VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELGAUM

S.D.M COLLEGE OF ENGINEERING AND TECHNOLOGY, DHARWAD

A seminar report on

ATM USING FRS

Submitted by

SHRUTI ANANT SIDDESHWAR

2SD06CS103

8th semester

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

2009-10

VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELGAUM

S.D.M COLLEGE OF ENGINEERING AND TECHNOLOGY, DHARWAD

DEPARTMENT OF COMPUTER SCIENCE AND

ENGINEERING

CERTIFICATE

This is to Certify that the seminar work entitled "ATM USING FRS" is a bonafide work presented by SHRUTI ANANT SIDDESHWAR bearing USN 2SD06CS103 in a partial fulfillment for the award of degree of Bachelor of Engineering in Computer Science and Engineering of the Visvesvaraya Technological University, Belgaum during the year 2009-10. The seminar report has been approved as it satisfies the academic requirements with respect to seminar work presented for the Bachelor of Engineering Degree.

………………… ………………

Staff in charge H.O.DCSE

ABSTRACT

With the advent of ATM, though banking became a lot easier, it also became vulnerable. There have been innumerable cases of misuse and fraud that have taken place in banking transactions. Thus there is an urgent need to provide high security. This seminar proposes the integration of Face Recognition System in the identity verification process employed in ATMs to enhance the security system.

Contents:

1.INTRODUCTION

The rise of technology brought into force many types of equipment that aim at more customer satisfaction. ATM is one such machine which made money transactions easy for customers. But along with its advantages came the disadvantages too. Current ATMs employ nothing more than an access card and PIN for identity verification. This has lead to a lot of fraudulent attempts and misuse through card theft, PIN theft, stealing and hacking of customer's account information and other breaches of security.

First let us know about Face Recognition systems (FRS)

What are Face Recognition Systems?

Face Recognition Systems is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source. One of the ways to do this is by comparing selected facial features from the image and a facial database.

When did they develop?

The pioneers of Automated Face Recognition include Woody Bledsoe, Helen Chan Wolf and Charles Bisson. During 1964 and 1965, Bledsoe, along with Helen Chan and Charles Bisson, worked on using the computer to recognize human faces. He was proud of his work, but because the funding was provided by an unnamed intelligence agency that did not allow much publicity, little of the work was published. Given a large database of images and a photograph, the problem was to select from the database a small set of records such that one of the image records matched the photograph. The success of the method could be measured in terms of the ratio of the answer list to the number of records in the database. However the recognition problem was made difficult by the great variability in head rotation and tilt, lighting intensity and angle, facial expression, aging, etc. In 1966, this work was continued primarily by Peter Hart. In his experiments performed on a database of over 2000 photographs, the computer consistently outperformed humans when presented with the same recognition tasks. The development stage for facial recognition started in the late 1980s and they were commercially available systems were made available in the 1990s. While many people first heard about facial recognition after September 11th, 2001, football fans were introduced to it at the 2004 Super Bowl.

2. How do they work?

A database of people's faces is maintained by the system that handles face recognition. Whenever a face needs to be identified, a photograph of the person's face is taken and compared to the faces present in the database to see if a match is found.

There are usually 3 parts to a face recognition system –

1,face detector,

2.eye localiser and

3.face recogniser.

1.The face detector:

The face detector detects the face, eliminating any other detail, not related to the face (like the background). It identifies the facial region, leaving out the non-facial region in the photograph of the person to be identified.

2.The eye-localiser :

It finds the location of the eyes, so that the position of the face can be identified better.

3 .The recogniser :

It then checks the database to find a match.

3.ALGORITHMS USED IN FACE RECOGNITION SYSTEMS

Some facial recognition algorithms identify faces by extracting landmarks, or features, from an image of the subject's face. For example, an algorithm may analyze the relative position, size, and/or shape of the eyes, nose, cheekbones, and jaw. These features are then used to search for other images with matching features. Other algorithms normalize a gallery of face images and then compress the face data, only saving the data in the image that is useful for face detection. A probe image is then compared with the face data.

Face Recognition Systems algorithms can be divided into two main approaches namely geometric based and image-template based.

i] *The geometric basedmethod:* It relies on the shape and position of the facial features. It analyzes each of the facial features, also known as nodal points, independently; it then generates a full picture of a face. The most commonly used nodal points are: distance between the eyes, width of the nose, cheekbones, jaw line, chin, and depth of the eye sockets.

Although there are about 80 nodal points on the face, most software measures have only around a quarter of them. The points picked by the software to measure have to be able to uniquely differentiate between people.

ii] *The image or photometric-based methods*: It create a template of the features and use that template to identify faces. Neural networks are often used to create the templates.

A study was conducted of leading recognition algorithms, notably one developed by two researchers at MIT, and one a commercial product from Identix called FaceIt. The MIT program is based on Principal Feature Analysis, an adaptation of template based recognition. FaceIt's approach uses geometry-based local feature analysis. Both algorithms have to be initialized by providing the locations of the eyes in the database image, from which they can create an internal representation of the normalized face. It is this representation to which future live images will be compared.

In the study, it was found that both programs handled changes in illumination well.

Another paper shows more advantages in using local feature analysis systems. For internal representations of faces, LFA stores them topographically; that is, it maintains feature relationships explicitly. Template based systems, such as PFA, do not. The advantages of LFA are that analysis can be done on varying levels of object grouping, and a system can examine just the eyes, or the eyes nose and mouth, or ears, nose, mouth and eyebrows, and so on, and that as better analysis algorithms are developed, they can fit within the data framework provided by LFA.

4.TECHNIQUES AND METHODS

There are three types of techniques employed. They are

i] 2-D,
ii] 3-D
iii] Surface Texture Analysis.

2-D Technique:

The 2-D recognition technique was one of the earliest techniques used. It maintained details of people's faces as seen 2 dimensionally. Details like width of the eye, width of the nose, jaw line, distance between the eyes, cheek bone shape and the like were used for comparison. This kind of face recognition was not very accurate. Difference in ambient lighting or a face

that is not directly looking into the camera, or a change in facial expression did not produce expected results.

3-D Technique:

Advancement in face recognition gave birth to the 3-D recognition technique. This stepped up technique, used features like contours of the eye sockets, nose, chin, peaks and valleys on the face for identification. The database stores such details of faces as well. The advantage of 3-D over 2-D method is that 3-D face detection works well even if the face is turned at 90 degree to the camera. Also, it is independent of lighting environment and facial expressions.

Surface Texture Analysis:

A more advanced method is Surface Texture Analysis (STA). This technique does not scan the entire face but a patch of skin on it. This patch is divided into blocks. The skin texture, the pores on the skin and other such characteristics are converted to a code, which is used for comparison.

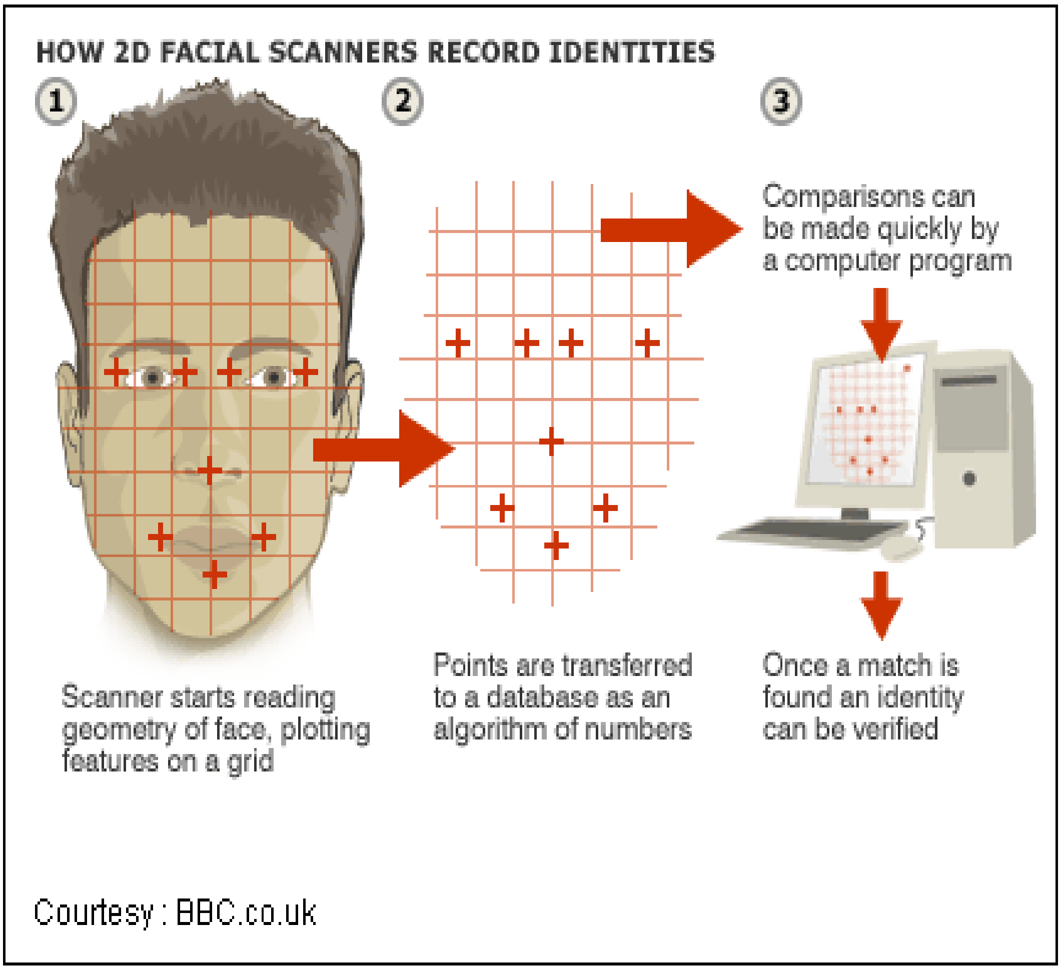
HOW 2D FACIAL SCANNERS RECORD IDENTITIES
1
2
3
Scanner starts reading geometry of face, plotting features on a grid
Points are transferred to a database as an algorithm of numbers
Comparisons can be made quickly by a computer program
Once a match is found an identity can be verified
Courtesy : BBC.co.uk

Fig 4.1

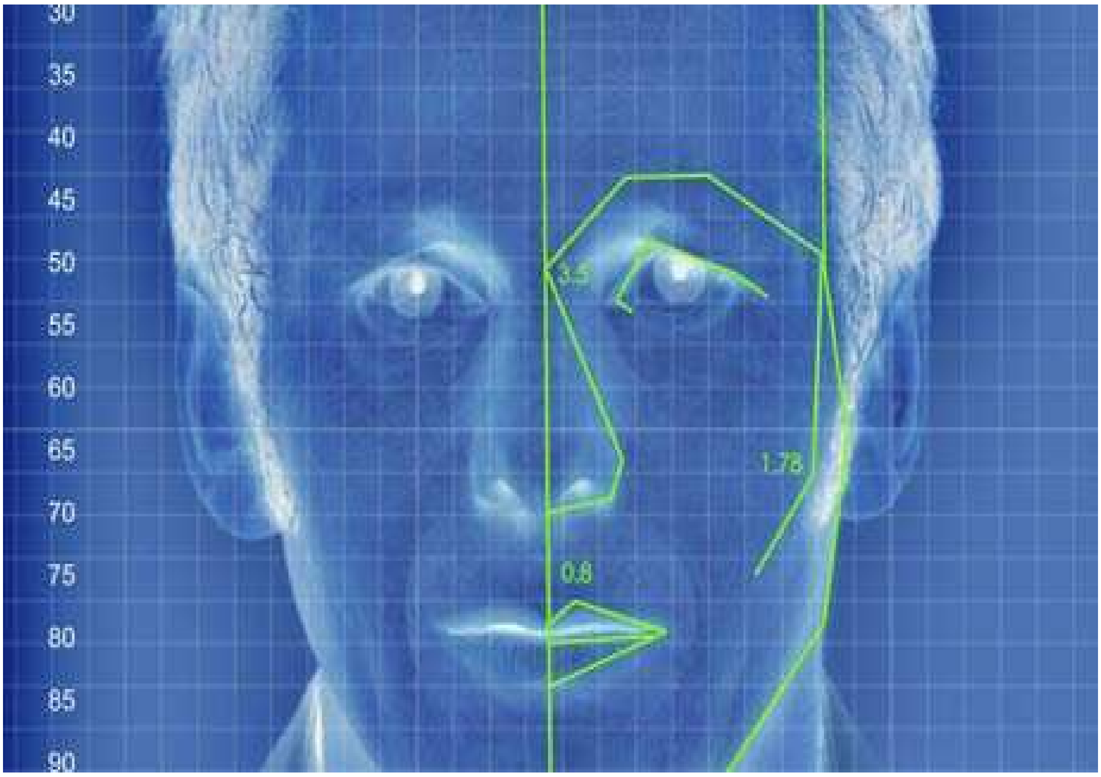

Fig 4.2 A 3-D IMAGE

5.ATMs

For most of the past ten years, the majority of ATMs used worldwide ran under IBM's now-defunct OS/2. Movement in the banking world is now going in two directions: Windows and Linux. NCR, a leading world-wide ATM manufacturer, recently announced an agreement to use Windows XP Embedded in its next generation of personalized ATMs.

For less powerful ATMs, KAL, a software development company based in Scotland, provides Kalignite CE, which is a modification of the Windows CE platform. This allows developers that target older machines to more easily develop complex user-interaction systems. Many financial institutions are relying on a third choice, Windows NT, because of its stability and maturity as a platform.

On an alternative front, the largest bank in the south of Brazil, Banrisul, has installed a custom version of Linux in its set of two thousand ATMs, replacing legacy MS-DOS systems. The ATMs send database requests to bank servers which do the bulk of transaction processing.

6.HOW FRS WORK IN ATMs AND WHAT IS NEEDED TO REALIZE IT

Face Recognition Systems (FRS) work in ATMs in the following way

1) Initially the customer's picture is taken when the account is opened and the user is allowed to set non-verified transaction limits.
2) At ATM, access card and PIN are used to pre-verify user.
3) User's picture is taken and an attempt is made to match it to the database image.
4) If the match becomes successful, allow transaction.
5) If the match is unsuccessful, limit the available transactions.

When a match is made with the PIN but not the images, the bank could limit the transactions in a manner agreed upon by the customer when the account was opened, and could store the image of the user for later examination by bank official.

In the case of credit card use at ATMs, such a verification system would not currently be feasible without creating an overhaul for the entire credit card issuing industry.

Now let us consider what is needed to realise it

The first and most important step of this project will be to locate a powerful open-source facial recognition program that uses local feature analysis and that is targeted at facial verification. This program should be compilable on multiple systems, including Linux and Windows variants, and should be customizable to the extent of allowing for variations in processing power of the machines onto which it would be deployed.

We will then need to familiarize ourselves with the internal workings of the program so that we can learn its strengths and limitations. Simple testing of this program will also need to occur so that we could evaluate its effectiveness. Several sample images will be taken of several individuals to be used as test cases – one each for "account" images, and several each for “live” images, each of which would vary pose, lighting conditions, and expressions.

Once a final program is chosen, we will develop a simple ATM black box program. This program will serve as the theoretical ATM with which the facial recognition software will interact. It will take in a name and password, and then look in a folder for an image that is associated with that name. It will then take in an image from a separate folder of “live” images and use the facial recognition program to generate a match level between the two. Finally it will use the match level to decide whether or not to allow “access”, at which point it will terminate. All of this will be necessary, of course, because we will not have access to an actual ATM or its software.

Both pieces of software will be compiled and run on a Windows XP and a Linux system. Once they are both functioning properly, they will be tweaked as much as possible to increase performance (decreasing the time spent matching) and to decrease memory footprint.

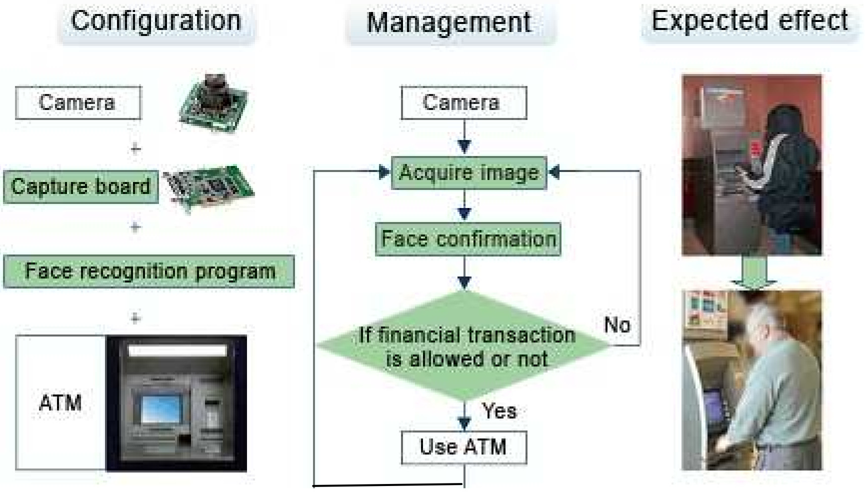

Fig 6.1

Following that, the black boxes will be broken into two components – a server and a client – to be used in a two-machine network. The client code will act as a user interface, passing all input data to the server code, which will handle the calls to the facial recognition software, further reducing the memory footprint and processor load required on the client end. In this sense, the thin client architecture of many ATMs will be emulated.

We will then investigate the process of using the black box program to control a USB camera attached to the computer to avoid the use of the folder of “live” images. Lastly, it may be possible to add some sort of DES encryption to the client end to encrypt the input data and decrypt the output data from the server – knowing that this will increase the processor load, but better allowing us to gauge the time it takes to process.

7.KEY FACTORS TO BE CONSIDERED AND OTHER CONCERNS

There are certain factors that affect verification process that have to be considered. They are

1. Lighting
2. Angle of view
3. Extreme facial expressions
4. Glasses
5. Facial hair

Other concerns are keeping the time elapsed in the verification process to a negligible amount, allowing for an appropriate level of variation in a customer's face when compared to the database image, and that credit cards which can be used at ATMs to withdraw funds are generally issued by institutions that do not have in-person contact with the customer, and hence no opportunity to acquire a photo.

The last consideration is that consumers may be wary of the privacy concerns raised by maintaining images of customers in a bank database, encrypted or otherwise, due to possible hacking attempts or employee misuse.

8.CAN ALL ATMs SUPPORT FRS ?

Most current generation ATMs run Windows CE, 2000, XP Embedded, or Linux – these machines can run facial recognition software locally

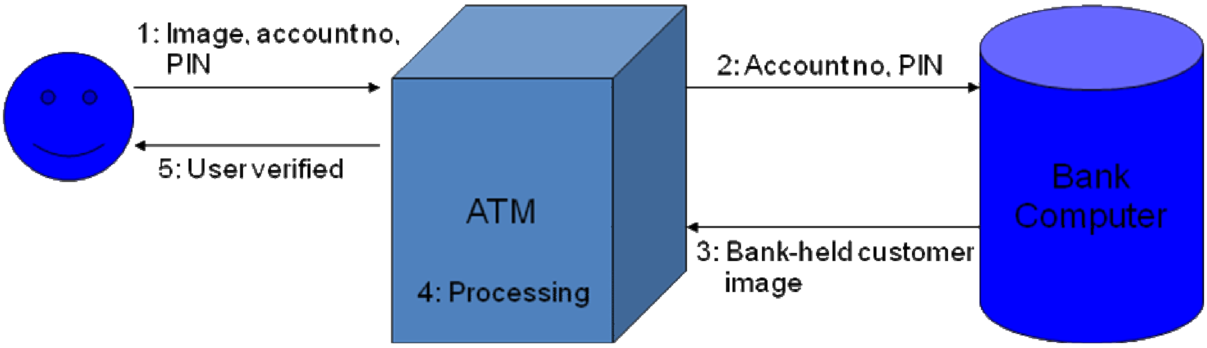

Fig 8.1

Older ATMs run DOS or OS/2 – these machines can offload the processing to the bank's computers.

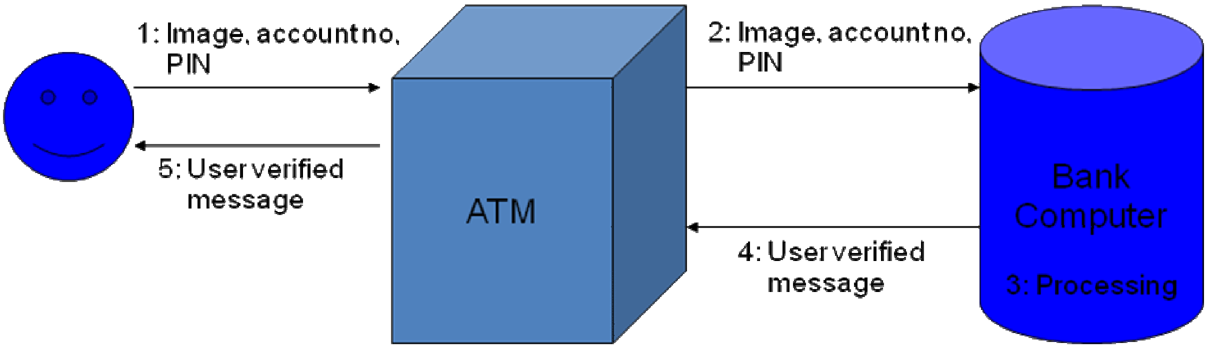

Fig 8.2

As we have seen before both Local Feature Analysis and Principle Feature Analysis programs have handled changes in illumination well. This is important because ATM occurs day and night, with or without artificial illumination.
Verification rates can be as high as 90% when the factors that affect facial recognition systems are taken care of.

9.INSTANCES SHOWING ITS IMPORTANCE IN ATMs

A forgery and theft case in Pierce County, Washington was solved with the use of facial recognition software being pilot tested by the Pierce County Sheriff's Department. An ATM surveillance image was compared to 16 years' worth of mug shots taken at the Pierce County Jail using Sagem Morpho Inc.'s new facial recognition software, Morphoface. It took less than 15 minutes to find a match. The property crime case that would have likely been cast to the side ended with an arrest and conviction.

In another instance in 2003, a group of men were convicted in the United Kingdom for a credit card fraud based on facial verification. Their images were captured on a surveillance tape near an ATM and their identities were confirmed later by a forensic specialist using facial recognition tools.

10.ADVANTAGES AND DISADVANTAGES

Advantages-

1) Verification rates as high as 90% have been achieved when face recognition systems have been used in ATMs.

2) As we have seen it has been used to strengthen security.

3) It can be used to reduce fraudulent attempts.

4) The algorithms used in Face Recognition Systems handle the changes in the illumination effectively. This is important because ATM use occurs day and night, with or without artificial illumination.

5) With appropriate lighting and robust learning software, slight variations in the images could be accounted for.

6) Positive visual match would cause the live image to be stored in the database so that future transactions would have a broader base from which to compare if the original account image fails to provide a match.

7) When a match is made with the PIN but not the images, the bank could limit transactions in a manner agreed upon by the customer when the account was opened, and could store the image of the user for later examination by bank officials.

8) In regards to bank employees gaining access to customer PINs for use in fraudulent transactions, this system would likewise reduce that threat to exposure to the low limit imposed by the bank and agreed to by the customer on visually unverifiable transactions.

Disadvantages-

1) False Positives- It means wrongly matching people attempting for fraud with those stored in the database.

2) False Negatives- Not identifying people correctly even if their photo is in the database.

3) Changes in lighting and expressions like scream expressions, squinted eyes, changes in disguise like wearing hats, glasses drop recognition rates significantly even though the user is a genuine account holder.

4) Matching profile changes worked reasonably well when the initial training image(s) were frontal, which allowed 70-80% success rates for up to 45 degrees of profile change however, 70-80% success isn't amenable to keeping ATM users content with the system.

5) Consumers may be wary of privacy concerns raised by maintaining images of customers in a bank database, encrypted or otherwise, due to possible hacking attempts or employee misuse.

11.CONCLUSION

The conclusion to be drawn for this seminar, is that facial verification software is currently up to the task of providing high match rates for use in ATM transactions. Adding facial recognition systems to the identity verification process used in ATMs can reduce fraudulent transactions to a great extent.

12.BIBLIOGRAPHY

All, Anne. "Triple DES dare you." ATM Marketplace.com. 19 Apr. 2002. http://www.atmmarketplace.com/research.htm?article_id=12243&pavilion=4&step=story

Wrolstad, Jay. "NCR To Deploy New Microsoft OS in ATMs." CRMDailyDotCom. 29 Nov. 2001. <http://www.crmdaily.com/perl/story/15051.html>

Kalignite CE. http://www.kal.com/Products/CE/

Linux Online. <http://www.linux.org/people/banrisul_english.html>

13.REFERENCES

Penev and Atick, Joseph J. "Local Feature Analysis: A General Statistical Theory for Object Representation." Network: Computation in Neural Systems, Vol. 7, No. 3, pp. 477-500, 1996.

Gross, Ralph, Shi, Jianbo, and Cohn, Jeffrey F. "Quo vadis Face Recognition." Third Workshop on Empirical Evaluation Methods in Computer Vision. Kauai: December 2001

Bone, Mike, Wayman, Dr. James L., and Blackburn, Duane. "Evaluating Facial Recognition Technology for Drug Control Applications." ONDCP International Counterdrug Technology Symposium: Facial Recognition Vendor Test. Department of Defense Counterdrug Technology Development Program Office, June 2001.