Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 10, October 2014, pg.192 – 202

RESEARCH ARTICLE

Face Recognition Technology

Ms. Swati S. Bobde[1], Mr. Sumit V. Deshmukh[2]

[1]Lecturer, Department of Computer Science, Shree Shivaji Science College, Amravati, India
[2]Post Graduate Student, Sinhgad Institute of Management, Vadgao (Bk), Pune, India
[1] swati.bobde@rediffmail.com; [2] sumitdeshmukh28@gmail.com

Abstract— ***Wouldn't you love to replace password based access control to avoid having to reset forgotten password and worry about the integrity of your system? Wouldn't you like to rest secure in comfort that your healthcare system does not merely on your social security number as proof of your identity for granting access to your medical records?***

Because each of these questions is becoming more and more important, access to a reliable personal identification is becoming increasingly essential .Conventional method of identification based on possession of ID cards or exclusive knowledge like a social security number or a password are not all together reliable. ID cards can be lost forged or misplaced; passwords can be forgotten or compromised. But a face is undeniably connected to its owner. It cannot be borrowed stolen or easily forged.

Face recognition technology may solve this problem since a face is undeniably connected to its owner expect in the case of identical twins. It's nontransferable. The system can then compare scans to records stored in a central or local database or even on a smart card.

Keywords— ***Face recognition, face identification, Biometrics, Face authentication***

I. INTRODUCTION

The information age is quickly revolutionizing the way transactions are completed. Everyday actions are increasingly being handled electronically, instead of with pencil and paper or face to face. This growth in electronic transactions has resulted in a greater demand for fast and accurate user identification and authentication. Access codes for buildings, banks accounts and computer systems often use PIN's for identification and security clearances.

Using the proper PIN gains access, but the user of the PIN is not verified. When credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. Despite warning, many people continue to choose easily guessed PIN's and passwords: birthdays, phone numbers and social security numbers. Recent cases of identity theft have heighten the need for methods to prove that someone is truly who he/she claims to be.

Face recognition technology may solve this problem since a face is undeniably connected to its owner expect in the case of identical twins. Its nontransferable. The system can then compare scans to records stored in a central or local database or even on a smart card.

II. BIOMETRICS

The term "biometrics" is derived from the Greek words "bio" (life) and "metrics" (to measure). Automated biometric systems have only become available over the last few decades, due to significant advances in the field of computer processing. Many of these new automated techniques, however, are based on ideas that were originally conceived hundreds, even thousands of years ago. **Biometrics** (or **biometric authentication**) refers to the identification of humans by their characteristics or traits. Biometrics is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance. A biometric system is a recognition system, which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. This method of identification is preferred over traditional methods involving passwords and PIN numbers for various reasons:

- The person to be identified is required to be physically present at the point of identification.
- Identification based on biometric techniques eliminates the need to remember a password or carry an identity.

Depending on the context on which a biometric system works, it can be Either classified as an identification system or a verification (authentication) system identification involves in establishing a person's identify whereas in verification involves confirming or denying a person's claiming identity. More traditional means of access control include token-based identification systems, such as a driver's license or passport, and knowledge-based identification systems, such as a password or personal identification number. Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods; however, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information.

Traditional security practices often involve the use of two authentication methods: possession based and knowledge based. Knowledge based authentication requires that the users remember a user name and password or PIN numbers or answers to security questions.

Possession based can use radio frequency IDs, Smart Cards, Interactive Tokens etc. Possession based authentication has the same usability issue as the knowledge based authentication, if the object used for authentication is forgotten at home, in the hotel room, in the car etc the authentication cannot be performed. Biometric security systems are using:

- Physical human identifiers like fingerprint, face, iris, retina, DNA, hand geometry and vein geometry
- Behavioral identifiers like speech, signature, and keystroke timing
- Chemical identifiers like odor and body heat. Biometric systems are used for two purposes. One is to verify that the user is genuine by comparing the acquired biometric trait with the one stored for that user. The other purpose the biometrics are used is to identify a user in which case the acquired biometric trait is compared with a collection of the same traits from multiple users.

A biometric is a unique, measurable characteristic of a human being that can be used to automatically recognize an individual or verify an individual's identity. Biometrics can measure both physiological and behavioral characteristics. Physiological biometrics (based on measurements and data derived from direct measurement of a part of the human body) include:

a. Finger-scan

b. Facial Recognition

c. Iris-scan
d. Retina-scan
e. Hand-scan

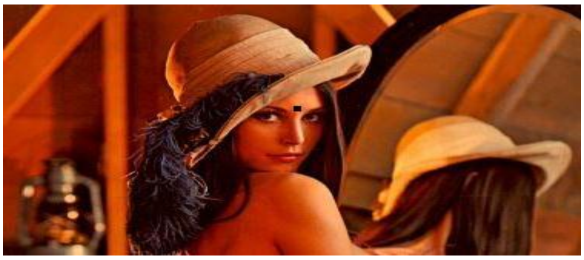
Behavioral biometrics (based on measurements and data derived from an action) include:
a. Voice-scan
b. Signature-scan
c. Keystroke-scan

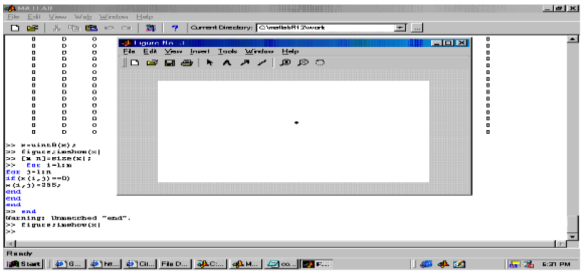
A "biometric system" refers to the integrated hardware and software used to conduct biometric identification or verification.

III. FACE RECOGNITION

The face is an important part of who you are and how people identify you. Except in the case of identical twins, the face is arguably a person's most unique physical characteristics. While humans have the innate ability to recognize and distinguish different faces for millions of years, computers are just now catching up. For face recognition there are two types of comparisons .the first is verification. This is where the system compares the given individual with who that individual says they are and gives a yes or no decision. The second is identification. This is where the system compares the given individual to all the Other individuals in the database and gives a ranked list of matches. All identification or authentication technologies operate using the following four stages:

a. Capture: A physical or behavioural sample is captured by the system during Enrollment and also in identification or verification process
b. Extraction: unique data is extracted from the sample and a template is created.
c. Comparison: the template is then compared with a new sample.
d. Match/non match: the system decides if the features extracted from the new Samples are a match or a non match. Facial recognition is considered to be one of the most tedious among all scans. Further, difficulty in acquisition of face and cost of equipments make it more complex. However, some WAP enabled phones like CX 400K and LG-SD1000 manufactured by LG electronics, have built in camera that can acquire images and can be transmitted over internet. This it is sent to the credit card company to verify the face received matches with the face in their database. If it matches, the goods are sent, else the order is rejected. We in our IMAGE PROCCESSING LAB took two faces with small differences (you see a small dot in the forehead of second face) and programmed MATLAB to find the difference between the two. The output is place below:




MATLAB
File Edit View Web Window Help
Current Directory: C:\matlabR12\work
Figure No. 1
File Edit View Insert Tools Window Help
Ready
Start
6:31 PM

```
      0         0         0                                                 0
      0         0         0                                                 0
      0         0         0                                                 0
      0         0         0                                                 0
      0         0         0                                                 0
      0         0         0                                                 0
      0         0         0                                                 0
      0         0         0                                                 0
      0         0         0                                                 0
      0         0         0                                                 0
      0         0         0                                                 0
      0         0         0                                                 0
      0         0         0                                                 0
      0         0         0                                                 0
      0         0         0                                                 0

>> x=uint8(x);
>> figure;imshow(x)
>> [m n]=size(x);
>>   for i=1:m
for j=1:n
if(x(i,j)==0)
x(i,j)=255;
end
end
end
>> end
Warning: Unmatched "end".
>> figure;imshow(x)
>>
```

Fig 1. Difference between two image can be found by MATLAB

The above simulations shows that even two persons having almost similar face with minute difference can also be differentiated. Now, there arises a problem. A man, without bread, make as a transaction successfully .A week later he makes another transaction with some hair grown on his chin and go for acquiring images of any part of the face like forehead, nose, ear etc. Hence, this type of facial scanning system can be used as a part of the multi-biometric system we have presented above.

IV.   CAPTURING OF IMAGE BY STANDARD VIDEO CAMERAS

The image is optical in characteristics and may be thought of as a collection of a large number of bright and dark areas representing the picture details. At an instant there will be large number of picture details existing simultaneously each representing the level of brightness of the scene to be reproduced. In other words the picture information is a function of two variables: time and space. Therefore it would require infinite number of channels to transmit optical information corresponding to picture elements simultaneously. There is practical difficulty in transmitting all information simultaneously so we use a method called scanning.

Here the conversion of optical information to electrical form and its transmission is carried out element by element one at a time in a sequential manner to cover the entire image. A TV camera converts optical information into electrical information, the amplitude of which varies in accordance with variation of brightness.

An optical image of the scene to be transmitted is focused by lense assembly on the rectangular glass plate of the camera tube. The inner side of this has a transparent coating on which is laid a very thin layer of photoconductive material. The photolayer has very high resistance when no light is falling on it but decreases depending on the intensity of light falling on it. An electron beam is formed by an electron gun in the TV camera tube. This beam is used to pick up the picture information now available on the target plate of varying resistance at each point.

The electron beam is deflected by a pair of deflecting coils mounted on the glass envelope and kept mutually perpendicular to each other to achieve scanning of the entire target area. The deflecting coils are fed separately from two sweep oscillators, each operating at different frequencies. The magnetic deflection caused by current in one coil gives horizontal motion to the beam from left to right at a uniform rate and brings it back to the left side to commence the trace of the next line. The other coil is used to deflect the beam from top to bottom.

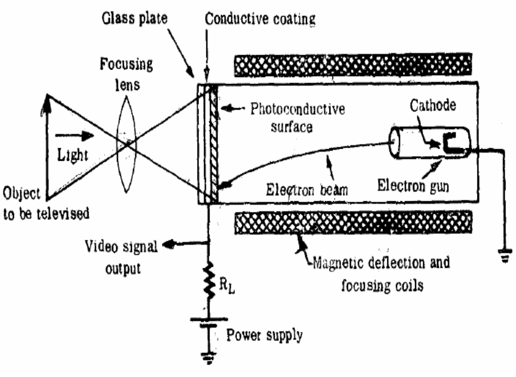


Fig. 2

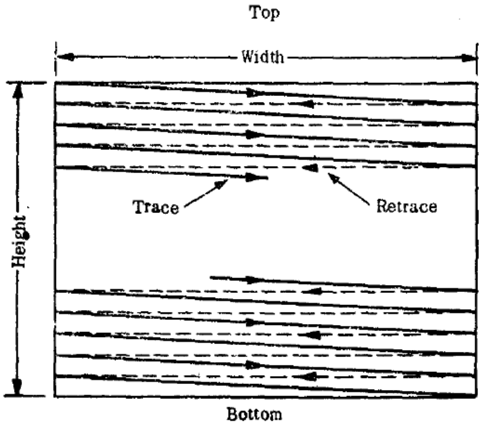


Fig. 3

As the beam moves from element to element it encounters different resistance across the target plate depending on the resistance of the photoconductive coating. The result is flow of current which varies in magnitude as elements are scanned. The current passes through the load resistance Rl connected to conductive coating on one side of the DC supply source on the other. Depending on the magnitude of current a varying voltage appears across the resistance Rl and this corresponds to the optical information of the picture.

V. COMPONENTS OF FACE RECOGNITION SYSTEMS

An automated mechanism that scans and captures a digital or an analog image of a living personal characteristics.(enrollment module)

Another entity which handles compression, processing, storage and compression of the captured data with stored data (database)

The third interfaces with the application system (identification module)

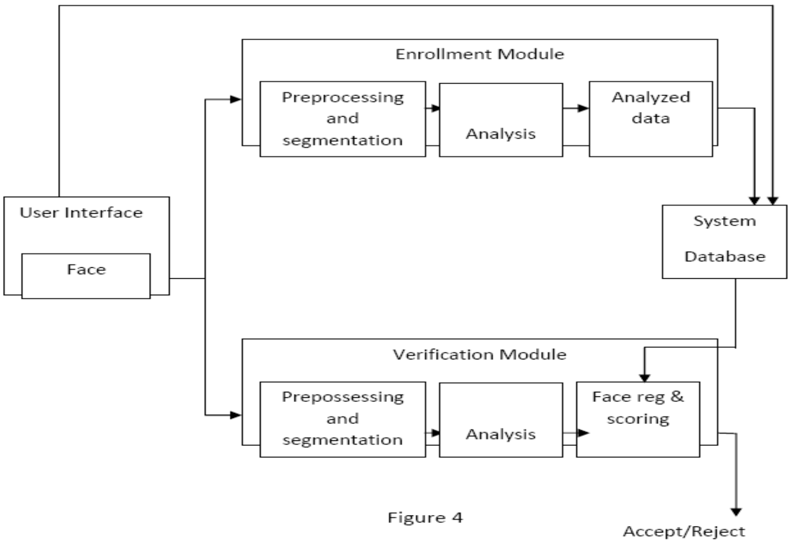


Figure 4

User interface captures the analog or digital image of the person's face. In the enrollment module the obtained sample is preprocessed and analyzed. This analyzed data is stored in the database for the purpose of future comparison.

The database compresses the obtained sample and stores it. It should have retrival property also that is it compares all the stored sample with the newly obtained sample and retrives the matched sample for the purpose of verification by the user and determine whether the match declared is right or wrong.

The verification module also consists of a preprocessing system. Verification means the system checks as to who the person says he or she is and gives a yes or no decision. In this module the newly obtained sample is preprocessed and compared with the sample stored in the database. The decision is taken depending on the match obtained from the database. Correspondingly the sample is accepted or rejected.

Instead of verification module we can make use of identification module. In this the sample is compared with all the other samples stored in the database. For each comparison made a match score is given. The decision to accept or reject the sample depends on this match score falling above or below a predetermined threshold.

VI. FACE RECOGNITION PROBLEM

Given a still image or video of a scene, identify or verify one or more persons in this scene using a stored database of facial images

Who is she?
http://picasa.google.com

Fig. 5

VII. FACE RECOGNITION/IDENTIFICATION

Who is this person?
He is David.

Fig. 6

VIII. FACE AUTHENTICATION/VERIFICATION

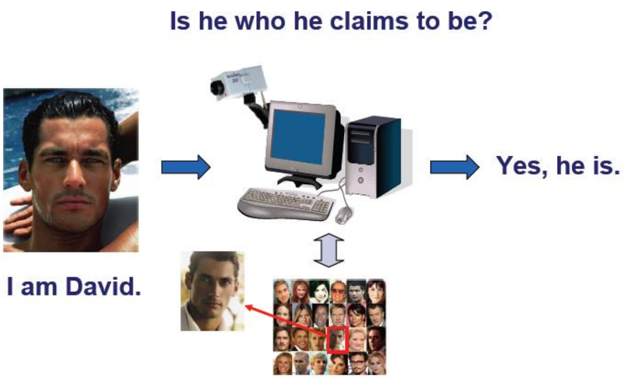


Fig. 7

IX. FACE RECOGNITION IN HUMANS

- The human visual system starts with a preference for face-like patterns
- The human visual system devotes special neural mechanisms for face perception
- Facial identity and expression might be processed separately
- Facial features are processed holistically
- Among facial features eyebrows are most important for recognition!
- Humans can recognize faces in very low dimensional images
- Tolerance to image degradation increases with familiarity
- Color and texture are as important as shape
- Illumination changes influence generalization
- View-generalization is mediated by temporal association

X. TYPICAL FACE RECOGNITION SYSTEM ARCHITECTURE

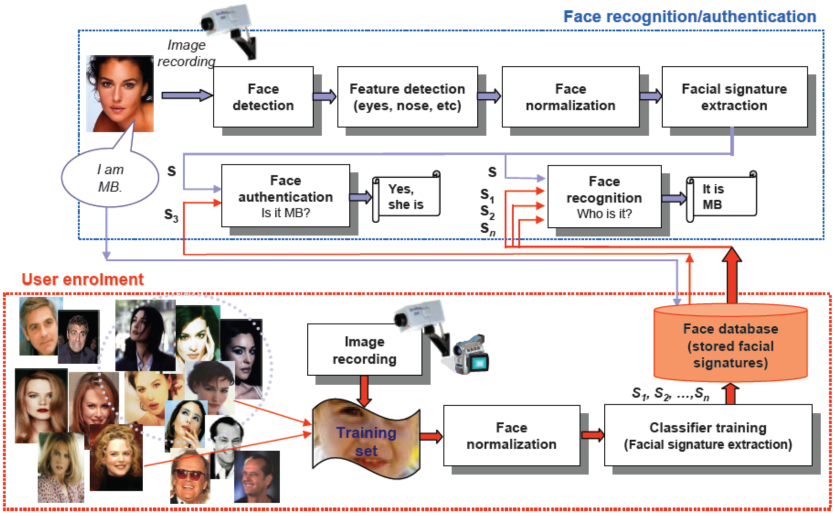

Face recognition/authentication
Image recording
Face detection
Feature detection (eyes, nose, etc)
Face normalization
Facial signature extraction
I am MB.
S
S3
Face authentication Is it MB?
Yes, she is
S
S1
S2
Sn
Face recognition Who is it?
It is MB
User enrolment
Image recording
Training set
Face normalization
Classifier training (Facial signature extraction)
Face database (stored facial signatures)
S1, S2, ...,Sn

Fig.8

XI. PERFORMANCE

False acceptance rate (FAR)

The probability that a system will incorrectly identify an individual or will fail to reject an imposter. It is also called as type 2 error rate

FAR= NFA/NIIA

Where FAR= false acceptance rate

NFA= number of false acceptance

NIIA= number of imposter identification attempts

False rejection rates (FRR)

The probability that a system will fail to identify an enrollee. It is also called type 1 error rate.

FRR= NFR/NEIA

Where FRR= false rejection rates

NFR= number of false rejection rates

NEIA= number of enrollee identification attempt

Response time:

The time period required by a biometric system to return a decision on identification of a sample.

Threshold/ decision Threshold:

The acceptance or rejection of a data is dependent on the match score falling above or below the threshold. The threshold is adjustable so that the system can be made more or less strict; depending on the requirements of any given application.

Enrollment time:

The time period a person must spend to have his/her facial reference template successfully created.

Equal error rate:

When the decision threshold of a system is set so that the proportion of false rejection will be approximately equal to the proportion of false acceptance. This synonym is 'crossover rate'. The facial verification process involves computing the distance between the stored pattern and the live sample. The decision to accept or reject is dependent on a predetermined threshold. (Decision threshold).

XII. IMPLEMENTATION OF FACE RECOGNITION TECHNOLOGY

The implementation of face recognition technology includes the following four stages:

Data acquisition

Input processing

Face image classification and decision making

A. Data acquisition:

The input can be recorded video of the speaker or a still image. A sample of 1 sec duration consists of a 25 frame video sequence. More than one camera can be used to produce a 3D representation of the face and to protect against the usage of photographs to gain unauthorized access.

B. Input processing:

A pre-processing module locates the eye position and takes care of the surrounding lighting condition and colour variance. First the presence of faces or face in a scene must be detected. Once the face is detected, it must be localized and

Normalization process may be required to bring the dimensions of the live facial sample in alignment with the one on the template.

Some facial recognition approaches use the whole face while others concentrate on facial components and/ or regions (such as lips, eyes etc). The appearance of the face can change considerably during speech and due to facial expressions. In particular the mouth is subjected to fundamental changes but is also very important source for discriminating faces. So an approach to person's recognition is developed based on patio- temporal modeling of features extracted from talking face.

Models are trained specific to a person's speech articulate and the way that the person speaks. Person identification is performed by tracking mouth movements of the talking face and by estimating the likelyhood of each model of having generated the observed sequence of features. The model with the highest likelyhood is chosen as the recognized person

C. Face image classification and decision making:

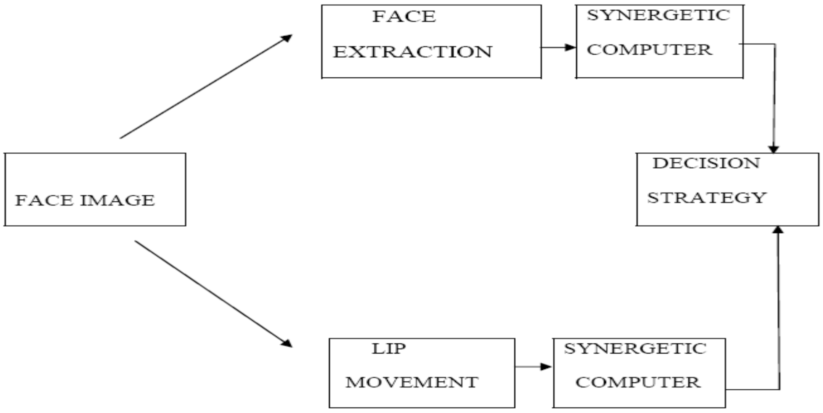


Fig. 9

XIII. HOW FACE RECOGNITION SYSTEMS WORK

An example

Visionics, company based in a New Jersey is one of the many developers of facial recognition technology. The twist to its particular software, Face it is that it can pick someone's face from the rest of the scene and compare it to a database full of stored images. In order for this software to work, it has to know what a basic face looks like. Facial recognition software is based on the ability to first recognize faces, which is a technological feat in itself.

Fig. 10

If you look at the mirror, you can see that your face has certain distinguishable landmarks. These are the peaks and valleys that make up the different facial features. Visionics defines these landmarks as nodal points. There are about 80 nodal points on a human face. Here are few nodal points that are measured by the software.

distance between the eyes

- width of the nose

- depth of the eye socket

- cheekbones

- jaw line

- chin

These nodal points are measured to create a numerical code, a string of numbers that represents a face in the database. This code is called faceprint. Only 14 to 22 nodal points are needed for faceit software to complete the recognition process.

XIV. ADVANTAGES AND DISADVANTAGES

Advantages:

a. There are many benefits to face recognition systems such as its convenience and Social acceptability. All you need is your picture taken for it to work.
b. Face recognition is easy to use and in many cases it can be performed without a Person even knowing.
c. Face recognition is also one of the most inexpensive biometric in the market and
Its price should continue to go down.

Disadvantage:

a. Face recognition systems can’t tell the difference between identical twins.

XV. APPLICATIONS

The natural use of face recognition technology is the replacement of PIN, physical tokens or both needed in automatic authorization or identification schemes. Additional uses are automation of human identification or role authentication in such cases where assistance of another human needed in verifying the ID cards and its beholder.

There are numerous applications for face recognition technology:

Government Use

a. Law Enforcement: Minimizing victim trauma by narrowing mugshot searches, verifying Identify for court records, and comparing school surveillance camera images to know child molesters.
b. Security/Counterterrorism. Access control, comparing surveillance images to
Know terrorist.
c. Immigration: Rapid progression through Customs.

Commercial Use

a. Day Care: Verify identity of individuals picking up the children.
b. Residential Security: Alert homeowners of approaching personnel

c. Voter verification: Where eligible politicians are required to verify their identity during a voting process this is intended to stop 'proxy' voting where the vote may not go as expected.
d. Banking using ATM: The software is able to quickly verify a customer's face.
e. Physical access control of buildings areas, doors, cars or net access.

XVI. CONCLUSION

Face recognition technologies have been associated generally with very costly top secure applications. Today the core technologies have evolved and the cost of equipments is going down dramatically due to the integration and the increasing processing power. Certain applications of face recognition technology are now cost effective, reliable and highly accurate.

ACKNOWLEDGEMENT

First of all, I would like to place myself at the feet of **God Almighty** for his everlasting love and for the blessings & courage that he gave me, which made it possible to me to see through the turbulence and to set me in the right path. I would also like to thank **Prof. D.N. Satange** for all the help and guidance that he provided to me. I would take this opportunity to thank my friend **Mr. Sumit V. Deshmukh** he is always a source of encouragement.

REFERENCES

[1] www.facereg.com
[2] www.Imagestechnology.com
[3] www.iee.com
[4] IEEE Intelligent Systems - May/June 2003
[5] Modern Television Engineering- Galati R.R
[6] www.facereg.com
[7] www.Imagestechnology.com
[8] www.iee.com