

## Embedded Fingerprint Matching Mechanism in HIS for Health Care Service

Gayathri Mohan

**Abstract:** As technologies develops, our needs can be increase and also it can be change. The invention of new medical equipment's in health care services can help both the patients and the doctors in several ways. In this paper an advanced ubiquitous echograph system is proposed, in such a way that, doctor can diagnoses the patient without seeing them face-to-face in hospital. Patient's having medical devices with advanced features (i.e., readings/outputs of device can be downloaded and transferred to pc) can send the test details to corresponding doctor of hospital, via wireless network. That is patient needs to consult the doctor, in hospital, only when an emergency situation arises. The recent technological innovations make this concept more realistic that is helpful in increasing the easiness of doctor's consulting duties and also decreases the maintenance cost of hospital. Some devices like AccuChek and glucose level checking device are used here to demonstrate my work, since almost all the echograph devices are expensive. A new prototype is embedded into HIS: a Fingerprint Matching System. By using this system, doctor's identification can be done easily, even if their fingers are altered. Since doctors can diagnose patients, even if they are not available in hospital, a valuable recognition system is needed to make ensure that doctor is authentic or not. So the fingerprint matcher is developed in such a way that it can detect any type of altered fingerprint and can matches altered ones to their respective unaltered fingerprint. This proposed paper is even applicable for telemedicine.

**Index Terms:** Fingerprints, obfuscation, alteration, ridge pattern, minutiae distribution, echograph, Hospital Information System (HIS), ubiquitous computing

### I. Introduction

Computerization of hospitals was happened because of advancement of communication and information technologies and also to meet the social demands for efficiency and safety of the services in healthcare. Most of GISs consist of huge computational servers which store and process EMRs. There were number of terminals to let clinicians to input and to browse EMRs, and networks to connect the terminals and servers. So, once aGIS is introduced in a hospital, the hospital can provide all-over computing services for clinicians and they can access information anytime anywhere inside the hospital as well as outside the hospital. This paper enhances the ubiquitous service concept in HIS [1].

The term ubiquitous computing is coined by Weiser [4]. Simply almost everyone understands this term as "access anytime anywhere easily". Bardram [5] implemented pad and wall system of Weiser into hospital as a CSCW tool. This system can share the on-going surgeries/treatments schedule and, information about patients. By considering medical device as a computer system, and a hospital as a gigantic computer system, the medical equipment's can be embedded into the hospital.

The GIS supports the patient, clinicians, doctors...etc., each and every one related to hospital. Patient can easily consult the doctor and can provide test details received from the echograph system that they have, without reaching the hospital. Doctors can diagnose patient from anywhere at any time, the only adequate requirement is wireless connection. Since server consists of all the details about patient, doctor and hospital infrastructure, it make easy for clinical staffs to manage all the details in computer system (Fig.1).

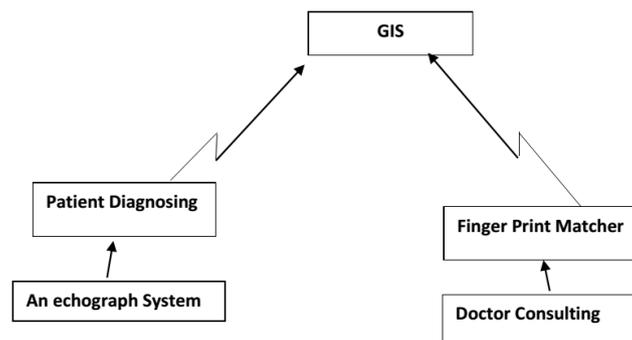


Fig.1. Prototype of GIS consists of echograph and finger print matcher

In order to identify the authentic person, a fingerprint matching system is used in HIS. The use of fingerprints in both government applications and civilian applications [employment background checks, border control, and secure facility access] as well as its usage in other personal identification applications (credit card usage verification, employment identification, high security installations) is increased as a result of the innovations in automatic fingerprint analysis and detection. These techniques can be also used for personal identification. Some of the large-scale fingerprint systems [used in the US government arena] are the US-VISIT's OBIM program [6] and the FBI's NGI service [7]. The main usage of fingerprint alteration [8] is to slip away identification using techniques varying from corrosion/searing (acids, alkalis, etc.), burning (using acid or fire), cutting (incisions, tearing or paring of skin), defacement of patterns and scrape/abrading (scratchy devices) fingers to performing plastic surgery (see Fig. 2). The altered fingerprints, that used to mask one's identity, constitute a serious "attack" against a border control biometric system. There is always need a matcher to distinguish a person is authentic or not.

The altered fingerprints are different from fake fingerprints. The fake finger can be made of glue, latex, or silicone and it can be used as a best method to evade fingerprint systems. Altered fingerprints are real fingers that are used to hide one's identity in order to find away round the identification by a biometric system whereas the fake fingers are typically used by individuals to adopt another person's identity. Many software [13] and hardware [14] solutions have been proposed to detect fake fingers attack. The fingerprint problems has not been studied in the literature and there are no reported techniques to identify those problems until the point in time under discussion. The lack of public databases of altered fingerprint images has interfere with research in this area



**Fig. 2. Picture of altered fingerprints. (a) Transplanted friction ridge skin [9]. (b) Bitten fingers [10]. (c) Acid burning [11]. d) Stitched fingers [12].**

Since HIS also needs other doctors from other hospitals also for major consultation, doctor identification system must be reliable. Those type of alterations can be occurred to the fingers naturally, means it's not happened intentionally. This paper is proposed to implement an automatic detection algorithm in a fingerprint matcher. Its highlight's the analysis and matching of the altered fingerprints, importance of the alteration problem, and also to use an automatic detection algorithm proposed [2].

The automatic matcher used in identification applications must satisfy the following two requirements:

- 1) The algorithm used must be extremely fast in order to attain the throughput requirement of the system. That means, computational burden of the matcher shouldn't be increased by that algorithm. Recently NGI (Next Generation Identification) matcher is used, since today's society demands more faster and advanced identification technologies. It shows that the extraction of minutiae and rules for making decisions used to match the altered fingerprints automatically, must be simple.
- 2) The matcher algorithm should work at a very low FPR (False Positive Rate).

This paper provide two prototypes, an echograph system and a fingerprint matching system, to be embedded into an HIS.

## **II. Related Works**

The ubiquitous services concept was included in HIS [1] to meet the social demands of society. In that paper, the authors embedded a medical device into hospital by the help of LAN network. They implemented two prototypes: a ubiquitous echograph system and a networked digital camera.

The healthcare services of hospitals in uses barcode checkup system to identify target patient, utilizes CCD to read it. Server ensures quality of picture by the help of QA approaches. It's applicable inside hospital networks.

The problem of altered fingerprints has not been studied in the literature and there are no reported techniques to identify them. The lack of public databases has limited research in this area. The altered fingerprint analysis and detection concept [2] was developed by S.Yoon, J.Feng, A.K.Jain. They introduced this paper to meet the needs of law enforcement agencies and other areas where the fingerprint authentication is crucial. The algorithm introduced provide more good quality of fingerprint images so it makes featureextraction simpler. They classified the altered fingerprint into 3 types and also found the countermeasures for each one.

The NFIQ algorithm [28] is provided by NIST in order to improve quality of altered fingerprints, but it's not suitable for detecting altered fingerprints, especially the distortion and imitation types.

The feature extraction based on ridge flow orientations introduced in [3] is a reliable and robust algorithm. The authors of paper provides a new segmentation approach, enhancement of the skeleton image and, quantitative evaluation of performance.

### III. Background

Some of the important cases that lead to implementation of a reliable fingerprint detection mechanism are given below.

In 1933, Gus Winkler who was a murderer and bank robber, was found to have fingerprint alteration on his left hand (except for the thumb) by tearing the flesh of the fingers (strip of skin down from center of finger is removed) [8] . That is, the pattern type of a finger was altered from double loop to left loop. In 1934, John Dillinger, who was a bank robber, choose corrosive acid to burn his fingertips (Fig.3) [8]. Another one is Jack Kluta's defacement of patterns by slashing across finger, but it's not effectual compared to others [8]. In 1941, Roscoe Pitts who was a criminal, had a plastic surgery to replace his fingertips skin with skin grafts from his chest [16]. The plastic surgeon revealed his original identity when he was arrested by police and confirmed when his joints were also matched with original fingerprint card.

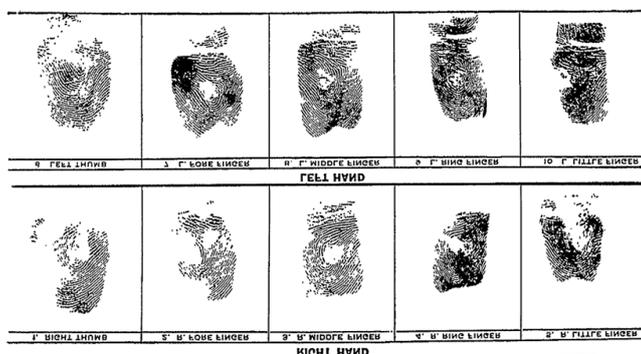


Fig 3. Partial Obliteration of Patterns in Fingerprints of Dillinger [8].

In 1995, Jose Izquierdo uses the name Alexander Guzman was found to have obfuscated fingerprints and arrested by Florida officials for using a false passport. Later they found that the reconstructed fingerprint of Guzman were resembles to fingerprints of Izquierdo who was an escaping drug criminal [15]. His mutilation process of fingerprint consisted of 3 steps: A "Z" shaped cut is made on the fingertip, then two triangular skin patches are lifted and switched, and stitching them back to the fingertip. In 2005, Marc George who was a drug dealer, was arrested because his limping gait as a result of surgery raised the curiosity of border officials (see Fig. 1a) [16].

In 2009, a woman successfully slipped away the Japanese immigration AFIS [17]. The scars on her hands by surgically swapping fingerprints of her left and right hands made the police suspicious and she was originally arrested for making a fake marriage license.

It has been reported by EURODAC [18], a European Union-wide fingerprint system, that hundreds of asylum seekers (someone who leaves their own country, often because of war or for political reasons and who travels to another country hoping that the government will allow them to live there and will protect them) had abraded, burned and cut their fingertips to prevent identification [19], [20]. Table 1 lists fingerprint alteration reported cases.

It is not very easy to calculate the actual number of individuals who have successfully slipped away fingerprint systems identification as a result of fingerprint alteration, even though there is not a large number of publicly disclosed cases of altered fingerprint. Almost all the people identified as having their fingerprints altered were not detected by AFIS [2], but they were detected by some other means [16], [17].

So it's important to introduce a matcher in order to identify the authentic person and thus helpful to detect suspects also. Because burning of fingers or other alteration of fingers can be occurred unintentionally or accidentally.

#### IV. Ubiquitous Echograph

An echograph is the most popular medical imaging devices. An echograph is a computer based system in which a computation unit, a display unit and a sensing unit, is connected by internal network named a bus, as in the composition of Siemens ACUSON P50 ultrasound system [21]. In this the medical device is embedded by replacing the bus with the information network supporting the HIS.

The system that already existing, consists of server software, mobile probe unit, and a display unit. The mobile probe obtains echo signals and then sends it via Wi-Fi. The server software in an HIS server reconstructs the echogram and then sends it to the display (PC or PDA terminal or wearable PC or any TV set connected to the intra-hospital cable TV). Also in the proposed paper if the patient has any echographs with themselves then they can send the results via Wi-Fi to the doctor whom with them registered already (Fig.4, an example).



Fig.4. Accu – chek glucometer readings can transfer to personal computer.

A medical doctor only needs to bring a mobile probe in his/her pocket in order to diagnose the patient with echograms at their bedside [1]. And, the hospital can easily update echograph functions by upgrading the server software; even 3-D echogram can be used when the hospital equips stereo displays. Same way patients can register to the hospital site by taking appointment of the corresponding doctor by paying through online transaction.

So if patients have needed echograph with them then they can send the test result to corresponding doctor through this site. Thus, this system increases mobility of the doctors. And also decreases load of the patients to move to doctor’s diagnostic room and also decreases maintenance cost of the hospital.

A new prototype was developed as shown in Fig. 5, based on the some prototypes established earlier [22].

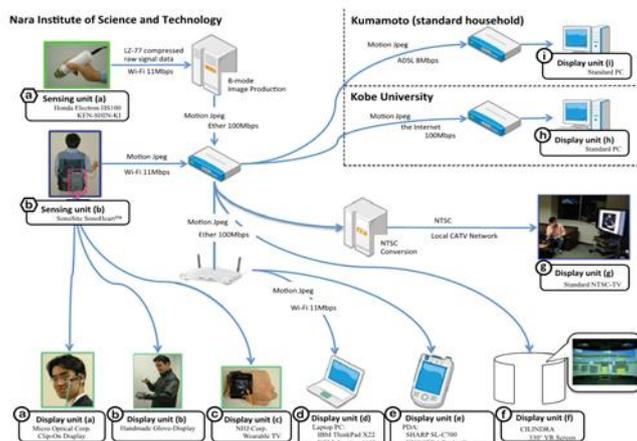


Fig. 5. Ubiquitous echograph prototype [22].

#### V. Altered Fingerprint

Based on a database of altered fingerprints available, altered fingerprints are classified into 3 types: a) obliteration, b) distortion, and c) imitation (see Figs. 6, 7, and 8).

##### A. Types of Altered Fingerprints

The altered fingerprints can be classified into 3 categories based on the changes in ridge pattern due to alteration. This categorization is done in following manner: 1) first try to getting a better understanding of thenature of alterations, 2) by modelling well-defined subcategories detecting altered fingerprints, and 3) for altered fingerprint restoration some methods are developed

**Table 1** Categorization of 50 Altered Fingerprints in Database

Type	Obliteration		Distortion		Imitation
	Scar	Mutilation	Z-cut	Transplantation	
No: of images	14	17	7	9	4

**A.1 Obliteration**

Friction ridge patterns on fingertips can be obliterated (its structure is rarely visible) by, cutting [8], abrading [26], burning [23], [19], [20], transplanting smooth skin [16] and applying strong chemicals (Fig. 2c). Some factors such as side effects of a cancer drug [24] and skin disease (for example leprosy [25]) can also obliterate fingerprints. From Table 1, obliteration appears to be the most used form of alteration. It's may be because obliteration type completely destroys ridge structures in fingers, which is much simpler to perform than other types which requires a surgical procedure. And also, detecting distorted or imitated fingerprints is very much difficult for human examiners.

Obliterated fingerprints can slip away the usage of fingerprint quality control software, based on the area of the damage occurred in finger. The existing fingerprint quality assessment softwares may fail to detect the affected finger area as an altered fingerprint if it is small, but AFIS [7] can correctly match the affected fingerprint to the original mated fingerprint (Fig. 6). But, if the altered area is much large, then that quality control software can easily detect the finger damage.



**Fig. 6. Fingerprint obliteration - Example of scar**

**A.2 Distortion**

Friction ridge patterns on fingertips can be damaged into unnatural ridge patterns [12], [15] replacing some portions with friction ridge skin from the sole or palm or by removing some portions of skin from a fingertip and placing back in different positions. These type of fingerprints has unusual ridge patterns, as compared to natural fingerprints. These abnormalities include changes in orientation field along the scars in fingers or abnormal spatial distribution of singular points.

Even though the global ridge pattern of finger is abnormal the distorted fingerprints can also pass the fingerprint quality test because their local ridge structure is similar to natural fingerprints. By swapping skin patches within the same finger, to form a distorted fingerprint, that retains the same ridge property over the entire fingerprint.

Fingerprints altered by “Z” cut can retain their original ridge structure, which enables the reconstruction of the original fingerprint before alteration happens. Once it's detected, the operations that may be performed to assist AFIS can be done as following way: 1) first to identify unaltered regions of the fingerprint and then manually mark the features like the minutiae in these regions and 2) after that reconstruct the original fingerprint as in the “Z” cut case [15].

**A.3 Imitation**

Friction ridge patterns on fingertips can keep fingerprint-like pattern after fingerprint alteration: 1) ridge skin from other parts of the body can be used to fill the removed part of the fingertip to make it as natural with the remaining ridge structure, 2) another way is transplantation of the entire fingertip, or 3) after removing a portion of the finger, the remaining skin is stitched together. By swapping the skin on fingertips between the left and right hands successfully slipped away AFIS [17]. Imitated fingerprints can startle human examiners and they cannot successfully pass the fingerprint quality assessment software.

## B. Automatic Detection of Altered Fingerprint

It's very hard to detect imitated and distorted fingerprints for any fingerprint image quality assessment algorithm (based on analysing local image quality). This section considers the problem of automatic alteration detection based on minutiae distribution and analysing ridge orientation field. The flowchart of the alteration matcher that implemented in this paper is given in Fig. 7.

### B.1. Analysis of Orientation Fields

Orientation field defines the ridge flow of fingerprints. It is described as the local ridge orientation in the range  $[0, \pi)$ . Except in the region

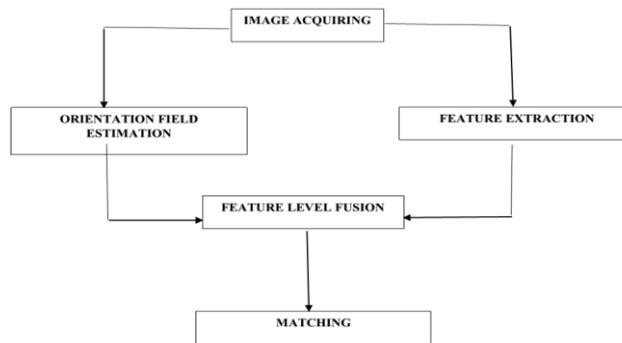


Fig. 7. Flow chart of the algorithm introduced

Near singular points like core and delta, good quality fingerprints have a smooth orientation field. The global orientation field model represents arch-type fingerprints that do not have any singularity, as well as, the overall ridge orientation field except singularity region in fingerprints. The difference between the observed orientation field and the model will be nonzero around the singular points, if the global orientation field model is only used for orientation field approximation. The model fitting error is observed in the altered region for obfuscated fingerprints. So the difference between the orientation field approximated by the model as a feature vector and the observed orientation field extracted from the fingerprint image is used for classifying a fingerprint as natural or altered one. The main steps in the proposed algorithm are described below:

1. Orientation field computation: - By using ratha method, the orientation field of the fingerprint,  $\theta(x,y)$ , is computed [3]. The first orientation field is smoothed by  $16 \times 16$  (an averaging filter), then followed by averaging the orientations in  $8 \times 8$  pixel blocks. A morphological process for removing isolated blocks and filling holes is performed.
2. Feature extraction: - Locate the ridges using peaks and variance in the projection.
3. Smoothing of directions: -The ridges are thinned and skeleton obtained is enhanced.
4. Minutiae distribution analysis: - Triplet orientation of minutiae is obtained.

#### B.1.1 Orientation Field Approximation

Fingerprint can be regarded as an oriented texture form. The optimal dominant ridge direction in each  $16 \times 16$  block is calculated by using the orientation field. Let  $\theta(x,y)$  be the orientation field. Steps used in orientation field computation is given below:

- (1) The gradient of the smoothed block, at pixel  $(i,j)$  is calculated. Let  $G_x(i,j)$  and  $G_y(i,j)$  be the gradient magnitude in x and y directions.
- (2) Obtain the dominant direction in a  $16 \times 16$  block using the following equation:

$$\theta_d = \frac{1}{2} \text{Atan} \frac{\sum_{i=1}^{16} \sum_{j=1}^{16} 2G_x(i,j)G_y(i,j)}{\sum_{i=1}^{16} \sum_{j=1}^{16} (G_x(i,j)^2 - G_y(i,j)^2)}$$

$$G_x \neq 0, G_y \neq 0 \quad (1)$$

The dominant direction computation is trivial if either  $G_x$  or  $G_y$  is zero ( $0^\circ$  or  $90^\circ$ ).  $\theta_d$  is quantized into 16 directions.

#### B.1.2 Feature Extraction

Consider a  $16 \times 16$  pixels image window and its projection in the direction perpendicular to the window orientation field. The centre of the ridge is the peak in the projection. The projection waveform helps the ridge

pixels detection. The image is smoothed before projection. Two neighbouring pixels on either side of the peak are held along the direction orthogonal to the orientation field. This approach is much better than the locally adaptive thresh holding scheme [27]. Because, the thresh holding scheme doesn't use any directional information and only use a window to check that at least one ridge and valley is included in window at every pixel. A value "1" is allotted for ridge pixels and "0" is allotted to other ones. The altered fingerprint's ridge flow can be discontinuous in non-singular regions such as severely distorted ridge areas, scarred areas (Fig. 6), and mutilated areas.

This approach to represent the global orientation field, is computationally efficient and also provides a good performance compared to other thresh holding schemes.

### **B.1.3 Smoothing of Directions**

Directional smoothing is applied to smooth the ridges. A mask is placed along the each window's orientation field. The number of 1's in the mask area can be counted. The ridge point can be held only if the number of 1's is greater than the 25% of total pixels.

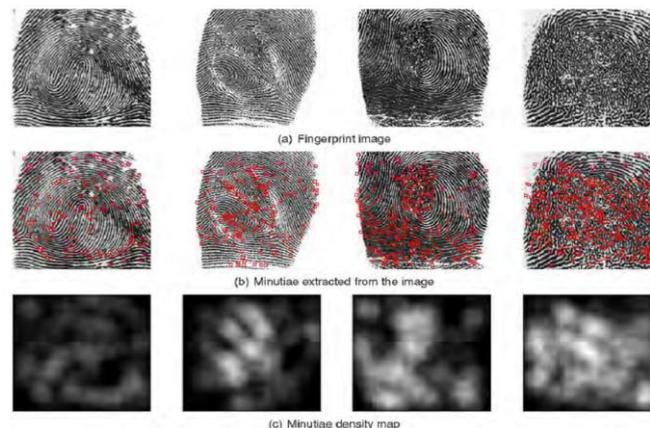
### **B.2. Analysis of Minutiae Distribution**

A minutia in the fingerprint indicates some ridge characteristics, for e.g. ridge bifurcation or ridge ending. The minutiae is used by almost all fingerprint recognition systems for matching. The minutiae distribution of altered fingerprints often differs from that of natural fingerprints.

Minutiae points can be placed in skeleton image easily. In the window, a ridge end point has only one neighbour and ridge bifurcation has 3 neighbours. So the counts of neighbours are sufficient for locating the ridges.

Fig. 8 shows the minutiae density maps of natural and 3 altered fingerprints. In the natural fingerprint, minutiae are well distributed almost uniformly.

In the altered fingerprints, the distributions of minutiae are quite different: 1) due to ridge discontinuity many minutiae are extracted along scars and in the obliterated region, and 2) when a new ridge-like pattern is formed after alterations an excessive number of minutiae appear. That means the minutiae distribution can be used for altered fingerprints detection



**Fig. 8. Minutiae density map. Column 1: Natural fingerprint. Column 2: Distorted fingerprint with more minutiae along scars. Column 3: Obliterated fingerprint with more minutiae distribution in the altered area. Column 4: Obliterated fingerprint with more minutiae distribution over the entire altered area.**

### **B.3 Fingerprint Matching**

Minutiae-based techniques is used for checking fingerprint matching in order to align two sets of minutiae points and also to determine the total number of matched minutiae.

The minutiae count obtained between the observed feature extraction of the model that used for registration and the calculated feature extraction count of the fingerprint that used for login is compared. If their count is almost similar then the login will be successful even if its altered otherwise it will be declared as invalid user (Fig.9).

## **VI. Evaluations**

The altered fingerprint database contains 50 fingerprints. When the fingerprintness of an input image is lesser than a threshold value, the system indicates that the image is an altered fingerprint. If this image is surely an altered fingerprint, it is viewed as a true positive; otherwise, it is viewed as a false positive. Same way, true

negative shows that a natural fingerprint is rightly sorted as natural and false negative shows that an altered fingerprint is not found as altered. The performance of proposed algorithm is much better than other matchers [TABLE 2].

The Receiver Operating Characteristic (ROC) curves can be used to evaluate the quality of the proposed approach [2]. Both distorted and obliterated fingerprints can be found by the proposed algorithm at same accuracy, while NFIQ [28] can only identify obliterated (Fig.9). But both of these algorithms are not accurate for finding imitated fingerprints.

The performance of the proposed matcher can be evaluated by checking similarity of the computed minutiae with minutiae obtained from same image by an expert. An example of the output obtained by fingerprint matcher is shown in Fig.9.

**Table 2. Shows the execution time of some algorithm steps.**

Step	Time(s)
Minutiae Extraction	5
Triplet formation	8
Matching checked	1.25

It's not like that the proposed algorithm can find out all of the altered fingerprints. That is because it's too hard to find out proof of the alteration if the altered area is too short. It can be observed that, in the case of imitation, the structure of ridge is raw even at boundary.

FPR are occurred due to a) poor quality of fingerprint, leads to incorrect feature extraction, and b) error occurred during manual checking (ground truth error). So alarms can be raised when image quality is poor since a) it needs to be checked manually and b) there is also a chance for criminals to present poor quality fingerprint purposely.



**Fig.9. matching checked for unaltered and scarred fingerprint**

### VII. Discussions

The echograph prototype conveys that even medical equipment can be embedded into HIS as the standard PC terminal and standard TV set presents sufficient quality of image. The prototype shows various combinations.

When a medical system is embedded into HIS, the system can use gigantic computational power of HIS via a sensor unit. For example, embedded echograph may provide a cardiac output, even though the prototype provides a Brightness-mode image. And also, once the server software is upgraded, all the sensor units enjoy the updated function. It is one of the best results of the embedded system.

The technological advances that take place recently make the echograph concept more realistic. The medical device such as GE Vscan [29] enable diagnosing at the bed side, and SonoSiteNanoMaxx [30] can be used by physicians to store obtained echogram to PACS servers. Various medical equipment like an electrocardiograph, a saturation monitor and a blood glucose meter, are connected over Bluetooth or Zigbee for monitoring purposes [31], [32].

### VIII. Conclusion And Future Works

This paper proposed to develop two prototypes: A ubiquitous echograph and a fingerprint scanner.

The echograph that can be implemented in a hospital or that can be used by a patient / doctor is very helpful for reducing the working load of the doctors and also due to recent technologies it's easier to update the server software in HIS with less maintenance cost. Patient's doesn't need to wait in front of doctor's room for consulting them in simple cases, that is patient can directly face doctor for only emergency cases.

The fingerprint spoofing (is an individual uses a fake fingerprint to adopt the identity of another one) is entirely different the problem of fingerprint alteration or obfuscation. The spoofing problem was included in the literature study, but the obfuscation problem was not provided in the biometric literature, even though there were a numerous cases of fingerprint alteration for the purpose slipping away identification is present.

This paper introduced the problem of fingerprint alteration and threat of altered fingerprints is analysed. Because of that the NFIQ [28] lacks the ability in distinguishing altered and natural fingerprints, an automatically detecting altered fingerprints algorithm was developed based on the characteristics of the minutiae distribution and fingerprint orientation field. This algorithm satisfies the 2 requirements for alteration detection algorithm: a) fast operational time and, b) ease of integration into AFIS/NGI.

This paper can be enhanced future along the following ways:

1. Automatically determining the alteration type so that countermeasures can be taken during that time.
2. Reconstructing altered fingerprints: - Reconstruction is possible for some types of altered fingerprints where the ridge structure is present on the finger but at a different location or the ridge patterns are damaged locally.

## References

- [1] T. Kuroda, H.Sasaki, T.Suenaga, Y.Masuda, Y.Yasumuro, K.Hori, N.Ohboshi, T. Takemura, K. Chihara, H. Y oshihara, "Embedded Ubiquitous Sevices on Hospital Information System", vol.16, no.6, pp 1216-1223, 2012.
- [2] Soweon Yoon, Jianjiang Feng, Anil K. Jain,Fellow, " Altered Fingerprint : Analysis and Detection", vol.34, no.3, pp 1-14,2012.
- [3] Nalini K. Ratha, Shaoyun Chen and Anil K. Jain, "Adaptive Flow Orientation-based Feature Extraction In Fingerprint Images", vol.28, no.11, pp 1657-1672, 1995.
- [4] M. Weiser, "Some computer science issues in ubiquitous computing,"Commun. ACM, vol. 36, no. 7, pp. 75–84, 1993
- [5] J. E. Bardram, "Pervasive healthcare as a scientific discipline," Methods Inf. Med., vol. 3, no. 47, pp. 129–142, 2008
- [6] The U.S. Department of Homeland Security, US-OBIM, <http://www.dhs.gov/obim>, 2013
- [7] The Fed. Bureau of Investigation (FBI), Next Generation Identification (NGI),<http://www.fbi.gov/about-cs/cjis/fingerprints-biometrics/ngi>, 2013.
- [8] H. Cummins, "Attempts to Alter and Obliterate Finger-prints", J. Am. Inst. Criminal Law and Criminology, vol. 25, pp. 982-991, 1935.
- [9] Surgically Altered Fingerprints, <http://www.clpex.com/images/feetmutilation/14.jpg>, 2011.
- [10] K.Singh,AlteredFingerprints,<http://www.interpol.int/Public/Forensic/fingerprints/research/alteredfingerprints.pdf>, 2008.
- [11] M. Hall, "Criminals Go to Extremes to Hide Identities," USA Today, [http://www.usatoday.com/news/nation/2007-11-06-criminal-extreme\\_N.htm](http://www.usatoday.com/news/nation/2007-11-06-criminal-extreme_N.htm), Nov. 2007
- [12] CriminalsCuttingoffFingertipstoHideIDs,<http://www.thebostonchannel.com/news/15478914/detail.html>, 2008
- [13] A. Antonelli, R. Cappelli, D. Maio, and D. Maltoni, "Fake Finger Detection by Skin Distortion Analysis,"IEEE Trans. Information Forensics and Security,vol. 1, no. 3, pp. 360-373, Sept. 2006
- [14] K.A. Nixon and R.K. Rowe, "Multispectral Fingerprint Imaging for Spoof Detection," Proc. SPIE, Biometric Technology for Human Identification II,A.K. Jain and N.K. Ratha, eds., pp. 214-225, 2005
- [15] K. Wertheim, "An Extreme Case of Fingerprint Mutilation," J. Forensic Identification,vol. 48, no. 4, pp. 466-477, 1998.
- [16] History of Fingerprint Removal, <http://jimfisher.edinboro.edu/forensics/fire/print.html>, 2011.
- [17] Surgically Altered Fingerprints Help Woman Evade Immigration, <http://abcnews.go.com/Technology/GadgetGuide/surgicallyaltered-fingerprints-woman-evade-immigration/story?id=9302505>, 2011.
- [18] EUODAC:aEuropeanUnionWideElectronicSystemofAsylumSeekers,[http://ec.europa.eu/justice\\_home/fsj/asylum/identification/fsj\\_asylum\\_identification\\_en.htm](http://ec.europa.eu/justice_home/fsj/asylum/identification/fsj_asylum_identification_en.htm), 2011
- [19] SwedenRefugees Mutilate Fingers, <http://news.bbc.co.uk/2/hi/europe/3593895.stm>, 2004.
- [20] Asylum Seekers Torch Skin off Their Fingertips So They Can't Be ID'd by Police, <http://www.mirror.co.uk/sunday-mirror/2008/06/29/asylum-seekers-torch-skin-off-their-fingertips-so-they-cant-be-id-d-by-police-98487-20624559/>, 2008
- [21] Siemens. (2008). ACUSON P50 ultrasound system[Online]. Available: [http://www.siemens.pl/upload/images/Acuson\\_P50.pdf](http://www.siemens.pl/upload/images/Acuson_P50.pdf)
- [22] Masuda, M. Naganawa, H. Sasaki, T. Suenaga, A. Yutani, Y. Yasumuro, M. Imura, Y. Manabe, O. Oshiro, and K. Chihara, "Ubiquitous tele-echography system: Down-sized wearable ultrasound probe with distributed processors and displays," Biocybern. Biomed. Eng., vol. 27, no. 1, pp. 247–251, 2007
- [23] Woman Alters Fingerprints to Deceive Taiwan Immigration Fingerprint IdentificationSystem,<http://www.zaobao.com/special/newspapers/2008/10/hongkong081002r.shtml>, (In Chinese), Oct. 2008.
- [24] M. Wong, S.-P. Choo, and E.-H. Tan, "Travel Warning with Capecitabine,"Annals of Oncology,vol. 20, p. 1281, 2009.
- [25] M.V. de Water, "Can Fingerprints Be Forged?,"The Science NewsLetter,vol. 29, no. 774, pp. 90-92, 1936.
- [26] J.W. Burks, "The Effect of Dermabrasion on Fingerprints: A Preliminary Report,"Archives of Dermatology,vol. 77, no. 1, pp. 8-11, 1958.
- [27] M. R. Verma, A. K. Majumdar and B. Chatterjee, Edge detection in fingerprints, Pattern Recognition 20(5), 513- 523 (1987).
- [28] E. Tabassi, C. Wilson, and C. Watson, "Fingerprint ImageQuality," NISTIR 7151, [http://fingerprint.nist.gov/NFIS/ir\\_7151.pdf](http://fingerprint.nist.gov/NFIS/ir_7151.pdf), Aug. 2004.
- [29] G.Healthcare.(2011).Vscanlet'stakealook.[Online]. Available:<http://vscanultrasound.gehealthcare.com>.
- [30] SonoSite.(2012).NanoMaxxultrasoundmachine.[Online]. Available:<http://www.sonosite.com/products/nanomaxx>.
- [31] J. S. Kim, B. O. Kim, and K. S. Park, "Development of HIHM (HomeIntegrated Health Monitor) for ubiquitous home healthcare," inProc. Int.Conf. IEEE Eng. Med. Biol. Soc., Lyon, France, Aug. 2007, pp. 363–365.
- [32] W. Y. Chung, Y. D. Lee, and S. J. Jung, "A wireless sensor network compatible wearable u-healthcare monitoring system using integrated ECG, accelerometer and SpO2," inProc. Int. Conf. IEEE Eng. Med. Biol.Soc., Vancouver, Canada, Nov. 2008, pp. 1529–1532.