Home Exam

Essay about a security topic chosen by student(s).

**Individual or group:** The home exam essay can be written either individually, or in groups of 2 or 3 students.

**Weight:** The home exam weighs 40% towards the final mark, on the condition of having at least a pass score on the written exam. Similarly, the written exam weighs 60% on the condition of having at least a pass score on the home exam.

**Due date for the home exam:** 04.11.2018 at 23:59h.

**Selection of topic and group:** In order to ensure good progress, try to select a topic and group by 12.10.2018. The topic can be chosen from a list of proposed topics available on the [IN2120 wiki](https://wiki.uio.no/mn/ifi/IN2120-2018/), or can be specified by the student/group. Students are welcome to suggest their own topic title and to discuss possible topics with the course lecturer if they wish to. Every group must choose a different topic title, but it is OK to focus on similar topics as other groups. The topic and group must be specified on the [IN2120 wiki](https://wiki.uio.no/mn/ifi/IN2120-2018/).

**Accessing the wiki:** First time users must first log in with their UiO user-id, but will not immediately be able to access the wiki pages. Access permission will be approved within the same day, after which the wiki pages can be accessed.

**General guidelines:**The report should be in the style of an academic paper. In particular it should contain full references and citations. Use of the Internet for research material is encouraged but any sources must be referenced and care should be taken to avoid reliance on unmoderated or unrefereed material. If you are unfamiliar with the structure of an academic report, or how to reference material, you can get advice from e.g. [University of Essex Academic Writing Guide](https://www.uio.no/studier/emner/matnat/ifi/IN2120/h18/docs/university_of_essex_writing_guide_2009.pdf). Be sure to reference your sources when needed, otherwise you are liable to be accused of plagiarism. As a guideline reports should be between 5000 and 10000 words (approximately 10 - 15 pages). Report structure will vary according to the topic selected but should always contain an introduction and conclusion as part of a logical structure. Write in English or Norwegian.

**Marking criteria:**

Reports will be assessed using the following criteria equally weighted:

1. **Structure and presentation**. Use a logical structure, present the material is clear and correct language.
2. **Scope and depth of content**. The scope must be well defined, and the depth of content should be adjusted to how wide or narrow the scope is. If the scope is wide the content is normally shallow, and if the scope is narrow the content goes deep.
3. **Evidence of independent research and analysis**. The presented material needs to show evidence of independent analysis and contribution. This can take many forms. E.g. draw some independent conclusion, or conduct an interview and reflect and analyse on the results.
4. **Proper use of references**. Always reference material used. Both traditional literature and articles as well as web references can be used.

As a general principle, reports consisting only of summaries of references will not gain a high score. **To gain a high score, reports should contain some independent thought or analysis, for example in the form of: critical comparisons of systems, critical analysis of existing solutions, critical analysis of previous work or proposals, experimental evidence (such as on a computer network), statistical analysis of data, or interviews with experts or lay persons.**

**How to submit this assignment:** Submit through Devilry or Inspera. The cover page must carry the **topic title and number**, **student candidate number(s)**(s), and optionally **student names(s)**. Students working together on the same essay only need to submit one essay.

Presentation Attacks Against Biometric Authentication

Presentation Attack

Attack Types

Masking, Sculpture, Printing etc.

Authentication

What is authentication in Security?

Why it is important?

Biometrics

Face Id

Iris

Fingerprint

Vein

DNA…

Biometric Authentication

What is BA?

History?

Applications

Market size

Pros-cons

Presentation attack detection mechanisms

Liveness, etc.

Pros-Cons

Conclusion

Biometrics

What is it?

Biometric technologies are used to recognize individuals based on biological and behavioral characteristics and, consequently, are often used as a component in security systems. A biometric technology assisted security system may attempt to recognize persons who are known as either friends or foes or may attempt to recognize persons who are unknown to the system either. (**ISO/IEC 30107-1:2016(E))**

*Biometrics* verifies an individual’s identity by analyzing a unique personal attribute or behavior, which is one of the most effective and accurate methods of verifying identification. Biometrics is a very technology; thus, it is much more expensive and complex than the other types of identity verification processes. A biometric system can make authentication decisions based on an individual’s behavior, as in signature dynamics, but these can change over time and possibly be forged. Biometric systems that base authentication decisions on physical attributes (such as iris, retina, or fingerprint) provide more accuracy because physical attributes typically don’t change, absent some disfiguring injury, and are harder to impersonate. Biometrics is typically broken up into two different categories. The first is the physiological. These are traits that are physical attributes unique to a specific individual. Fingerprints are a common example of a physiological trait used in biometric systems.

The second category of biometrics is known as behavioral. This is based on a characteristic of an individual to confirm his identity. An example is signature dynamics. Physiological is “what you are” and behavioral is “what you do.”

A biometric system scans a person’s physiological attribute or behavioral trait and compares it to a record created in an earlier enrollment process. Because this system inspects the grooves of a person’s fingerprint, the pattern of someone’s retina, or the pitches of someone’s voice, it must be extremely sensitive. The system must perform accurate and repeatable measurements of anatomical or behavioral characteristics. This type of sensitivity can easily cause false positives or false negatives. The system must be calibrated so these false positives and false negatives occur infrequently and the results are as accurate as possible. (**CISSP All-in-One Exam Guide p.746)**

Generally speaking, the way to recognize something of a human being Mankind is to recognize sound, face, gait, odor, etc. Through a person’s face or sound afar, we are able to identify who he/she is. The biometric recognition technology basically is imitating the human being’s recognition to carry on same recognition, for example, the face recognition technique and speech recognition technique. Moreover, because of human beings having some features of physiology, which own the anatomy uniqueness, the biometric technology is developing and can quickly recognize an individual through these features, for example, fingerprint, eye pupil, finger vein, DNA, etc. These features come from human’s body and are easily obtained by self and do not be forged. The biometrics recognition is very convenient on the application. Consequently, various applications need to identify individuals adopt the biometrics recognition gradually. For example, the passport inspection has already adopted the face recognition technique and fingerprint recognition technique to carry on the identification work at the border check. Currently, the development of biometrics technology in recognition has been rather mature. At the court, the biometrics technology also has been used to find or recognize the suspecting person through the collected fingerprint or DNA at the crime scene.

The biometric features have a few following characteristics [1]:  
1) Universality: everyone has the features.  
2) Distinctiveness: the features could be used to distinguish different identities.  
3) Permanence: the features would not change with time.  
4) Collectability: the features could be collected via a biometrics system,

and formed uniqueness codes to process the identification and verification. Applying biometric features to carry on identifying individuals are usually depended on the convenience of obtaining the biometric features. Take an example, most of the biometric features used to control at gate system is person’s face, fingerprint and eye pupil, because these three kinds of biometric features are easily to provide at any one time for everyone without help of any instrument equipment. Most of the collected biometric features at crime scene are DNA and fingerprint because these two kinds of biometric features are easily left behind from human beings on the spots among daily life or behaviors. We will introduce some biometric features used in current most applications. (Patrick S.P. Wang **Pattern Recognition, Machine Intelligence and Biometrics p.608)**

Biometric modalities, examples:

Since there are number of biometric methods in use (some commercial, some "not yet"), a brief overview of various biometric characteristics will be given, starting with newer technologies and then progressing to older ones [2]:

Infrared thermogram (facial, hand or hand vein). It is possible to capture the pattern of heat radiated by the human body with an infrared camera. That pattern is considered to be unique for each person. It is a noninvasive method, but image acquisition is rather difficult where there are other heat emanating surfaces near the body. The technology could be used for covert recognition. A related technology using near infrared imaging is used to scan the back of a fist to determine hand vein structure, also believed to be unique. Like face recognition, it must deal with the extra issues of three-dimensional space and orientation of the hand. Set-back is the price of infrared sensors.

Gait. This is one of the newer technologies and is yet to be researched in more detail. Basically, gait is the peculiar way one walks and it is a complex spatio-temporal biometrics. It is not supposed to be very distinctive but can be used in some low-security applications. Gait is a behavioral biometric and may not remain the same over a long period of time, due to change in body weight or serious brain damage. Acquisition of gait is similar to acquiring a facial picture and may be an acceptable biometric. Since video-sequence is used to measure several different movements this method is computationally expensive.

Keystroke. It is believed that each person types on a keyboard in a characteristic way. This is also not very distinctive but it offers sufficient discriminatory information to permit identity verification. Keystroke dynamics is a behavioral biometric; for some individuals, one could expect to observe large variations in typical typing patterns. Advantage of this method is that keystrokes of a person using a system could be monitored unobtrusively as that person is keying information. Another issue to think about here is privacy.

Odor. Each object spreads around an odor that is characteristic of its chemical composition and this could be used for distinguishing various objects. This would be done with an array of chemical sensors, each sensitive to a certain group of compounds. Deodorants and parfumes could lower the distinctiveness.

Ear. It has been suggested that the shape of the ear and the structure of the cartilaginous tissue of the pinna are distinctive. Matching the distance of salient points on the pinna from a landmark location of the ear is the suggested method of recognition in this case. This method is not believed to be very distinctive.

Hand geometry. The essence of hand geometry is the comparative dimensions of fingers and the location of joints, shape and size of palm. One of the earliest automated biometric systems was installed during late 60s and it used hand geometry and stayed in production for almost 20 years. The technique is very simple, relatively easy to use and inexpensive. Dry weather or individual anomalies such as dry skin do not appear to have any negative effects on the verification accuracy. Since hand geometry is not very distinctive it cannot be used for identification of an individual from a large population, but rather in a verification mode. Further, hand geometry information may not be invariant during the growth period of children. Limitations in dexterity (arthritis) or even jewelry may influence extracting the correct hand geometry information. This method can find its commercial use in laptops rather easy. There are even verification systems available that are based on measurements of only a few fingers instead of the entire hand. These devices are smaller than those used for hand geometry.

Fingerprint. A fingerprint is a pattern of ridges and furrows located on the tip of each finger. Fingerprints were used for personal identification for many centuries and the matching accuracy was very high [3]. Patterns have been extracted by creating an inked impression of the fingertip on paper. Today, compact sensors provide digital images of these patterns. Fingerprint recognition for identification acquires the initial image through live scan of the finger by direct contact with a reader device that can also check for validating attributes such as temperature and pulse. Since the finger actually touches the scanning device, the surface can become oily and cloudy after repeated use and reduce the sensitivity and reliability of optical scanners. Solid state sensors overcome this and other technical difficulties because the coated silicon chip itself is the sensor. Solid state devices use electrical capacitance to sense the ridges of the fingerprint and create a compact digital image. Today, a fingerprint scanner costs about 20 USD and has become affordable in a large number of applications (laptop computer). In real-time verification systems, images acquired by sensors are used by the feature extraction module to compute the feature values. The feature values typically correspond to the position and orientation of certain critical points known as minutiae points [4]. The matching process involves comparing the two-dimensional minutiae patterns extracted from the user's print with those in the template. One problem with the current fingerprint recognition systems is that they require a large amount of computational resources.

Face. Facial images are the most common biometric characteristic used by humans to make a personal recognition, hence the idea to use this biometric in technology. This is a nonintrusive method and is suitable for covert recognition applications. The applications of facial recognition range from static ("mug shots") to dynamic, uncontrolled face identification in a cluttered background (subway, airport). Face verification involves extracting a feature set from a two-dimensional image of the user's face and matching it with the template stored in a database. The most popular approaches to face recognition are based on either: 1) the location

and shape of facial attributes such as eyes, eyebrows, nose, lips and chin, and their spatial relationships, or 2) the overall (global) analysis of the face image that represents a face as a weighted combination of a number of canonical faces [2]. Although performance of commercially available systems is reasonable there is still significant room for improvement since false reject rate (FRR) is about 10% and false accept rate (FAR) is 1% [5]. These systems also have difficulties in recognizing a face from images captured from two different angles and under different ambient illumination conditions. It is questionable if a face itself is a sufficient basis for recognizing a person from a large number of identities with an extremely high level of confidence [6]. Facial recognition system should be able to automatically detect a face in an image, extract its features and then recognize it from a general viewpoint (i.e., from any pose) which is a rather difficult task. Another problem is the fact that the face is a changeable social organ displaying a variety of expressions.

Retina. Retinal recognition creates an "eye signature" from the vascular configuration of the retina which is supposed to be a characteristic of each individual and each eye, respectively. Since it is protected in an eye itself, and since it is not easy to change or replicate the retinal vasculature, this is one of the most secure biometric. Image acquisition requires a person to look through a lens at an alignment target, therefore it implies cooperation of the subject. Also retinal scan can reveal some medical conditions and as such public acceptance is questionable.

Iris. The iris begins to form in the third month of gestation and the structures creating its pattern are largely complete by the eight month. Its complex pattern can contain many distinctive features such as arching ligaments, furrows, ridges, crypts, rings, corona, freckles and a zigzag collarette [7]. Iris scanning is less intrusive than retinal because the iris is easily visible from several meters away. Responses of the iris to changes in light can provide an important secondary verification that the iris presented belongs to a live subject. Irises of identical twins are different, which is another advantage. Newer systems have become more user-friendly and cost-effective. A careful balance of light, focus, resolution and contrast is necessary to extract a feature vector from localized image. While the iris seems to be consistent throughout adulthood, it varies somewhat up to adolescence.

Palmprint. Like fingerprints, palms of the human hands contain unique pattern of ridges and valleys. Since palm is larger then a finger, palmprint is expected to be even more reliable than fingerprint. Palmprint scanners need to capture larger area with similar quality as fingerprint scanners, so they are more expensive. A highly accurate biometric system could be combined by using a high-resolution palmprint scanner that would collect all the features of the palm such as hand geometry, ridge and valley features, principal lines, and wrinkles.

Voice. The features of an individual's voice are based on physical characteristics such as vocal tracts, mouth, nasal cavities and lips that are used in creating a sound. These characteristics of human speech are invariant for an individual, but the behavioral part changes over time due to age, medical conditions and emotional state. Voice recognition techniques are generally categorized according to two approaches: 1) Automatic Speaker Verification (ASV) and 2) Automatic Speaker Identification (ASI). Speaker verification uses voice as the authenticating attribute in a two-factor scenario. Speaker identification attempts to use voice to identify who an individual actually is. Voice recognition distinguishes an individual by matching particular voice traits against templates stored in a database. Voice systems must be trained to the individual's voice at enrollment time, and more than one

enrollment session is often necessary. Feature extraction typically measures formants or sound characteristics unique to each person's vocal tract. The pattern matching algorithms used in voice recognition are similar to those used in face recognition.

Signature. Signature is a simple, concrete expression of the unique variations in human hand geometry. The way a person signs his or her name is known to be characteristic of that individual. Collecting samples for this biometric includes subject cooperation and requires the writing instrument. Signatures are a behavioral biometric that change over a period of time and are influenced by physical and emotional conditions of a subject. In addition to the general shape of the signed name, a signature recognition system can also measure pressure and velocity of the point of the stylus across the sensor pad.

DNA. Deoxyribonucleic acid (DNA) is probably the most reliable biometrics. It is in fact a one-dimensional code unique for each person. Exception are identical twins. This method, however, has some drawbacks: 1) contamination and sensitivity, since it is easy to steal a piece of DNA from an individual and use it for an ulterior purpose, 2) no real-time application is possible because DNA matching requires complex chemical methods involving expert's skills, 3) privacy issues since DNA sample taken from an individual is likely to show susceptability of a person to some diseases. All this limits the use of DNA matching to forensic applications. (A SURVEY OF BIOMETRIC RECOGNITION METHODS Kresimir Delac 1, Mislav Grgic 2 )

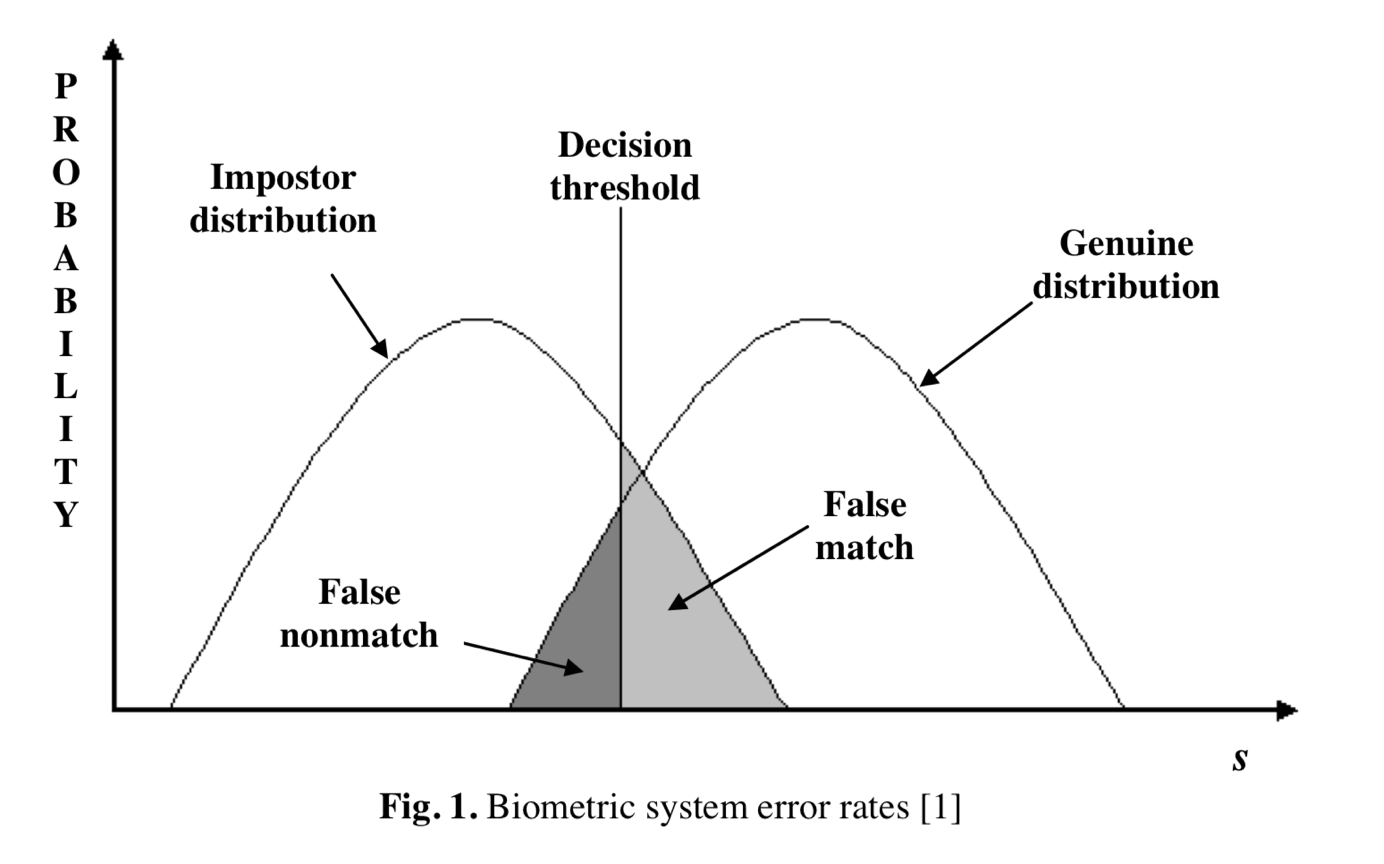
**A simple biometric system consists of four basic components:**

1)  Sensor module witch acquires the biometric data;

2)  Feature extraction module where the acquired data is processed to extract feature vectors; 3)  Matching module where feature vectors are compared against those in the template; 4)  Decision-making module in which the user's identity is established or a claimed identity is accepted or rejected. *(A SURVEY OF BIOMETRIC RECOGNITION METHODS Kresimir Delac 1, Mislav Grgic 2 )*

**4. BIOMETRIC SYSTEM PERFORMANCE**

Due to different positioning on the acquiring sensor, imperfect imaging conditions, environmental changes, deformations, noise and bad user's interaction with the sensor, it is impossible that two samples of the same biometric characteristic, acquired in different sessions, exactly coincide. For this reason a biometric matching systems' response is typically a matching score s (normally a single number) that quantifies the similarity between the input and the database template representations. The higher the score, the more certain the system is that the two samples coincide [1]. A similarity score s is compared with an acceptance threshold t and if s is greater than or equal to t compared samples belong to a same person. Pairs of biometric samples generating scores lower than t belong to a different person. The distribution of scores generated from pairs of samples from different persons is called an impostor distribution, and the score distribution generated from pairs of samples of the same person is called a genuine distribution, Figure 1 [1].

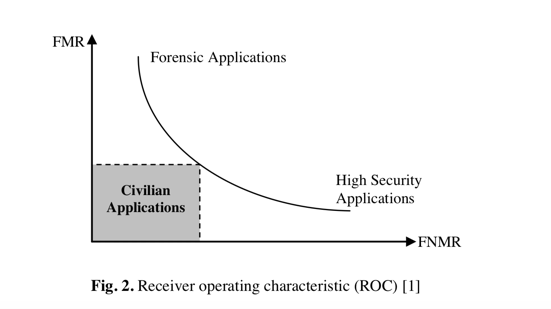


The main system errors are usually measured in terms of:  
• FNMR (false nonmatch rate) – mistaking two biometrics measurements from the

same person to be from two different persons;  
• FMR (false match rate) – mistaking biometric measurement from two different

persons to be from the same person.

FNMR and FMR are basically functions of the system threshold t: if the system's designers decrease t to make the system more tolerant to input variations and noise, FMR increases. On the other hand, if they raise t to make the system more secure, FNMR increases accordingly [1]. FMR and FNMR are brought together in a receiver operating characteristic (ROC) curve that plots the FMR against FNMR (or 1-FNMR) at different thresholds, Figure 2 [1].



There are two other recognition error rates that can be also used and they are: failure to capture (FTC) and failure to enroll (FTE). FTC denotes the percentage of times the biometric device fails to automatically capture a sample when presented with a biometric characteristic. This usually happens when system deals with a signal of insufficient quality. The FTE rate denotes the percentage of times users cannot enroll in the recognition system. ***(A SURVEY OF BIOMETRIC RECOGNITION METHODS Kresimir Delac , Mislav Grgic)***

Biometrics: Requirements

What biological measurements qualify to be a biometric? Any human physio- logical and/or behavioral characteristic can be used as a biometric characteristic as long as it satisfies the following requirements:

* –  Universality: each person should have the characteristic;
* –  Distinctiveness: any two persons should be sufficiently different in terms of

the characteristic;

* –  Permanence: the characteristic should be sufficiently invariant (with respect

to the matching criterion) over a period of time;

* –  Collectability: the characteristic can be measured quantitatively.

However, in a practical biometric system (i.e., a system that employs biomet- rics for person recognition), there are a number of other issues that should be considered, including:

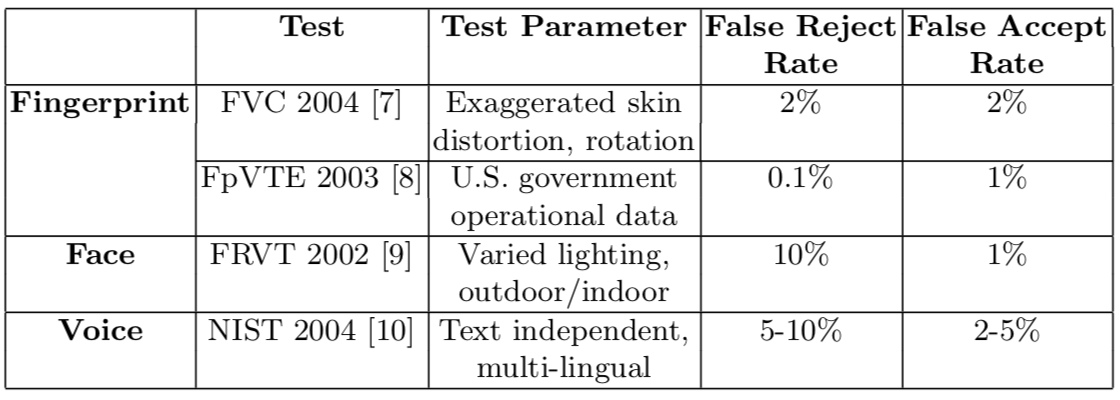
* –  Performance, which refers to the achievable recognition accuracy and speed, the resources required to achieve the desired performance, as well as the operational and environmental factors that affect the performance;
* –  Acceptability, which indicates the extent to which people are willing to ac- cept the use of a particular biometric identifier in their daily lives;
* –  Circumvention, which reflects how easily the system can be fooled using fraudulent methods.
* A practical biometric system should meet the specified recognition accuracy, speed, and resource requirements, be harmless to the users, be accepted by the intended population, be easy to use and be sufficiently robust to various fraudulent methods and attacks on the system. Among the various biometric measurements in use, fingerprint-based systems [5] and face recognition systems [6] are the most popular.

A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. Depending on the application context, a biometric system may operate either in a verification mode or an identification mode. A biometric system is designed using the following four main modules: (i) sensor module, (ii) feature extraction module, (iii) matcher module, and (iv) system database module.

The response of a biometric system is a matching score that quantifies the similarity between the input and the database template representation. Higher score indicates that the system is more certain that the two biometric mea- surements come from the same person. The system decision is regulated by the threshold: pairs of biometric samples generating scores higher than or equal to the threshold are inferred as mate pairs (i.e., belonging to the same person); pairs of biometric samples generating scores lower than the threshold are inferred as non-mate pairs (i.e., belonging to different persons). A biometric verification system makes two types of errors: (i) mistaking biometric measurements from two different persons to be from the same person (called false match), and (ii) mistaking two biometric measurements from the same person to be from two different persons (called false non-match). These two types of errors are often termed as false accept and false reject, respectively.

Deployment of biometric systems in various civilian applications does not imply that biometric recognition is a fully solved problem. Table 1 presents the state-of-the-art error rates of three popular biometric traits. It is clear that there is a plenty of scope for improvement in the performance of biometric systems. We not only need to address issues related to reducing error rates, but we also need to look at ways to enhance the usability of biometric systems and address the return on investment issue.

Table 1. State-of-the-art error rates associated with fingerprint, face and voice bio- metric systems. Note that the accuracy estimates of biometric systems are dependent on a number of test conditions.



Multimodal Biometrics

Biometric systems that perform person recognition based on a single source of biometric information are often affected by the following problems [11]:

– Noisy sensor data : Noise can be present in the acquired biometric data mainly due to defective or improperly maintained sensors. For example, ac- cumulation of dirt or the residual remains on a fingerprint sensor can result in a noisy fingerprint image. The recognition accuracy of a biometric system is highly sensitive to the quality of the biometric input and noisy data can result in a significant reduction in the accuracy of the biometric system [12].

–  Non-universality: Not all biometric traits are truly universal. The National Institute of Standards and Technology (NIST) has reported that it is not possible to obtain a good quality fingerprint from approximately two per- cent of the population (people with hand-related disabilities, manual workers with many cuts and bruises on their fingertips, and people with oily or dry fingers) [13]. Hence, such people cannot be enrolled in a fingerprint verifi- cation system. Similarly, persons having long eye-lashes and those suffering from eye abnormalities or diseases cannot provide good quality iris images for automatic recognition [14]. Non-universality leads to Failure to Enroll (FTE) and/or Failure to Capture (FTC) errors in a biometric system.

–  Lack of individuality: Features extracted from biometric characteristics of different individuals can be quite similar. For example, appearance-based facial features that are commonly used in most of the current face recognition systems are found to have limited discrimination capability [15]. A small proportion of the population can have nearly identical facial appearance due to genetic factors (e.g., father and son, identical twins, etc.). This lack of uniqueness increases the False Match Rate (FMR) of a biometric system.

–  Lack of invariant representation: The biometric data acquired from a user during verification will not be identical to the data used for generating the user’s template during enrollment. This is known as “intra-class variation”. The variations may be due to improper interaction of the user with the sensor (e.g., changes due to rotation, translation and applied pressure when the user places his finger on a fingerprint sensor, changes in pose and expression when the user stands in front of a camera, etc.), use of different sensors during enrollment and verification, changes in the ambient environmental conditions (e.g., illumination changes in a face recognition system) and inherent changes in the biometric trait (e.g., appearance of wrinkles due to aging or presence of facial hair in face images, presence of scars in a fingerprint, etc.). Ideally, the features extracted from the biometric data must be relatively invariant to these changes. However, in most practical biometric systems the features are not invariant and therefore complex matching algorithms are required to take these variations into account. Large intra-class variations usually increase the False Non-Match Rate (FNMR) of a biometric system.

–  Susceptibility to circumvention: Although it is difficult to steal someone’s biometric traits, it is possible for an impostor to circumvent a biometric system using spoofed traits. Studies [16] have shown that it is possible to construct gummy fingers using lifted fingerprint impressions and utilize them to circumvent a biometric system. Behavioral traits like signature and voice are more susceptible to such attacks than physiological traits. Other kinds of attacks can also be launched to circumvent a biometric system [17].

Some of the problems that affect unimodal biometric systems can be alle- viated by using multimodal biometric systems [18]. Systems that consolidate cues obtained from two or more biometric sources for the purpose of person recognition are called multimodal biometric systems. Multimodal biometric sys- tems have several advantages over unimodal systems. Combining the evidence

obtained from different modalities using an effective fusion scheme can signif- icantly improve the overall accuracy of the biometric system. A multimodal biometric system can reduce the FTE/FTC rates and provide more resistance against spoofing because it is difficult to simultaneously spoof multiple biometric sources. By asking the user to present a random subset of biometric traits (e.g., right index finger followed by right middle finger), the system ensures that a “live” user is indeed present at the point of data acquisition. Thus, a challenge- response type of authentication can be facilitated by using multimodal biometric systems. However, multimodal biometric systems also have some disadvantages. They are more expensive and require more resources for computation and storage than unimodal biometric systems. Multimodal systems generally require more time for enrollment and verification causing some inconvenience to the user. Finally, the system accuracy can actually degrade compared to the unimodal system if a proper technique is not followed for combining the evidence provided by the different modalities. However, the advantages of multimodal systems far outweigh the limitations and hence, such systems are being increasingly deployed in security-critical applications.

The design of a multimodal biometric system is strongly dependent on the application scenario. A number of multimodal biometric systems have been pro- posed in literature that differ from one another in terms of their architecture, the number and choice of biometric modalities, the level at which the evidence is accumulated, and the methods used for the information fusion. Fusion at the matching score level is generally preferred due to the presence of sufficient in- formation content and the ease in accessing and combining matching scores. A principled approach to score level fusion is the computation of likelihood ratios based on the estimates of genuine and impostor score distributions [19]. Infor- mation obtained from soft biometric identifiers like gender, ethnicity and height can also be integrated with the primary biometric information like face and fingerprint, to improve the recognition accuracy of the biometric system [20].

3 Biometric System Vulnerabilities //En sona guvenlik kismina eklenebilir!!!

Biometric systems are vulnerable to several kinds of attacks that can compro- mise the security afforded by the biometric component and causing the failure of the system that it is intended to protect. Figure 1 summarizes the ways in which a biometric system can be attacked. The failure of a biometric system can be classified into two types. Large inter-class and small inter-class variability may result in the matcher erroneously accepting an impostor. Studies on the individ- uality of the biometric trait attempt to calculate the theoretical probability of this type of biometric system failure. For example, individuality of the minutiae information in a fingerprint was studied in [21].

The second kind of biometric system failure occurs when an impostor is deliberately attempting to masquerade the system. Ratha et al. [17] identified different levels of attacks that can be launched against a biometric system. These attacks are intended to either circumvent the security afforded by the system or

24 A.K. Jain

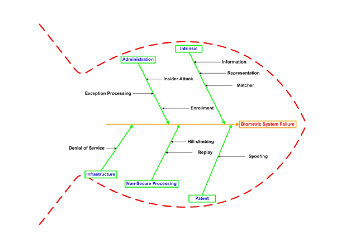


Fig.1. Fishbone (cause & effect) illustration of biometric failures. The security af- forded by a biometric system can be undermined by: (a) Administration: The system administrator can abuse and compromise the system. (b) Intrinsic: The inherent limi- tations of the representation/matching schemes may result in erroneously accepting an intruder. (c) Infrastructure: Denial of service attacks can disable system functionality. (d) Non-secure processing: An impostor can hack system processes to gain access into the system. (e) Patent: Since biometric identifiers are not secrets, an impostor could create physical or digital artifacts to fool the system.

to deter the normal functioning of the system: (i) A fake biometric trait such as an artificial finger may be presented at the sensor. (ii) Illegally intercepted data may be resubmitted to the system. (iii) The feature extractor may be replaced by a Trojan horse program that produces pre-determined feature sets. (iv) Legitimate feature sets may be replaced with synthetic feature sets. (v) The matcher may be replaced by a Trojan horse program that always outputs high scores thereby defying the system security. (vi) The templates stored in the database may be modified or removed. Alternately, new templates may be introduced in the database. (vii) The data in the communication channel between various modules of the system may be altered. (viii) The final decision output by the biometric system may be overridden.

Among these attacks, the presentation of fake biometric traits at the sen- sor and the protection of biometric templates have been widely studied in the literature and a number of solutions have been proposed to guard against such attacks. A challenge-response type of authentication can prevent the problem of fake biometric submission to a great extent. Other methods such as detection of liveness during the presentation of the biometric trait have also been suggested.

For the protection of biometric templates, Jain and Uludag [22] suggested the use of steganography principles that hide biometric data (e.g., eigen-coefficients of a face image) in host images (e.g., fingerprints). Ratha et al. [23] proposed the use of distortion functions to generate biometric data that can be canceled if necessary. Thus, careful design and planning is necessary to ensure the integrity of the biometric system and thwart the impostor attempts to circumvent the security of the system.

4 Summary

Reliable person recognition is critical to many government and business pro- cesses. The conventional knowledge-based and token-based methods do not really provide positive person recognition because they rely on surrogate representa- tions of the person’s identity (e.g., exclusive knowledge or possession). It is, thus, obvious that any system assuring reliable person recognition must necessarily in- volve a biometric component. This is not, however, to state that biometrics alone can deliver error-free person recognition. In fact, a sound system design will often entail incorporation of many biometric and non-biometric components (building blocks) to provide reliable person recognition. As biometric technology matures, there will be an increasing interaction among the market, technology, and the applications. This interaction will be influenced by the added value of the tech- nology, user acceptance, and the credibility of the service provider. It is too early to predict where and how biometric technology would evolve and get embedded in which applications. But it is certain that biometric-based recognition will have a profound influence on the way we conduct our daily business.

**(**Fabio Roli Sergio Vitulano (Eds.) Image Analysis and Processing – ICIAP 2005 13th International Conference Cagliari, Italy, September 6-8, 2005 Proceedings )

Biometrics: Practical considerations

**Accuracy**

– The correctness of a biometric system, expressed as ERR (Equal Error Rate), where a low ERR is desirable. //Ders notundan

To make biometric system practical, satisfactionaly high recognition accuracy is required. Therefore, we have to make sure the recognition is accurate enough for an application.(R.Khosla et al. (Eds.) KES 2005, LNAI 3683, pp.1168, 2005)

• **Performance**:  
– the achievable speed of analysis,  
– the resources required to achieve the desired speed,

(IN2120 ders notundan)

### **Measuring Performance**

Evaluating the performance of a biometric identification system is a challenging research topic [[12](https://cacm.acm.org/magazines/2000/2/7730-biometric-identification/fulltext#R12)]. The overall performance of a biometric system is assessed in terms of its **accuracy, speed, and storage**. Several other factors, like **cost** and **ease-of-use**, also affect efficacy.

Biometric systems are not perfect, and will sometimes mistakenly accept an impostor as a valid individual (a false match) or conversely, reject a valid individual (a false nonmatch). The probability of committing these two types of errors are termed false nonmatch rate (FNR) and false match rate (FMR); the magnitudes of these errors depend upon how liberally or conservatively the biometric system operates. [Figure 3](https://cacm.acm.org/magazines/2000/2/7730-biometric-identification/fulltext#F3) shows the trade-off between a system's FMR and FNR at different operating points; it's called the "Receiver Operating Characteristics (ROC)" and is a comprehensive measure of the system accuracy in a given test environment.

High-security access applications, where concern about break-in is great, operate at a small FMR. Forensic applications, where the desire to catch a criminal outweighs the inconvenience of examining a large number of falsely accused individuals, operate their matcher at a high FMR. Civilian applications attempt to operate their matchers at the operating points with both a low FNR and a low FMR. The error rate of the system at an operating point where FMR equals FNR is called the equal error rate (EER) which may often be used as a terse descriptor of system accuracy. Accuracy performance of a biometrics system is considered acceptable if the risks (benefits) associated with the errors in the decision-making at a given operating point on ROC for the given test environment are acceptable. Similarly, accuracy of a biometrics-based identification is unacceptable/poor if the risks (benefits) associated with errors related to any operating point on the ROC for a given test environment are unacceptable (insufficient).

The size of a template, the number of templates stored per individual, and the availability of compression mechanisms determine the storage required per user. When template sizes are large and the templates are stored in a central database, network bandwidth may become a system bottleneck for identification. A typical smartcard may only hold a few kilobytes of information (for instance, 8K) and in systems using smartcards to distribute the template storage, template size becomes an important design issue.

The time required by a biometric system to make an identification decision is critical to many applications. For a typical access-control application, the system needs to make an authentication decision in real-time. In an ATM application, for instance, it is desirable to accomplish the authentication within about one second. For forensic applications, however, the time requirements may not be very stringent.

All other factors remaining identical, the widespread use of biometrics will be stimulated by its adoption in the consumer market. The single most important factor affecting this realization is the cost of the biometrics systems including the sensors and related infrastructure. Some sensors, such as microphones, are already very inexpensive, while others, such as CCD cameras, are now becoming standard peripherals in a personal computing environment. With the recent advances in solid-state technology, fingerprint sensors will become sufficiently inexpensive in the next few years. Storage requirements of the biometric templates and processing requirements for matching are among the two major considerations towards the infrastructure cost.

The human factors issue is also important to the success of a biometric-based identification. How easy and comfortable is it to acquire a given biometric? For example, biometric measurements that do not involve touching an individual, such as face, voice, or iris, may be perceived as more user-friendly. Additionally, biometric technologies requiring very little cooperation/participation from the users (such as face and thermograms) may be perceived as more convenient to users. A related issue is public acceptance. There may be a prevalent perception that biometrics are a threat to the privacy of an individual. In this regard, the public needs to learn that biometrics could be one of the most effective, and in the long run, more profitable means for protecting individual privacy. For instance, a biometrics-based patient information system can reliably ensure that medical records can only be accessed by medical personnel and the individual concerned. As in any industry, government regulations and directives may either provide a boost or lead to the demise of certain types of biometric technologies. Upcoming U.S. legislation such as the Health Information Portability Act (HIPA), may have a favorable impact on the biometrics industry. A good approach to piloting and gaining gradual acceptance of a biometrics solution could be to introduce it on a voluntary basis with either explicit or implicit incentives for opting biometrics-based solution. **(By Anil Jain, Lin Hong, Sharath Pankanti Communications of the ACM, February 2000, Vol. 43 No. 2, Pages 90-98)**

**Acceptability**:  
– the extent to which people are willing to accept the use of

a particular biometric identifier (characteristic) //Ders notundan

this indicates the extent to which people are willing to accept the use of a particular biometric identifier (characteristic) in their daily lives; ***(December 2004 Biometrics Acceptance - Perceptions of Use of Biometrics Angela Chau Greg Stephens Rodger Jamieson )***

In conclusion, the context of use does affect an individual’s perceptions of benefits and levels of comfort with biometrics. Application contexts with obvious, apparent benefits will lead to greater perceptions of usability and higher acceptance opinions of biometrics than contexts where there are little obvious benefits. However, there is a hesitation due to insufficient knowledge of the technology or its ramifications. There is also a hint of privacy concerns, although they were not clearly defined in participants' minds. ( Perception and acceptance of fingerprint biometric technology Rosa R. Heckle Andrew S. Patrick Ant Ozok 2007 )

**Circumvention/spoofing resistance:**  
– The difficulty of fooling the biometric system

**• Safety:**  
– Whether the biometric system is safe to use

**Biometric authentication can be safety risk**

– Attackers might want to “steal” body parts

– Subjects can be put under duress to produce biometric authenticator

• Necessary to consider the physical environment where biometric authentication takes place.

//Ders notlarindan

**Biometrics: Modes of operation**

**• Enrolment:**

* –  analog capture of the user’s biometric attribute.
* –  processing of this captured data to develop a template of the user’s attribute which is stored for later use.

**• Verification of claimed identity (1:1, one-to-one):**

* –  capture of a new biometric sample.
* –  comparison of the new sample with that of the user’s stored template.

**• Identification (1:N, one-to-many)**

* –  capture of a new biometric sample.
* –  search the database of stored templates for a match based solely on the biometric.

Just like any other means of biometrics, a speaker verification system is not only expected to be accurate for regular users, but also secure against spoofing attacks. As discussed in [2], possible spoofing attack happens at two points: sensor level and transmission of the sensed signal. At the sensor level, an adversary, that we call an impostor, could deceive the system by impersonating someone at the microphone, and at the transmission time when the acquired voice signal could be replaced by a synthetically generated signal or imitated voice. In general, spoofing attack is to use a falsifying speech signal as system input (See Fig. 1) for feature extraction and verification, therefore, presenting a threat to speaker verification systems.

As digital recording has become widely accessible, *replay attack* is the simplest method to deceive a speaker verification system. Replay attack involves repetition of a pre-recorded speech sample or a sample created by concatenating basis speech segments from a given target speaker. Indeed, replay attack has been shown to be an effective way to spoof text-independent recognizers which do not impose constraints on linguistic content [3], [4]. However, the replay technique is not flexible in generating specific utterances as required by text-dependent speaker verification systems.

Aside from replay attack, *human voice mimicking* or *impersonation* has also received considerable attention [5], [6], [7]. As impersonation requires special skills, it is difficult to judge its effectiveness as a general spoofing technique. Partial evidence, however, suggests that humans are most effective in mimicking speakers with “similar” voice characteristics to their own, while impersonating an arbitrary speaker appears challenging [5]. Professional voice mimics, often voice actors, tend to mimic prosody, accent, pronunciation, lexicon and other high-level speaker traits, rather than spectral cues used by automatic systems. Therefore, human voice mimicking is not considered as a cost-effective adversary to speaker verification systems.

*Speech synthesis* represents a much more genuine threat. Due to the rapid development of *unit selection [8], statistical parametric* [9] and *hybrid* [10]methods, speech synthesis systems are now able to generate speech with a certain speaker's voice characteristics, such as spectral cues, and acceptable quality. In early studies [11], [12], [13], vulnerability of text-prompted *hidden Markov model* (HMM) based speaker verification was examined using a small database of 10 speakers. More recently, [14] used a flexible adapted HMM-based speech synthesis system to simulate spoofing attacks against text-independent recognizer on a corpus of around 300 speakers. Even though HMM-based synthesis poses a threat, a lot of training speech (usually one hour or more) is needed to train the speech synthesis system. Even for adapted HMM-based speech synthesis system, one needs additional speakers' data to train an average voice model for target speaker adaptation [15]. Therefore, it is expensive for attackers to conduct spoofing attack using an HMM-based speech synthesis system.

Different from replay attack, human voice mimicking and text-to-speech, *voice conversion* is to modify one speaker's (source) voice to sound like it was pronounced by another speaker (target) without changing the language content. While keeping the language content unchanged, the conversion technique works in two ways, one is to change the source voice to sound differently - to disguise oneself; the other is to change the source voice to a target voice - to mimic someone else. As real-time voice conversion not only is possible, but also offers voice quality and characteristics that even human ears are hard to distinguish, it presents a genuine threat to both text-dependent and text-independent speaker verification systems.

In summary, human voice can be seen to have three attributes, the language content, the spectral pattern, and the prosody. The individuality of human voice is described by the spectral patterns, called voice quality or timbre, and by the prosodic patterns carried by the speech. Professional voice mimicking typically modifies the prosodic patterns while voice conversion modifies the spectral patterns. As it is more reliable to characterize speakers by their spectral cues [16], most of the state-of-the-art speaker verification systems are built to detect the difference of spectral patterns. In this paper, we will focus on the conversion spoofing attack, and review the most recent research works on voice conversion, speaker verification, spoofing attack and anti-spoofing attack techniques.

# (Voice conversion and spoofing attack on speaker verification systems

**2**

**Author(s)**

[Zhizheng Wu](file:////search/searchresult.jsp%3fsearchWithin=%22First%20Name%22:%22Zhizheng%22%0a%09%09%09%09&searchWithin=%22Last%20Name%22:%22Wu%22&newsearch=true); [Haizhou Li](file:////search/searchresult.jsp%3fsearchWithin=%22First%20Name%22:%22Haizhou%22%0a%09%09%09%09&searchWithin=%22Last%20Name%22:%22Li%22&newsearch=true)

**View All Authors**

**)**

**III. BIOMETRIC SYSTEM VULNERABILITY**

In the developing area of biometric computing technology have affordable and very easily inbuilt the various consumer devices. To avert any potential security crisis, vulnerabilities of the biometric system must be identified and addressed systematically [5]. There are different methods of vulnerability attack that could be analysis. Biometric recognition systems are prone to deliberate attacks as well as inadvertent security lapses that can lead to illegitimate intrusion, sabotage [6] or theft of sensitive information such as the biometric templates of the users enrolled in the system. There may be many factors which lead to such security lapses. A biometric system is vulnerable to different types of attack that can compromise the security afforded by the system, thereby resulting in system failure [7]. (**To study of various security attacks against Biometric template in a generic Biometric Recognition System** Manish Kumar, Kunwar Singh Vaisla**)**

Presentation Attack

* ISO Standards underway:

• **Presentation Attack** Definition: Presentation of an artefact or human characteristic to the biometric capture subsystem in a fashion that could interfere with the intended policy of the biometric system\*

* [#1] - [ISO/IEC 30107-1:2016](https://www.iso.org/standard/53227.html) - based on information obtained 2017-03-19

# BBC fools HSBC voice recognition security system

Security software designed to prevent bank fraud has been fooled by a BBC reporter and his twin. BBC Click reporter Dan Simmons set up an HSBC account and signed up to the bank's voice ID authentication service. HSBC says the system is secure because each person's voice is "unique". But the bank let Dan Simmons' non-identical twin, Joe, access the account via the telephone after he mimicked his brother's voice.The bank said it would "review" ways to make the ID system more sensitive following the BBC investigation.(**https://www.bbc.com/news/technology-39965545)**

**11. CONCLUSION**

The vulnerability of face recognition systems to low-cost artifacts such as photo print or video replay attacks indicates the resilience of face recognition systems to presentation attacks. To this end, a substantial number of face presentation attack detection algo- rithms are presented. In this article, we present a comprehensive review of publicly available databases and the relevant standards that define the performance metrics, and report the performance of face PAD algorithms. Finally, we also discuss the open issues and challenges that remain to be addressed. Even though there exist a large number of techniques to address various kinds of face artifacts, there is still a need to design a robust face PAD system that can be generalized to different face artifacts. Overall, this article can serve as a quick reference for face presentation attack detection techniques for both newcomers andexperts. (**Presentation Attack Detection Methods for Face Recognition Systems: A Comprehensive Survey** RAGHAVENDRA RAMACHANDRA and CHRISTOPH BUSCH, Norwegian Biometric Laboratory, Norwegian University of Science and Technology (NTNU), Gjøvik, Norway )

28.13 Conclusion

The biometric security system rely on FRR and FAR values of system, hash- ing mechanism to retrieve template from database, liveliness detection mech- anisms, anti-spoofing mechanisms and efficiency of communication media. Anti-spoofing identify fake properties. The fake aspects in iris detection are plastic fingers. Liveness detection process identifies alive properties. The uti- lization of external physiological biometrics with behavioral biometrics in- creases the reliability of authentication system. An application with different biometric information on a single algorithm of authentication, creates adap- tiveness of the interactions. The factors for security with convenience lead to proper biometric selection. With varying performance of devices to extract features, multimodal methods create trustworthy system for large popula- tion sectors. Anatomical biometric is a constant signal. Behavioral biometric provides self-certification. With common algorithm, a method for userdepen- dent threshold decisions are achieved for both biometrics in uniform fashion. The integration of static iris information and signature dynamic information can be achieved at decision level, to improve response time of the security system as compared to feature level and score level. In feature level, all fea- tures of both biometrics are integrated which increases the dimensionality. Score-level integration is at the classifier level. At decision level, inferences are drawn using voting techniques. Cancelable biometrics incorporates protection and replacement of features. In general, using a trajectory generation method comprising data compression and mining technique, a suitable authentication method for web and m-commerce applications can be provided. A server is a computer in network that is used to provide services to other computers. A client is a computer in network that uses the services provided by server. In on-line scenario, the authentication from server side can be performed by passing only the parameters of biometric sample from the client side. The bio- metric sample can be reconstructed at server-side. A good parameter mining method using unique biometric vault generation can be developed for authen- tication purpose. These methods search large databases for augmentation of stroke parameters. Instead of providing an image of constant size to recog- nizer, a numerically augmented parameter value with topological ordering is provided to make the authentication process faster in on-line database search scenario. The abundance applications on PDAs and smartphones represent a new scenario for automatic signature verification. (Patrick S.P. Wang **Pattern Recognition, Machine Intelligence and Biometrics )**

**5. CONCLUSION**

There are several attacks that try to negotiate a computer system using a variety of methods such as unauthorized access. These attacks could be reduced if an identification tool is used to complement already deployed intrusion detection system. The most reliable identification systems are based on biometrics. Therefore, several biometrics technologies start to accompany host-based Intrusion detection systems. Until Now, behavioral biometric was the only techniques that have been used so far, since they do not need any special devices. In contrast, some researchers proved that these techniques are not very efficient which was the motivation to design an identification system based on fingerprint technique. (International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.2, No.1, February 2012 )( BIOMETRICS AUTHENTICATION TECHNIQUE FOR INTRUSION DETECTION SYSTEMS USING FINGERPRINT RECOGNITION Smita S. Mudholkar 1, Pradnya M. Shende 2, Milind V. Sarode 3)

For fingerprint;

The security of a system is given by the amount of effort needed to circumvent it. So far, most authors have reported the liveness detection performance of their methods as universal rates for all the fakes their method has been tested with. However, the detection performance can vary greatly as it depends on the specific fake type, and the mere quantities do not yield accurate information on the case. In spite of the research effort so far, the state-of-the-art methods cannot be considered reliable in the environments that require high security levels. A 3D scanning technology, such as the OCT, can provide for highly detailed representations of the structure of a scanned fingertip and thus significantly increase the amount of information available for the liveness detection purposes. A reliable method, which was able to verify the genuine structure of the scan, would render the fake fabrication process extremely difficult. The development of such a method has the potential to provide for a very secure fingerprint recognition solution. **(Presentation attack detection methods for fingerprint recognition systems: a survey Ctirad Sousedik, Christoph Busch 2013 )**

## **5. Conclusion**

In this work, we have analyzed the impact of a spoof attack in multimodal biometric systems. Our experiments show that when using traditional fusion schemes (i.e. LLR or weighted sum), a forger can dramatically increase the chances of cracking a multimodal system by spoofing only one of the biometrics. To reduce this weakness, we proposed two new fusion schemes that take into account the security of each unimodal biometric system. The experiments indicate the existence of a tradeoff between recognition accuracy and robustness against spoof attacks. **(Robustness of multimodal biometric fusion methods against spoof attacks** Author links open overlay panel[Ricardo N.Rodrigues](https://www.sciencedirect.com/science/article/pii/S1045926X09000068" \l "!)[a](https://www.sciencedirect.com/science/article/pii/S1045926X09000068" \l "!)[Lee LuanLing](https://www.sciencedirect.com/science/article/pii/S1045926X09000068" \l "!)[b](https://www.sciencedirect.com/science/article/pii/S1045926X09000068" \l "!)[VenuGovindaraju](https://www.sciencedirect.com/science/article/pii/S1045926X09000068" \l "!)[a](https://www.sciencedirect.com/science/article/pii/S1045926X09000068" \l "!) [**Journal of Visual Languages & Computing**](https://www.sciencedirect.com/science/journal/1045926X)[Volume 20, Issue 3](https://www.sciencedirect.com/science/journal/1045926X/20/3), June 2009, Pages 169-179)