# Comparative Study and Evaluation of Six Face Recognition Algorithms with a View of their Application on Mobile Phones

N.Mahmoud and N.L.Clarke

Centre for Information Security and Network Research,
University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

## Abstract

Mobile phones are rapidly becoming one of the most popular and powerful tools in our lives everywhere in the world (Clarke et al, 2003). They have provided a powerful ability whilst on move and increasingly sophisticated functions. Nowadays mobile phones are allowing people to access an increased amount of data and much more such as paying for products using micro-payments, surfing the Internet, buying and selling stocks, transferring money and managing bank accounts (Dagon et al, 2004). . However, security levels provided on the mobile phones these days such as PIN numbers and passwords do not provide substantial protection. This has highlighted the need for another strong way to protect the information being held on these devices as well as the services being served. It was proposed to implement methods of controlling access to these devices namely, biometrics. Face recognition is one of biometrics techniques can be implemented on mobile phones these days as most have integrated digital cameras which can be used to capture an image and used for authenticating legitimate users. It is based on the use of underlying algorithms to implement a solution. Six such algorithms cover provide a good coverage of the techniques available today were evaluated based on two experiments, a control experiment to evaluate the normal operating performance of the algorithms and a test experiment to test the ability of the algorithms to deal with facial images with varying facial orientation. The best performed algorithm in the control experiment was Gabor filters for face recognition with 4.5% misclassification rate and the best performed algorithm in the test experiment was Fisherfaces for face recognition with 35.1% misclassification rate.

## Keywords

Face recognition, face recognition algorithms, mobile phones.

## 1 Introduction

Personal digital assistants (PDAs) and of mobile phones are portable devices and both are meeting at many points which could be easily noticed in these days; the latter including ever more features than of the former. The evolution obviously tends in the direction of multi-functional communications including a wide range of smart capabilities, such as wireless internet, image or/and video camera, GPS, task manager (i.e. organizer), etc. in addition, to wireless telephone. As a result therefore, is that an increasing number of personal (private) and potentially sensitive information being hold on such a device and/or are transferred to remote locations, which evidently asks for improving security levels. User data security and privacy have been achieved in third generation mobile phones by encrypting all communications during their transmission. In the same way, the subscriber account is protected by codes that are exchanged between the mobile phone and the network. However, none of these methods tends to protect the access to the mobile phone as a device holding sensitive information itself (Nagel et al, 2003).

Authentication of users of any security system can be achieved by using one of the three fundamental methods something the user knows (password, PINs), something the user has (tokens), and something the user is (biometric) (Furnell et al, 2000). The first two methods known as have their own weakness in contrast to other methods, the third approach of authentication does not need to be carried or to be remembered by the users; it just required them to be themselves. Such techniques are known as biometrics (Clarke et al, 2007).

Not surprisingly, the first biometric techniques that those users would be agreeable to implement is fingerprint recognition (74% of positive responses). This can be understood by the fact that fingerprint recognition is the most common biometric techniques that the majority of users already had some experience with this technique, while it is generally not the same situation with biometric face recognition. However, the availability of digital cameras in common mobile phones makes the implementation of face recognition cost-effective, since no additional sensor is required (Nagel et al, 2003).

This research aims to suggest a new approach which can be used to authenticate legitimate users to access their mobile phones. Since the image capturing is with the user holding the mobile phone including the camera, both the viewpoint and the lighting conditions are unrestricted. The algorithm which would be implemented must therefore take into account for differences in scale, different angles, and associated geometries (Nagel et al, 2003).

Face recognition is one of biometric techniques that can be used to provide the required level of security in order to protect the information being held in mobile phone these days. Hence, the opportunity is taken to evaluate six face recognition algorithms proposed by number of researches interested in face recognition technology. The aim is to find the best algorithm that can cope with varying facial orientations. Consequently, a suggestion may be made to implement one of the evaluated algorithms. The web site www.advancedsourcecode.com provided a good coverage of the available techniques available today (see the web site for more information). There algorithms evaluated were the following algorithms:

- Eigenfaces for recognition.
- Fourier-Bessel Transform for Face Recognition.
- Fourier spectra for Face Recognition.
- FisherFaces for Face Recognition.
- Gabor filters for Face Recognition.
- High Speed Face Recognition based on Discrete Cosine Transforms and Neural Networks.

## 2 Background

According to a survey performed by Clarke in 2002 on user attitudes towards mobile phone security, around 80% of the mobile phones users believe that enhancing the security level would be good to very good. Even five years later, inconvenience and low confidence in use of PIN numbers are the most commonly mentioned explanation of why subscribers are not using them (Nagel et al, 2003). With the growing of the mobile phones market, and their functionality as mentioned earlier, the need for implementing a high level of security would become very necessary in order to protect users and increase their trust in the new applications which would be introduce in the near future.

In summer 2004 Halifax General Insurance being one of UK’s leading providers of home insurance announced that Mobile phone theft doubled compared to previous year. This was an increase of mobile phone theft and consequential insurance payments by 123% in 2003 compared to 2002. In May 2006 Halifax General Insurance approximated mobile phone theft costs in the UK at around £390 million a year (HBOSplc, 2007).

However, these estimates gives figures based on the number of mobile phones stolen, but the question that should be asked is the cost is only based on the price of the mobile phone itself, what about the information being held on the mobile whether it has been used for other purposes. In other words these reports give some figures just about the number of stolen mobile phones and its price, but do not give ideas whether the information in these mobile phones have been used to fraud purposes, or even some employees of some companies keep sensitive information and recordings about their work, and so no body knows how this information would be used and what would be the consequent cost. This highlights the emergency steps needed to provide mobile phones a real protection in order to cut down the theft costs and /or minimizing the danger of using the kept sensitive information in them.

There are some solutions introduced by some companies to implement biometrics techniques such as fingerprint recognition or face recognition in order to increase the security levels of mobile phones. However, it might not be practical to authenticate the authorised user each time he/she would use the mobile phone. Moreover, the fact that the suggested technique in this research being face recognition technique, is non-intrusive and this is done by authenticating the user for example while he/she using the phone. Consequently the mobile phone would accept or reject the commands based on the face recognition system (match/ non-match).

## 3 The database used in this research

FERET database was selected to be the dataset for this research experiments. FERET database is a huge database that contains 14126 images for 1199. This database was created and collected by FERET program which started in 1993 to support algorithm development and evaluation. The final set of images consists a greyscale images 256×384 pixel size of individuals. The best point that makes FERET database one of the most important databases within the related researches to face recognition is that it consists a large number of images for each individual, most importantly some images taken within different periods of time extended to more than two year elapsed between first and most recent sittings for some individuals, so that some face features have changed. This element is important for evaluating the performance of face algorithms and its robustness of face recognition algorithms over time (Zana & Cesar-Jr, 2006; Black et al, 2002; Phillips et al, 2000).

# 4 Experimental methodology

Two experiments were designed in order to evaluate these algorithms – a control experiment and test experiment. The database which has been selected to evaluate these algorithms was FERET database. The experiments were conducted in a controlled fashion to evaluate the normal operating performance of the algorithms and a test experiment to test the ability of the algorithms to deal with facial images with varying facial orientation. Specifics relating to each experiment are as follows:

The control experiment was designed to evaluate the accuracy of these algorithms to recognise 200 users, the images used were normal frontal facial images, taken under normal lighting conditions, including different faces with different gender, different age, and different ethnic origin, which to an accepted level increased the difficulty of the recognition task.

The test experiment was designed to evaluate the accuracy of the six algorithms in order to recognise the same subjects based on variation in face orientations, however the images selected to achieve this experiment were different in the way that the images were taken in different pose angles in order to evaluate the accuracy of these algorithms to recognise those subjects' within different pose angles.

## 4.1 Test methodology for the control experiment

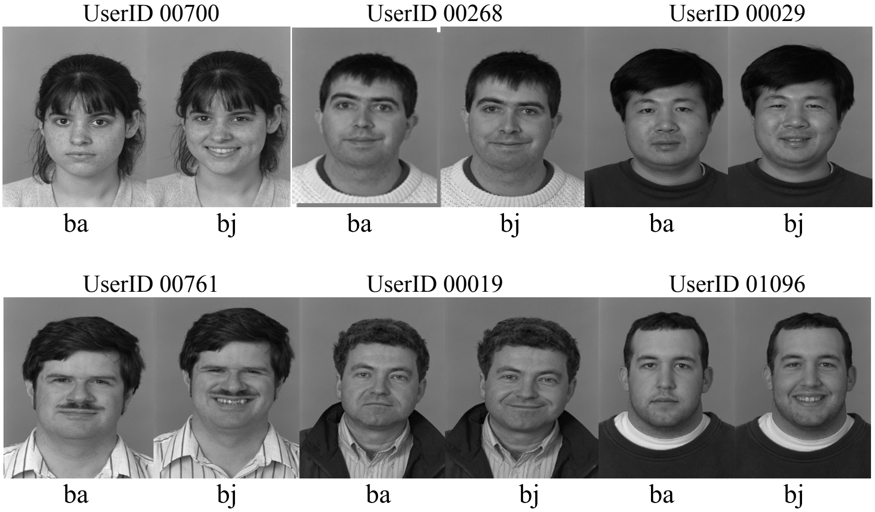

**Figure 1 . Examples of some frontal facial images (ba & bj images) from FERET database.**

The control experiment was designed to evaluate the performance of the algorithms to recognize (classify) frontal facial images. The images which would be used to achieve this goal are ba and bj subsets (normal frontal face images) of data (200 subjects), 2 images per subject, totalling 400 images. Some examples of images which would be used in the test are shown in Figure 1.

### Description of data set

The collection of images which would be used to evaluate those algorithms was taken from FERET database. Table 1 shows ba and bj images subsets, their pose angel, description, number in database, and number of subjects for each group.

| *Two letter code* | *Pose Angle (degrees)* | *Description* | *Number in Database* | *Number of Subjects* |
|---|---|---|---|---|
| ba | 0 | Frontal "b" series | 200 | 200 |
| bj | 0 | Alternative expression to ba | 200 | 200 |

**Table 1 shows ba and bj images subsets (Source: (NIST, 2007).**

### Description of the actual process

The test would evaluate the performance of facial recognition algorithms in order to recognize (classify) users' normal frontal facial images.

The evaluation process will based-on identification scenario; all users' images (authorised users) would be stored in the system's database. . After storing all users' images, the system then compares each sample image against the database, the system then either would correctly or incorrectly recognize (classify). In this phase the comparison would be 1:200 (200 here refers to the number of the images in the system's database). The actual process would take the following steps:

- In the first stage system would acquire an image for the first user (this image would be used as a template), and then the system would acquire the image of the second user. The system would continue to acquire all users' images which are here 200 images for 200 users. This process is called enrolment phase.
- After finishing the whole enrolment process for the 200 subjects, the second step would be an identification process which is based-on making the comparison for each sample image against the system's database in order to find out whether the system would correctly or incorrectly recognize (classify) an authorized user. This process would be repeated for each of the six algorithms described earlier in this section.

### Calculation of misclassified rate for the first experiment

As the total number of subjects is 200 (200 images, 1 image per subject), so the misclassification rate for the first experiment can be calculated from the following equation:

$$\text{Misclassification rate} = \frac{number\_of\_misclassified\_images}{200} \times 100$$

## 4.2 Test methodology for the test experiment

The purpose of the test experiment is to evaluate the performances of the six face recognition algorithms to recognize (classify) users' images taken at different angles. These images were taken at different angles. The images which will be used to achieve this goal are divided into two groups. The first group of images was taken where the subject was facing to his/her left (photographer's right). These includes (bb, bc, bd, be) image groups. The second group was taken where subject was facing to his/her right (photographer's left). This includes bf, bg, bh and bi image groups. Each subject has eight images (each image was taken at different angle). Some examples of images used in the second experiment are shown in figure 2.

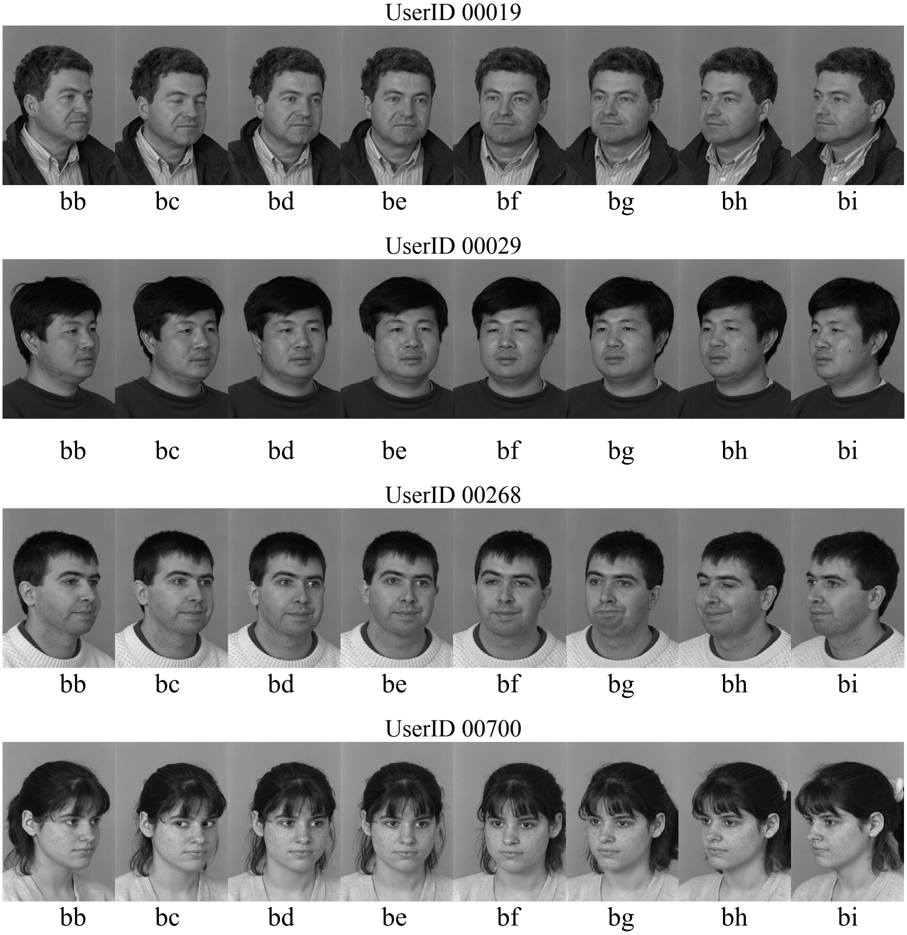

**Figure 2. Some examples of images which would be used in the second experiment taken from FERET database.**

### Description of data set

The collection of images which will be used to evaluate those algorithms was taken from FERET database. Table 2 shows the subsets of the images, their pose angle, description, number in database and number of subjects.

| *Two letter code* | *Pose Angle (degrees)* | *Description* | *Number in Database* | *Number of Subjects* |
|---|---|---|---|---|
| bb | +60 | Subject faces to his left which is the photographer's right | 200 | 200 |
| bc | +40 | | 200 | 200 |
| bd | +25 | | 200 | 200 |
| be | +15 | | 200 | 200 |
| bf | -15 | Subject faces to his right which is the photographer's left | 200 | 200 |
| bg | -25 | | 200 | 200 |
| bh | -40 | | 200 | 200 |
| bi | -60 | | 200 | 200 |

**Table 2 shows the subsets of the images (Source: (NIST, 2007).**

### Description of the actual process

The evaluation process will base on identification scenario; all users' images (authorised users) will be stored in the system's database. After storing all users' images, the system compares each sample image against the database, the system would either correctly or incorrectly recognize (classify) the user. In this phase the comparison will be 1:1600 (1600 refers to the number of the images in the system's database). The actual process would take the following steps:

- In the first stage system would acquire eight images for the first user (bb, bc, bd, be, bf, bg, bh, bi) these images will be used as a templates and then the system would acquire the images of the second user. The system will continue to acquire all users' images (1600 images for 200 users).
- After finishing the whole enrolment process for the 200 subjects, the second step will be an identification process which is based on making the comparison for each sample image against the system's database in order to find out whether the system will correctly or incorrectly recognize (classify) an authorized user. This process would be repeated for each of the six algorithms.

### Calculation of misclassified rate for the second experiment

As the total number of the users is 200 and each user has eight images within the system database so the total number of images is 1600. The misclassification rate in this case can be calculated from the following equation:

$$\text{Misclassification rate} = \frac{number\_of\_misclassified\_images}{1600} \times 100$$

# 5 Results

We performed two experiments and presented the results within this section. The control experiment was performed with 400 frontal facial images grouped into ba and bj groups, for 200 subjects (each subject has two frontal images). 200 images were used as templates (i.e. a database was created of the system by using one of the two frontal image for each subject), then the other image was used as a sample which basically would be used to authenticate the subject. The test experiment was performed with the same 200 subjects; however, 8 images were used for each subject which grouped into two groups. The first group of images was taken where the subject was facing to his/her left (photographer's right). These include (bb, bc, bd, be) image groups. The second group was taken where subject was facing to his/her right (photographer's left). This includes bf, bg, bh and bi image groups. There was no special standard for selecting these groups of images. So, the face images used in our experiments are much diversified, for example there are faces with different gender, different age, different ethnic origin, which to an accepted level increases the difficulty of the recognition task.

Table 3 and table 4 illustrate the final results of the control experiment and the test experiment. The output of the first experiment was the misclassification rate for each algorithm.

| **Algorithm** | **Misclassification rate** |
|---|---|
| Eigenfaces for recognition | **38.5%** |
| Fourier-Bessel Transform for Face Recognition | **31.5%** |
| Fourier spectra for Face Recognition | **24.5%** |
| FisherFaces for Face Recognition | **21%** |
| Gabor filters for Face Recognition | **4.5%** |
| High Speed Face Recognition based on Discrete Cosine Transforms and Neural Networks | **96.5%** |

**Table 3 illustrates the results of the control experiment**

| **Algorithm** | **Misclassification rate** |
|---|---|
| Eigenfaces for recognition | **52%** |
| Fourier-Bessel Transform for Face Recognition | **55.4375%** |
| Fourier spectra for Face Recognition | **41.75%** |
| FisherFaces for Face Recognition | **35.0625%** |
| Gabor filters for Face Recognition | **51.125%** |
| High Speed Face Recognition based on Discrete Cosine Transforms and Neural Networks | **97.125%** |

**Table 4 illustrates the results of the second experiment**

# 6 Comparison of the experimental results

Turk and Pentland presented results of evaluating *eigenfaces algorithm* based on a database of 16 subjects with different head orientation, scaling and lighting as well. For different illumination their system achieved 96% correct classification, for different head orientation their system achieved 85%, and for different scale their system achieved 64% correct classification. Lawrence et al (1997) reported in his research paper that Pentland et al (1993; 1994) had methodologically found good results being attributable to a large database, 95% correct recognition of 200 subjects from a database of 3000. Also, it is hard to draw clear conclusion as many of the images of the same subjects may look very similar, and the database has accurate registration and position (Lawrence et al, 1997). However, in the control experiment eigenfaces algorithm resulted in 38.5% misclassification rate (i.e. 61.5 % correct classification rate) based on 400 images where 200 images used as templates and 200 images used for samples, there is enough differences between the 200 subjects and this might make it hard for the algorithm to achieve the same results as Turk and Pentland reported. Moreover, these images where taken in the same lighting conditions with only difference that the subject in the second image had a little facial smile. In the test experiment eigenfaces algorithm resulted in 52% misclassification rate (i.e. 48% correct classification). This is expected as in the second experiment the number of images used was 1600 images for the 200 subjects (eight images for each subject) taken at different angles, so this fact would increase the difficulty for the algorithm to recognise subject (i.e. classify the images correctly). In brief eigenfaces algorithm appears as fast simple and practical algorithm. "However, it may be limited because optimal performance requires a high degree of correlation between the pixel intensities of training and set images. "This limitation has been addressed by using extensive pre-processing to normalise the images" (Lawrence et al, 1997).

*Fourier-Bessel Transform for Face Recognition algorithm* in the control experiment resulted in 31.5% misclassification rate (i.e. 68.5 % correct classification rate). This algorithm was proposed by Zana and Cesar-jr 2006. They tested this algorithm on two types of databases namely FERET and ORL databases, whereas they used the largest probe set within FERET database which called "fb" in FERET terminology, this probe set consisting of a single image for 1195 subjects, a modification has been applied to this probe set (for more details see Zan and Cesar-jr 2006). Zana and Ceasr-jr reported that FBT algorithm resulted in 3.8% misclassification error rate with five images per subject taken from ORL database (they did not mention to the description of the images they used in their experiment from the ORL database).

However in the test experiment the FBT resulted in 55.4375% misclassification error rate. As 1600 images were used for 200 within different pose angles taken from FERET database. It is hard to compare our results that Zana ans Cesar-jr reported because they only used normal frontal facial images. The results from our control experiment and from Zana and Cesar-jr 2006 experiment (which was based on using 1195 normal frontal facial images from FERET database) indicates that the FTB perhaps can perform much better when it is evaluated in recognising normal frontal facial images. However in the test experiment indicates that the FTB would not perform a good recognition when evaluated within images taken in different pose angles.

The third algorithm evaluated within this research was *Fourier spectra for Face Recognition algorithm* introduced by Spies and Ricketts 2000. The control experiment resulted in 24.5% (i.e. correct classification rate is 75.5%) performance for this algorithm. Within the test experiment the algorithm performed 41.75% (i.e. 58.25% correct classification rate) as misclassification error rate. However, Spies and Ricketts 2000 reported highly different results; they reported a 98% correct recognition (classification). Spies and Ricketts have used the ORL database to evaluate this algorithm (the 400 images of the ORL database were used). Spies and Ricketts have modified the resolution of the images in order to speed up the algorithm (for details see Spies and Ricketts 2000). Whereas, in our both experiments no modification have been applied to the used images. Within this case no comparison can be made according to the differences of the images and the size of the database used and the modifications applied to the database.

The forth evaluated algorithm was *FisherFaces for Face Recognition*. Belhumeur et al 1997 introduced this algorithm which was evaluated in this research. Belhumeur et al evaluated this algorithm by three experiments (the three experiments were carried out to evaluate other different algorithms (see Belhumeur et al 1997 for more details); each experiment was based on different scenario due to the type of the database and the number of images as well as the number of subjects. The first experiment was designed to test the hypothesis under variable illumination. The images used in this experiment were constructed by Hallinan at the Harvard Robotics Laboratory. The number of images was 330 images of five subjects (each subject has 66 images). Belhumeur et al extracted five subsets to quantify the effects of varying lighting (see Belhumeur et al 1997 for more details about the five subsets). For this experiment, classification was performed by using a nearest neighbour classifier. According to Belhumeur et al the results of this experiment was that this algorithm performs perfectly when lighting is nearly frontal (within subset 1 there was no error as well as within subset 2, the error rate within the subset 3 was 4.6% with a reduced space by 4). This algorithm had error rate lower than the Eignfaces algorithm based on the same database and the same scenario.

The second experiment related to this algorithm was based on different scenario where the database differs along with the number of subjects. The scenario of this experiment was to evaluate the performance of this algorithm within variation in facial expression, eye wear and lighting. The database used in this experiment contains 16 subjects (subjects include females and males (with some facial hair) and some wore glasses. In this test the error rate was determined by the “leaving one-out” strategy. Recognition was performed by nearest neighbour classifier. The fisherfaces algorithm gave excellent result (within the close crop the algorithm performed 7.3% error rate and within the images of full face performed 0.6% error rate).

The third experiment was carried out to evaluate the performance of the algorithm in recognising subject wearing glasses. The database contains 36 images forming the primary set of the Yale database, half with glasses. The result of this experiment was that this algorithm performed at 5.3% error rate with reduced space by 1. According to Belhumeur et al 1997, fisherfaces methods can be viewed as obtaining a template which is appropriate for finding glasses and ignoring other traits of the face.

This research evaluated this algorithm in entirely different scenario where the database is bigger than the databases used in Belhumeur et al 1997, the number of subjects as well as the number of images per subject. The most important difference that both experiment carried out in this research was that there were no subjects with glasses and there were no images with different lighting. In brief, in the control experiment this algorithm performed 21% misclassification error rate (i.e. 79% correct classification rate), and with the test experiment performed 35.0625% misclassification error rate (i.e. 64.9375 correct classification rate). Clearly, this algorithm can work better in scenario of recognising frontal facial images, but it does not work better in the scenario of recognising frontal facial images in different pose angles.

The fifth algorithm evaluated was *Gabor filters algorithm for Face Recognition*. This algorithm was introduced by Hjelmås 2000. The evaluation of the algorithm was on the ORL database. Moreover, Hjelmås 2000 used two strategies within this experiment. Within the first strategy the algorithm was evaluated considering a single best matching feature vector being used (in pervious works by same author examination was focused in respect of face recognition provided the only available information were for example the eyes), the result (according to Hjelmås 2000) of this strategy was not satisfactory (only 76.5% for rank 1), the result here being reported in terms of cumulative match score. This result was expected as only very small amount of information from image was used. In this situation the classification is based only on the match of a single automatically extracted feature vector in the image to a stored one in the gallery. In the second strategy, the all sited feature locations were used to recognise the face. Within the second strategy the result was 83.4% which is better than the first strategy but not as good as expected (Hjelmås, 2000). However, within the control experiment the algorithm performed the highest with respect to the other five algorithms, i.e. only 4.5% misclassification error rate resulted (i.e. the correct classification rate is 95.5%). Within the test experiment it performed at 51.125% misclassification rate (i.e. 48.875% correct classification rate). Although this algorithm gave an excellent result within the control experiment, it is not possible to make logical comparison for several reasons. Firstly the database was different as the database used was the ORL database and secondly the methodology was also entirely different, within this experiment, 10 images per subject were used (divided into two groups five images each group, one for training and the second for testing) and the images within each group were selected randomly. Whereas, in the control experiment the images used were normal frontal facial images. In brief, this algorithm gave the best result (4.5% misclassification rate) within the control experiment.

The last evaluated algorithm within this research was *High Speed Face Recognition based on Discrete Cosine Transforms and Neural Networks algorithm* which was introduced by Pan and Bolouri 1999. Pan and Bolouri used the ORL database in order to evaluate this algorithm. The scenario was that the ORL database divided into two groups one for training purpose (the first five images for each subject were chosen for this group) and the rest for testing purpose (the last five images for each subject). As a result 200 images were used for training, 200 images for testing, and no overlap exists between the training and the test images. The experiment that carried out in their research paper based on reducing the unwanted information within the face recognition system, since (according to them) the high unwanted information within the face image the less efficiency of recognition when such image is used directly for recognition. Pan and Bolouri 1999 reported a best average recognition rate at 92.87% (see Pan and Bolouri 1999 for more details).

However, within both of the experiments carried out in this research, unsatisfactory results were obtained. In the control experiment the misclassification rate was 96.5% (i.e. correct classification rate was only 3.5%). This is a surprising result comparing it to the result that Pan and Bolouri 1999 obtained (92.87%). Although the database is different as well as the number of subjects, however, there should be a reasonable difference between the two results. The same result was obtained within the test experiment where the misclassification was at 97.125% (i.e. 2.875% correct classification rate).

At last, it is possible to learn several facts the evidently can have impact on the evaluation process of face recognition algorithms. The two experiments carried out within this research have evidenced several facts as following:

- Evaluating the same algorithms based on different type of database would give different results pointing out the best available option.
- Different number of images used to evaluate the same algorithm in different scenarios would lead to different results.
- Evaluating the same algorithm based on different image conditions (variations in illumination, orientation, ethnic origin, age, and gender) would result in different performance level for the same algorithm.
- Finally, the scenario of the evaluation process would have an impact on the performance of the algorithm as well.

# 7 Conclusions

Mobile phones are one of the ubiquitous tools used nowadays, and have become quite powerful. Now mobile phones are not just providing the traditional meaning of communication (making call or using text messages), but are also being used to surf the most unsecured world “the internet”. Since the implementations of two cameras (back and front cameras) in some common types of mobile phones, the chance of implementing face recognition biometric system in order to control the access to the mobile phone is highly possible. Classical security technique that is being used based on some thing the user knows (i.e. a password or PIN) and does not provide the recommended (needed) security level needed to protect the information being held on mobile phones these days.

This research found out (based on the control experiment and the test experiment) that, Gabor filters for face recognition algorithm is the best algorithm amongst the evaluated algorithms in recognising the frontal facial images with 4.5% misclassification rate and Fisherfaces for face recognition algorithm is the best algorithm amongst the evaluated algorithms in recognising users with different facial orientations. It could be said that the result was not satisfactory and improvements should be applied to this algorithm in order to meet the accepted level of error.

# 8 References

Belhumeur, P.N., Hespanha, J.P. and Kriegman, D.J., (1997). “Eigenfaces vs. Fisherfaces: recognition using class specific linear projection”. IEEE Transactions on Pattern Analysis and Machine Intelligence. Volume 19, Issue 7, July 1997. pp711 – 720

Black, J. A., Gargesha, M., Kahol, K., Kuchi, P., and Panchanathan, S. (2002). “Framework for performance evaluation of face recognition algorithms”. Proceedings of SPIE, Volume 4862, Internet Multimedia Management Systems III, 2002, pp. 163-174. Retrieved on 12th of August 2007 from http://cubic.asu.edu/people/students/publications/ITCOM_2002.pdf

Clarke, N.L, Furnell, S.M., Lines, B. M. and Reynolds, P.L. (2003).“Keystroke dynamics on a mobile handset: a feasibility study”. Information Management & Computer Security. Volume, 11 Issue, 4, pp161-166

Clarke, N. L. and Furnell. (2007). “Advanced user authentication for mobile devices”. Computer & Security. Volume 26, Issue 2, 2007, pp109-119

Dagon, D., Martin, T., and Starner, T. (2004). “Mobile phones as computing devices: the viruses are coming!”. IEEE Pervasive Computing, Volume 3, Issue 4. pp11- 15.

Furnell, S. M., Dowland, P. S., Illingworth, H. M., and Reynolds, P.L. (2000). “Authentication and Supervision: A Survey of User Attitudes”. Computer & Security.Vol. 19, No. 6. pp529-539

HBOSplc. (2007). “Halifax press release: Mobile phone theft doubles as Halifax General Insurance warns of summer crime wave”. Retrieved on 15th of December 2007 from http://www.hbosplc.com/media/pressreleases/articles/halifax/2004-04-17-00.asp?fs=/media/press_releases.asp

HBOSplc. (2007). “Halifax press release: Mobile phone theft costs UK £390 million a year”. Retrieved on 15th of December 2007 from http://www.hbosplc.com/media/pressreleases/articles/halifax/2006-05-16-01.asp?section=Halifax

Hjelmås, E. (2000). “Biometric Systems: A Face Recognition Approach”. Retrieved on 30th July 2007 from http://www.nik.no/2000/Erik.Hjelmaas.pdf

Lawrence, S., Giles, C.L., Tsoi, Ah. C. and Back, A.D. (1997). “Face recognition: a convolutional neural-network approach”. IEEE Transactions on Neural Networks. Volume 8, Issue 1. Jan. 1997. pp98 – 113

Nagel, J.-L., Stadelmann, P., Ansorge, M. and Pellandini, F. (2003). “Comparison of feature extraction techniques for face verification using elastic graph matching on low-power mobile devices”. Computer as a Tool. The IEEE Region 8, EUROCON 2003. Volume 2, Issue , 22-24 Sept. 2003.pp365-369

Pan, Z. and Bolouri, H. (1999). "High Speed Face Recognition Based on Discrete Cosine Transforms and Neural Networks". Retrieved on 12th August 2007 from http://citeseer.ist.psu.edu/cache/papers/cs/13206/http:zSzzSzstrc.herts.ac.ukzSzNSGwebzSzPanzSzpaperszSzdct.pdf/pan99high.pdf

Pentland, A., Starner, T., Etcoff, N., Masoiu, A., Oliyide, O., and Turk, M. (1993). “Experiments with eigenfaces. In Looking at People Workshop, International Joint Conference on Artificial Intelligence 1993, Chamberry, France, 1993.

Pentland, A., Moghaddam, B., and Starner, T. (1994). “View-based and modular eigenspaces for face recognition”. IEEE Computer Society Conference on Computer Vision and Pattern Recognition. Volume , Issue , 21-23 Jun 1994.pp84-91

Phillips, P.J., Moon, H., Rizvi, S.A., and Rauss, P.J. (2000). “The FERET evaluation methodology for face-recognition algorithms”**.** IEEE Transactions on Pattern Analysis and Machine Intelligence. Volume 22, Issue 10, Oct. 2000 .pp 1090- 1104

National Institute of Standards and Technology (NIST). (2007). “FRVT 2006 and ICE 2006: Large-Scale Results”. NISTIR 7408. Retrieved on 12th August 2007 from http://www.frvt.org/FRVT2006/docs/FRVT2006andICE2006LargeScaleReport.pdf

Spies, H., and Ricketts, I. (2000). “Face Recognition in Fourier Space”. Retrieved on 2nd of August 2007 from http://citeseer.ist.psu.edu/cache/papers/cs/22946/http:zSzzSzklimt.iwr. uniheidelberg.dezSz~hspieszSz.zSzpdfzSzSpies_VI2000.pdf/face-recognition-in-fourier.pdf

Rosa, L. (2007). “Face Recognition System”. Retrieved on 25th September 2007 from http://www.advancedsourcecode.com/

Zana, Y. and Cesar-JR, R.M., (2006). “Face Recognition Based on Polar Frequency Features”. ACM Transactions on applied perception (TAP). Volume 3, No.1, January 2006, pp62-82. retrieved on 12th of August 2007 from http://arxiv.org/ftp/cs/papers/0509/0509082.p**df**