ANALYSIS AND DETECTION OF ALTERED FINGERPRINT MATCHING

Nadhiya Nazeer Khan

M.G University, Mount Zion College of Engineering, Pathanamthitta, India

Abstract: **Alteration may be encountered with other biometric modalities which includes face, iris and fingerprints etc. The problem of alteration is especially significant in the case of fingerprints and this is due to the extensive deployment of AFIS in government applications and the simplicity with which fingerprints can easily be complicated. So, here developed an algorithm to automatically detect alteration in fingerprints which is based on the characteristics of the fingerprint features like orientation field and minutiae distribution. The proposed algorithm satisfies the three essential requirements for alteration detection algorithm. They are fast operational time, high true positive rate at low false positive rate, and ease of integration into AFIS (Automated Fingerprint Identification Systems). Fingerprint obfuscation refers to the deliberate alteration of the fingerprint arrangement by a distinct for the purpose of masking his /her identity. Several cases of alterations have been reported. Orientation field describes the ridge movement of fingerprints. Good quality fingerprints offers smooth orientation fields but poses exception near the singular points (core and delta). Gradient-based method is used for computing the orientation field. Mainly it uses the difference between the observed orientation field extracted from the image of fingerprint and the orientation field estimated by the model. The estimated value is represented as a feature vector for classifying the available fingerprint as natural or altered one. In addition, feature extracted from minutiae distribution can also be used for this purpose. Here, minutiae density map is firstly constructed using uniform kernel function and feature vectors from both orientation field discontinuity map and the minutiae density map are shared by concatenating local histograms in each cell which is then fed into a support vector machine (SVM) for further classification**.

Keywords: **Alteration, Fingerprint obfuscation, NFIQ.**

I. INTRODUCTION

In order to identify the victims and defendants, fingerprint identification systems have been widely used by the law enforcement agencies for more than 100 years. It finds its increased applications in both government and civilian areas due to the advancement in AFIS technologies, along with the need of identifying the reliable persons. US-VISIT’s IDENT program and the FBI’s IAFIS service are the examples of large scale fingerprint systems in government areas. The main goal of fingerprint alteration is to to avoid identification using methods changing from scraping, cutting and scorching fingers to performing plastic surgery.

It is important to notice that altered fingerprints differ from that of fake fingerprints. The usage of fake fingerprint is a well know method to duplicate the fingerprint systems. On the other hand, altered fingerprints are the real fingerprints which are used to hide one’s identity by using biometric system. Fake fingers are normally used by personalities to adopt another person’s identity while the altered fingers are often used to disguise one’s own identity in an effective manner. Altered fingers falls under a wider category of attacks know as biometric obfuscation. This can be defines as a deliberate attempt by an individual to mask his/her identity. It is done using biometric systems. Disturbing the texture of the iris by wearing theatrical lenses and altering facial attributes are some the examples of alterations (Fig 1). So, it is necessary to control the problem of fingerprint obfuscation for the following reasons. They are:

- Wider application of fingerprint identification systems than systems based on other modalities like face and iris.
- Easier alteration is possible for fingerprints using chemicals.
- Lack of urgency of problem with fingerprint alteration due to previous studies conducted by law enforcement agencies and immigration officials.

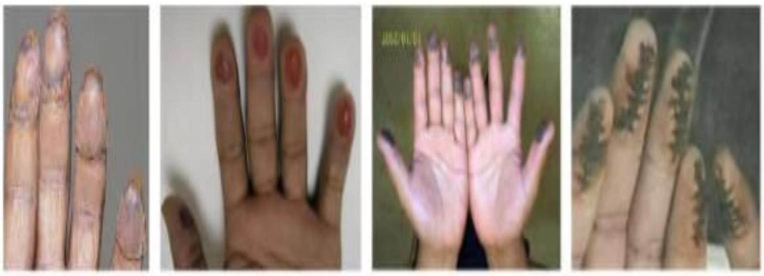

Fig 1: Altered Fingerprints

The first step in defeating fingerprint alteration is to develop an automatic solution in a good manner. Existing approach is to use fingerprint quality assessment routine, NFIQ. But the problem is that it is applicable only when the image quality of altered fingerprint is of poor. So, an algorithm is proposed which is able to determine whether the available fingerprint is altered or natural one. It is based on the feature extracted from orientation field and minutiae distribution.

II. EXISTING SYSEM

Altered Fingerprints Classifications:

Altered fingerprints can be categorized into three. They are

- Obliteration
- distortion &
- imitation

Obliteration:

It is possible to obliterate ridge patterns in fingers by adopting procedures such as grinding, cutting, burning, applying robust chemicals and via smooth skin transplantation. Leprosy and side effects of cancer drugs falls under this category. It is considered to be the most popular form of alteration. Ridge structure is completely destroyed in this method. Moreover, detecting distorted or imitated fingerprints is much more difficult for human inspectors than obliterated fingerprints.

Distortion:

It is done by turning the friction ridge patterns on fingertips into abnormal ridge patterns, by removing portions of skin from a fingertip and fixing them back in different positions .Such distorted fingerprints have ridge patterns that are not usual and also they are not found in natural fingerprints. Distorted fingerprints can also positively pass the NFIQ test. This is due to the fact that local ridge structure of distorted fingerprints remains similar to that of natural fingerprints, but their global ridge pattern is irregular.

Imitation:

It is not possible for the Imitated fingerprints to pass the fingerprint quality assessment software. They can also confuse human examiners. Removing portion of a skin and the remaining skin is pulled and stitched together, replacement of the entire fingertip etc. Imitation fingerprint has the highest NFIQ value of 1.

Permanence and uniqueness are considered to be the two important principles that form the basis of friction ridge identification. This includes fingerprint and palmprint identification. There are 3 main types of fingerprints patterns, and they are loop, whorl and arches (Fig 2). Loops begins on one side of the finger and exits on the other side. The two main types of loops are: Ulnar loops and Radial loops. Whorls may form spiral or circular patterns. Arches on the other hand, are just like marrow mountains with slopes towards up and then down.

Existing system for identifying the altered fingerprint is the NFIQ software. It stands for NIST Fingerprint Image Quality software. But this will provide us with good results if and only if the quality of available image is poor , but it is not necessary that all the available altered fingerprints must be of poor quality. So, the proposed method introduces an algorithm which is able to detect alteration in available fingerprints in efficient manner.

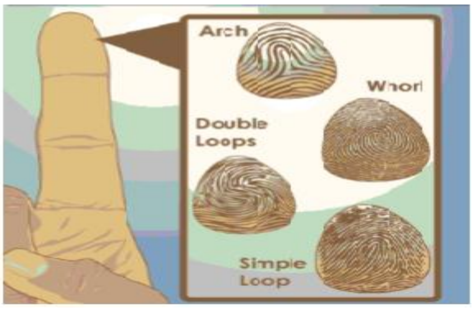

Fig 2:- Fingerprints Patterns

III. PROPOSED SYSTEM

The methods for identifying the altered fingerprints include:

- Pre-processing of image
- Minutiae extraction
- Post-processing

Preprocessing:

In order to obtain the enhanced image, firstly the image must be preprocessed (Fig 3). It includes the following steps: image segmentation, orientation field estimation, smoothening, frequency computation.

-. In order to ensure the proper removal of noise, we need to segment the input image, which is known to be the segmentation process. For this, the complete image is divided into blocks of size 16×16, and after that the variance of each block is computed which is then compared with threshold value. Block portion is permanently deleted from the original figure, if its variance is lesser than the computed threshold value. This process is carried out for the entire image. It then undergoes normalization process to get the desired variance of the given image.

-Orientation estimation of the entire image is then performed as the next step. Here also the entire image is divided into blocks of size 16x16, after which the local orientation is perfectly computed.

-To obtain the appropriate angle between the blocks, smoothening process is done via passng it through low pass filter.

-X-signatures of each block is calculated for the computation of frequency. It is usually calculated along the direction perpendicular to the orientation angle of each block. The window of magnitude 16×32 is usually used for this purpose. Distance between the peaks obtained via X-signatures computation process is used for frequency computation. This step is an optional one, if the global frequency is given

-Finally, Gabor filter is used for the filtration process, which will provide as with suitable value of variance.

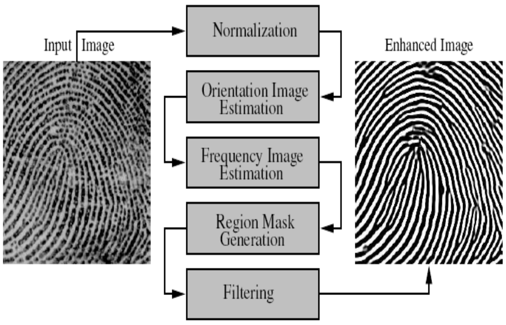

Fig 3:- Pre-Processing steps

Minutiae Extraction:

Extraction of minutiae is the next step to be performed after getting the enhanced image. For this, binarization is performed first which results in the formation of skelton image. The minutiae points are then extracted as follows. The binary image is thinned which removes the existence of redundant pixels if any and makes ridges of one pixel wide. The minutiae points are thus those which have ridge endings and ridge bifurcations in their neighborhood. This describes the procedure of minutiae extraction.

Post Processing:

The existence of spurious minutiae's are caused due to the occurrence of ridge breaks in the given figure itself. In some cases, this may reside even after the formation of enhanced image, which results in false minutiae points that must be removed as soon as possible. This can be easily removed by final stage, known as post processing stage.

The main modules includes Normalization, orientation image, orientation field approximation, feature extraction and finally the minutiae extraction and distribution.

Normalization can be defined as a pixel wise operation that would not change the clearness of ridge and valley structures. The main aim of this process is to decrease gray level value variations in both ridges and valleys. The intrinsic property of the fingerprint images can easily be represented by using Orientation Image. Here ,we have developed an algorithm for computing the orientation.

least mean square orientation estimation algorithm.

- Divide the normalized image into blocks of size w X w
- For each pixel (i, j), compute the gradients ∂x (I, j) and ∂y (I, j)
- For each block centered at(i, j), local orientation estimation is performed.
- Low pass filtering is done to avoid the presence of noise if any.
- Finally, the local ridge orientation at pixel (i, j) is calculated

This will provide us with an impartial smooth orientation field estimate. It is then followed by orientation field approximation, feature extraction and finally the minutiae extraction and distribution.

IV. PERFORMANCE ANALYSIS

Four fingerprint images like one original fingerprint and three altered fingerprints of types obliterated, distorted and imitated were taken out from the first 1,00 fingerprints in SD4. The normalized score is called as fingerprintness. System will raise an alarm if the fingerprintness of the available input image is smaller than the pre-computed value of threshold .It is considered to be a true identification, if the image is an improved one otherwise the alarm is said to be a false one.

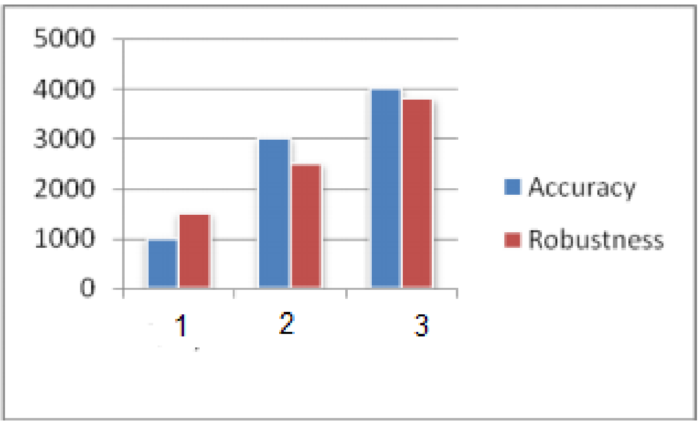

Fig 4: Performance analysis

One finger evaluation of the available image is done using the proposed algorithm. The performance of differences between natural and altered fingerprints is evaluated first and the corresponding database for this data contains two impressions for each finger, called file and search; In our experiments, we prefer file impressions. For having accurate classification with 10-fold cross-validation, we use LIBSVM along with radial basis kernel function. The output scores generated by LIBSVM are then linearly scaled to the range [0; 1] . The normalized score is called as fingerprintness. System will raise an alarm if the fingerprintness of the available input image is smaller than the pre-computed value of threshold . It is said to be a true detection, if the image is an altered one otherwise it is a false alarm. If this image is an altered fingerprint, it is believed to be a true positive; otherwise, it is said to be a false positive. If a natural fingerprint is correctly classified as natural one then it clearly indicates that it is true negative whereas false negative indicates that an altered finger- print is not noticed as an altered one. The Receiver Operating Characteristic (ROC) curves of the proposed approach and the NFIQ software are used for detecting the altered fingerprints. At the false positive rate of 2.1 percent, natural fingerprints in NIST SD14 and the NIST Fingerprint Image Quality value of 5 are determined as altered fingerprints, the proposed algorithm attains a 70.2 percent true positive rate while NFIQ on the other hand attains only 31.6 percent. NFIQ can only identify obliterated cases whereas the proposed algorithm can detect both obliterated and distorted fingerprints at similar accuracy. On the other hand, imitated fingerprints exhibits challenging problems for both algorithms. At the false positive rate of 1 percent, the fingerprintness poses a threshold score of 0.60. Not all of the altered fingerprints can be detected by using the proposed algorithm. The evidence of alteration is difficult to identify if the altered area is too small. In the imitation case, the boundary of altered region may provide as with natural ridge structure; and also the orientation field is continuous and there is only slight abnormality in minutiae density along marks. The main reasons for the generation of false positive cases are: poor image quality, that may lead to the development of incorrect fingerprint feature extraction ground truth error.

V. CONCLUSION

Alteration may be encountered with other biometric modalities which include face, iris and fingerprints etc. The problem of alteration is especially significant in the case of fingerprints and this is due to the extensive deployment of AFIS in government applications and the simplicity with which fingerprints can easily be complicated. So, here developed an algorithm to automatically detect alteration in fingerprints which is based on the characteristics of the fingerprint features like orientation field and minutiae distribution. With this proposed algorithm, we can efficiently satisfy the three basic requirements for alteration detection algorithm. They are fast operational time, high true positive rate at low false positive rate, and ease of integration into AFIS.

ACKNOWLEDGEMENT

I would like to extend my appreciativeness to the reference authors, as well as evaluator of my paper.

REFERENCES

[1] J. Feng, A.K. Jain, and A. Ross, “Detecting Altered Fingerprints,” Proc. 20th Int’l Conf. Pattern Recognition, pp. 16221625, Aug. 2010.

[2] Jianjiang Feng, A. K. Jain, A. Ross, "Fingerprint Alteration", MSU Technical Report, MSU-CSE-09-30, Dec. 2009.

[3] Yoon, Feng, A.K. Jain, ―Altered Fingerprints analysis and detection, ‖IEEE transaction on pattern analysis and machine intelligence 2012.

[4] Soweon Yoon, Jianjiang Feng, and Anil K. Jain. Altered Fingerprint Analysis and Detection, IEEE Trans., 2012.

[5] ChandrakanthBiradar, Vijeth Rao,” A challenge to analyze and detect altered human fingerprint”,IOSR-JCE, volume 13, Aug. 2013.

[6] J. Feng, J. Zhou, and A. Jain, “Orientation field estimation for latent fingerprint enhancement,” IEEE Transactions on Pattern Analysis and Machine Intelligence, 2013.