios characterized by factors like different spoofing techniques and attackers' capability etc. Such factors are summarized in our models in a single parameter associated to the degree of similarity of the fake score distribution to the genuine one, which is named accordingly "attack strength". The proposed models exploit only information on genuine and impostor samples which is collected for the training of a biometric system. The main feature of our method is that it allows analyzing the performance of a multimodal system against several spoof attack distributions for different "attack strength" values, namely non-worst case scenarios. Our models allow developing a method to empirically or analytically numerically evaluate the security of biometric systems against attacks, by simulating their effect on the match scores. The proposed method can be applied to any multimodal system, namely, to any set of matchers combined with any score fusion rule, and it allows to simulate a spoof attack against any subset of the component matchers. Furthermore, we proposed extension of security evaluation method aimed at ranking several score-level fusion rules under attack.

REFERENCES

[1] R. O. Duda, P. E. Hart, and D. G. Stork. Pattern classification. Wiley, second edition, 2001.

[2] B. Biggio. Adversarial Pattern Classification. PhD thesis, University of Cagliari, Cagliari (Italy), 2010.

[3] M. D. Garris, C. I. Watson, and C. L. Wilson. Matching performance for the US-Visit IDENT system using flat fingerprints. Technical report, 7110, National Institute of Standards and Technology (NIST), July 2004.

[4] C. Wilson, A. R. Hicklin, M. Bone, H. Korves, P. Grother, B. Ulery, R. Micheals, M. Zoepfl, S. Otto, and C. Watson. Fingerprint vendor technology evaluation 2003: Summary of results and analysis report. Technical Report NISTIR 7123, National Institute of Standards and Technology (NIST), June 2004.

[5] A. Lanitis. A survey of the effects of aging on biometric identity verification. Int. J. Biometrics, 2:34–52, December 2010.

[6] NIST Report to the United States Congress. Summary of NIST standards for biometric accuracy, tamper resistance, and interoperability. Available at ftp://sequoyah.nist.gov/pub/nist_internal_reports/NISTAPP_Nov02.pdf, 2002.

[7] G. Feng, K. Dong, D. Hu, and D. Zhang. When faces are combined with palmprints: A novel biometric fusion strategy. In First International Conference Biometric Authentication, pages 701–707, 2004.

[8] J. Daugman. Combining multiple biometrics. Available http://www.cl.cam.ac.uk/~jgd1000/combine/combine.html, 2000.

[9] N. K. Ratha, J. H. Connell, and R. M. Bolle. An analysis of minutiae matching strength. In Proceedings of the Third International Conference on Audio- and Video-Based Biometric Person Authentication, AVBPA '01, pages 223–228, London, UK, 2001. Springer-Verlag.

[10] B. Geller, J. Almog, P. Margot, and E. Springer. A chronological review of fingerprint forgery. Journal of Forensic Sciences, 44(5):963–968, 1999.

[11] T. Putte and J. Keuning. Biometrical fingerprint recognition: Don't get your fingers burned. In 4th Working Conf. on

Smart Card Research and Advanced Applications, pages 289–303, 2000.

[12] M. M. Chakka, A. Anjos, S. Marcel, R. Tronci, D. Muntoni, G. Fadda, M. Pili, N. Sirena, G. Murgia, M. Ristori, F. Roli, J. Yan, D. Yi, Z. Lei, Z. Zhang, S. Z. Li, W. R. Schwartz, A. Rocha, H. Pedrini, J. Lorenzo-Navarro, M. Castrillon-Santana, J. Maatta, A. Hadid, and M. Pietikainen. Competition on counter measures to 2-D facial spoofing attacks. In International Joint Conference on Biometrics (IJCB 2011). In press, 2011.

[13] X. Tan, Y. Li, J. Liu, and L. Jiang. Face liveness detection from a single image with sparse low rank bilinear discriminative model. In Proceedings of the 11th European conference on Computer vision: Part VI, pages 504–517, 2010.

[14] V. Ruiz-Albacete, P. Tome-Gonzalez, F. Alonso-Fernandez, J. Galbally, J. Fierrez, and J. Ortega-Garcia. Direct attacks using fake images in iris verification. In Proc. Workshop on Biometrics and Identity Management, pages 181–190, 2008.

[15] X. He, Y. Lu, and P. Shi. A fake iris detection method based on FFT and quality assessment. In Proc. Chinese Conf. on Pattern Recognition, pages 316–319, 2008.

[16] A. Godil, Y. Ressler, and P. Grother. Face recognition using 3d facial shape and color map information: comparison and combination. In Proceedings of the SPIE The International Society for Optical Engineering, pages 351–361, 2005.

[17] Suvarnsing G. Bhable, Sangramsing Kayte, Jaypalsing N. Kayte, Dr. Charansing Kayte"Robust Multimodal Biometrics Recognition: A Review" International Journal of Advanced Research in Computer Science and Software Engineering -Volume 5, Issue 10, October-2015.

[18] Sangramsing N. Kayte , Suvarnsing G. Bhable , Jaypalsing N. Kayte , Raju Maher " A Review Paper on Multimodal Biometrics System using Fingerprint and Signature" International Journal of Computer Applications (0975 – 8887) Volume 128 – No.15, October 2015