Detection of face spoofing using low-level features and shape analysis

DD Arini¹, KN Ramadhani², F Sthevanie³
¹,²,³ School of Computing, Telkom University
E-mail:¹ arinidian@student.telkomuniversity.ac.id,
² kurniawannr@telkomuniversity.ac.id,
³ sthevanie@telkomuniversity.ac.id

Abstract. Face as a security system has a vulnerability to the spoofing attack because by falsifying faces using certain media such as photos or videos can fool the system. In this study, we proposed a spoofing detection system on human faces that good to distinguish spoof and non-spoof face using Low-Level Feature: Speeded-Up Robust Features (SURF) and Shape Analysis: Pyramid Histogram of Oriented Gradient (PHOG) as the feature extraction. We tested our method on 2 scenarios: intra-database and cross-database, using 4 different public datasets: MSU MFSD, NUAA Imposter, CASIA FASD, and IDIAP Replay-Attack. We used Support Vector Machine (SVM) and k-Nearest Neighbors (k-NN) as classification.

1. Introduction
Nowadays, high-level security is a necessity on mobile device, such as smart phones, so that biometric techniques get a lot of attention. Facial recognition system for security system are widely utilized, but this facial recognition system is vulnerable to spoofing attacks or commonly called face spoofing.

Face spoofing is falsifying faces using certain media such as photos or videos to get into the system. Without anti-spoofing, facial biometrics are particularly vulnerable to attack because the photo or video of a human face displayed onto the screen can fool the system. Therefore, the research is conducted to prevent spoofing [1].

In previous research, the database was limited because the training and testing images used were captured under the same the same imaging conditions [2]. Whereas, it is important to create a system that can well generalize to the database with the new condition. In order to achieve that goal, it takes approach that can find the most discriminating part around the face, such as the texture and the shape.

In this study, in order to be able to distinguish between spoof and non-spoof images, the authors used a combination of low-level feature of Speeded-Up Robust Feature (SURF) [3] as a texture analysis which invariant of illumination, scale, and rotation, with the Pyramid Histogram of Oriented Gradient (PHOG) [4] that extracts gradient intensity and direction to describe image appearance. SVM and KNN classifiers is used for the classification of spoof and non-spoof faces. We also used 4 databases, called MSU MFSD, CASIA, NUAA, and IDIAP.

2. Related work
Some summaries of face spoof detection algorithms published in the literature. There are some types of cues used in face spoof detection:

(i) Texture based method: There are many studies using texture as an extracted feature [5–7].

In [5], author using Local Binary Pattern (LBP) to extract the texture of face to distinguish
spoof and non-spoof image. The HTER on IDIAP database was 13.87%. However, the generalization ability of many texture based methods has been found to be poor [2]. A study from [8] reported that HTER increased on cross-database scenario.

(ii) Method based on texture and shape analysis: A recent work [1] proposed a spoof attack detection method on fingerprint. Author using the combination of Speeded-Up Robust Features (SURF) and Pyramid Histogram of Oriented Gradient (PHOG). SURF which invariant to scale and illumination extracts the texture while PHOG extracts the gradient intensity and edge direction to describe the appearance of the image. Combination of these two methods result the feature that discriminate well between spoof and non-spoof fingerprint images. The EER using these methods was 3.99%.

3. Speeded-Up Robust Features (SURF)
SURF have been used to recognize objects, such as face or object, to track object, and to extract interest points. To detect interest points, SURF uses the determinant of Hessian blob detector. Its feature descriptor is based on sum of the Haar wavelet response in x-direction and y-direction around the point interest.

3.1. Interest point detection
In SURF [3], determinant Hessian obtained from Hessian matrix which defined as follows

\[
H(X, \sigma) = \begin{bmatrix}
L_{xx}(X, \sigma) & L_{xy}(X, \sigma) \\
L_{yx}(X, \sigma) & L_{yy}(X, \sigma)
\end{bmatrix}
\]

(1)

where \(L_{xx}(x, \sigma)\) is the convolution of the Gaussian second order derivative with the image \(l(x, y)\), and similarly for \(L_{yx}(x, \sigma)\) and \(L_{yy}(x, \sigma)\).

The determinant of this hessian matrix, known as the determinant, is calculated by:

\[
det(H) = L_{xx}(X, \sigma)L_{yy}(X, \sigma) - (L_{xy}(X, \sigma))^2
\]

(2)

Since SURF is invariant to scale, SURF constructs a pyramid scale space. SURF directly change the scale of the filters to implement the scale space. To locate the interest points, each pixels compared to its 26 neighbors, 8 neighbor pixels in the native scale and 9 neighbor pixels of the scale above and below. Those pixels which have maximal value will be the interest points.

![Figure 1. Interest point on face spoof[7].](image)

3.2. Interest point description
In [3], the first step is create a square region around the interest point with size 20x20. The square is split up equally into 4x4 square sub-region. For each sub-region, we compute the Haar wavelet response in x-direction \((dx)\) and y-direction \((dy)\). Then, the wavelet response are summed up over each sub-region. We also compute the absolute values of the response. Hence,
each sub-region has a four dimensions descriptor vector \( v = (\sum dx, \sum dy, \|\sum dx\|, \|\sum dy\|) \)
and the total of feature vector would be 64 dimensions.

![Figure 2. Interest point descriptor[3].](image)

4. Pyramid Histogram of Oriented Gradient (PHOG)
HOG descriptors provide excellent performance than the other existing feature [9]. HOG is used to capture information about gradient and edge direction to describe the shape and appearance of an image[1]. PHOG is an extension of Histogram of Oriented Gradient (HOG).

In [4], image is divided into regions based on spatial pyramid matching. HOG is computed in each region at each pyramid resolution kernel. The final PHOG descriptor is a concatenation of all HOG vectors. Length of the PHOG is based on number of levels and bin used. Level 0 is represented by a \( K \)-vector corresponding to the \( K \)-bins of the histogram, level 1 by a \( 4K \)-vector etc. and the PHOG descriptor of the entire image is a vector with dimensionality \( K = \sum_{i=0}^{L} 4^i \) The illustration can be seen on figure 3.

![Figure 3. Illustration of PHOG[10].](image)

5. Research methodology
System built on this research is a system that can detect face spoof attack using SURF and PHOG method. There are two processes: modelling and testing scheme. The flowchart of the scheme can be seen on figure 4 and figure 5.
5.1. Feature Extraction
On this step, the feature obtained from the input data is interest points extracted by SURF and histogram extracted using by PHOG.

5.2. Classification
On this step, the classification used is SVM and KNN for intra-database and cross-database scenario. The classification will result model to be used for testing scheme.

5.3. Evaluation
From the result of prediction class on testing scheme, then the evaluation is performed on the system by performing the calculation of the performance of the system. Performance calculation using Half Total Error Rate (HTER).

The database used in this research are from NUAA, CASIA, IDIAP, and MSU database. These databases consist of:

| Table 1. A summary of four spoof face database[6]. |
|----------------|----------------|----------------|----------------|----------------|
|                | NUAA           | IDIAP          | CASIA          | MSU            |
|                | Train | Test | Train | Test | Train | Test | Train | Test |
| #Subject       | 8     | 7    | 120   | 160  | 20    | 30   | 34    | 28   |
| Attack         | Warped photo  | Intact photo   | 1. Warped photo|
|                | 2. Cut photo  | 3. Video playback|
|                | 1. Printed photo |
|                | 2. Video playback |
6. Testing result
There are two scenarios for testing scheme. The first scenario is spoofing detection in intra-database. The second scenario is spoofing detection in cross-database.

6.1. Intra-database
On this scenario, we compare the intra-database performance between SURF+PHOG, SURF, and PHOG on four databases that mention above. The result can be seen on table 2.

| Method     | MSU  | NUAA | CASIA | IDIAP |
|------------|------|------|-------|-------|
| SURF       | 35.2%| 32.3%| 60.1% | 34.2% |
| PHOG       | 14.1%| 25.2%| 64.3% | 48.4% |
| SURF+PHOG  | 13.0%| 23.8%| 66.9% | 47.6% |

The table shows the performance comparison of SURF+PHOG, SURF, and PHOG in HTER (Half Total Error Rate). From table 2, can be seen that SURF+PHOG has the lowest HTER at some databases: MSU and NUAA.

6.2. Cross-database
On this scenario, we compare the intra-database performance between SURF+PHOG, SURF, and PHOG, but the dataset for modelling process will be different from dataset for testing process. The result can be seen on table 3.

|          | SURF | PHOG | SURF+PHOG |
|----------|------|------|-----------|
| NUAA     | 54.70% | 47.20% | 47.80% |
| IDIAP    | 72.80% | 44.60% | 39.50% |
| CASIA    | 52.80% | 38.70% | 38.30% |

(a) Cross-database scenario performance comparison with MSU as data train

|          | SURF | PHOG | SURF+PHOG |
|----------|------|------|-----------|
| MSU      | 41.30% | 38.80% | 37.90% |
| IDIAP    | 53.40% | 51.00% | 49.40% |
| CASIA    | 51.96% | 45.20% | 44.90% |

(b) Cross-database scenario performance comparison with NUAA as data train

|          | SURF | PHOG | SURF+PHOG |
|----------|------|------|-----------|
| MSU      | 42.30% | 42.20% | 42.30% |
| IDIAP    | 43.60% | 28.90% | 29.00% |
| NUAA     | 58.10% | 56.00% | 56.10% |

(c) Cross-database scenario performance comparison with CASIA as data train

|          | SURF | PHOG | SURF+PHOG |
|----------|------|------|-----------|
| MSU      | 55.20% | 62.60% | 61.80% |
| CASIA    | 53.80% | 43.00% | 41.20% |
| NUAA     | 37.50% | 54.40% | 54.40% |

(d) Cross-database scenario performance comparison with IDIAP as data train

The table shows the performance comparison of SURF+PHOG, SURF, and PHOG in HTER (Half Total Error Rate). From table 3 can be seen that for some databases as data train, such a
MSU, NUAA, and IDIAP, SURF+PHOG method has the lowest HTER. This can be interpreted that SURF+PHOG has generalization ability because it can detect spoof attack in different database which is different subject, illumination, camera quality, and spoof attack.

7. Conclusion
In this research, we implemented the spoofing detection on facial using the combination of texture and shape analysis. We used Speeded-Up Robust Features (SURF) as texture analysis and Pyramid Histogram of Oriented Gradient (PHOG) as shape analysis. From experiment result, the proposed method showed good result than that of using single feature extraction algorithm, such as SURF and PHOG. On intra-database, the proposed method gave the HTER 13.0% on MSU database and 23.8% on NUAA database. On cross-database scenario, the proposed method gave the lowest HTER 38.3% on MSU-vs-CASIA database to detect face spoofing attack so it can be concluded that the proposed method has generalization ability.

References
[1] Dubey R K, Goh J and Thing V L 2016 IEEE Transactions on Information Forensics and Security 11 1461–1475
[2] Wen D, Han H and Jain A 2015 IEEE Trans. Information Forensic and Security 10 746–761
[3] Bay H, Tuytelaars T and Van Gool L 2006 Surf: Speeded up robust features European conference on computer vision (Springer) pp 404–417
[4] Huang H M, Liu H S and Liu G P 2012 Advances in information Sciences and Service Sciences 4 1–8
[5] Chingovska I, Anjos A and Marcel S 2012 On the effectiveness of local binary patterns in face anti-spoofing Biometrics Special Interest Group (BIOSIG), 2012 BIOSIG-Proceedings of the International Conference of the (IEEE) pp 1–7
[6] de Freitas Pereira T, Anjos A, De Martino J M and Marcel S 2012 Lbp- top based countermeasure against face spoofing attacks Asian Conference on Computer Vision (Springer) pp 121–132
[7] Du G, Su F and Cai A 2009 Face recognition using surf features MIPPR 2009: Pattern Recognition and Computer Vision vol 7496 (International Society for Optics and Photonics) p 749628
[8] de Freitas Pereira T, Anjos A, De Martino J M and Marcel S 2013 Can face anti-spoofing countermeasures work in a real world scenario? Biometrics (ICB), 2013 International Conference on (IEEE) pp 1–8
[9] Mao L, Xie M, Huang Y and Zhang Y 2010 Preceding vehicle detection using histograms of oriented gradients Communications, Circuits and Systems (ICCCAS), 2010 International Conference on (IEEE) pp 354–358
[10] Li H, Sun F, Liu L and Wang L 2015 Neurocomputing 169 77–88