

HARATI Computer Services Private Ltd.

Technical Details

The Computerized Time Attendance system is electronic attendance system in which every employee make their attendance in computer rather than using attendance book. The system is integrated with bio-metric devices like Finger print scanner or Swap card. Using this devices makes less chance of fraud or other user malicious activities. The Electronic Time Attendance system tracks all the employee related details including over-time, under-time, leave etc.

Basic Features

- Computerized Log In/Log Out System
- Automatic Leave Calculation
- Over Time/ Under Time Calculation
- Electronic Attendance Processing
- Aesthetically designed general and MIS reports
- Backup and Restore Facilities
- User Definable Security System
- Files Import Features
- Integrated with Personnel MGMT and Payroll MGMT system
- Web-based database system

Finger Vien Authentication

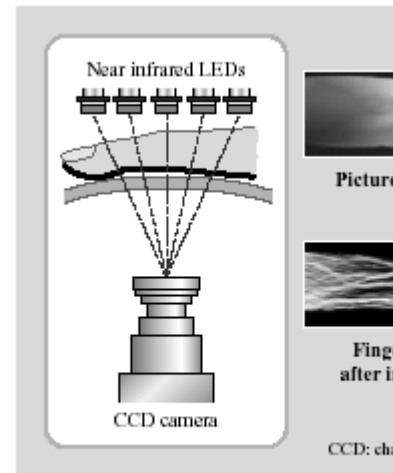
The basic principle on which the finger-vein authentication system is based is shown in Fig. 3. Nearinfrared rays generated from a bank of LEDs (light emitting diodes) penetrate the finger and are absorbed by the hemoglobin in the blood. The areas in which the rays are absorbed (i.e. veins) thus appear as dark areas in an image taken by a CCD camera located on the opposite side of the finger. Image processing can then construct a finger-vein pattern from the camera image. This pattern is then compressed and digitized so that it can be registered as a template of a person's biometric authentication data. The finger-vein pattern and the template can be authenticated by means of a pattern-matching technique. The device developed to perform the above described detection process (finger-vein pattern scanner) is shown in Fig. 4. The part of the finger-vein scanner on the right or holding up a legitimate person's photo. Face and voice authentications are thus only effective methods in an environment in which an attendant or guard is present to ensure that fraud is impossible.

HARATI Computer Services Private Ltd.



*Fig. 4—Finger-vein Scanner.
The finger-vein scanner detects the finger-vein pattern and sends it to the controller.*

*Fig. 2—Fingerprint Sensor.
Fingerprint sensor can be used to replace a password for a personal computer.*



*Fig. 3—Theory of Finger-vein Authentication
Near-infrared rays form a vein pattern on*

Fingerprint authentication is a reliable method widely acknowledged across society. When a person places their finger on a special semiconductor pad (i.e. a fingerprint sensor), their fingerprint is extracted and its image is analyzed. The analysis result is then checked against that person's previously registered fingerprint for authentication. Being easy to operate by means of a compact device (see Fig. 2), this method is widely used as a replacement for PC passwords. Although fingerprint authentication is useful for individual applications like PC access, applying it to door-access control faces several problems from the viewpoint of usability. For example, pressing the whole fingerprint up against a sensor gives an uncomfortable feeling, and the sensor gets dirty, thus decreasing the authentication success ratio. In addition, fingerprint systems have a negative image associated with crime. Iris authentication uses image processing to authenticate an image of the iris taken by a camera.