Your face is NOT your password

Face Authentication ByPassing
Lenovo – Asus – Toshiba

Nguyen Minh Duc *and* ***Bui Quang Minh***
Security Vulnerability Research Team
Bach Khoa Internetwork Security (Bkis)
Ha Noi University of Technology – Viet Nam
http://security.bkis.vn

Contents

[ABTRACTS]

Biometrics has nowadays been of universal interest and has been developed and used for many purposes such as for the detection of criminals and undesirables, identification and *access control.* Within this paper, we would like to concern about Facial Cognitive Biometric Systems and their application in User Authentication Based on Face Recognition.

The most well-knowned authentication system to many people is the user authentication mechanisms on PCs, which make use of Username and Password. Other than that, fingerprint authentication is also widely used. Yet as users' demands are so diversified, they are caring more and more about face authentication due to the fact that it is a hands-free and user friendly way to logon.

Lenovo, Asus, and Toshiba are known as the first three big computer manufacturers to put that technology into practical use and to bring about greater convenience for their customers. The one question to ask is whether such technology is really safe and secure for its users to enjoy. Our research, which is concluded in this paper, will prove that the mechanisms used by those three vendors haven't met the security requirements needed by an authentication system and that they cannot wholly protected their users from being tampered.

I. BIOMETRICS & SECURITY

1. Biometrics

Biometrics includes the study of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits such as eye iris, voice tones, palm print, face outline...

Biometric Technologies fill the role of analyzing and measuring unique biological properties in order to produce unique identifications which is then digitalized and stored.

Biometrics can be divided into two main classes:

- *Physiological biometrics is related to the shape of the body:*
  - • Face Recognition
  - • Finger-scan
  - • Iris-scan
  - • Retina-scan
  - • Hand-scan
  - • ADN.
- *Behavioral biometrics is related to the behavior of a person.*
  - • Voice-scan
  - • Signature-scan
  - • Keystroke-scan

This paper would discuss about face recognition in details and its application in authentication systems.

2. Access Control System using Face Recognition

Face recognition applications are more and more being taken interest in and developed since [1] [2] [7]:

- *They are non-intrusive.*
- *Biometric data of the faces (photos, videos) can be easily taken with available devices like cameras.*
- *One biometric data is used in many different environments.*
- *And facial recognition sounds rather interesting in comparison with other biometric technologies.*

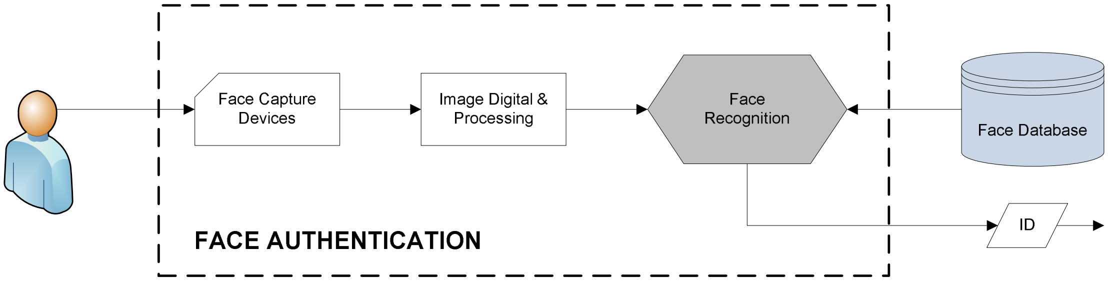
Therefore, face recognition has been widely used in identification and access management.

At the moment, there have been a lot of researches on access control applications and those have been utilized in personal computers' and handheld devices' authentication. They are also integrated into office and home access control systems. *We will talk further about applications of face recognition in access control systems and their security drawbacks.*

II. FACE AUTHENTICATION

1. Model

The following figure describes an access control system base on face authentication. In this model, each user has an account and a corresponding ID in the Face Database. On a user logging in the system, Face Authentication will use face recognition technologies to analyze and determine his ID as well as his permissions on the system [3] [4] [6].



Access Control System Based on Face Authentication Model

This model can be applied to access control systems where the number of people is small; for example, user accounts in an operating system, members of an office or a family.

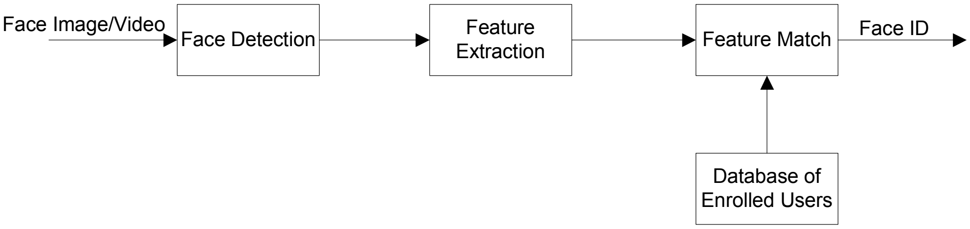
When receiving a request, an access control system based on face authentication must find out exactly whether the person requesting is a client or an impostor. Right after that, it decides whether to accept the login or to treat him/her as an impostor and cry out "*access denial*" [9].

In order for Face Authentication to satisfy all the security issues that an access control system asks for, the face recognition algorithms in operation must be almost completely exact.

2. Algorithms in Use

2.1 Face Recognition Model

As you can see from the diagram below, face recognition requires a wide range of technologies [5]:



Face Recognition Processing Flow

Face recognition systems in general, and access control systems based on face authentication in particular, use a "*learning*" mechanism to collect data on facial characteristics if users. Hence, the first important point to care about in a face recognition model is the *Face Database* storing this information.

When the system finishes scanning a video or photo of a user's face, the digitalized information will go through these following modules one after another:

- *Face Detection*: locating the face in the photo or video and removing unnecessary details on the background.
- *Feature Extraction*: extracting facial characteristics needed for recognition.
- *Feature Match*: comparing scanned information with database to decide if it matches some user's face. If the face matched, the ID of the corresponding is returned.

Most of present researches try to create an Automatic Face Recognition model. The hardest part of it is how to get best biometric information on the faces. Therefore, *Feature Extraction* is the most important module of the system. In the next section, we will focus on basic algorithms used for extracting facial characteristics.

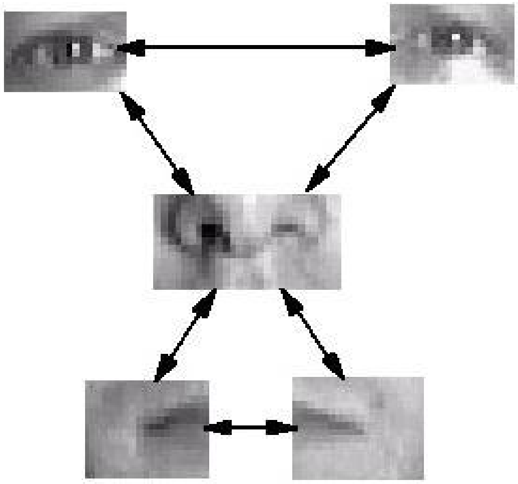
2.2 Face Recognition Algorithm

Geometric feature-based approach

In the 1980s, researches on face recognition were mostly based on the geometric characteristics of faces [5] [9] [10]. Using this approach, parts of human faces such as eyes, nose, and mouth are located together with their attributes and their mutual relationships and measurements (*distances, angles, area*s). The system will distinguish faces based on this information. This approach is quite effective for small database, with steady lighting and viewpoint. But it has lots of disadvantages:

- *Not effective for unstable lighting condition and changing viewpoint.*
- *The scanning technology is not yet reliable.*
- *The information extracted is not enough for an information-rich organ like face.*

Considering these disadvantages, this method is no longer used today.

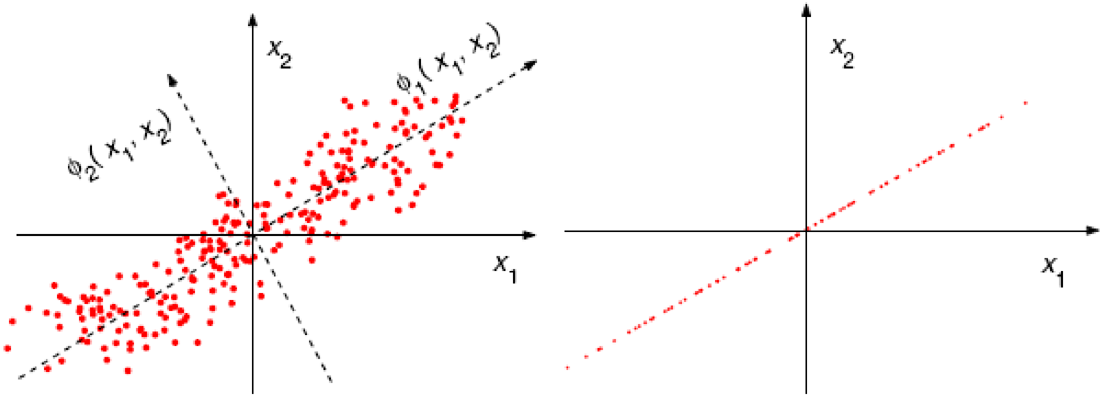


Geometric feature-based approach

Appearance-based approach

At the beginning of 1990s, more and more researchers were inspired by a new approach based on human appearance.. This technology transforms the face space into subspaces which have less dimensions but those are the directions that depict the most important parts of the face.

The studies that are talked about the most is Principal Component Analysis (PCA) and KLT – Karhunen- Loève Transform [6] [11] [12] [13]. The following graphs show a typical example of PCA. We can easily spot that the majority of 2D points locate close to the the 1st PC line, which means that we can perform a projection of these points on the 1st PC line without losing essential 2D information.



(a) PCA basis (b) PCA reduction to 1D

Principal Component Analysis Method

PCA Method uses eigenvectors and eigenvalues for representing face images. These eigenvectors can be thought of as a set of features which together characterize the variation between face image. Each image location contributes more or less to each eigenvector, so that we can display the eigenvector as a sort of ghostly face which we call an eigenface [11].

On the basis of PCA, other methods with higher efficiency have been developed:

- Independent Component Analysis (ICA) [14].
- Linear Discriminant Analysis (LDA), utilizing FisherFace Algorithm [15].
- And other improvement established on subspace.

Appearance-based approaches have been able to extract quite enough information on the faces. However, they haven't yet worked well in varied lighting conditions and especially have ignored non-linear variation of the faces.

Other approach

In order to solve the limitations of the Appearance-based approach, other approaches have been proposed.

The first are the improved methods based on PCA, PLA, and ICA that can project non-linear on the subspace, such as: Kernel PCA, Kernel LDA algorithm [5] [13].

To get rid of these limitations, Local appearance-based feature space technology with a huge database of facial characteristics has been developed. Some methods and algorithms based on this technology are [5] [13]:

- Local Features Analysis (LFA) method.
- Gabor wavelet-based features method (same with Elastic Graph Bunch Matching - EGBM).
- Local Binary Pattern (LBP) method.

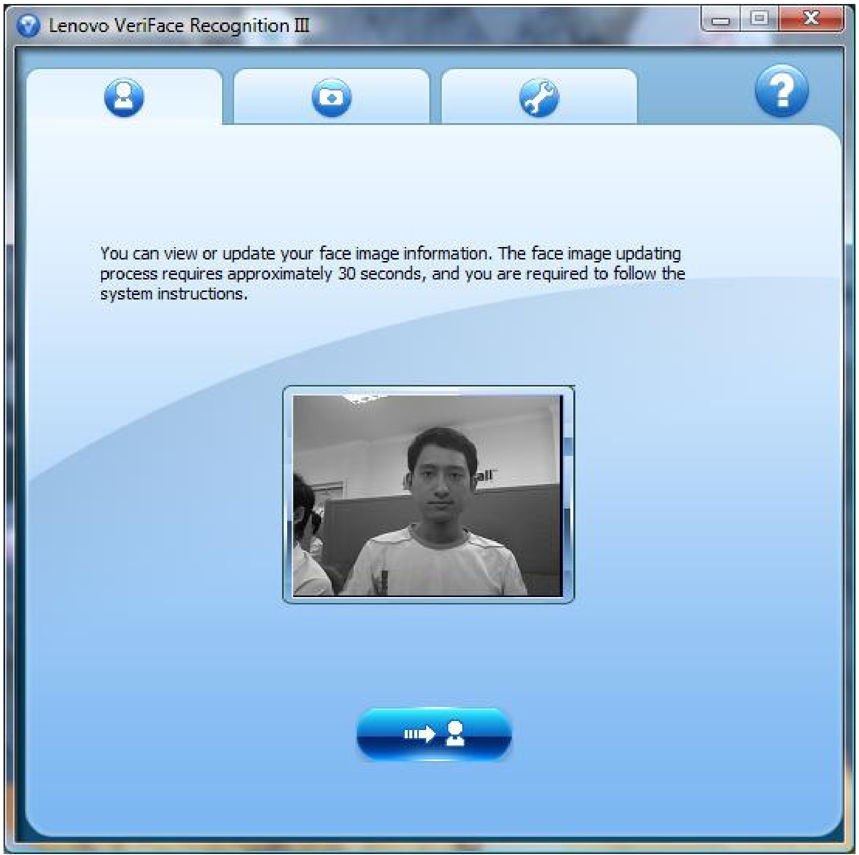
Moreover, as modern image capturing devices are becoming better and better, a new method called 3D Face Recognition are becoming the new target [5] [13] [16] [17].

In general, face recognition technologies have been improved robustly and become more accurate and effective. We have just talked about the most popular approaches used in researches on algorithms that extract the facial characteristics. There are indeed many organizations and individuals studying this problem using their own approaches but we cannot discuss here due to limited space.

3. Lenovo – Asus – Toshiba

The previous sections have introduced the access control systems based on face recognition and several basic algorithms in use. In this section, we will talk about the access control system provided by three well-known computer manufacturers: Lenovo, Asus and Toshiba.

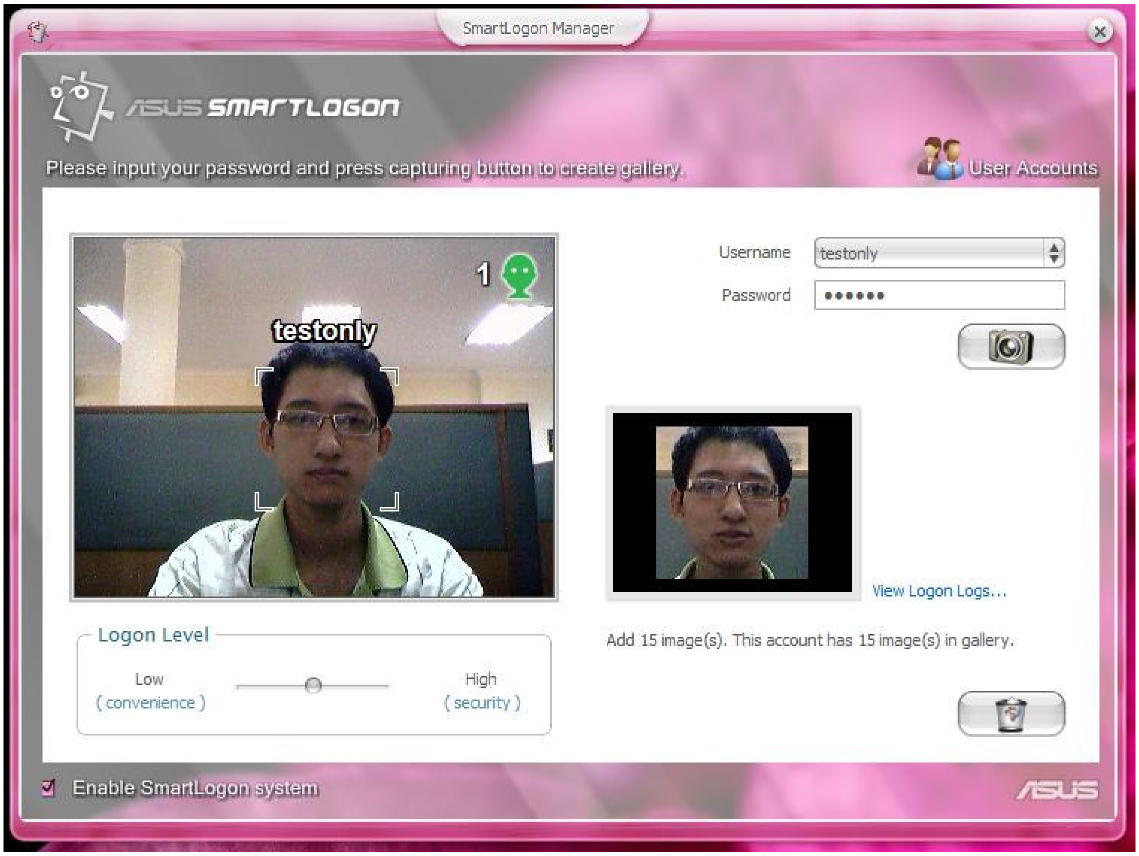
Lenovo Veriface III



You can view or update your face image information. The face image updating process requires approximately 30 seconds, and you are required to follow the system instructions.

User interface of Veriface III, released on Aug 06th 2008.
Lenovo has had interesting ads with Robinson and his wife.

Asus SmartLogin



Please input your password and press capturing button to create gallery.

Username: testonly

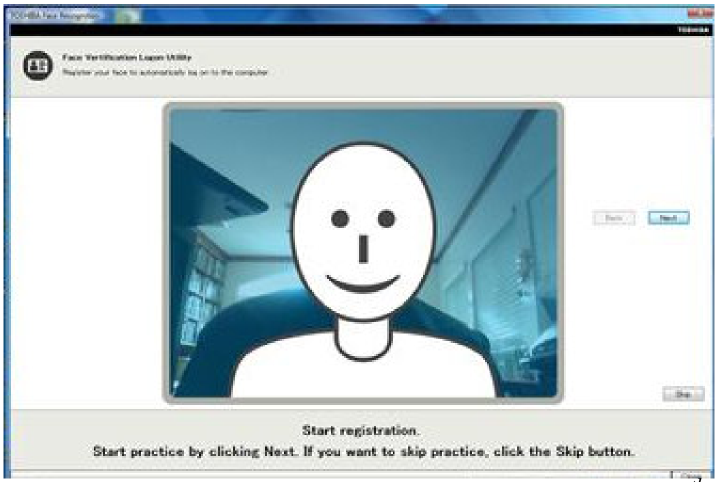
Password: ••••••

Add 15 image(s). This account has 15 image(s) in gallery.

☑ Enable SmartLogon system

SmartLogin V1.0.0005 User Interface.
Asus have it on market on July 07th 2008.

Toshiba Face Recognition



Start registration.

Start practice by clicking Next. If you want to skip practice, click the Skip button.

Toshiba Face Recognition 2.0.2.32 User Interface, Jun 24th 2008.
This is the most complicated but the most secure of the three applications.

All of the three applications apply to access control system based on face recognition on Windows installed on laptops of the three vendors. In general, these products can recognize the real users when they want to log in.

However, when enjoying these systems, we sensed there something wrong and started to wonder: "*Does the solutions provided by the three vendors for their customers meet the security needs of an access control system?*"

III. BYPASSING

1. Drawbacks

On suspicion of these security capabilities of the three products talked above, we have embarked on doing a research on those and quickly found weak points that can be taken advantages of. The model used to bypass user authentication based on face recognition of the threes is also discussed.

Let us present the security threat posed to Lenovo's – Asus's – Toshiba's products, based on the basis face recognition algorithms and the tests we have performed on them:

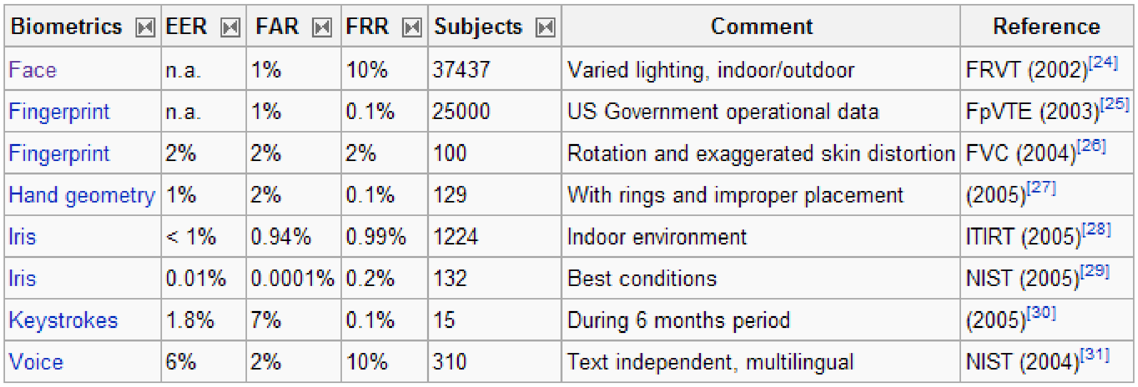
- *Face Recognition in comparison with other biometric recognition systems*
- *Influences of varied lighting*
- *Influences of image capturing devices*
- *Influences of Image Processing*

Face Recognition in comparison with other biometric recognition systems

The following table shows the state of art of some biometric systems, measured n 2005.

Here come some terms used in the table [18]:

- *FRR: False Rejection Rate (FRR).*
- *FAR: False Acceptance Rate (FAR).*



Biometrics	EER	FAR	FRR	Subjects	Comment	Reference
Face	n.a.	1%	10%	37437	Varied lighting, indoor/outdoor	FRVT (2002)[24]
Fingerprint	n.a.	1%	0.1%	25000	US Government operational data	FpVTE (2003)[25]
Fingerprint	2%	2%	2%	100	Rotation and exaggerated skin distortion	FVC (2004)[26]
Hand geometry	1%	2%	0.1%	129	With rings and improper placement	(2005)[27]
Iris	< 1%	0.94%	0.99%	1224	Indoor environment	ITIRT (2005)[28]
Iris	0.01%	0.0001%	0.2%	132	Best conditions	NIST (2005)[29]
Keystrokes	1.8%	7%	0.1%	15	During 6 months period	(2005)[30]
Voice	6%	2%	10%	310	Text independent, multilingual	NIST (2004)[31]

State of art of biometric recognition systems

When concerning recognition systems, people often care about how to minimize the FAR. As a result, in Face Recognition Vendor Test (FRVT) [24], they rated the performance by measuring False Rejection Rate (FRR) regarding a definite False Acceptance Rate, which is small and acceptable. As for the above table, when FAR is 1%, FRR comes up to 10% for face recognition.

In practice, when implementing the algorithms, they usually have to balance between FAR and FRR. This makes the efficiency of face recognition the lowest of all regarding the table. Its security is also lower than other biometric recognition system, especially compared to fingerprint scan.

Influences of varied lighting

As introduced, the basis algorithms have not worked well when there are changes in lighting. Many studies have been carried out in order to solve this problem [19][20], but no thorough solutions have appeared. In the latest performance measurement report of face recognition algorithms, the result was only good when the lighting did not change. *Does the solution proposed by the three vendors wipe those disadvantages out?*

Influences of image capturing devices

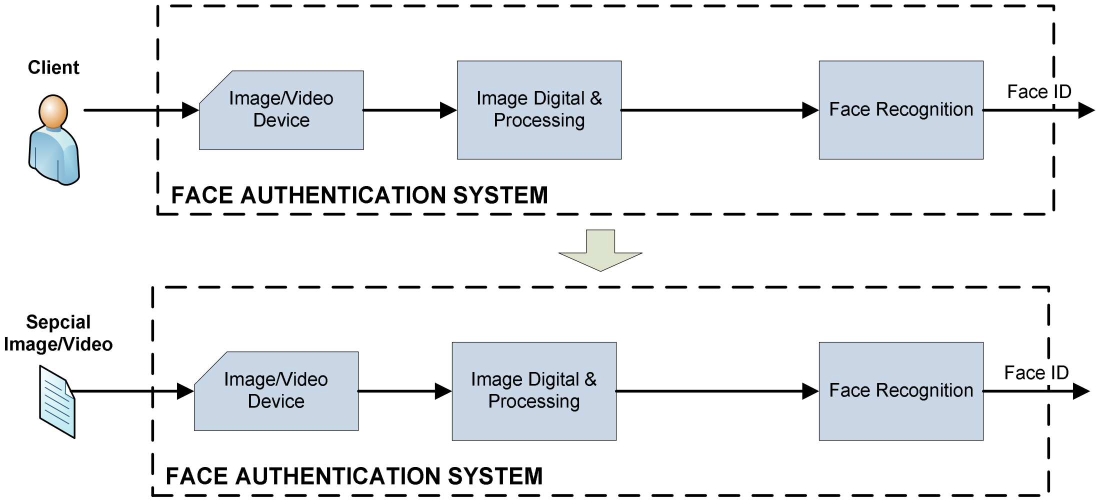
The algorithms applied to tested environments where the database in use was limited and the images had high resolutions while the majority of cameras produced by the threes have low resolution (the highest is only 1.3 Megapixel, and the lowest is 0.3 Megapixel). *Might low resolution images become flaws that can be taken advantage of?*

Influences of Image Processing

One special point we found out when studying those algorithms is that all of them work with images that have already been digitalized and gone through image processing. Consequently, we think that this is the weakest security spot in face recognition systems generally and access control system of the three vendors particularly.

2. Bypass Model

Based on the previously discussed drawbacks, we built a bypass model to test the products of the three vendors.



Bypass Model

The model exploits the flaw in image processing. In other words, it uses a photo of a person instead of his/her real face. It works because the algorithms will process in effect digital information.

Provided those conditions, an attacker might take some photos of one user within the system, perform some image editing, regenerate "***special pictures***" and penetrate into the system.

3. Fake Face

This section covers how an attacker could produce a fake face of a user and some methods used to bypass the three access control systems of the three vendors.

3.1 How to get an target's image

At the moment, it is very easy to get a photo of a person as everyone seems to have at least once taken a photo. Moreover, there are lots of ways to obtain such photos, like from the Internet or using sophisticated but popular devices. Let us give out some methods among those:

- *Webcam chat (MSN, Yahoo Messenger, AOL, Skype, ...)*
- *Searching on the Internet, especially on personal website or blog making use of Web 2.0 Technologies (Flickr, Yahoo Blog, Facebook ...).*
- *Using camera with tele-lens to get a photo of the target from long distances.*
- *Hacker asks that person to take a picture with him directly.*
- *And many other methods ...*

3.2 Fake Face Bruteforce

In fact, hacker cannot just get into the system with whichever images taken from a user because the lighting, viewpoint and even some characteristics of that person might be different from those when the system learned his/her face.

To make sure that the photo would pass the checking of the application, hacker would have to edit it to adjust the lighting and the viewpoint. Due to the fact that hacker doesn't know exactly how the face learnt by the system looks like, he has to create a large number of images (Fake Face) - let us call this method of attack *"Fake Face Bruteforce"*. It is just easy to do that with a wide range of image editing programs at the moment.

There are several things to concern about in image editing so as the BruteForce to be successful, including:

- *The image's viewpoint.*
- *Lighting effect*

4. Tests and results

Performing tests on laptops with 1.3 Megapixel camera produced by Lenovo – Asus – Toshiba, using the Bypass Model above with photos or videos of some users, we have been able to pass the User Authentication Based on Face Recognition and log into user accounts on Windows Vista without difficulty.

All the applications tested are of their latest versions and are set to Highest Security Level.

- *Lenovo Veriface III*
- *Asus SmartLogon V1.0.0005*
- *Toshiba Face Recognition 2.0.2.32*

Lenovo Veriface III

Veriface provides the easiest usage amongst the three applications for its users in which users only have to take some photos of them and the result is stored as Black and White images.

The introduction on Veriface III of Lenovo comes below [21]:

"Now that some systems include integrated cameras with much better quality (1.3MP), facial recognition has become much better. The included software lets you log onto your Windows account simply by sitting in front of your system. Your face is your password."

Veriface is in fact the least secure of the threes as we can log into the account using a plain image of the owner without much effort.

Asus SmartLogon V1.0.0005

Smart Logon uses a more complicated method of learning a user's face. Thirty images of the user, all of which are color, are saved as default. More images can be added to the database to make it more reliable.

Here comes what Asus told about their SmartLogon [22]:

"It's always more pleasant to be welcomed into an establishment where the manager knows you by sight than it is to be aggressively prodded for ID by the security guard at the door. That's the difference a notebook with ASUS SmartLogon with face recognition technology brings to the computing experience. With ASUS SmartLogon with face recognition technology, users waltz past the notebook's security functions without lifting a finger."

According to the test, it is harder to bypass SmartLogon. However, by changing the viewpoint so that the posture looks like what is used by the user when capturing his/her face, it is yet not too hard to enter into the system.

Toshiba Face Recognition 2.0.2.32

This seems to be the most complicated of the threes since users have to move their head up and down in accord with the application's requests. The results of the scan are saved in the form of color images. All of these are to ensure that the database has a wide range of viewpoint.

In addition, it is also reported in the FRVT that the algorithm proposed by Toshiba had high performance in all of the tests.

Toshiba has had some attractive words in their advertisements of Face Recognition [23]:
"Toshiba Face Recognition is the ultimate hands-free, hassle-free way to logon to your laptop. No keeping track of hard-to-remember passwords. No unnecessary typing. Just your handsome visage gazing into the built-in Webcam on your notebook and presto—you've got access! How's that for sci-fi technology?"

This application is in effect more difficult to be bypassed compared to Veriface of Lenovo and SmartLogon of Asus. However, still making use of BruteForce with a little change in the viewpoint and especially the lighting, we yet succeeded in penetrating into the system.

Result estimation

The following table shows results of the tests on the Bypass Model performing on three applications, where:

- *BruteForce: trying to bypass using a lot of face photos.*
- *No BruteForce: trying to bypass using an arbitrary photo taken from a user.*
- *High: easily being bypassed*
- *Medium: somewhat more difficult to be bypassed*
- *Low: cannot be bypassed*

	Veriface		**SmartLogon**		**Face Recognition**	
	Gray	***Color***	***Gray***	***Color***	***Gray***	***Color***

	Image	***Image***	***Image***	***Image***	***Image***	***Image***
BruteForce	High	High	-	High	-	High
No BruteForce	High	High	-	Medium	-	Low

IV. CONCLUSION

In this paper, we have introduced basic face recognition algorithms as well as their applications in authenticating users based on their faces in present access control systems. We have also pointed out weak points that might allow one to bypass into the systems of the three big computer manufacturers Lenovo – Asus – Toshiba.

The main purpose of the paper is to give sufficient evidences that the authentication technologies being used by these three manufacturers are not efficient and secure enough as they are prone to be bypassed putting users' data at serious risk.

V. REFERENCE

[1] http://en.wikipedia.org/wiki/Facial_recognition_system

[2] Titanium Group, "*Comparing face recognition against other types of biometric authentication methods*".

[3] Ching-Han CHEN,Chia -Te CHU, "*Face Authentication System for Information Security*".

[4] Anthony Ronald Grue, "*Facial Recognition: Limited Application in Safety and Security*".

[5] Stan Z. Li Anil K. Jain, "*Handbook of Face Recognition*".

[6] Keren Tan, Weiming Chen, Rong Yang, "*A PCA-based feature extraction method for face recognition*".

[7] John D. Woodward, Jr., Christopher Horn, Julius Gatune, and Aryn Thomas, "*A Look at Facial Recognition*".

[8] Sebastien Marcel and Yann Rodriguez, "*Biometric Face Authentication using Pixel-based Weak Classiers*".

[9] A. J. Goldstein, L. D. Harmon, and A. B. Lesk, "*Identification of human faces*" – 1971

[10] T. Kanade, "*Picture Processing by Computer Complex and Recognition of Human Faces*" - 1973.

[11] Matthew M. Turk and Alex P.Pentland, "*Face Recognition using EigenFaces*".

[12] Lindsay I Smith, "*A tutorial on Principal Components Analysis*".

[13] Xiaoguang Lu, "*Image Analysis for Face Recognition*".

[14] A. Hyvarinen, "*Survey on independent component analysis*",

[15] Berlin Chen, "*Discriminative Feature Extraction and Dimension Reduction*" - 2004

[16] V. Blanz and T. Vetter, "*A morphable model for the synthesis of 3D faces*".

[17] Volker Blanz, Sami Romdhani, and Thomas Vetter, "*Face identification across different poses and illuminations with a 3D morphable model*".

[18] http://en.wikipedia.org/wiki/Biometrics

[19] Y. Adini, Y. Moses, and S. Ullman, "*Face recognition: The problem of compensating for changes in illumination direction*".

[20] A. Georghiades, D. Kriegman, and P. Belhumeur, "*Illumination cones for recognition under variable lighting: faces*".

[21] http://lenovoblogs.com/insidethebox/?p=132

[22] http://promos.asus.com/US/Features/SmartLogon/index.html

[23] http://explore.toshiba.com/innovation-lab/face-recognition

[24] National Institute of Standards, "*FRVT 2006 and ICE 2006 Large-Scale Results*".