A good number of systems need genuine personal gratitude schemes either to authenticate or regulate the identity of an individual demanding their use. The aim of such systems is to guarantee that the much needed services are retrieved only by genuine user, and not by any other individual. Applications are secure access to bank accounts, cell phones, laptops, computer systems and different electronic gadgets. In lack of tough individual recognition measures, these systems are exposed to the tricks of an impostor. General authentication techniques which are based on passcodes and keys are limited due to their inability to take care of following concerns.

Host attack - person using plain text, image file and document comprising passwords

Client attack - person guessing, robbing or stealing tokens or password

Eavesdropping - password shared by many individuals

Trojan horse attack – Stealing password by installing fake log-in screen.

Denial of service – Using incorrect password to disable the system.

Non-Repudiation - individual claiming that password was lost or misplaced.

Negative recognition - A procedure, by means of which a recognition system decides the person is indeed genuine and recognized in the system, however the person later denies it. The effectiveness of an authenticator system is based on its toughness to different kinds of malevolent attacks. Though, few of these issues can be stopped by designing suitable defensive measures with secure entry in to the system by using passwords, etc. The dawn of biometrics has addressed some of the short comings of this old-style authentication system.

1.1 Biometrics

An accurate authentication of a person is essential in daily routine works such as bank transactions, access to computer, entry to office etc. The recognition of a person from national database of human beings is required for national security. The term Biometric is derived from the Greek words bios and metrics (measurement) [1] that recognizes an individual based on biometric qualities obtained from a specific physiological or behavioral specific of a person. The biometric system [2] is accurate and more reliable compared to conventional security systems such as password, PIN, ID card etc. The conventional security systems can be easily breached since the password may be forgotten and identification card may be lifted or lost. The biometric system uses parts of body and behavior of a person as biometric traits which cannot be stolen or lost, hence biometric system is highly reliable to avoid intruders from

neighboring countries. The biometrics is a promising technique to identify a person accurately.

The personal uniqueness is obtained by acquiring and comparing the captured image with the image of same individual present in the databank. The system conducts a one-to-one assessment for personal verification.

Identification mode: In Identification mode, the system identifies the person by searching all the templates present on the database based on matching

The biometric traits are classified into two types [4] such as (i) Physical and (ii) Behavioral traits. The physical biometric is related to body parts of person which are stable over a period of time that include face, fingerprint, iris etc., and behavioral trait changes with time due to age, health, physiological state, mood, circumstances etc., of a person that includes signature, gait, voice, keystroke, etc.

1.1.1 Physiological Biometrics

(A) Fingerprint

The pattern of ridges and furrows present in finger is a fingerprint as shown in Fig 1.1

Fig 1.1: Image of fingerprint.

The fingerprints are classified as

(i) **Latent fingerprints**: The unintentional impressions left o n t he sur face by r idge, irrespective of t hat one is visible or invisible at the time of admission.

(ii) **Patent fingerprints or visible fingerprints**: The imprints caused by the transfer of ink ingredients on the finger onto a surface and fingerprint taken on a scanner.

(iii) **Captivated fingerprints**: The finger impression that has the ridge details which is on a material is taken. Correlation based, Minutiae-based, Ridge feature based and Pores based approaches are used for fingerprint matching. Various fingers namely index, middle, ring and little fingers have distinctive fingerprint pattern. Fingerprint recognition is widely used, since capturing the fingerprint image is easy and universally acceptable. The fingerprint is used in all fields such as forensic, automobiles, cell phones, property registration, personal computers etc.

(ii) IRIS:

The unique and complex texture of an iris begins to form throughout fetal growth in the two years of life of any individual [6]. The iris of identical twins is different and distinctive. The curved contractile membrane of an eye on hold between the cornea and lens which is perforated by the pupil, this membrane is an iris as shown in Fig 1.2. The texture fine points in the iris image such as cornea, crypts, filaments, flecks, radial furrows, stripes, bending ligaments etc., make an iris pattern unique. These unevenly shaped microstructures are very erratically distributed patterns which make the human iris as one of the most significant and distinct biometric characteristics. The iris is encircled by two concentric rings i.e., inner boundary is among iris and pupil and the outer edge is among iris and sclera.

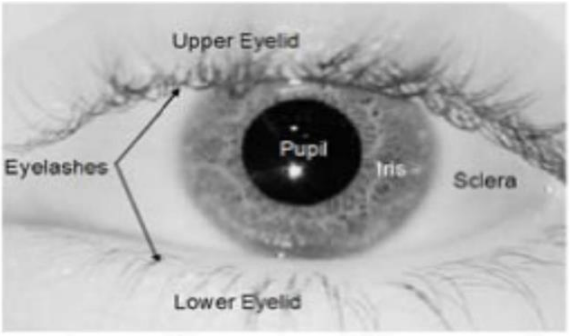


Fig 1.2: Image of Iris

The tampering of an iris texture using surgery is extremely difficult as it is invasive and highly sensitive organ of the body. The iris-based recognition schemes required substantial user contribution and costly.

(B) Deoxyribose Nucleic Acid (DNA):

The one-dimensional final single structure of DNA [7] for one's individuality is shown in Fig 1.3. Naturally identical twins have indistinguishable DNA patterns. Presently DNA is used as an evidence for person recognition in forensic applications. The biometric application of DNA is restricted because of the following disadvantages.

(i) **Contamination and sensitivity:** The DNA can be stolen easily from any individual from a single point of blood. At a later stage mistreated for a hidden drive.

(ii) **Real-time recognition matters**: The current technology used for DNA identification needs different chemical approaches containing a specialist's skills.

(iii) **Confidentiality concerns**: Personal health data of an individual suffering from particular disease can be known from DNA pattern and there is a worry that unintentional abuse of genetic data may effect in sensitivity.

Fig 1.3: Image of DNA.

(C). Face:

The face identification/verification [8] is the most effective biometric system used in today's world and sample images of face images as shown in Fig 1.4. The presentations of face recognition vary from a static, confirmation to dynamic, uncontrolled face proof of identity in a disorderly manner. The face recognition systems are dependent on (i) The position and form of features such as the eyes, eyebrows, nose, lips and chin, (ii) The complete study of the image that denotes a face as a biased arrangement of a Fig of eigen faces.

Fig 1.4: Images of Faces

(D). Hand vein infrared thermogram:

The Vein patterns are distinctive among persons and do not change with time, even in the case of similar twins, hence it is used to confirm persons [9]. It is problematic to capture the hand vein structure, meanwhile the veins typically move and they bend as the blood is forced in the person structure. Special devices are used to capture and resize the image. The main disadvantage of this biometric trait is cost.

(E) Hand and Finger structure:

The hand geometry recognition system is the development of recognition of individual based on a series of quantities in use from the particular individual hand, plus its palm size, shape, lengths and sizes of the fingers [10] as shown in Fig 1.5. The hand and finger geometry pattern are variant during the growing stages of adolescents and are not unique. The ecofriendly factors does not have any negative special effects on the confirmation correctness of hand geometry based systems. The drawbacks of hand geometry created recognition systems are (i) it could not be used for systems demanding proof of identity of an individual from a large residents (ii) An extraction of hand geometry is difficult if jewelry on fingers and arthritis and (iii) Due to the length of the hand being considerably large, it cannot be entrenched in certain devices like tabs..

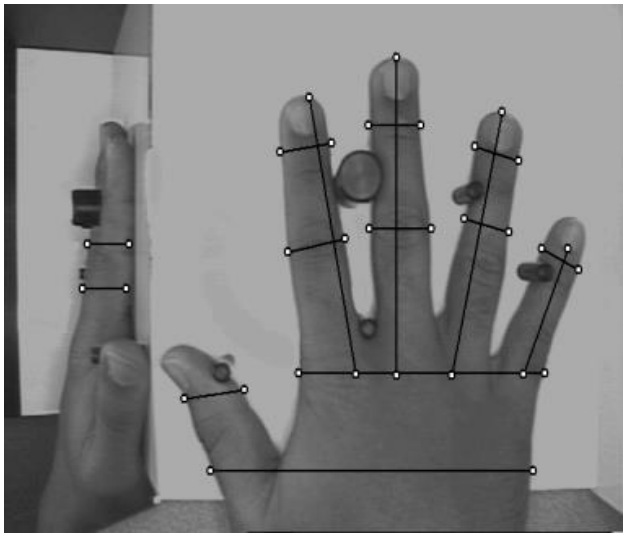


Fig 1.5: Hand geometry device

1.1.2 Behavioral Biometrics

(i) **Signature**

It is the person who writes his/her name as signature [4] as shown in Fig 1.6. The signature verification system is the most popular among numerous identification strategies. It is wide accepted methodology for endorsing money transactions.

A verification strategy is needed to separate correlation regions, compare them individually separately one by one with reference signatures and mix the leads to an overall verification confirmation. The verification system should be able to observe forgeries and at identical time reduce rejection of real signatures. Differing types of forgeries thought of for signature verification systems are:

difference exists between person to person in the way they type on keyboard. More storage is required to create the database; hence it is used in low security applications.

Fig 1.8: Image of Keystroke.

(iv) **Odor**

Every individual possesses body odor which is typical of its chemical arrangement [14]. It changes between persons, hence can be treated as biometrics for identification. A whiff of an air adjacent a person is propelled over an array of chemical feelers, each delicate to an assured group of aromatic compounds. A part of an odor emitted by any individual is differentiable to a specific person. It is very rarely used biometric system since chemical sensors are used.

(v) **Voice**

It is a behavioral biometric and the body parts like mouth, lips, teeth, throat are responsible for voice [15]. It varies with age, health conditions, emotions etc., of person. The voice of person is recorded and stored as database; speech processing is done to identify a person. Since the process takes more time it is rarely used.

1.2 Biometric Architecture:

The schematic diagram of the common biometric system used to identify a person is shown in fig 1.9. The biometric arrangement has blocks of data acquisition, preprocessing, feature extraction, comparison and decision.

(iii) Hybrid domain features:

The final features are obtained by combining spatial domain and transform domain features. This technique is considered as hybrid domain technique . The image is decomposed into two cells, features are extracted by applying spatial domain on one cell and transform domain technique on another cell and the features obtained are fused to get final feature vector.

1.2.4 Matching:

The topographies of test biometric is related with qualities of database using classifiers such as Euclidean , Hamming , Chi Square distances, Support Vector Machine, Random Forest, K- Nearest Neighborhood algorithm, Neural Network etc., to authenticate a person. The results obtained in the classifiers determine whether the individual sample is accepted or rejected by the biometric system.

The spatial domain and transform domain features of database and test images are extracted. The presentation factors such as FRR, FAR, and TSR are calculated separately utilizing spatial and transform domain features. The performance parameters of spatial and transform domain are fused to obtain better performance parameter values compared to individual domain parameter values.

1.3 Characteristics of Biometrics :

The biometrics is accepted in finding the uniqueness of an individual if it fulfills the next parameters.

Universality: The personal feature ought to be universally acceptable.

Distinctiveness: Any of two individuals would be adequately dissimilar in terms of the characteristics.

Permanence: The distinguishing should be adequately unchanged with reference to the matching measure over a period of time.

Collectability: The characteristics can be stated quantitatively.

Performance: The precision and the speed of recognition.

Acceptability: It provides a range to which individuals are to receive the articular biometric identifier or features in their communications.

Uniqueness: It is the property of that biometric how best it can separate the individuals

The evaluations of several biometric features are given in Table 1.1 [12].

Biometric identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facial thermogram	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand geometry	M	M	M	H	M	M	M
Hand vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Palmprint	M	H	H	M	H	M	M
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

H ,M ,L indicates HIGH,MEDIUM,LOW

Table 1.1 Evaluation of several biometrics

Through the growing demand of enhanced security in our daily lives, consistent personal ID through biometric is presently a lively topic. Biometric is basically a pattern-recognition scheme that distinguishes an individual features resulting from physiological or behavioral characteristics that the person owns. The feature vector is normally stored in file or recorded on a smart tag card after being extracted. Efficient representation of feature vector, storage space, enrollment and matching time are some of the biggest hardware and software challenges.

Main aim of person identification is greater Genuine Acceptance Rate (GAR) at the same time minimum False Acceptance Rate (FAR), less computational complexity and less space for storage.

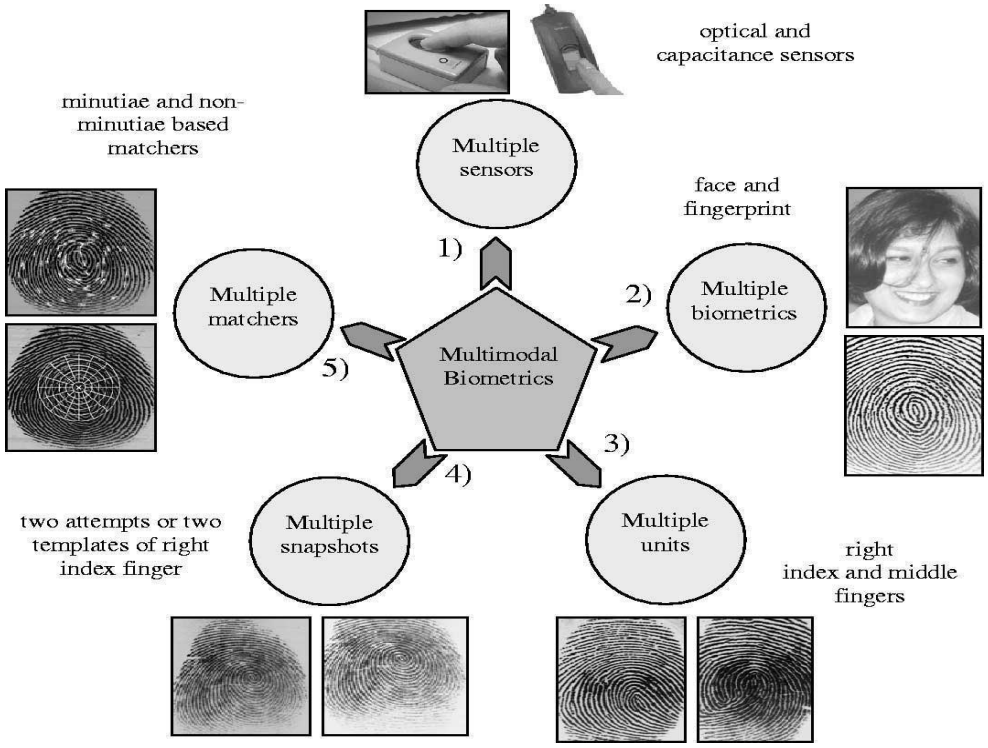


Fig 1.13 Various settings in a multimodal biometric system [12]

1.6 Biometric System Performance Measures

The dispersal of values produced from pairs of trials from diverse individuals is named as impostor distribution, and the distribution produced from sets of samples of the identical individual is called a genuine distribution, as shown in Fig.1.14 [4].

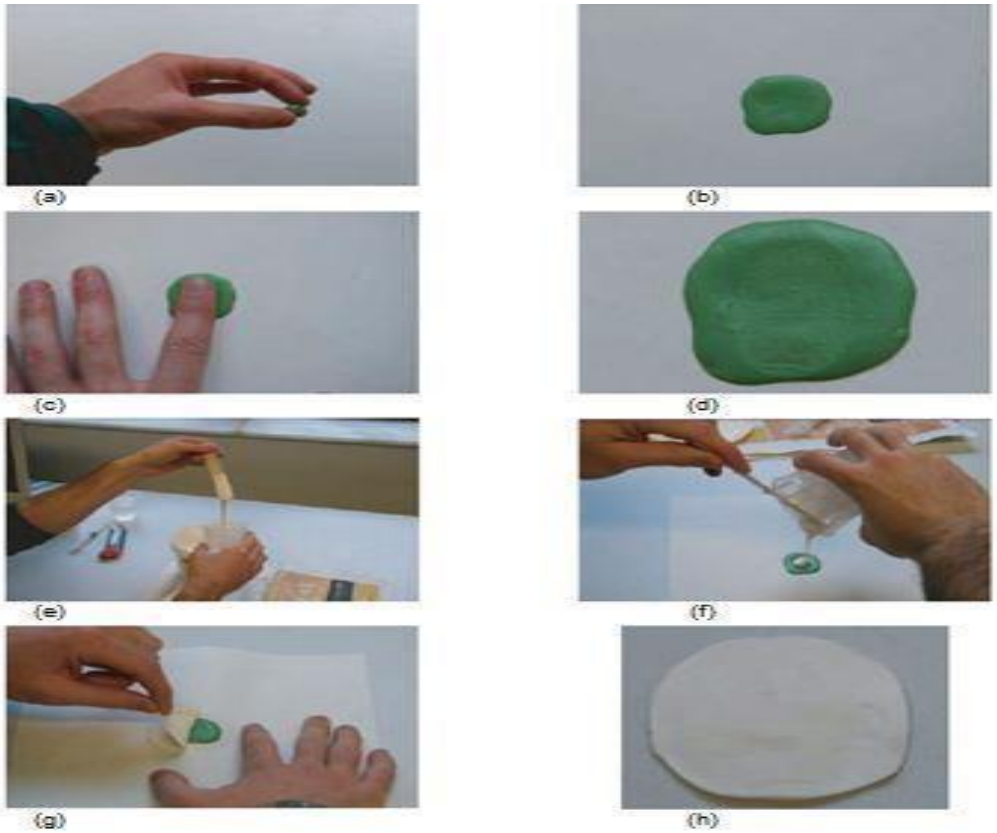
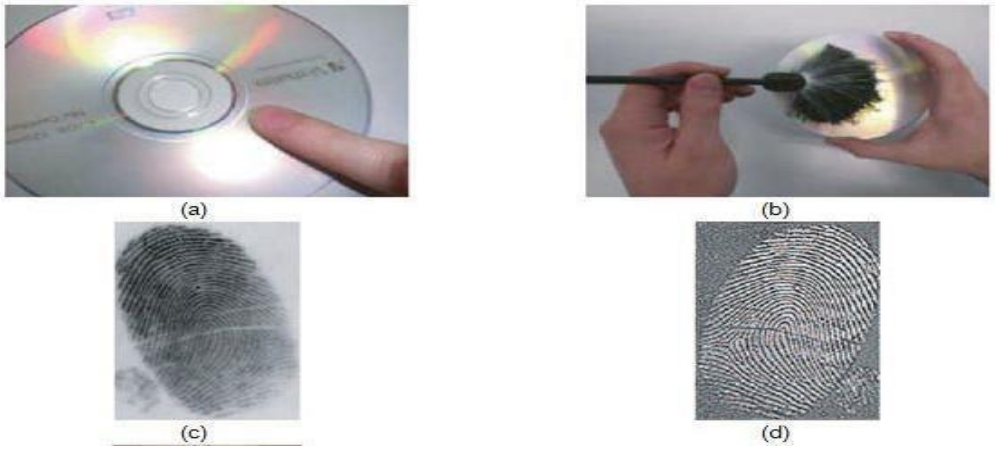


Fig 4.4 process of gummy finger generation with consent of the person.

we create a latent fingerprint that the user has unnoticed left behind. The hidden fingerprint is elevated using a particular fingerprint growth toolkit and then digitalized through a scanning device. Key steps of this non-cooperative procedure are depicted in Fig.2.5.



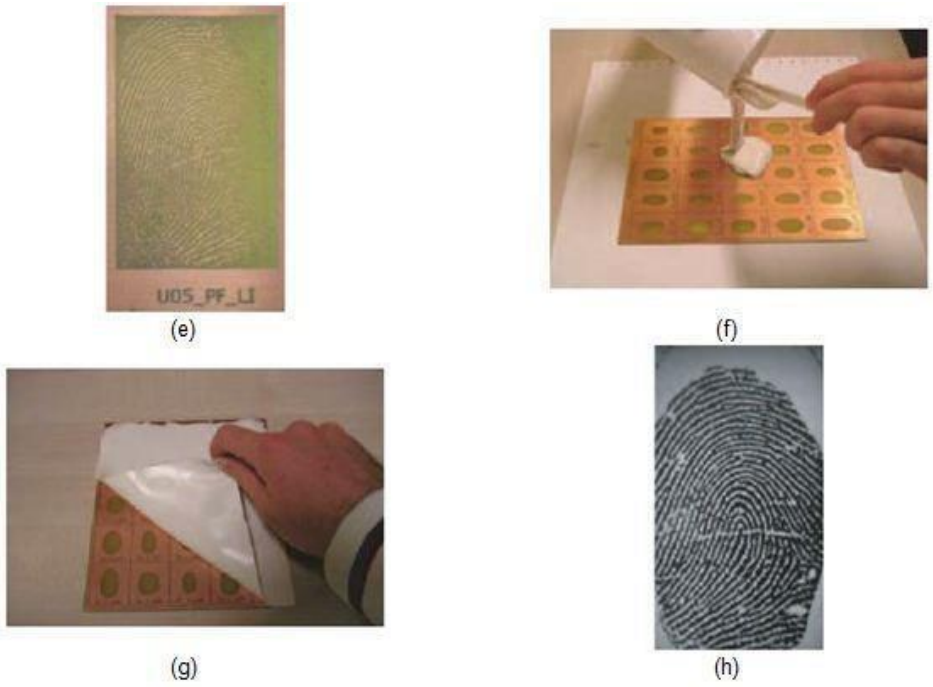


Fig 4.5 Generation of fake fingerprint without the consent of the user

Method of creating gummy finger is used for generating 3-D fake finger from 2-D reconstructed image. From ISO template the image has been created, the colors are altered and the altered image is printed on a slide that will assist as a shield for creating a PCB where the valleys are nothing but the circuit lines of the original fingerprint. Once the PCB has been formed the process is shown as the steps e to f shown in Fig.2.6. The entire method to create gummy finger edge from reproduced fingerprint image is depicted in Fig.2.7.

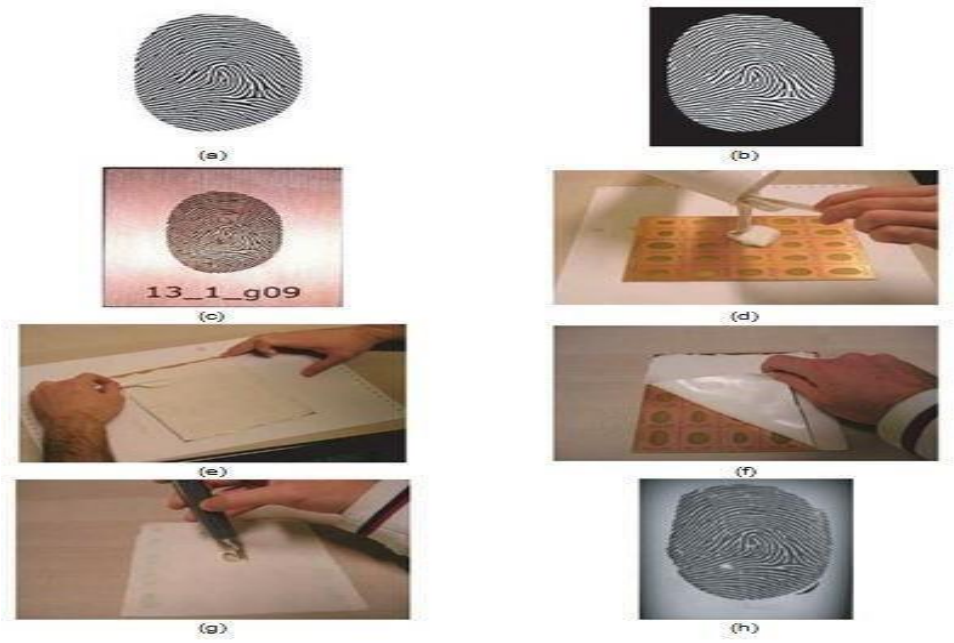


Fig 4.7 fake fingerprint generation method

recreated copy (a), negative of the reproduced image (b), finger on the printed circuit board (c), dispense the silicone and catalyst combination on the Printed Circuit board(d), spread the combination completed on the PCB (e), separate when it solidifies (f), remove apiece forged finger (g), final counterfeit fingerprint attained (h)

4.6 Counter measuring direct Attacks through Liveness Detection:

Liveness detection methods using hardware can be categorized as:

a. Temperature measurement
b. Optical properties
c. Pulse oximetry
d. Blood Pressure measurement
e. Electric resistance
f. Combining ECG, pulse oximetry
g. Detection under epidermis
h. Skin deformation
i. Pores and Perspiration