Automatic Detection of Altered Fingerprints

P. Velayutham, Dr. V. Vijayalakshmi

Abstract— Fingerprints have always been the most practical and positive mean of identifications. Offenders being well known of this have been coming up with many ways to escape identification by that mean. Erasing left over fingerprints, using gloves, fingerprint forgery are certain examples of methods tried by them over last few years. Failing to prevent themselves, they moved to an extent of fingerprint Obfuscation by altering their finger ridge flow pattern. These articles based on obliteration, Distortion and imitation of fingerprint ridge pattern and discuss some encountered fingerprint altered cases in chronological order: Analysis of altered fingerprints using available NIST SD 4 Database and types of alteration recorded by the various law and enforcement and border security agencies.

Index Terms – Fingerprints, AFIS, obfuscation, alteration, ridge pattern, minutiae distribution,

I.INTRODUCTION

Fingerprint recognition has been used successfully in law enforcement agencies to identify intruders or suspects for almost 100 years. The success of fingerprint recognition system in accurately identifying individuals has allowed some persons to engage in extreme measures for the purpose of evading the Identification system. The primary objective of fingerprint alteration is to escape from identification using techniques varying from scrape or wear away by rubbing the fingerprint ridge flow and burning the fingers and performing plastic surgery. The use of altered fingerprints is to mask one’s identity to give series attack against a border control biometric system since, it defeats the very purpose of which the system was designed. In order to detect attacks based on fake fingerprints, many software and hard ware has been proposed. However the problems of altered fingerprint has not been studied in the literature and there are no techniques are available to detect the altered fingerprints. Fur thermore, the lack of public data bases of altered fingerprints has an obstruct to the research in this area. This Altered fingerprint attack in biometric system is known as biometric obfuscation. The obfuscation can be defined as a deliberate attempt by an individual’s to mask his identity from a biometric system by altering the biometric characteristics of a person prior to its acquisition by the system. Mutilating or destroy the ridges of one’s fingerprints by abrasive materials. Perturbing or disordering the texture of the iris by wearing theoretical lenses and altering the facial attributes such as nose and lips by plastic surgery are the some of the examples of biometric obfuscation. As we know that fingerprint based biometric system are used in large scale in the country like India having large populations in comparisons with other biometric systems since, it is simple and fast. The altered fingerprints are being encountered by law enforcement and immigration agencies in several countries and there by underscoring the urgency of finding solution to this problem. Developing an automatic solution to detect altered fingerprint is the first step in defeating fingerprint alteration. Open source NFIQ (NIST Fingerprint Image Quality) software may be useful in detecting altered fingerprint and this software algorithm designed to examine 1) if an image contains sufficient information for matching. 2) They have limited capability in detecting if an image is a natural fingerprint or altered fingerprint. If an altered fingerprint is encountered in the system, the automatic detector must satisfy the following requirements 1) the algorithm must be extremely fast. 2) Feature extraction and detection rule used to automatically detect altered fingerprint must be simple.3) It must operate with very small false positive rate say 1% or lower. 4) Detector should be easily integrated into any AFIS (Automatic fingerprint identification system).

II HISTORY OF FINGERPRINT ALTERATION

A. A case study- Criminal cases

Case 1: In 1993, Gus Winkler, a murder and bank robber was found to have altered the fingerprints of all the fingers of his left hand except the thumb by slashing and tearing the flesh of the fingers. He performed that act on all of his left hand fingers, except for the thumb. It was believed that he took inspiration from a previous accidental cut to his right index finger. Moreover, the left middle finger seemed to have been altered in a way to change the whorl pattern in to loop indicating prior planning as shown in figure 1.

Fig. 1 Inked impression of Gus Winkler before and after mutilation of his left middle finger

Case 2: Moving to another interesting example of fingerprint alteration, it was the case of John Dillinger, a famous Chicago bank robber who tried to change his fingerprints as shown in fig 2. and hide his identity by burning off his fingers, back in 1934, Dillinger made cut to his fingers and poured sulfuric acid in to his all fingers, in order to remove the ridge patterns and make the fingerprints unidentifiable, but the ridge patterns
reappeared after a while, through the identification was made on the basics of the unaffected peripheral areas was still intact. Dillinger was dead by the Chicago police in July 1934.

Fig 2. Image showing the fingerprint patterns from John Dillinger, after alteration, the centre of the ridge pattern shows the obliteration

Case 3: In 1941, Robert J. Philips, had all his fingers sutured to his chest for some week that the skin of his fingertips gets smoothened, erasing the ridge patterns on them. He had a long criminal history and committed various burglaries and bank robberies. He served sentence at a point in time but again, was released due to lack of evidence. To escape from his past criminal record, keep committing crimes and not convicted; he visited a physician in New Jersey, who performed a painful surgery on Phillip’s fingers replacing the finger skin from his chest as shown in fig 3. Philips was still identified, on the basics of the unaltered areas on his fingertips and pattern on the second joint of his fingers.

Fig. 3. Shows J. Philips’s fingers transplanted with his chest skin and smoothened.

Case 4: In 1995, a man using the name Alexander Guzman, arrested by Florida officials for processing a false passport, was found to have obfuscated fingerprints. After a two weeks search based on manually reconstructing the damaged fingerprints and after comparing a 70 million records, the reconstructed fingerprints of Alexander Guzman were linked to the fingerprints of Jose Izquierdo who was an abscording drugs criminals.

Case 5 & 6: In 2005, a drug dealer named Marc George was arrested because of his limping gait as a result of surgery caught the attention of border officials. In 2007, a man arrested for vehicle theft and found that he had changed his fingers by obliteration. When he is in the custody of Massachusetts State police, he tried to mutilate his finger ridge pattern by chewing off centre portion of his finger tips, as shown in fig. 5. In order to escape conviction and another man named Mateo Cruz-Cruz found to have blackened fingerprints as a result of applying acid as shown in fig. 5.

Case 7: In 2008, a man called Edgardo Tirado was detained by Lawrence Police in the U.S., he had stitches on all his fingers and both thumbs, he explained the Police that it was the result of a fight with another man who attacked him and cut all his fingers with a knife, but later, it was found that the person was George Perez and not Edgardo Tirado and stitches on his fingers resulted from the procedure he got performed in the Dominican Republic, to modify his fingerprints and the altered image of George Perez is shown below.

Fig. 4. Image showing the before and after altered finger prints of Jose Izquierdo

Fig. 5. The bitten and acid applied fingerprints
Fig. 6. The stitched fingerprints of George Perez

B. A Case study - Non criminal cases:

It is not just the criminals who have been found to alter their fingerprints. In 2009, a woman successfully evaded the Japanese immigration AFIS by surgically swapping of her left and right hands. Although she was originally arrested for faking marriage license, scars on her hands made the police suspicious. Finger print alteration has even been performed at a much larger scale involving group of individuals. It has been reported that hundreds of asylum seekers had cut, abraded and burned their fingers tips to prevent identification. Although the number of publically disclosed cases of altered fingerprints is not very large, it is extremely difficult to estimate the actual number of individuals who have successfully evaded identification by fingerprint system as a result of fingerprint alteration. Almost all the people identified as having altered their fingerprints were not detected by AFIS, but some other means the altered fingerprints are detected. The different altered fingerprint cases are listed below.

<table>
<thead>
<tr>
<th>Case</th>
<th>Year</th>
<th>Alteration type</th>
<th>Description of alteration</th>
</tr>
</thead>
<tbody>
<tr>
<td>A woman at a border crossing</td>
<td>2007</td>
<td>Obliteration</td>
<td>A surgery was performed on her fingertips to make strange pattern</td>
</tr>
<tr>
<td>A woman was attempt to evade</td>
<td>2008</td>
<td>Obliteration and distortion</td>
<td>Thumb print was altered by laser surgery</td>
</tr>
<tr>
<td>Taiwan border security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asylum seeker enter in Europe</td>
<td>2008</td>
<td>Obliteration</td>
<td>Their fingertips was abraded and burned</td>
</tr>
<tr>
<td>A woman attempting to evade</td>
<td>2009</td>
<td>Imitation</td>
<td>Friction skins from thumbs and index fingers were swapped between left and right hands</td>
</tr>
<tr>
<td>the Japanese border control</td>
<td></td>
<td></td>
<td>system</td>
</tr>
<tr>
<td>system</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Three people charged with</td>
<td>2010</td>
<td>Obliteration</td>
<td>A physician, a broker and a patient were involved in a finger print alteration.</td>
</tr>
<tr>
<td>fingerprint alteration</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1: Non criminal cases encountered in various Finger print identification System

C. Recent Cases in Altered Fingerprints

A Dominican man allegedly tried to get by custom and Border protection anti terrorism in Boston by altering his fingerprints. Freddy Davila was arrested on June 9th of 2011, said customs and border protection in a statement released on 29th, while he was trying to board a flight from Boston to Santo Domingo in the Dominican Republic. He was stopped and questioned by CBP officers who found his fingerprints had been intentionally altered to avoid law enforcement identification. Davila was arrested by the CBP officials, said the agency.

Jose Elias Zaiter-Pou, 62, pleaded guilty of conspiring to conceal illegal aliens from detection by law enforcement authorities, by surgically altering their fingerprints in exchange for payment. He was sentenced to a year and one day of imprisonment, followed by deportation and three years of supervised release. Authorities said Zaiter-Pou met at a hotel in Woburn, Massachusetts, with a government informant who was posing as an illegal alien, and agreed to alter the informant’s fingerprints for $4,500. The doctor brought surgical equipment, antibiotics and pain medication to the meeting, which was secretly recorded. Zaiter-Pou described how he would surgically remove a portion of the fingertip, then suture the tip back together to make a new, unrecognizable fingerprint.

Feds arrest Lynn woman in fingerprint altering scam. LYNN - Federal agents say a Lynn woman, a Dominican doctor and another man altered fingerprints to conceal illegal aliens, charging $4,500 for surgeries conducted in hotel rooms. Luz Martinez-Lebron, 41, of Lynn, was charged this week by the United States Attorney with conspiracy to conceal and shield illegal aliens from detection along with Jose Elias Zaiter-Pou, 61, a physician with a clinic in the Dominican Republic, and Ricky Dario Baez-Cruz, 29, also a Dominican. The three made an initial appearance in U.S. District Court Wednesday and are scheduled to return to court Tuesday for detention hearings. If convicted, they each face 10-year maximum sentences followed by three years supervised release time and up to a $250,000 fine. The trio’s arrest is the latest case of fingerprint alteration to surface in local courts.

III. ANALYSIS OF ALTERED FINGERPRINTS

With the background of the altered fingerprints and Based on the Data base available by law enforcement agencies we first analyze the altered fingerprints before the methods to be used to detect the altered fingerprints. We first discuss 1) the impact on fingerprint alteration on the matching performance using the existing Database. 2) Classify the altered fingerprints in to three categories namely Obliteration, Distortion and Imitation. 3) assess the utility of an existing fingerprint quality measures in terms of altered fingerprints detection. The data base contains 4433 altered fingerprints 535 ten print cards of 270 subjects from. Not all of the 10 fingers in a ten print card may have been altered. In the altered finger distribution 57% of ten print cards all 10 finger prints were altered; 85% of the
ten prints card have more than 5 fingers altered. A total of 87 subjects out of 270 subjects have multiple ten print cards due to multiple arrests. Fingerprint alteration is a serious threat to automatic finger identification systems since fingerprints is a invariant biometric identity during one’s life time. To establish a reference line NIST SD 4 special database which contains 2000 fingers with two impressions per fingers were used to obtain genuine and imposter match with 1335 altered finger prints using Verifinger SDK. Fig below shows the score distributions for pre/post altered finger prints pair matches according to type and genuine and imposter matches in NIST SD 4.

The following observations are noted.1) Match score distributions of pre/post altered fingerprints follows imposter score distributions.2) The match score distributions of Pre/Post altered fingerprints alterations are not always successful in Evading AFIS.3) AFIS is unable to link most of the altered fingerprints to their true mate and there is no guarantee that fingerprint alteration will always be successful in evading AFIS.4) As long as there are a sufficient number of minutiae that can be extracted in the unaltered area, pre/post altered fingerprints mates can successfully matched. This is the biggest vulnerability in AFIS.

A. Types of Altered Fingerprints:

According to the changes made to the ridge pattern the fingerprint alteration may be categorized in to three types: Obliteration, Distortion, and Imitation. For each types of Alteration its characteristics and possible counter measures are described.

Obliteration: Friction ridge pattern on fingertips can be obliterated by abrading, cutting burning applying strong chemicals, and transplanting smooth skins. Further, factors such as skin diseases and side effects due to cancer drugs can also obliterate the fingertips. Obliterated fingerprints can defeat automated fingerprint matches and successfully pass fingerprint quality software, based on the depth and area of damages. If the damage does not reach the generating layer in the epidermis, the skin will generate to the original pattern after a few months time. However if the damage is done to the generation layer, scar tissues instead of well defined ridge details, will replace the damaged area. If the affected finger area is small, automated matches are successfully matching the damaged fingerprints with original mated fingerprints. But, if the affected area is sufficiently large to defeat automated matches, human operators or fingerprint quality software can easily detect the damage. Appropriate threshold values need to be set in fingerprint quality control software to detect significantly obliterated fingerprints that automated matches cannot identify. If the image is severely obliterated, it will treat as latent fingerprint image and perform AFIS search using manually marked features.

Distortion: By using a plastic surgery friction ridge pattern converted into unusual ridge pattern. Some portion of skin are removed from the finger and grafted back in to different position resulting a unusual pattern as shown in fig below. As distorted images may have the sufficient image quality, it may pass the automated fingerprint identification system. For instance the distorted images have the image quality value i.e. NFIG value as 1 or 2 which shows the best quality. The Z cut cases of alteration has been found in border security control applications. So it is important to find the type of altered fingerprints. Once the Types are known, it is easy to reconstruct the original mates of altered one.

Imitation: Here the surgical procedure is performed in such a way that the altered finger prints appear as natural fingerprints. The surgery is made in large area of the fingertips. It is very difficult to evade the system by the altered fingerprints. But if the area of alteration is small, it can easily defeat the AFIS. The main clue to detect the transplanted fingerprints is the presence of surgical scars.
Further, it is clear that, there are three types of altered fingerprint images namely, Obliterated, Distortion and Imitation. The obliterated can be easily detected by the fingerprint image quality software (NFIQ software) by fixing the appropriate Image quality threshold NFIG value. NFIG value =1 denote best quality and NFIG =5,donote poor quality .Similarly the Imitated type alteration can also detected by Minutiae matcher( verifinger SDK) algorithm by fixing the threshold matching score value . The matching score value of imitation type is found less. The distorted alteration is a challenge to an automatic finger print identification system because it can to be detected either by image quality software or by minutiae matching algorithm. The distorted images pass the AFIS since it has sufficient ridge pattern and matching scores.

IV. AUTOMATIC DETECTION OF ALTERED FINGERPRINTS:

In the previous section, we showed that the NFIQ algorithm is not suitable for detecting altered fingerprints, especially the distortion and imitation types. In fact, the distorted and imitated fingerprints are very hard to detect for any fingerprint image quality assessment algorithm that is based on analyzing local image quality. In this section, we consider the problem of automatic detection of alterations based on analyzing ridge orientation field and minutiae distribution. The flowchart of the proposed alteration detector is given in Fig. 11.

Fig. 10. Fingerprint imitation:

Fig. 11 block diagram of proposed algorithm

1. **Normalization.** An input fingerprint image is normalized to 512x 480 pixels by cropping a rectangular region of the fingerprint, which is located at the center of the fingerprint and aligned along the longitudinal direction of the finger, using the NIST Biometric Image Software (NBIS) . This step ensures that the features extracted in the subsequent steps are invariant with respect to translation and rotation of finger.

2. **Orientation field estimation.** The orientation field of the fingerprint, $\theta(x,y)$ is computed using the gradient-based method. The initial orientation field is smoothed by a 16x16 averaging filter, followed by averaging the orientations in 8x8 pixel blocks. A foreground mask is obtained by measuring the dynamic range of gray values of the fingerprint image in local blocks and morphological process for filling holes and removing isolated blocks is performed.

3. **Orientation field approximation.** The orientation field $\theta(x,y)$ is approximated by a polynomial model to obtain $\hat{\theta}(x,y)$.

4. **Feature Extraction.** The error map, $E(x, y)$ is computed as the absolute difference between $\theta(x, y)$ and $\hat{\theta}(x,y)$ used to construct the feature vector. More details of Steps 3 and 4 are given below.

A. **Normalization:** Normalization is a pixel wise operation. It does not change the clarity of ridge and valley structures. The main purpose of normalization is to reduce the variations in gray level values along ridges and valleys. Let $(i,j)$ denote the gray level value at pixel $(i,j)$, $M$ and $VAR$ denote the estimated mean and variance respectively and $G(i,j)$ denote the normalized gray level value at pixel$(i,j)$. The normalized image is defined as follows.

$$G (i,j) = \frac{VARo (I(i,j) - M)^2}{VAR}$$

if $I(i,j) > M$;

$$= M - \frac{VARo (I(i,j) - M)^2}{VAR}$$

otherwise;

Where $Mo$ and $VARo$ are the desired mean and variance values respectively.

**Orientation Image:** The Orientation Image represents an intrinsic property of the fingerprint images and defines invariant coordinates for ridges and valleys in a local neighborhood. By viewing a fingerprint image as an oriented texture, a number of methods have been proposed to estimate the orientation field of fingerprint images. We have developed a least mean square orientation estimation algorithm. Given a normalized image, $G$, the main steps of algorithm is as follows:

1. Divide G in to blocks of size $w x w$ (16x16).

2. Compute the gradients $\partial x (I, j)$ and $\partial y (I, j)$ at each Pixel $(I,j)$.

3. Estimate local orientation of each block centered at each pixel $(I,j)$ using the following equation.

$$V (I, j) = \sum_{u=-w/2}^{w/2} \sum_{v=-w/2}^{w/2} 2 \partial x (u, v) \partial y (u, v),$$

Where $\theta (i, j)$ is the least square estimate of the local ridge orientation at the block centered at pixel $(i, j)$. Mathematically, it represents the direction that is orthogonal to the dominant direction of the Fourier spectrum of the $w x w$ window.
4. Due to the presents of noise, corrupted ridge and valley structures, minutiae, etc. in the input image, the estimated local ridge orientation \( \theta(i,j) \), may not always be correct. Since local ridge orientation varies slowly in a local neighborhood where no singular points appear, a low-pass filter can be used to modify the incorrect local ridge orientation. In order to perform the low-pass filtering, the orientation image needs to be converted into a continuous vector field, which is defined as follows;

\[
\varphi_x(i,j) = \cos(20(i,j)),
\]

\[
\varphi_y(i,j) = \sin(20(i,j))
\]

Where \( \varphi_x \) and \( \varphi_y \) are the x and y components of the vector field, respectively. With the resulting vector field, the low pass filtering can then be performed as follows;

\[
\hat{\varphi}_x(i,j) = \frac{1}{\sum_{u=\Phi/2}^{\Phi/2} \sum_{v=-\Phi/2}^{\Phi/2} W(u,v) \theta x(i-uw,j-vw)}
\]

\[
\hat{\varphi}_y(i,j) = \frac{1}{\sum_{u=\Phi/2}^{\Phi/2} \sum_{v=-\Phi/2}^{\Phi/2} W(u,v) \theta x(i-uw,j-vw)}
\]

Where \( W \) is a two dimensional low pass filter with unit integral and \( w \phi x w \phi \) specifies the size of the filter. Note that the smoothing operation is performed at the block level. Default size of the filter is 5 x 5.

5. Compute the local ridge orientation at \((i,j)\) using

\[
O(i,j) = \frac{1}{2} \tan^{-1}\left(\frac{\hat{\varphi}_x(i,j)}{\hat{\varphi}_y(i,j)}\right)
\]

With this algorithm a fairly smooth orientation field estimate can be obtained.

C. Orientation field Approximation:

To represent the global orientation field, a set of polynomial functions is used, which is not only computationally efficient, but also provides good approximation in orientation field modeling. Let \( \theta(x,y) \) denote the orientation field. Then, the cosine and sine components of the doubled orientation at \((x,y)\) can be represented of polynomial of order \( n \):

\[
g_c^x(x,y) = \cos(20(x,y)) = \sum_{i=0}^{n} \sum_{j=0}^{n} a(i,j) x^i y^{j-1}
\]

\[
g_c^y(x,y) = \sin(20(x,y)) = \sum_{i=0}^{n} \sum_{j=0}^{n} a(i,j) x^i y^{j-1}
\]

\[
g_s^x(x,y) = \cos(20(x,y)) = \sum_{i=0}^{n} \sum_{j=0}^{n} b(i,j) x^i y^{j-1}
\]

\[
g_s^y(x,y) = \sin(20(x,y)) = \sum_{i=0}^{n} \sum_{j=0}^{n} b(i,j) x^i y^{j-1}
\]

Where \( a(i,j) \) and \( b(i,j) \) are the polynomial coefficients for cosine and sine functions respectively. The order of polynomial is selected as 6 for best fitting results.

Using the orientation field \( \theta(x,y) \) obtained above, the polynomial coefficients \( a(i,j) \) and \( b(i,j) \) can be estimated by a least square method. For simplicity the above equation in matrix forms:

\[
G_c(x,y) = X^T a, \quad G_s(x,y) = X^T b.
\]

Where \( X= [\begin{bmatrix} 1 & x & y & x^2 & xy & y^2 & \ldots & x^n & xy & y^n \end{bmatrix}]^T \), and \( a \) and \( b \) are the coefficient vectors. The problem of estimating \( a \) and \( b \) can be formulated as

\[
\hat{a} = \arg \min_G \min (Gc - Xa)^2, \quad \hat{b} = \arg \min_G (Gs - Xb)^2,
\]

Finally, the orientation field approximated by the polynomial model, \( \hat{\theta}(x,y) \) is obtained by

\[
\hat{\theta}(x,y) = \frac{1}{2} \tan^{-1} \left( \frac{\hat{g}_c(x,y)}{\hat{g}_s(x,y)} \right)
\]

Where \( \hat{G}_c(x,y) = X^T \hat{a} \)

\[
\hat{G}_s(x,y) = X^T \hat{b}
\]

D. Feature Extraction: The observed characteristics of altered fingerprints shows that their ridge flow is discontinuous in non singular region as well, such as severely scared areas, mutilated areas and distorted areas. The difference between the observed orientation field and modeled orientation field indicates the locations and amount of altered regions in the ridge flow. We define the error map \( C(x,y) \) as

\[
C(x,y) = \min(|\theta(x,y) - \hat{\theta}(x,y)|, \| -\theta(x,y) - \hat{\theta}(x,y) \|) / (\|/2).
\]

Figure 12. shows the error maps of natural and altered fingerprints. The size of the error map is 60 x 60. The feature vector from the error map consists of histograms of local spatial regions. The error map is divided in to 3 x 3 cells, where each cell of size 20 x 20 blocks. The histogram of each error map in each cell is computed in 21 bins in the range of [0,1] and the histogram of nine cells results in to 189 dimensional feature vector.
D. Minutiae Extraction & Distribution:

Minutiae in the fingerprint indicate the ridge characteristics such as ridge endings and ridge bifurcations. Almost all finger print recognition system use minutiae for matching. The minutiae of the natural fingerprint is equally distributed but in the altered fingerprint, the minutiae distribution is different according to the types alteration made in the fingerprint by the imposters. Based on the minutiae extracted from the fingerprint by the method[5], the minutiae density map is constructed by Parzen window method using uniform kernel function.

\[ S_m = \{ x|x = (x,y) \text{ is the position of the minutiae} \} \]

Then, the minutiae density map is computed as follows:

1. The initial minutiae map, \( M_d(x) \), is estimated by
   \[ M_d(x) = \sum_{x \in S_m} K_r(x-x_0) \]
   Where \( K_r(x-x_0) \) is a uniform kernel
   Centered at \( x_0 \) with radius \( r \) ( \( r \) with 40 pixels)

2. Low pass filtering. \( M_d(x,y) \) is smoothed by Guassian filter of size 30 x 30 pixels with standard deviation of 10 pixels

3. Normalization. \( M_d(x,y) \) is transformed to lie in the interval\([0 1]\) by
   \[ M_d(x,y) = M_d(x,y)/T \quad \text{if} \quad M_d(x,y) \leq T = 1 \quad \text{otherwise} \]

   Where \( T \) is a predetermined threshold

Figure 13 below shows that minutiae density maps of natural and altered fingerprints. It is noted that the natural has well spread and uniformly distributed minutiae, on the other hand in the altered fingerprints the distribution of minutiae are different. The feature vector from the minutiae density map also constructed by local histogram in 3x3 cells. Then the feature vectors from the orientation field discontinuity map and minutiae density map are combined in each cells by concatenating the local histogram and fed in to the SVM for classifications.

V. EXPERIMENTS

The proposed algorithm was evaluated at two levels: finger level (one finger) and subject level (all 10 fingers). At the finger level, we evaluate the performance of distinguishing between natural and altered fingerprints. At the subject level, we evaluate the performance of distinguishing between subjects with natural fingerprints and those with altered fingerprints. Since most AFIS used in law enforcement, national ID, and border control applications process all 10 fingerprints of a person, the subject level performance utilizes this information of the application domain.

A. Finger level evaluation: The altered fingerprint database available to us contains 4,433 fingerprints from 535 ten print cards. For a non altered fingerprint database, we use 27,000 fingerprints from the 2,700 ten print cards in the NIST SD14. This database contains two impressions for each finger, called file and search; the file impression is used in our experiments. LIBSVM with radial basis kernel function is used for classification with 10-fold cross-validation. The scores out-put by LIBSVM are linearly scaled to the range \([0; 1]\). The normalized score is termed a measure of the fingerprintness of the input fingerprint. When the fingerprintness of an input image is smaller than a predetermined threshold value, the system raises an alarm to indicate that the image is a possible altered fingerprint. If this image is indeed an altered fingerprint, it is deemed to be a true positive; otherwise, it is deemed to be a false positive. Similarly, true negative indicates that a natural fingerprint is correctly
classified as natural and false negative indicates that an altered finger-print is not detected as altered. The Receiver Operating Characteristic (ROC) curves of the proposed approach and the NFIQ software for detecting altered fingerprints are given in Fig. 18&19. At the false positive rate of 2.1 percent, where natural fingerprints in NIST SD14 with the NFIQ value of 5 are determined as altered fingerprints, the proposed algorithm attains a 70.2 percent true positive rate while the true positive rate of the NFIQ is only 31.6 percent. Fig. 18. shows the ROC curves of three approaches for detecting altered fingerprints (orientation field discontinuity minutiae distribution, and their feature level fusion) and the NFIQ algorithm. Fig. 19. shows the ROC curves of the proposed fusion algorithm and the NFIQ algorithm according to alteration type. Both obliterated and distorted fingerprints can be detected by the proposed algorithm at similar accuracy, while NFIQ can only identify obliterated cases. On the other hand, imitated fingerprints are challenging for both algorithms. At the false positive rate of 1 percent (which means 270 fingerprints among the 27,000 in NIST SD14 would be misclassified as altered fingerprints), the threshold value for fingerprintness score is 0.60. Fig. 17 shows examples of successfully detected alterations using the proposed algorithm even though the NFIQ measure assigns acceptable quality level to these images. Not all of the altered fingerprints can be detected by the proposed algorithm. If the altered area is too small the evidence of alteration is difficult to detect. In the imitation case, the ridge structure is very natural even at the boundary of altered region; the orientation field is continuous and there is insignificant abnormality in minutiae density along scars (Fig. 16b). The main reasons for false positive cases are: 1) poor image quality, leading to incorrect fingerprint feature extraction (see Fig. 17a) ground truth error; some of the fingerprints in NIST SD14 may possibly have been altered.

Table 2 shows the NFIQ distribution of the false positive examples found by the proposed algorithm at the false positive rate of 1 percent. Most of the false positive images have NFIQ of 4 or 5. Note that it is acceptable to raise alarms on poor quality fingerprints since 1) poor quality images need to be manually checked and 2)

Table 2

<table>
<thead>
<tr>
<th>NFIQ Value</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of images</td>
<td>2</td>
<td>1</td>
<td>39</td>
<td>145</td>
<td>83</td>
</tr>
</tbody>
</table>

NFIQ Distribution for False Positive Detected at the Rate of 1 Percent by the Proposed Algorithm

criminals may purposely present poor quality fingerprints to the fingerprint system to evade identification [41]. All three false positive cases with NFIQ ¼ 1 or 2 appear to have been altered (two of them are shown in Figs. 19b and 19c).

Fig.15. True Positive detection cases

Fig.16. True Negative detection cases

Fig.17. False positive cases

Fig.18. ROC curves for proposed method
B. Subject-Level Evaluation: In our altered fingerprint database, we observed that when a person resorts to fingerprint alteration, he tries to alter as many fingers as possible. This makes sense since large-scale AFIS applications typically use a fusion of match scores from all 10 fingerprints for identification. So, altering just one or two fingerprints is not likely to change the identification decision. Based on this observation, we use the following decision level fusion rule to perform the subject level detection for altered fingerprints. When six or more fingerprints are detected as altered, the subject is claimed to have altered fingerprints. Subjects with fewer than six altered fingerprints are not considered as a threat to AFIS since even five (out of 10) natural fingerprints are generally sufficient for reliable identification. For the subject level evaluation, 453 ten print cards with more than five altered fingerprints and 2,700 ten print cards in NIST SD14 are used. Fig. 20 shows the ROC curves of the proposed algorithm (including three approaches) as well as the NFIQ criterion for detecting subjects with altered fingerprints. At a false positive rate of 0.3 percent, where the NFIQ criterion determines subjects with six or more fingerprints of NFIQ $\frac{3}{4}$ 5 in NIST SD14 as people who altered the fingerprints, the proposed algorithm attains a true positive rate of 66.4 percent, while the NFIQ criterion obtains a 26.5 percent true positive rate. Fig. 21 shows an example of a ten print card where the subject level decision is successful. Even though one altered finger is not correctly detected due to the smoothness of the orientation field and the absence of abnormality in minutiae distribution in altered area, our subject level fusion algorithm still flags this person because as many as nine fingers are determined to be altered. Fusion of multiple fingerprints also helps to reduce the false positive for a person who either did not alter his fingerprints or simply has one or two fingerprints that appear to have been altered due to accidents or occupational reasons. In this case, however, the NFIQ criterion will falsely raise an alarm for this subject since six of the 10 fingerprints are assigned the NFIQ value of 5.
VI CONCLUSIONS AND FUTURE WORK

The success of AFIS and their extensive deployment all over the world have prompted some individuals to take extreme measures to evade identification by altering their fingerprints. The problem of fingerprint alteration or obfuscation is very different from that of fingerprint spoofing, where an individual uses a fake fingerprint in order to adopt the identity of another individual. While the problem of spoofing has received substantial attention in the literature, the problem of obfuscation has not been addressed in the biometric literature, in spite of numerous documented cases of fingerprint alteration for the purpose of evading identification. While obfuscation may be encountered with other biometric modalities (such as face and iris), this problem is especially significant in the case of fingerprints due to the widespread deployment of AFIS in both government and civilian applications and the ease with which fingerprints can be obfuscated. We have introduced the problem of fingerprint alteration and conducted a quantitative analysis of the threat of altered fingerprints to a commercial fingerprint matcher. We also evaluated the capability of well-known fingerprint image quality assessment software, NFIQ, for detecting altered fingerprints. Since the NFIQ has limited ability in distinguishing altered fingerprints from natural fingerprints, we developed an algorithm to automatically detect altered fingerprints based on the characteristics of the fingerprint orientation field and minutiae distribution. The proposed algorithm based on the features extracted from the orientation field and minutiae satisfies the three essential requirements for alteration detection algorithm:

1. Fast operational time,
2. high true positive rate at low false positive rate,
3. ease of integration into AFIS.

The proposed algorithm and the NFIQ criterion were tested on a large public domain fingerprint database (NIIST SD14) as natural fingerprints and an altered fingerprint database provided by a law enforcement agency. At a false positive rate of 0.3 percent, the proposed algorithm can correctly detect 66.4 percent of the subjects with altered fingerprints, while 26.5 percent of such subjects are detected by the NFIQ algorithm.

This study can be further extended along the following directions:

1. Determine the alteration type automatically so that appropriate countermeasures can be taken.
2. Reconstruct altered fingerprints. For some types of altered fingerprints where the ridge patterns are damaged locally or the ridge structure is still present on the finger but possibly at a different location, reconstruction is indeed possible.
3. Match altered fingerprints to their unaltered mates. A matcher specialized for altered fingerprints can be developed to link them to unaltered mates in the database utilizing whatever information is available in the altered fingerprints.
4. Use multibiometrics to face the growing threat of individuals evading AFIS. However, other biometric traits can also be altered successfully. It has been reported that plastic surgery can significantly degrade the performance of face recognition systems and that cataract surgery can reduce the accuracy of iris recognition systems. To effectively deal with the problem of evading identification by altering biometric traits, a systematic study of possible alteration approaches for each major biometric trait is needed.

VII. REFERENCES


