TDDC03 Project No.17, spring 2007

Comparative study of freeware/shareware/open source face recognition software

Jon Hällholm, Jia Li

Supervisor: Christoph Schuba

Comparative study of freeware/shareware/open source face recognition software

Jon Hällholm Jia Li
Linköpings universitet, Sweden
Email: {jonha931, jiali173}@student.liu.se

Abstract

Facial Recognition has been a popular biometric technique for a while and its popularity mainly has to do with that it is easy to use and that it is accepted by the public. Face recognition can be divided into two types; image-based and video-based where video is the more popular one. The lifecycle of face recognition could be divided into getting the object data, face detection, image pre-processing (extract the features) and face verification.

In this comparative study we have measured the time it takes for the software to recognize a face in different environments, this gave us an answer to which software performed the best with respect to accepting or rejecting users correctly. After comparing the two software packages to each other it is clear that FaceMetrix has the highest level of security of the two and is the best in accepting the right users. Using only face recognition as security for your computer will not be enough, you need to use some complimentary technique as e.g. passwords, smart card or another biometric technique.

1. Introduction

Facial recognition is one of the most accepted biometric techniques today, mainly because it doesn't require the test subject to assist in the process of extracting characteristic features in the face. The only thing that is required from the user is to look into a camera and that's all. This biometric technique is also widely accepted since humans recognize faces every day in their regular life, every time that we see another person we make face recognition and our algorithm is very good at it.

In this report we will compare different software in order to find the ones that can be useful as a secure biometric system. The different software will be compared with a number of both usability and performance metrics, usability metrics are the requirements of the test subjects and the environment the test is being conducted in. Performance metrics on the other hand are how well the system can perform when it comes to accepting the correct biometric input.

1.1 Problem Statement

The goal is to find and explore a number of freeware/shareware/open source face recognition software packages and evaluate them with real user input in form of real-time images from a web-camera. The different software will be evaluated with respect to their usability and performance metrics.

1.2 Methodology

For the comparison we will use two face biometric software packages that have similar features which makes them comparable according to their usability and performance metrics. Usability metrics are failure to enroll (FTE) and failure to acquire (FTA), and performance metrics are false acceptance rate (FAR) and false rejection rate (FRR). These metrics will be used to see how well the systems are performing when it comes to capturing and recognizing faces. We will use a web-camera as input to the software with different environments and conditions e.g. light conditions, facial expressions like smiling and distance from the camera to the user. The tests will be performed in the same environment and with the same equipment in order to give a fare result. The two software packages have a number of security levels which we will change in order to see if there is any difference in security and in the time it takes for the software to identify and recognize a face.

2. Face recognition

The strong need for user-friendly systems that can secure our assets and protect our privacy without losing our identity in a sea of numbers is obvious [1]. Nowadays, people need to remember lots of complex passwords to keep their own information secure, face recognitions and other biometric technologies can make things simple, your biometric feature is the password to access your private information.

Face recognition technology gets more and more attention in form of computer applications with image/video analysis and verification [1]. The applications are being used for automatically detecting a face from a digital image or a web camera, fetching the key feature values through some algorithms and comparing them

with existing valid templates in a database. It is mainly used for preventing unauthorized people getting into the system without the right permissions and to make approved users enter the system easily.

2.1 Working procedure

User enrollment should be done at first to establish the valid template database which is the face feature comparison object and would be updated continuously.

Normally, after enrollment, a face recognition system will follow the procedure to make personal face identification: Getting object data, face detection, image pre-processing (extract the features) and face verification, which can be implemented in different ways according to various designs from the manufacturers of the software. Here follows a more detailed description of the individual steps:

- **Getting object data**

The system collects the detailed information from the object. For the image-based face recognition system, this procedure consists of taking a picture of the object to get the static photo, while for the video-based system, that would be capturing images with a web-camera in order to get live data.

- **Face detection**

Many algorithms can be used to detect the face, which one being used depends on every company; all systems have one thing in common, they should detect the faces from static photos or live video. Face detection is the fatal step of the face recognition, because the data being detected here are used in every preceding step. Faces can be detected at different distances, in complex backgrounds and under other unpredictable situations.

- **Images pre-processing (Extract the features)**

Once the facial detection application has targeted a face, it can be analyzed. Facial recognition analyzes the spatial geometry of distinguishing features of the face [3]. System will use some proper algorithms to extract the feature values which are enough to make identification from the detected face. After extracting the features, the template is generated so that the system can compare it with the known templates stored in the database.

- **Face verification**

The system will compare the template it got from the previous step with the already enrolled information in the database to get a percentage of the similarity, which means how closely the generated template matches with the template stored in the database. This is done to be able to determine whether the person can be authorized to access the system, some access logs will be written at the same time.

2.2 Two face recognition types

Face recognition technology ranges from static personal photos to live webcams, posing a wide range of technical challenges and requiring an equally wide range of techniques from image processing, analysis, understanding, and pattern recognition. We can classify the face recognition algorithms according to their integration of motion information [2].

Input	Method	Use of motion
Static images	Still image-based	No
Video	Still image-based	Partially
Video	Spatio-temporal	Yes

Table 1. Face recognition types [2].

Still image-based face recognition and video-based face recognition are two kinds of face recognition systems which are widely used. Still image-based system can only extract the feature from digital photos using specific algorithm, meanwhile, the video-based system will have some extra features to catch the motions of the face and it uses video sequences as the training and test data.

2.3 Advantages and disadvantages:

Compared with other biometric systems, face recognition system can be implemented in a public area without much legal concerns, it's easily to be accepted by people and the device, the common camera, is cheap to get, user enrollment is very simple as well. All of these advantages make face recognition system an easiest system to realize and operate.

However, there are disadvantages too: the main one is that current face recognition system may not be sufficiently robust for different surrounding environments, such as the background, lights, eyeglasses, hats. It's hard to keep a high veracity in different conditions.

3. Comparison of face recognition software

The comparison has been made using a PC with Windows operating system with two different biometric face recognition software installed on it. The capturing device has been a web-camera with the resolution of 320x240 and a frame rate of 30 fps. The tests have been carried out during daytime with normal lightning conditions. Each case has been carried out three times to get a reasonable result, since two times could mean that

one was false and the other one correct and then it's hard to know which the correct one was.

3.1 The different software

The first software we have used is called FaceMetrix (will be denoted FM) from PENPOWER Technology Ltd in Taiwan and the other one is FaceCode (will be denoted FC) from the Israelian Company Recognix Technologies LTD. Both software packages are free to try with full functionality for a limited number of days, 30 for FM and 14 for FC. The purpose of these two software packages is to function as a login system for your computer, in this case a PC running the Windows operating system. The login system replaces the normal login procedure with username and password and instead accepts users according to their facial characteristics. Both of the software uses a web-camera for identification and recognition of the users face.

The enrollment in FM is done by capturing a series of two dimensional (2D) photos by the web-camera and combining these into a three dimensional (3D) model. During the enrollment phase the users being enrolled need to rotate their heads, but not more than 20 degrees horizontally and 15 degrees vertically from their heads starting positions in order to generate a good 3D model of the face. It is also important to always have the eyes visible to the camera the whole time. A facial model takes up around an average of 240KB in storage space at the first enrollment, and could use up to 460KB after processed by so called model adaptation to improve the model. A single facial feature has a size of 2KB, and number of facial features can vary and depends on if it's a detection or a recognition of the face that is being carried out [4].

Figure 1. Enrollment of a user in FaceMetrix

The FM software uses two major face modules: one is used for the detection and the other one for recognition. The detection module is built from template matching, local feature matching, and multiple resolution analysis. The recognition module on the other hand is being created via fast optical flow analysis, graphical modeling techniques, and Bayesian network (Probabilistic graphical model) determination [4].

The recognition module analyzes the waveforms across the face from top to bottom. Different faces have different complexity so the number of these waveforms can vary between 300 and 600. It is said that these varying waveforms are unique features of every person's face which makes it possible to use it as a biometric identifier [4].

FC enrolls a user by taking several pictures of the users face. To get a good result it is preferred if the user being enrolled uses different angles of the face and makes different facial expressions during the enrollment. The software scales the captured images to a standard image size and this stored image will be used in later comparisons [5].

FC measures physical characteristics and personal behavioral traits in order to detect and verify faces of users. The algorithms used in FC try to simulate the function of the human eye, and how the eye percept objects. The technique for this is pattern analysis (frequency domain field) using the Fourier transform. The images captured in the enrollment is broken down to spectrums of frequencies, after this has been done the algorithm does a correlation match between the stored images on the computer and the live images captured by the web-camera [6].

3.2 Result of the comparison

After comparing the different software it is clear that FM is the better one of them with respect to security that means a low FAR and a low FRR, which are very important for a biometric security system. A system shouldn't use too much time to accept or reject a user; there must be a balance between them. If we look at the time it took for the different software then FC is the winner. FC performs much faster but accepts almost everything as a match which is definitely a big security risk. The result from the facial expression test is that FM takes an average of 4.4, 3.5 and 18.3 seconds for low, medium and high security level respectively, while FC had <1, <1 and 2.1. The next thing we tried was to change the distance between the user and the camera, the distance was changed from 1 to 2.5 meters. Once again FC proved to be faster with an average of 1.3, 5.2 and 39 seconds, in this test FM didn't accept the user on the highest security settings at all.

With changing lightning conditions, we saw some interesting results. For normal conditions FC performed faster as usual with an average on the highest security level of 2.4 seconds while FM had 17.7 seconds. When we made the room brighter it took a bit longer for the software to recognize the face but FC was still fast with 3.7 seconds in average while FM failed one test and had

74 seconds on the other at security level high. With the room almost dark the performance didn't drop as one might had expected. Here FM actually won against FC on the medium (default) security level with 10.1 compared to 13.7 seconds, but with the highest level of security on, the performance dropped and FM didn't work at all while FC had 31,7 seconds in average time.

Next we wanted to see if the software would make any difference between a person with or without normal glasses and sunglasses. In these tests there was a great difference between the two software packages, where FM took as always longer time to recognize the face, but also rejected the user in one test with high security on. FC accepted the user wearing glasses in every time and was very fast as usual, no difference from a user without glasses. For sunglasses it didn't work at all with FM but surprisingly it worked every time with FC! One other surprise was that it accepted the user really fast as well, almost the same time as without sunglasses.

When the user was wearing a hat, FM performed okay on the low and medium security level, with 6.9 seconds for medium settings, at high on the other hand it didn't accept the user at all while FC always accepted the user without any particular problem.

We also tested how long it took for the software to enroll a user to the system. We compared a distance of one meter to 2.5 meters. For one meter they both performed just as well with 22 seconds each while at a longer distance it took 148.4 seconds for FM and only 17.4 seconds for FC! This could be compared to when we changed the distance for the recognition tests where FM failed to recognize anything and FC needed some time but recognized the face after around 30 seconds.

When it comes to the two software capabilities in FAR and FRR we could really see some differences which of course is related to the other results presented above. These trials where carried out with normal light conditions and a distance of one meter from the camera.

When we compared the face of a Swedish person and a Chinese person FM didn't accept the other face in any of the tests and any of the security levels. FC accepted all faces at low and medium level but none at the highest security level. We also compared persons with similar faces since Swedish and Chinese people have very different facial features. With similar facial features it turns out that it is relatively easy to fool the system and FM accepted 1 out of 10 on low security and two out of 10 on medium which is a bit surprising. The good thing was that it didn't accept any one on the highest security level. For FC it was just as bad as before, accepted every face on the two lower security levels but none at the highest which was a relief. The producer of the FM software lists the FAR and FRR rates on their webpage and they achieved an astonishing rate of 0.0173% for FAR and 0.0764% FRR [1]. Of course this is with best possible conditions but we still managed to come up with

		FaceMetrix			**Facecode**		
Usability & performance metrics		*Low*	*Medium*	*High*	*Low*	*Medium*	*High*
Light	*Normal*	4.2/4.5/3	5.3/3.6/3.6	8.7/13.9/30.6	<1	<1	0.9/2.6/3.7
	Bright	5.1/5.7/13.7	8.2/7.4/5.5	74.3/28.6/ failed	1.9/2.3/1.1	2.6/2.4/3.3	3.9/4.2/3.0
	Dark	5.1/4.8/5.3	8.2/8.9/13.3	failed	1.4/2.1/1.3	11.4/13.7/16/1	31.4/27.6/36.2
Facial expressions	*Smiling*	3.6/5.2/4.3	2.6/4.1/3.7	12.1/23.4/19.3	0.4/0.5/0.6	0.3/0.5/0.6	0.8/3.5/2.1
Distance	*2 meters*	11/6.8/3.4	3.8/5.5/6.7	failed	1.3/1.8/0.8	5.0/4.7/5.8	39.1/41.3/36.5
Glasses	*Normal*	5.8/2.5/4.6	4.7/8.1/12.2	failed/30.5/59.1	0.8/1.1/1.3	0.9/0.6/1.5	2.0/1.6/2.8
	Sunglasses	failed	failed	failed	0.8/1.2/0.9	1.1/1.4/1.9	3.8/3.2/4.7
Hat		4.3/5.1/4.8	6.5/5.9/8.4	failed	1.2/2.0/1.5	1.8/2.3/1.9	2.5/1.8/3.6
Enrolment	*1 meters*	22,2			21,8		
	2.5 meters	148,4			17,4		
False possitives	*Chineese compared to Swedish*	none	none	none	10 out of 10	10 out of 10	none
	Chineese compared to Chineese	1 out of 10	2 out of 10	none	10 out of 10	10 out of 10	none
False negatives		none	none	8 out of 45	none	none	none

Table 2. Test results from the comparison between the different software

a rate of 0.05% for FAR (when testing ten times with both a similar face and a very different face). It was worse for the FRR, here we weren't able to come up with such a good result as with the FAR, for FRR we got 0.24% and much of that is because of the poor performance on the highest security level.

The company behind FC doesn't list the FAR and FRR for their product but we got a FAR of 66%! A catastrophic result but they managed do perform excellent on the FRR where they had 0%! The result that is sought is a balance between the FAR and the FRR and preferable a low value for both. It is very hard to create a system that has a low value for both these properties, if the system is too accurate it will probably reject all invalid users and some of the correct users which will result in high FAR and low FRR.

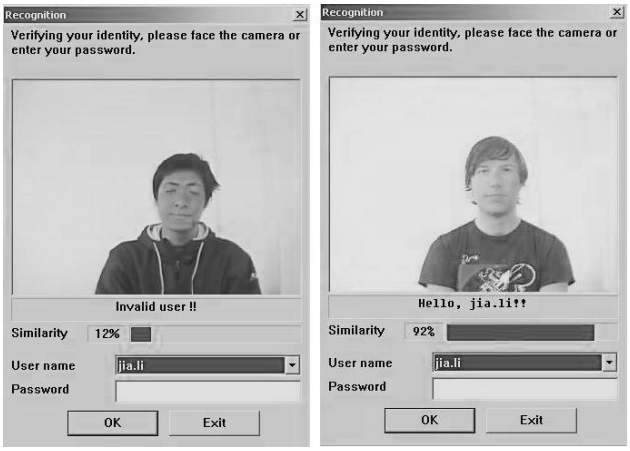

Figure 2. FaceMetrix rejecting an invalid user.

4. Discussion

We started this project with the idea that it was going to be very easy to find a number of free software or at least trial versions and demos to compare. After some searching on the web it turned out to be the opposite, after three days of constantly searching for some software in numerous places we hadn't found anything except for one real-time PC-login software. We decided after consultation with our supervisor that we should drop the idea of using digital photos and focus on the real-time face recognition instead. In the end we at least found two software packages so that we could compare them to each other.

4.1 Discussion about the result

The result from the comparison shows that you have to choose between high security and performance in time. It is obvious after our tests that the FaceCode system is not secure enough for protecting your computer from unwanted login tries. It is very fast but it's so fast that it looks like it is only concerned if there is someone in front of the camera, at least for the low and medium security levels. It could be possible though that during certain conditions not tested by us that it works perfectly fine. We have a strong feeling that it wouldn't do that though since all of our results shows that it has a too high rate of false acceptances.

The FaceMetrix system performed pretty well during low and medium security but was really performing poor when the highest security level was used, so this system had too high false rejection rate instead. This is better to have than a high FAR though, since it will keep any unauthorized persons from logging on to your system. It should be mentioned that FM has five security levels compared to FC's three, which means that you could have a much more fine grained control over the level of security for your computer. Some quick tests revealed that the next highest level in the FM software, called medium-high, worked very well where the highest didn't. But for comparison reasons we couldn't use that in any of the tests between the two software.

One very interesting observation was the total differences in accepting users wearing sunglasses, where FM rejected all attempts while FC accepted every attempt. Using a system that accepts someone wearing sunglasses doesn't feel very secure and implies that it is pretty easy to fool such a system. Also it was interesting to see that both systems performed quite badly when the user who wanted to login was some distance away from the camera, and it was not a very large distance. One has to keep in mind that these login systems are likely to have the camera at a close distance from the person it should recognize, which will increase the possibility for a correct result. The result from the tests shows though that it can't really be used in for example a passage system where you could get access to a building by a camera that recognizes the face. In an environment with probably poor lightning conditions and a larger distance, other equipment must me used.

From a usability metrics standpoint, the tests reveal that these factors had a fairly large impact on the performance of the FM system when moving from the lower security levels upwards. Also the performance metrics were affected when increasing the level of security, where the FRR was the one that increased the most, going from not rejecting any one on false grounds to rejecting a lot on security level high. For the FC system the usability metrics didn't had that big impact on the system's performance as it had in FM, instead here we saw that it was the difference in the performance metrics that really stood out after the tests. With a FAR of 66% and a FRR of 0% the FC system proved to be not that secure as the manufacturer claims on their webpage.

5. Conclusions

Face recognition is easy to implement and operate. It could be nice to add security features for a system which can make users access the system conveniently and secure. This will also make it possible for the users to choose easy passwords that they can remember. One big advantage of Biometric systems in general and face recognition systems in particular is that people don't need to have access to passwords, or ID cards, your biometric identifier is the best password. Face recognition systems have the features of easy enrollment and recognition of a user, this can help making the system more acceptable.

However, the security features that you posses will not be secure features if the face recognition system can not keep a high accuracy. This could be the effect from many surrounding factors, the administrator should consider the relationship between FAR and FRR in advance before installing the face recognition system, how high security is needed and is the system fast enough to use? It might also be possible to have other ways to give a user access to the system even if the face recognition system doesn't grant access from the facial characteristics.

It could also be important for a face recognition system to have some extra features, such as taking a photo of the object if he or she has failed to be recognized by the system after a certain number of times tried in a specified period. This could raise a silent alarm and that photo could be sent to the administrator in order to change the security level and minimize the risk of an unauthorized person getting through.

After testing the software the conclusion is that it is not very safe to only use face recognition as a biometric technology to prevent access to your computer, there are too many factors that needs to be fulfilled in order to have a safe system. Perhaps if you combine face recognition with other biometric technology like fingerprints, you would achieve a good security level, even with passwords and face recognition the amount of security would probably be much higher.

References

[1] W. Zhao, R. Chellappa, P. J. Phillips, A. Rosenfeld, Face Recognition: *A Literature Survey, ACM Computing Surveys, Vol. 35, No. 4, December 2003,* pp. 399–458.

[2] A. Hadid, M. Pietikäinen. From Still Image to Video-Based Face Recognition: An Experimental Analysis. *In Proc of the Sixth IEEE International Conference on Automatic Face and Gesture Recognition (FGR'04),* 2004.

[3] D. Woodward, Jr., Christopher Horn, Julius Gatune, Aryn Thomas. *Biometrics, A Look at Facial Recognition.* RAND. Santa Monica. 2003.

[4] Frequently Asked Questions, FaceMetrix Facial Recognition System. http://www.facemetrix.com/FaceMetrix%20FAQ.pdf. 2007-04-13

[5] Recognix Technologys LTD Biometrics. http://www.recognix.com/technology/Default.aspx?sub=biometrics. 2007-04-13

[6] Recognix FaceCode Technology. http://www.face-code.com/Technology.aspx. 2007-04-13