Face Recognition – Lenovo VeriFace Login Application

Usman Dastgeer Hassam Nadeem
Email: {usmda512,hasna890}@student.liu.se
Supervisor: Viiveke Fåk, { viiveke@isy.liu.se }
Project Report for Information Security Course
Linköpings universitetet, Sweden

Abstract

Biometric applications are increasing in modern system's security. Face recognition has gained popularity in computer login as a replacement to traditional password technology. Different vendors' solutions are available with variation in quality and specifications. This study is based on a set of experiments with a commercial application (Lenovo VeriFace) for measuring certain parameters with respect to its face recognition technology. This includes aliveness detection, spectacles, male vs female, light and distance variations. Analysis of the experiment data showed various points of improvements that need further work. Overall, the tested system was found less acceptable for people with glasses, under poor light and increased distance.

1. Introduction

In our daily lives, we often remember and recognize people by looking at their face. This is a part of the body that is highly visible and is important for an interaction. We store information of a face and later use that information for recognition and matching purposes. This mechanism can be used by machines to recognize and authenticate a human being.

1.1 Background

With increasing importance of technology in business and human lives, security is becoming a critical concern for modern applications. User authentication is critical for securing an application from unauthorized access. For this, knowledge based, token based and biometric systems can be used. Traditional knowledge-based and token-based systems are losing focus due to issues associated with their usage. This situation increases focus on biometric (what we are) characteristics rather than knowledge (what we know) and token (what we have) approaches.

1.2 Purpose

The purpose of this study is to recognize the applications, obstacles and issues to face recognition technology in the security of commercial application with special focus on computer login application.

1.3 Audience

The target audience of this report is university students having basic understanding of information and computer security with special interest in biometrics.

1.4 Problem Domain

Some of the major questions associated with a face recognition technology are:

- *Is face recognition mature enough to be used as an acceptable recognition biometric in a commercial application such as computer login security?*
- *What are the requirements for a biometric system in this domain and what is the standing of face recognition technology?*
- *What are acceptable FAR (False Acceptance Rate) and FRR (False Rejection Rate) for a system in this domain?*
- *Where does current commercial solutions of face recognition stand with respect to the traditional password security?*

Above are some major questions that we will focus on in this study and will try to find answers. This study will set the direction for future research in this domain by pointing out major issues and flaws in current systems.

1.5 Method

We have studied literature including the books, research papers and some other material available in physical and electronic form. Then we focused on a specific computer login face recognition application named Lenovo VeriFace recognition (see section 3). After initial exploration of the system we carried out experiments with the system. The major focus during the experiments was to execute the system with different variations and exceptions to point out flaws and weaknesses in the system. Due to the resource constraints, we limited ourselves to a small population size, trying to cover as much variations and possibilities as possible.

1.6 Methodological Critique

This report depends on available literature regarding face recognition and Lenovo VeriFace recognition software. Moreover, the approach used for the experiments may be influenced by the author's previous experiences. The limitations of the method largely depend on the experiment's design.

2. Biometrics & Face Recognition

2.1. Biometrics

Biometric refers to the usage of distinctive physiological and behavioral characteristics to recognize and identify an individual's identity. There is no clear distinction between a physiological (fingerprint, face, iris etc.) and a behavioral (signatures, gait etc.) characteristic and often they overlap. There are several biometrics characteristics with varying capabilities and limitations whose discussion is beyond the scope of this document. Following is a list of some common biometric identifiers:

- DNA
- Ear
- Face
- Facial thermogram
- Hand thermogram
- Hand vein
- Hand geometry
- Fingerprint
- Iris
- Gait
- Retina
- Signature
- Voice
- Keystroke dynamics
- Odor

2.2. Face Recognition

In the last twenty years, face recognition has gained considerable attention as a biometric identifier for determining an individual's identity, mainly due to its wide acceptability as a biometric identifier in different cultures. Face recognition can be 2-dimensional and 3-dimensional. In 2-dimensional (2D) face recognition fewer resources are required but it can be vulnerable to still images and other 2D material. 3-dimensional face recognition uses depth information besides 2D information and is more powerful but expensive and complex than the 2-dimensional techniques. Moreover, there are several challenges faced in terms of

- Light variations and surrounding environment,
- Face expressions,
- Spectacles and other personal attire,
- Twin faces,
- Apparent changes in a face (beard, mustache etc.)

Applications of face recognition are increasing. There are many novel applications of the face biometric, including:

- Face Recognition for Smart Environments
- Wearable Recognition Systems

Some other applications are listed in Table 1.

Table 1: Applications of face recognition as mentioned in [1]. These are some broad categories and this study is focused on Lenovo Veriface application that is login security applications for a laptop.

Areas	Specific Applications
Biometrics	Drivers' Licenses, Entitlement Programs
	Immigration, National ID, Passports, Voter Registration
	Welfare Fraud
Information Security	Desktop Logon (Windows NT, Windows 95)
	Application Security, Database Security, File Encryption
	Intranet Security, Internet Access, Medical Records
	Secure Trading Terminals
Law Enforcement and Surveillance	Advanced Video Surveillance, CCTV Control
	Portal Control, Post-Event Analysis
	Shoplifting and Suspect Tracking and Investigation
Smart Cards	Stored Value Security, User Authentication
Access Control	Facility Access, Vehicular Access

3. Laptop face recognition technology

Use of digital face recognition in commercial products is increasing. In computer login to provide security, traditional lengthy passwords are still dominant. However, some laptop vendors developed face recognition systems as replacement to passwords for login security. Still, there is a tradeoff between the security and the convenience and both can't be maximized at the same time in normal circumstances. These applications work by taking a number of images of a legitimate user and store it in a database to later match with an authentication request. When a user require a login, the system matches the current user with the images stored in the database and make the decision to either allow or deny the request. Currently there are three face recognition solutions for computer login. These are:

3.1. Lenovo

Figure 1: Lenovo VeriFace Recognition

VeriFace provides maximum user convenience rather than more robustness and security in comparison to the other two vendors [2]. VeriFace stores images in black and white form [2]. The system restricts still the photo problem by detecting aliveness using eye movements of the user [3]. Also it does not work for nonhuman faces like cats, dogs, birds etc. VeriFace III is termed as least secure among all three solutions [2].

3.2. Asus

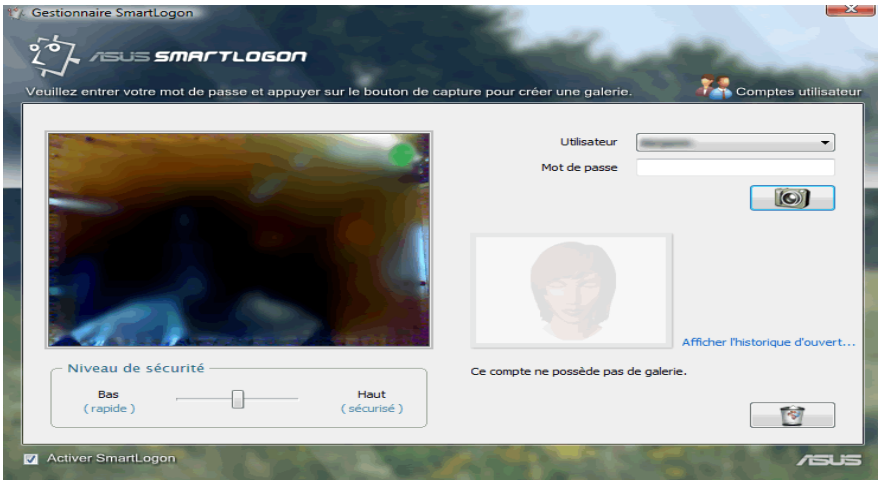

Figure 2: Asus SmartLogin [http://www.geekandtech.net/wp-content/uploads/asus-smart-login.png]

Asus SmartLogin uses a more complex and secure way than the Lenovo solution. It takes a much larger number of images to make it more dependable [4]. However, results showed that this system can also be forged with some effort [2].

3.3. Toshiba

Figure 3: Toshiba software [http://www.computerworld.com/common/images/site/features/2008/052008/face_start.jpg]

This is considered to be the more secure among the three solutions [2]. It uses complex but an efficient algorithm. The downside is that it requires cooperation from the user to make an authentication. It enables secure sharing of your laptop with family and friends [5].

We have selected Lenovo VeriFace for our experiments. Following are a few reasons for this selection:

1. Lenovo software is compatible with Windows Vista and can run on any laptop with camera (internal or external).

2. As all these are propriety software, so getting them for the experiments is not trivial. We managed to have the Lenovo VeriFace for the experiments.

3. It enables us to accomplish our experiments objectives as the underlying technology and the technique used by all vendors is the same to a large extent.

4. Experiments

Experiments were conducted with consideration to the constraints. Keeping a small population and still measuring different parameters is a tough task. We tried to incorporate all possibilities required for the observed parameters.

a. Population

Experiments were carried out with twenty people. Details about the population are given in Table 2.

Table 2: Sample Population for experiments

Gender	With Glasses	Without Glasses	Total
Male	5	8	13
Female	3	4	7

Total	8	12	**20**

b. Limitations

Cost and time associated with the experiments are major factors that posed limits on the experiments' design. Besides this, the age of our sample population was between 20-35 years. All were students of Linkoping University and most of them were having a technology background.

c. Parameters

i. Spectacles

This parameter includes people with glasses and lenses. Due to our resource constraints we limited ourselves to glasses only. In a face recognition system, people with glasses are an important parameter both due to the growing population and issues surrounding their seamless recognition.

ii. Aliveness

This parameter means measuring ability of the system to detect aliveness in a candidate presented for recognition. Forging the system with still pictures of a legitimate user can make the system highly vulnerable and less secure.

iii. Light & Distance

The surrounding environment condition (especially light) results in significant variations. Moreover, we tried to measure the greater possible distance of a candidate from a computer screen, where the candidate was still recognized correctly by the system.

iv. Male vs Female

Gender difference is an interesting topic with respect to face recognition. Whether a face recognition system has different acceptance ratio for male and female is an important question to answer.

d. Constant Factors

i. Safety Level

Lenovo VeriFace supports five safety levels (Highest, Higher, Normal, Lower, and Lowest). Due to our resource constraints (time, cost), we did not carry out the experiments for all levels. During the experiments the most common and default level (i.e. Normal) is used that balances security and convenience.

ii. Acceptance Criteria

The time the system takes to decide whether a face is legitimate or not is an important factor. We set the threshold to 20 seconds for our experiments. This is the maximum time that the system can take in to recognize. Any recognition exceeding that time is not considered. This time-bounding greatly affects the results.

e. Experiment Design

In order to keep the statistics simple for analysis, we distributed samples equally across the population. Every person in our population had 15 attempts. In those 15 attempts, 8 were with favorable conditions (having proper light and the face close to camera on ideal distance) and 7 were with light and distance variations (with half light than normal and distance of the face ranging to 3 feet approximately). All the experiments were conducted in a controlled (not external) environment and most of the laptops used in the experiment had built-in camera.

The criterion for a successful recognition was specified as 20 seconds maximum to recognize a face. Otherwise it was regarded as a failed attempt.

Table 3: Sample distribution across population, every candidate got fifteen attempts. This table shows the distribution across people with glasses and without glasses.

Gender	With Glasses		Without Glasses		Total	
Male	40	35	64	56	104	91

	75		120		195	
Female	24	21	36	24	56	49
	45		60		105	
Total	64	56	100	80	**160**	**140**
	120		180		**300**	

With Ideal Conditions	With light and distance variations

In Table 3, details about the attempts made by different population segments under different conditions are presented. This gives a clear idea about the number of attempts and how they are distributed in the population.

5. Results Analysis

The results of the study were interesting in some aspects and we will consider them with respect to our parameters.

a. Spectacles

5 male and 3 female participants were wearing glasses. The results of the experiments are given in Table 4. These results may have different interpretations, possibly more than one. We left this interpretation open for this report and will not consider any single interpretation.

Table 4: System acceptance for people with spectacles, this is further influenced by light and distance variations and it becomes less than half for a male candidate

	With ideal Conditions		With light and distance variations	
Male	33	7	13	22
Female	20	4	11	10
Total/All	53	11	24	32

Successful Attempt	Failed Attempt

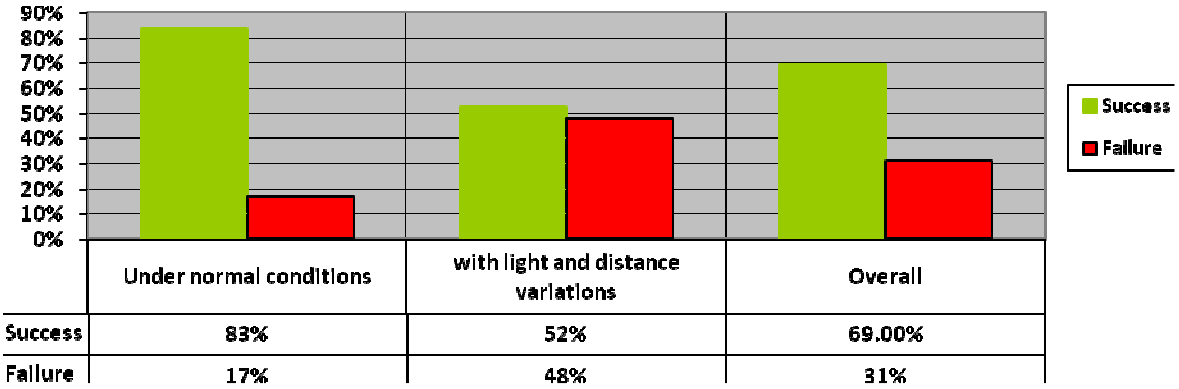

Figure 4: Ratio of Success to Failure, Female with Spectacles

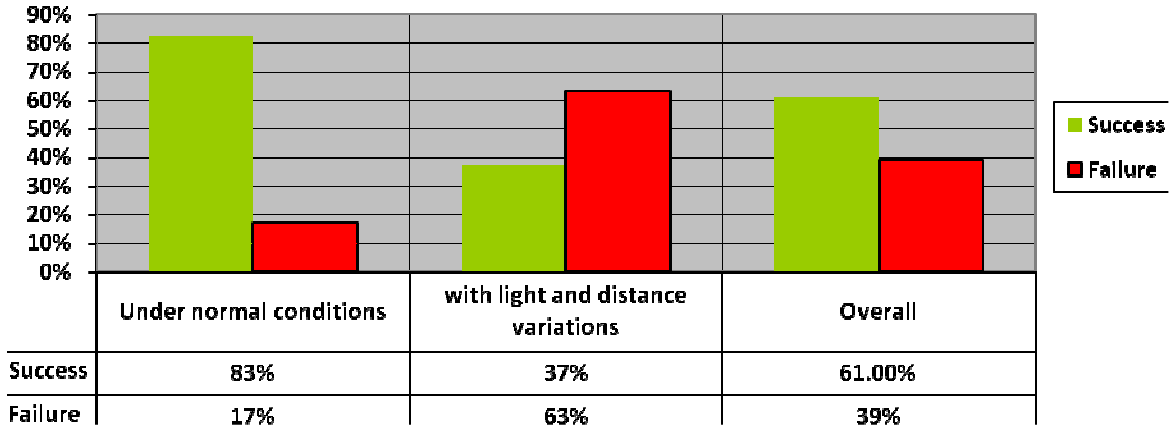

Figure 5: Ratio of Success to Failure, Male with Spectacles

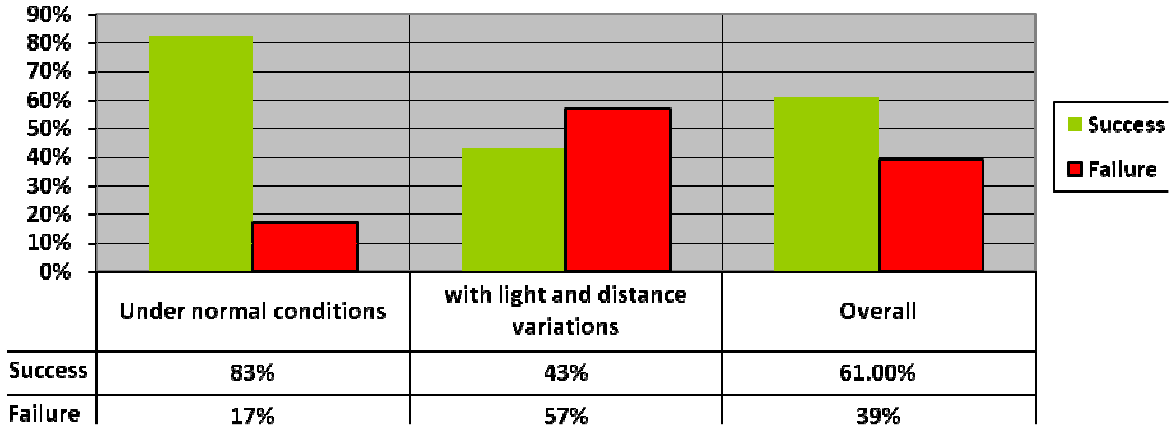

Figure 6: Ratio of Success to Failure, All with Spectacles

b. Aliveness

Lenovo VeriFace uses eye movement to detect aliveness in the object presented. According to [2], it can be forged by still pictures of a legitimate user with some mutations. However, we were unsuccessful in forging the system with still images.

We have tried pictures of 3 users (2 male, 1 female) but the system didn't allow an access. Moreover, we tried to keep some candidate's eyes still for some time to check whether it recognizes this and it did. Keeping the eyes still is tough and there may be some minor movements detected by the system. Thus, our experiments with the system were unable to forge it for aliveness.

c. Light & Distance

With significant variations in light and distance, we observed major changes in the system acceptance behavior. From Table 5, as you can see the failure rate for both male and female candidates is significantly higher under poor light and greater distance. This effect is acknowledged by Lenovo as limitations of the operating environment [3]. The effect of these environmental issues needs to be minimized and greater attention needs to be paid towards their resolution.

Table 5: Light & Distance effect on the system acceptance, light and distance variations had severe impact on the system acceptance and this needs increase focus of researchers as this effects the system ability to operate in an external environment

	With ideal Conditions		With light and distance variations	
Male	91 (88%)	13 (12%)	37 (41%)	54 (59%)
Female	51 (91%)	5 (9%)	30 (61%)	19 (39%)
Total/All	142 (89%)	18 (11%)	67 (48%)	73 (52%)

Successful Attempt	Failed Attempt

d. Male vs Female

During the experiments, the system is observed to have more acceptances for females than their counterparts. Table 6 gives an overview of statistics regarding the system acceptance for male and female candidates.

Table 6: The system acceptance for Male and Female, Lenovo Veriface behaved more favorable during the experiments for female than male candidates in general. There may be different reasons for this and we leave this analysis for the future.

	Successful Attempt	Failed Attempt	Total
Male	128 (66%)	67 (34%)	195
Female	81 (78%)	24 (22%)	105
Total/All	209 (70%)	91 (30%)	300

6. Future Work

This research poses certain research questions that need further investigation. A more thorough analysis of the experiment data can be carried out to gain more insights. Different interpretations of the experiment data are possible and it may reflect different findings with varying parameters. Other parameters such as the system threshold, acceptance criteria etc. need to be analyzed alongside to make strong statements about results. With all limitations, this experiment-based study would undoubtedly contribute to the greater effort for improving performance of a face recognition system.

7. Conclusion

Face recognition is an important application of biometrics in an identification system. Several face recognition systems for laptop login application exist. This study experiments with Lenovo VeriFace laptop login system. We carried out small experiments to check the system for different parameters. Data collected by the experiments can have different meanings, and interpretations may be different based on an analysis. We failed to forge Lenovo Veriface for aliveness with still pictures and by other means. Variations in light and distance caused a great effect on the acceptance ratio of the system and need greater research focus especially if the system operated in an external environment. People with spectacles found difficulty with the system and this is further worsened under poor light and greater distance circumstances. Moreover, during the experiments we have found the system relatively favorable towards females. This study is based on the experiments; and thus is insufficient to provide any strong statements about Lenovo Veriface face-recognition technology. Nevertheless it provides certain points for future research; both for face recognition application designers and face biometric researchers in general.

8. References

[1]. Face recognition: a literature survey, W. Zhao, R. Chellapa, A. Rosenfeld and P.J. Phillips

[2]. BlackHat-DC-09-Nguyen-Face-not-your-password, http://www.blackhat.com/presentations/bh-dc-09/Nguyen/BlackHat-DC-09-Nguyen-Face-not-your-password.pdf

[3]. Lenovo Face Recognition, http://lenovoblogs.com/insidethebox/?p=132

[4]. Asus Special Features, http://promos.asus.com/US/Features/SmartLogin/index.html

[5]. Face Recognition Toshiba, http://explore.toshiba.com/innovation-lab/face-recognition