International Journal of Computer Science & Communication (ISSN: 0973-7391)
Volume 10 • Issue 1 pp. 250-255 Sept 2018 - March 2019 www.csjournals.com

Spoof Attack Detection in Fingerprint Authentication using Hybrid fusion

Navpreet Kaur
Assistant Professor, Department of Computer Science, Govt.College for women, Bhodia Khera

Abstract: In the modern era, with the growing need of biometric technologies, spoof attacks are becoming a serious concern. A number of solutions have been proposed to detect the use of fake fingerprints[3]. This paper takes advantage of skin elements in fingerprints, namely: minutiae points and Ridge Bifurcations to investigate spoof attacks. Graphical results using histogram approach in MATLAB show the difference between both genuine and fake fingerprints. In this paper, an ordered approach of minutiae based and ridge based matching is carried out. The minutiae based fingerprint verification method has the advantage of working fast and efficient even with small systems while ridge based verification along with minutiae approach enhances the security.
Keywords: biometrics, component, fake fingerprints, fingerprint recognition, minutiae points detection, spoof attacks, thinning.

1. Introduction

Fingerprint verification has been the most widely used identification system, its confidence has been demonstrated through long-term research and it is a biometrics that requires minimal cost and equipment, is convenient to use, and compact. The same is true for the risks associated with this technology. The vulnerability to attacks directed against the sensor, such as spoofing attacks,
constitutes an important threat. A spoofing attack consists ridge skin portion of a genuine fingertip. These reproductions can be produced by either using a cast of the original finger or from a fingermark left by the legitimate user [12,14]. The term of "direct production" is commonly used to designate the first situation, for which the finger is directly pressed on a soft material in order to produce the cast. The term of "indirect production" includes all the techniques used to produce a tridimensional cast from a flat image, such as the photography of a fingermark or print. Since, the quality of reproduction is greatly influenced by the production method, direct or indirect, both methods have been tested. By fake, we mean a tridimensional reproduction of the friction Numerous solutions have been proposed to protect fingerprint sensors against these attacks, such as the use of perspiration, skin optical properties or skin temperature [2,10]. in using a fake to impersonate a legitimate user.
Recently, to overcome the errors of the minutiae-based fingerprint verification[11], many studies on improved fingerprint identification using more than two features, like methods in which pre-processing stage is improved or both minutiae and ridge based fingerprint matching are used[6], have been tested over spoof attacks. This paper used ridge bifurcations in connection to minutiae, to enhance security performance of the fingerprint verification as well to prevent spoofing. The minutiae-based fingerprint verification method has the advantage of working fast and efficient even with small systems because it uses minimal data[5]. In the literature, some works aimed at taking benefit of minutiae points to detect perspiration activity in time-series captures [1,4] or to detect liveness [8]. These studies show that minutiae points could be used in this field. Numerous studies have demonstrated the influence of the distortion on minutiae locations[7]. The hypothesis here is as follows: since the materials used for producing fakes present reduced elasticity than natural skin, the location and quantity of the reproduced minutiae points and ridge bifurcations on fake fingerprints should not dramatically change when comparing a distorted fingerprint image with a non-distorted one whereas more variation is expected on genuine entries.

2. Steps to Detect Spoofs

A. Sample production and materials

Direct and indirect production methods were used to elaborate fakes[13]. For direct cast production, two materials were chosen to reproduce the inverse of the friction ridge skin: a thermoplastic (Utile Plast, produced by Pascal Rosier) and a silicon molding paste (Siligum, produced by Gedeo). The fake is obtained by pouring casting material (latex, produced by Gedeo) in that inverse initial mould. For indirect casts production, only one production method has been applied: Fingermarks which are left on glass, can be photographed using low angled light. The digital

image is then processed using an image processing software and then printed on an acetate sheet using a laser printer that is used as the blueprint for the production of the cast that will be used as a fake. That final cast is then obtained by pouring either glue (produced by Geistlich) or latex (produced by Gedeo).

B. Image Acquisition

Fingerprint images (genuine and fake) can be captured using an optical sensor. For the acquisition of genuine friction ridge skin, the donor simply applied his finger on the device. For fakes, the impostor is placing the fake moulded reproduction on his finger and applies it on the capturing device (figure 1). For each acquisition (genuine and fake), two images are captured. The first image was captured in "normal conditions", which means that the user or the impostor was allowed to place his finger on the sensor without any further instruction. The second image was captured in "distortion conditions", which means that the person was asked to apply an upward movement when pressing the finger on the sensor.

Figure 1. Fake placed on the impostor's finger

C. Difference between Query and Reference Image:

Due to the proximity of the overall minutiae and bifurcation's quantity distributions, computed respectively for genuine and fake fingerprints(figure 5), we chose to investigate the differences in locations of these quantities, where the reference image R is always chosen as the image of genuine source for any query image Q (either fake or genuine). As illustrated in figure 5, the discrimination between genuine and fake fingerprints for a known reference is more efficient. In most cases, the genuine distribution is more flat than for the fakes images and the two distributions are not separated enough, which avoids a good discrimination between samples. The separation is even more tangible when differences are computed between the undistorted genuine reference R and any corresponding query Q but acquired with distortion applied during the transaction. A linear discriminant analysis (LDA) was performed in order to classify our images into two groups: "genuine" and "fake" fingerprints[9]. Equal prior probabilities have been chosen to set a priori the belonging of any query image to one of these two groups.

3.Proposed Hybrid Scheme

The proposed hybrid method consists of two stages, namely; First stage is extraction phase in which extraction of minutiae points along with ridge bifurcations in a given query input image of fingerprint sample is carried out. This stage is further can be studied in 3 main steps, namely: providing input to th e program, applying thinning effect over the supplied input, and finally obtaining the extracted minutiaes along with ridges. Then comes the second stage, in which we can find the location of extracted features in query image. The results, thus obtained can be compared with the results of Reference image which has already gone through above two stages. At the end of above scenario spoof attacks can be detected if no match has occurred between the processed results of both Query and Reference image samples. No match condition corresponds to unauthorized attempt by any intruder into the authentication system, thus leading the system to become vulnerable to spoof attacks. Whereas, a matching condition corresponds to Absence of spoofs or we can say presence of genuine user.

International Journal of Computer Science & Communication (ISSN: 0973-7391)
Volume 10 • Issue 1 pp. 250-255 Sept 2018 - March 2019 www.csjournals.com

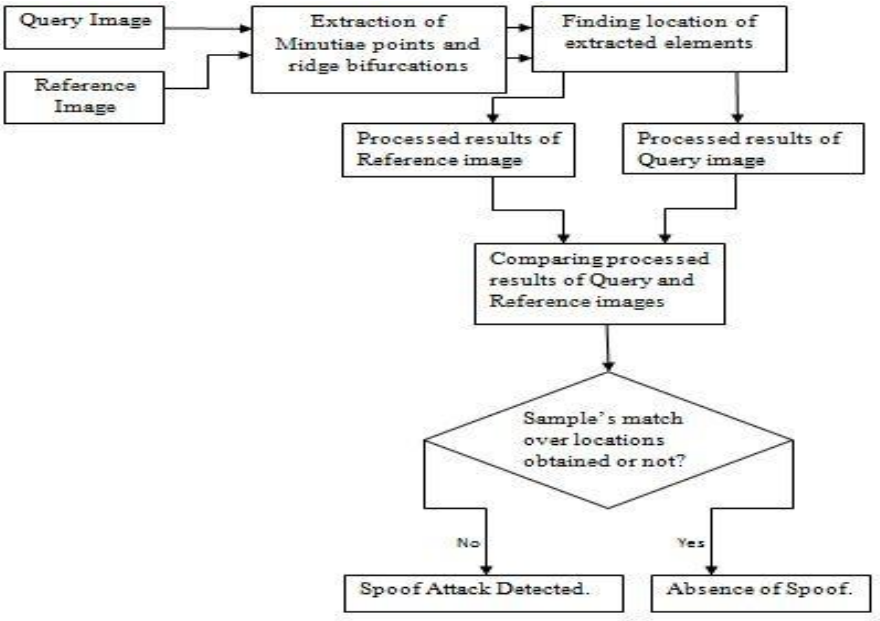

Figure 2: Framework of proposed hybrid fusion method.

4. Code For Extraction of Minutiae and Ridge Bifurcations

```
%Program Description
%This program extracts the ridges and bifurcation from a fingerprint image
%Read Input Image
binary_image=im2bw(imread('input_1.tif'));

%Small region is taken to show output clear
binary_image = binary_image(120:400,20:250);
figure;imshow(binary_image);title('Input image');

%Thinning
thin_image=~bwmorph(binary_image,'thin',Inf);
figure;imshow(thin_image);title('Thinned Image');

%Minutiae extraction
s=size(thin_image);
N=3;%window size
n=(N-1)/2;
r=s(1)+2*n;
c=s(2)+2*n;
double temp(r,c);
temp=zeros(r,c);bifurcation=zeros(r,c);ridge=zeros(r,c);
temp((n+1):(end-n),(n+1):(end-n))=thin_image(:,:);
outImg=zeros(r,c,3);%For Display
outImg(:,:,1) = temp .* 255;
outImg(:,:,2) = temp .* 255;
outImg(:,:,3) = temp .* 255;
for x=(n+1+10):(s(1)+n-10)
    for y=(n+1+10):(s(2)+n-10)
        e=1;
        for k=x-n:x+n
            f=1;
            for l=y-n:y+n
```

```
                mat(e,f)=temp(k,l);
                f=f+1;
            end
            e=e+1;
        end;
         if(mat(2,2)==0)
            ridge(x,y)=sum(sum(~mat));
            bifurcation(x,y)=sum(sum(~mat));
         end
    end;
end;

% RIDGE END FINDING
[ridge_x ridge_y]=find(ridge==2);
len=length(ridge_x);
%For Display
for i=1:len
    outImg((ridge_x(i)-3):(ridge_x(i)+3),(ridge_y(i)-3),2:3)=0;
    outImg((ridge_x(i)-3):(ridge_x(i)+3),(ridge_y(i)+3),2:3)=0;
    outImg((ridge_x(i)-3),(ridge_y(i)-3):(ridge_y(i)+3),2:3)=0;
    outImg((ridge_x(i)+3),(ridge_y(i)-3):(ridge_y(i)+3),2:3)=0;

    outImg((ridge_x(i)-3):(ridge_x(i)+3),(ridge_y(i)-3),1)=255;
    outImg((ridge_x(i)-3):(ridge_x(i)+3),(ridge_y(i)+3),1)=255;
    outImg((ridge_x(i)-3),(ridge_y(i)-3):(ridge_y(i)+3),1)=255;
    outImg((ridge_x(i)+3),(ridge_y(i)-3):(ridge_y(i)+3),1)=255;
end

%BIFURCATION FINDING
[bifurcation_x bifurcation_y]=find(bifurcation==4);
len=length(bifurcation_x);
%For Display
for i=1:len
    outImg((bifurcation_x(i)-3):(bifurcation_x(i)+3),(bifurcation_y(i)-
3),1:2)=0;
    outImg((bifurcation_x(i)-
3):(bifurcation_x(i)+3),(bifurcation_y(i)+3),1:2)=0;
    outImg((bifurcation_x(i)-3),(bifurcation_y(i)-
3):(bifurcation_y(i)+3),1:2)=0;
    outImg((bifurcation_x(i)+3),(bifurcation_y(i)-
3):(bifurcation_y(i)+3),1:2)=0;
     outImg((bifurcation_x(i)-3):(bifurcation_x(i)+3),(bifurcation_y(i)-
3),3)=255;
    outImg((bifurcation_x(i)-
3):(bifurcation_x(i)+3),(bifurcation_y(i)+3),3)=255;
    outImg((bifurcation_x(i)-3),(bifurcation_y(i)-
3):(bifurcation_y(i)+3),3)=255;
    outImg((bifurcation_x(i)+3),(bifurcation_y(i)-
3):(bifurcation_y(i)+3),3)=255;
end
figure; imshow(outImg);title('Minutiae');
```

International Journal of Computer Science & Communication (ISSN: 0973-7391)
Volume 10 • Issue 1 pp. 250-255 Sept 2018 - March 2019 www.csjournals.com

5. Experimental Results:

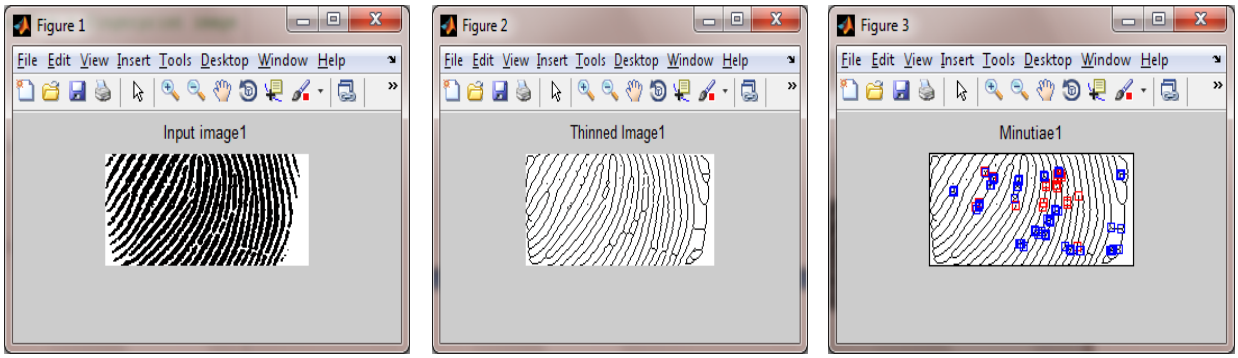

Figure3 (a)input image of genuine user's fingerprint for a particular chosen area (b) thinned image corresponding to genuine input

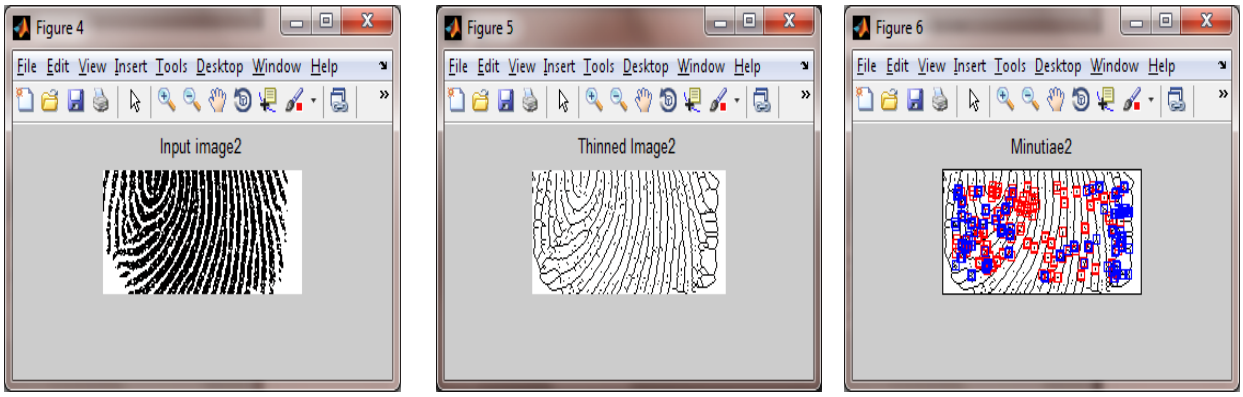

Figure4 (a)input image of query user's fingerprint for a particular chosen area (b) thinned image corresponding to query input (c) extracted minutiaes

The difference can be viewed using histograms of the two samples as:

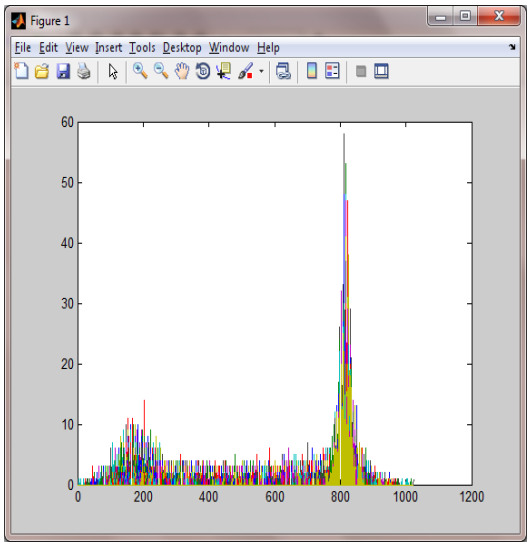

Figure 5: (a) Histogram corresponding to Genuine user.

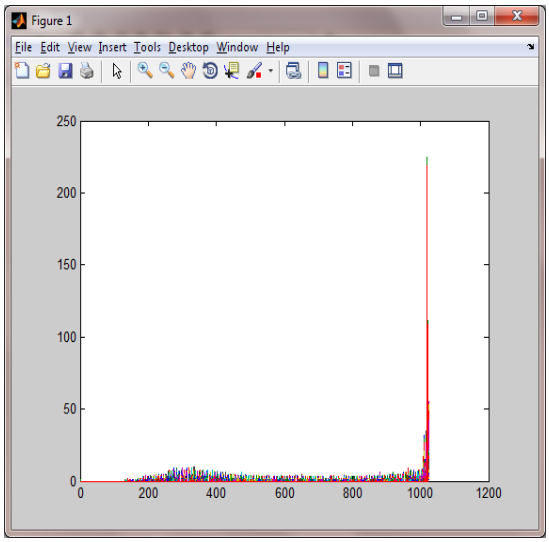

Figure 5 (b) Histogram corresponding to Fake user.

As illustrated in the histograms shown above corresponding to the genuine and fake user's fingerprint template images respectively; various spikes are distributed in the both figures. The spikes are distributed based on the presence and locations of minutiaes in both Reference and Query images. That's why figure 5(a) shows presence of relatively larger number of minutiae points as compared to the points extracted for the Query image in figure 5(b).Moreover, the graphical difference using histograms also depends upon presence of ridge bifurcations, along with minutiae point concept. This difference so obtained is clearly helpful in differentiating a genuine user from a fake user and thus detects the presence of spoof attack into the authentication system.

6. Conclusion

This research aimed at exploring the use of minutia points and ridge bifurcations to detect spoofing attacks. Minutiae points and Ridge bifurcations have been detected automatically using a basic detection algorithm. For each image minutiae points and ridge bifurcations along with their extracted locations can be used as a predicting variable. The performance of proposed scheme can be tested by considering a number of image samples. We have shown that intrinsic features, such as minutiae points, obtained directly at the acquisition of friction ridge skin areas can be used as a mechanism to detect spoofing attacks.

7. References

[1] A. Abhyankar and S. Schuckers, "Towards integrating level-3 features with perspiration pattern for robust fingerprint recognition", in *17thInternational Conference on Image Processing*, Hong Kong, 2010.
[2] A. Abhyankar and S.S. Schuckers, "Integrating a wavelet based perspiration liveness check with fingerprint recognition", *Pattern Recognition*, vol. 42, pp. 452-464, 2009.
[3] A. Nagar, K. Nandakumar, and A. Jain, "A hybrid biometric cryptosystem for securing fingerprint minutiae templates," Pattern Recogn. Lett., vol. 31, pp. 733–741, 2010.
[4] B. Tan and S. Schuckers, "Spoofing protection for fingerprint scanner by fusing ridge signal and valley noise", *Pattern Recognition*, 2010.
[5] D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar, "Handbook of fingerprint recognition" Springer, 2nd Edition, 2009.
[6] F. Ahmad, and D. Mohamad, "Fingerprint Classification Based on Analysis of Singularities and Image Quality", IVIC, LNCS5857, pp. 551-560, 2009.
[7] F. Chafia, C. Salim, and B. Farid, "A biometric crypto-system for authentication," in Proc. of Int. Conf. on Machine and Web Intelligence (ICMWI), 2010, pp. 434–438.
[8] G. L. Marcialis, F. Roli and A. Tidu, "Analysis of fingerprint pores for vitality detection", in *International Conference on Pattern Recognition*, vol. 1, pp. 1289-1292, 2010.
[9]H. Xu and R. N. Veldhuis, "Binary representations of fingerprint spectral minutiae features," in Proc. of the 20th Int. Conf. on Pattern Recognition (ICPR'10), 2010, pp. 1212–1216.
[10] J. Jia, L. Cai, K. Zhand and D. Chen, "A new approach to fake finger detection based on skin elasticity analysis", Advances in Biometrics, LNCS, vol. 4642, pp. 309-318, 2009.
[11] K. Nandakumar, "A fingerprint cryptosystem based on minutiae phase spectrum," in Proc. of IEEE Workshop on Information Forensics and Security (WIFS), 2010.
[12] M. Espinoza and C. Champod, "Risk evaluation for spoofing against a sensor supplied with liveness detection", *Forensic Science International*, vol. 204, pp. 162-168, 2011.
[13] M. H. Bhuyan, S. Saharia, D. Kr Bhattacharyya, "An Effective Method for Fingerprint Classification", International Arab Journal of e-Technology, Vol: 1, Issue: 3, pp. 89-97, Jan 2010.
[14] M. Espinoza, C. Champod and P. Margot, "Vulnerabilities of fingerprint reader to fake fingerprints attacks", *Forensic Science International*, vol. 204, pp.41-49, 2011.