ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

ESTIMATION OF FACE USING WARPING AND DISTORTION ANALYSIS

E.Akilandeswari[1], (akilaelumalai0334@gmail.com) ,S.Divya[2], (divyasece31@gmail.com),

M.Karthika[3], (karthi30145@gmail.com), R.Sathiya[4], (sathiyarp.ece26@gmail.com)

Department of Electronics and Communications Engineering

Bharathiyar Institute of Engineering for Women

Guided by

R.Kavitha, (HOD/ECE),(kavitharbe@gmail.com)

Abstract—Face recognition (FR) systems in real-world applications need to deal with a wide range of interferences, such as occlusions and change appearance in face images. A novel approach, coined dynamic image-to-class warping (DICW), is proposed in this work to deal with this challenge in FR. The face consists of the forehead, eyes, nose, mouth, and chin in a natural order and this order does not change despite occlusions. Thus, a face image is separated into patches.Face recognition has raised concerns about face spoof attacks (also known as biometric sensor presentation attacks), where a photo or video of an authorized person's face could be used to gain access to facilities or services. Four different features (specular reflection, blurriness, chromatic moment, and color diversity) are extracted to form the IDA feature vector. Our method is able to deal with occlusions which exist in both gallery and probe images. Our results also highlight the difficulty in separating genuine and spoof faces.

***Index Terms*—Face recognition, image distortion analysis, ensemble classifier, cross-database, dynamic time warping.**

I.INTRODUCTION

Face recognition- Nowadays, automatic FR system achieves significant progress in controlled conditions. However, the performance in unrestricted conditions (e.g., large variations in illumination, pose, expression, etc.) is still unsatisfactory. In the real-world environments, faces are easily lied by facial accessories (e.g., sunglasses, scarf, hat, veil), objects in front of the expression (e.g., hand, food, mobile phone), extreme illumination (e.g., shadow), self-occlusion (e.g., non-frontal pose) or poor image quality (e.g., blurring). The difficulty of occluded FR is twofold. there are two related but different problems to Face Recognition with occlusions: occluded face detection and occluded face recovery. The first task is to determine whether a face image is occluded or not , which can be used for automatically rejecting the occluded images in applications such as passport image enrolment. The second task is to restore the occluded region in face images .

It can recover the lied area handling occlusion in FR is to detect the lied region first and then perform recognition using only the unlied part. Min et al. adopted a SVM classifier to detect the occluded region in a face image then used only the unlied area of a probe face (i.e., query face) as well as the corresponding area of the gallery faces (i.e., suggestion faces) for recognition. The location, size and shape of occlusions are unknown, hence increasing the difficulty in segmenting the lied region from the face images. . There are two main categories of approaches in this direction. The first is the rebuilding corresponded approaches which treat occluded FR as a reconstruction problem. The reconstruction based approaches usually require a large number of samples per subject to represent a probe image. However, a sufficient number of samples are not available in practical scenarios. The second category is the local identical based approaches. Facial features are extracted from local areas of a face. We propose a local matching based method; Dynamic Image-to-Class Warping (DICW), for

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

occluded FR. DICW is motivated by the Dynamic Time Warping (DTW) algorithm which allows elastic match of two time sequences.

In our work, an image is partitioned into patches, which are then concatenated in the raster scan order to form a sequence. In this way, a face is represented by a patch sequence which contains the order information of facial features. DICW calculates the Image-to-Class distance between a query face and those of an enrolled subject by finding the optimal alignment between the query sequence and all enrolled sequences of that subject. Our method allows elastic match in both time and with-class directions. a novel approach that takes the facial order, which contains the geometry information of the face, into account when recognising partially occluded faces. Anovel approach that takes the facial order, which contains the geometry information of the face, into account when recognising partially occluded faces.

AS A convenient user authentication technique, automatic face recognition has attracted increasing attention in various access control applications, especially for mobile phone unlocking. With the release of face unlocking functionality in the Android mobile operating system, face recognition becomes another biometric authentication technique for mobile phones, similar to fingerprintauthentication(Touch ID) in the iOS system. Unlike fingerprint authentication, face recognition does not require any additional sensor since all smart phones come equipped with a front facingcamera.

Fig. 1. A genuine face image (a) of a subject in the Idiap databases and three examples of spoofs of the same subject using a (b) printed photo,(c) displayed photo (on a tablet screen), and (d) 3D face mask.

It is relatively easier to acquire a person's face image or video (e.g., with a digital camera or from social media) than it is to acquire other biometric traits such as fingerprint, palm print, and iris. Further, the cost of launching a face spoof attack, such as a printed photo, displayed photo, or replayed video is relatively low.

Face spoof detection, published methods can be categorized into four groups:

(i) motion based methods,

(ii) texture based methods,

(iii) method based on image quality analysis,

(iv)methods based on other cues.

i)Motion Based Methods: The subconscious motion of organs and muscles in a live face, such as eye blink, mouth movement and head rotation. The frequency of facial motion is restricted by the human physiological rhythm, which ranges from 0.2 to 0.5 Hz. Additionally, motion based methods can be easily confused by other motions,e.g.,background motion.

(ii) Texture Based Methods: To counter both the printed photo and replayed video attacks Unlike motion based methods, texture based methods need only a single image to detect a spoof.

(iii) Image Quality Analysis Based Methods: A recent work proposed a biometric liveness detection method for iris, fingerprint and face images using 25 image quality measures,

(iv) Methods Based on Other Cues: Face spoof counter- measures using cues derived from sources other than 2D intensity image, such as 3D depth , IR image , spoofing context , and voice have also been proposed. An IR sensor was required, microphone and speech analysers were required, and multiple face images taken from different viewpoints were required.

II. DYNAMIC IMAGE-TO-CLASS WARPING

A.Image Representation

An image is partitioned into J non-overlapping patches of d×dpixels. Those patches are then concatenated in the raster scan order (i.e., from left to right and top to bottom) to form a single sequence. The reason for doing so is that the forehead, eyes, nose, mouth and chin are located in the face in a natural order, which does not change despite occlusions or imprecise registration. This spatial facial order, which is contained in the patch

sequence, can be viewed as the temporal order in the time sequence.

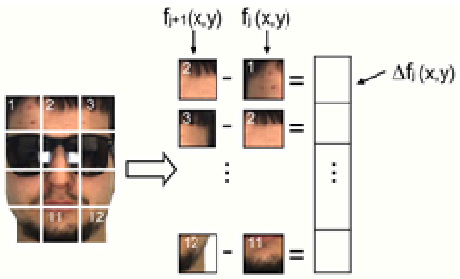


Fig. 1. Image representation of DICW.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

B.Implementationthrough Dynamic Programming

To compute distDICW(P,G) in (4), one could test every possible warping path but with a high computational cost. Fortunately, (4) can be solved efficiently by Dynamic Programming. A three-dimensional matrix D ∈ RM×N×K is created to store the cumulative distance.

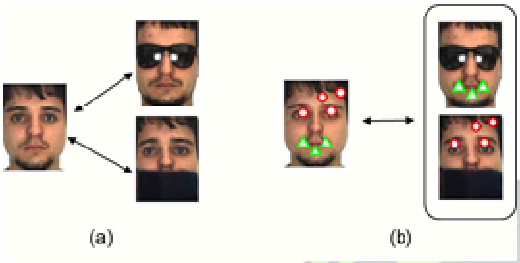


Fig. 5. The illustration of (a) the *Image-to-Image* and (b) the *Image-to-Class*

Matched features are indicated by the same symbol.

The Image-to-Class distance is the globally optimal cost for matching. Although occlusions are not directly removed, avoiding large distance error by warping is helpful for classification from our experimental results.

Image-to-Class distance based Naive Bayes Nearest Neighbour (NBNN) as ours and the baseline, Hidden Markov models (HMM) which also consider the order information in a face.

Algorithm 1 Dynamic Image-to-Class Warping Distance DICW(P,G,l)

Input:

P: a probe sequence with M patches;

G: a set ofK gallery sequences (each with N patches) of a given class;

l: the window width;

Output:distDICW: theImage-to-Class distance between P and G;

1: Set each element in D to ∞;

2: D[0,0,1: K]=0;

3: l=max{1,|M −N|};

4: Compute the local distance matrix C;

5: **for** m =1 toM do

6: **for** n =max{1,m−l} to min{N,m+l} do

7: minNeighbour=min{$\boldsymbol{D}[m-1, n-1, 1{:}K]$,
$\boldsymbol{D}[m-1, n, 1{:}K]$,
$\boldsymbol{D}[m, n-1, 1{:}K]$};

8: **for** k =1 toK do

9: D[m,n,k]=minNeighbour+C[m,n,k];

10: **end for**

11: **end for**

12: **end for**

13: distDICW =min{D[M, N,1: K]};

14: **return**distDICW;

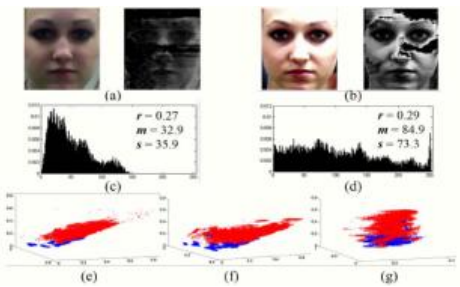
III. FEATURES DERIVED FROM IMAGE DISTORTION ANALYSIS

In mobile applications, the real-time response of face spoof detection requires that a decision be made based on a limited number of frames, e.g., no more than 30 frames (∼1 sec. for videos of 30 fps). Therefore, we aim to design discriminative features that are capable of differentiating between genuine and spoof faces based on a single frame.

1)Printed Photo Attack: In printed photo attack, I(x) is first transformed to the printed ink intensity on the paper and then to the final image intensity through diffusion reflection from the paper surface

2)Replay Video Attack: In replay video attack, I(x) is transformed to the radiating intensity of pixels on LCD screen.

A. Specular Reflection Features - In this paper, we separate the specular reflection component is from an input face image or video frame.



ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

Fig. 4. Illustration of specularreflection features. (a) A genuine face image and the detected specular reflection component; (b) A spoof face (replayed video) and the detected specular reflection component; (c-d) histograms and specific feature values of the specular reflection components in (a) and (b), respectively; (e-g) distributions of the three specular reflection features (blue: genuine samples, red: spoof samples) in the Idiap training, Idiap testing, and MSU testing sets, respectively.

B. Blurriness Features -For short distance spoof attacks, spoof faces are often defocused in mobile phone cameras

C. Chromatic Moment Features -Recaptured face images tend to show a different color distribution compared to colors in the genuine face images. This is caused by the imperfect color reproduction property of printing and display media.

D. Color Diversity Features-Another important difference between genuine and spoof faces is the color diversity. In particular, genuine faces tend to have richer colors

IV. CLASSIFICATION METHOD

A. Ensemble Classifier -Given that our aim is to design an efficient face spoof detection system with good generalization ability and quick response, it is desirable to have an efficient classifier for the extracted IDA features.

B. Multi-Frame Fusion- Given the face spoof detection classifier working on a single image, a multi-frame fusion scheme is proposed to achieve a more stable face spoof detection performance for a video**.**

V. FACE SPOOF DATABASES

A. Public Domain Face Spoof Databases- three public-domain face spoof databases: NUAA Photograph Imposter database , Idiap REPLAY-ATTACK database and CASIA Face Anti-Spoofing Database.

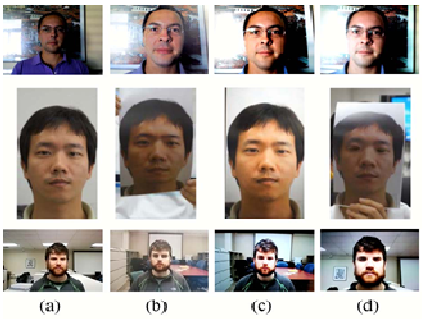


Fig. 6. Typical face samples from the Idiap (first row), CASIA H subset(second row) and MSU (third row) spoofing databases. (a) Genuine faceimages; (b) Spoof faces generated for printed photo attack; (c) Spoof faces generated by HD tablet screen; (d) Spoof faces generated by mobile phonescreen (first and third row) or cut photo (second row).

B. MSU MFSD Database- The MSU MFSD database10 consists of 440 video clips of photo and video attack attempts of 55 subjects. Two types of cameras were used in collecting this database: i) built-in camera inMacBookAir13referred to as laptop camera; ii) front-facing camera in the Google Nexus 5 Android phone, referred to as Android camera.

1) Genuine Face- The (true) subject presents his face close to the camera, and a genuine face video is recorded using both the Android and laptop cameras.

2) Spoof Attack - Video Replay: The video of the subject's face is first recorded using a Canon 550D Single-lens reflex (SLR) camera and an iPhone 5S back-facing camera.

3) Spoof Attack - Printed Photo: The Canon 550D camera is also used to capture a HD picture (5184 × 3456) of the subject's face, which is then printed on an A3paper(11.7using a HP Color Laserjet CP6015xh printer (1200×600dpi) to generate a printed photo for attack.

VI. TESTING PROTOCOL AND BASELINE METHODS

To evaluate the effectiveness and generalization ability of the proposed face spoof detection methods

A. Intra-Database Testing Protocol

B. Cross-Database Testing Protocol

C. Baseline Methods

VII. EXPERIMENTAL ANALYSIS

We evaluated three different types of spoof detection feature vectors: LBP features, DoG-LBP features and IDA features.

A. Intra-Database Spoof Detection -This experiment is to compare the intra-database performance of the proposed method with the baseline methods and state-of-the-art methods on three databases: Idiap, CASIA (H protocol),and the MSU database.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

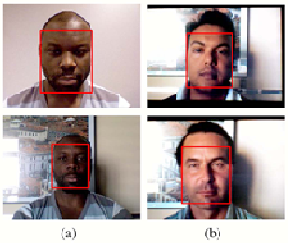


Fig. 8. Examples of mis-classified face images by the proposed approach intheIdiap intra-database experiment. (a) Genuine face images (dark skin) aremisclassified as spoof attacks; (b) Spoof attack face images with relativelysmall image distortions are misclassified as genuine face images.

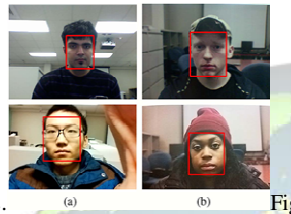


Fig.9. False negative and false positive examples in the MSU intra-databaseexperiment. (a) Genuine face images with dark skin (top) and with motionblurriness (bottom); (b) Spoof face images with small image distortion (top)and with dark skin (bottom).

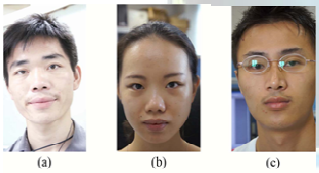


Fig. 10. Genuine faces with over saturated exposure in the CASIA (H) database, which is misclassified by the proposed approach in theCASIA (H) intra-database experiment.

B. Cross-Database Spoof Detection- Besides the intra-database performance, we are more interested in the cross-database performance of different face spoof detection methods. Since the IDA features do not contain any characterization of facial appearance, they are expected to have better cross-database generalization ability than the texture features

A. Face Identification With Randomly Located Occlusions

We first evaluate the proposed method using the Face Recognition Grand Challenge (FRGC) database with randomly located occlusions. Note that in each image, the locations of occlusions are randomly chosen and unknown to the algorithm.

Fig.6. Sample images from the FRGC database with randomly located occlusions.

To simulate the randomly located occlusions, we create an occluded image set by replacing a randomly located square patch (size of 10% to 50% of the originalimage) from each image in the original image set with a black block (Fig. 6).

B. Face Identification With Facial Disguises

We next test the proposed method on the AR database which contains real occlusions. First, we consider that no occlusion is present in both gallery and probe setsThe AR database contains over 4,000 colour images of 126 subjects faces. For each subject, 26 images in total are taken in two sessions (two weeks apart). All images are cropped and re-sized to 83×60 pixels and the patch size is 5×5 pixels.

1) Without Occlusion: each subject, 14 images are chosen. Seven images from Session 1 are used as the gallery set and the other seven from Session 2 as the probe set

Fig. 11. Sample images from the TFWM database.

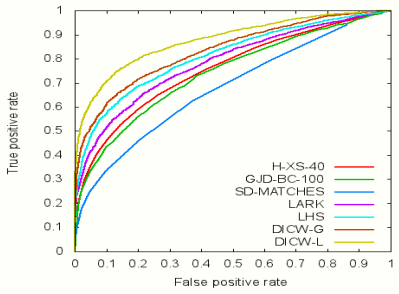
A. Face Identification With General Occlusions in Realistic Environment

In this Section, we test our method on the Face We Make (TFWM) database captured under natural and arbitrary conditions. It has more than 2,000 images which contains frontal view faces of strangers on the streets with uncontrolled lighting.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

B. Discussion:

1) The Effect of Patch Size: To investigate this the impact of patch size on the performance, we use 400 unoccluded images (size of 80×65 pixels) of 100 subjects



from the FRGC database as the gallery set and 400 images in each of six probe sets, which contain randomly located occlusions from 0% to 50% level, respectively.

2) The Effect of Patch Overlap: In the previous experiments we used the difference patch to enhance the textured features in patches.

3) The Effect of Image Descriptor: In Section III-D2, our experiments indicate that the difference patch leads to better accuracy since it is able to enhance the textured regions in a face image.

4) Robustness to Misalignment:The face registration error can largely degrade the recognition performance as we mentioned in Section I. To evaluate the robustness of DICW to the misalignment of face images, we use a subset of the AR database with 110 used in the work in..

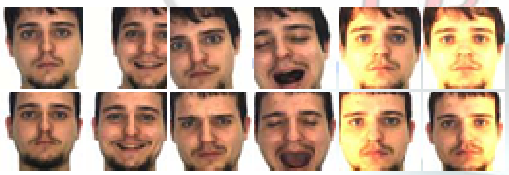


Fig. 16. Sample images of the same subject from database withoutalignment (AR-VJ).

Different from the images in the original AR database which are well cropped (Fig.5), these images contain large crop and alignment errors as shown in Fig. 16.

5)Exension to Face Verification in the Wild:In this Section, we extend DICW for face verification tasks using the Labelled Faces in the Wild (LFW) database which is the most active benchmark for FR. Note that in the verification of each pair, it is an Image-to-Image comparison.

Fig.17. Sample images from the LFW database (six matched image pairs for six subjects)

Fig.18. ROC curves of the-state-of-the-art methods and DICW on the LFW database.

6)Computational Complexity and Usability Analysis:From Algorithm 1 in Section II-C we can see that the time complexity of DICW for computing the distance between a query image and an enrolled class is O(max{M, N}IK), where M, N are the numbers of patches in each probe sequence and gallery sequences

XI.FURTHER ANALYSIS AND IMPROVEMENT

In the previous sections, we evaluate DICW using extensive experiments with face images with various uncontrolled variations.

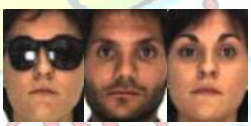


Fig. 19. (a) The probe image from class 74. (b) Classification result (class 5) by NBNN. (c) Classification result (class 74) by DICW.

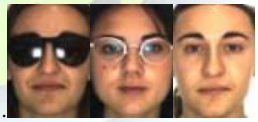
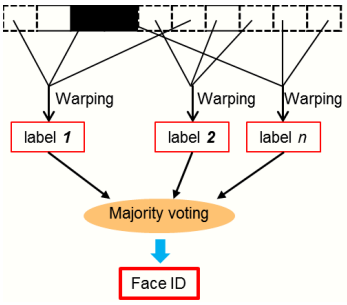


Fig. 20. (a) A probe image from class 51. (b) The wrong class (class 72) classified by DICW.(c) The gallery image from class 51.



ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

Fig.21. Random selection and majority voting scheme for improving the performance of DICW

X. CONCLUSION AND FUTURE WORK

Our suggestions for future work on face spoof detection include: (i) understand the characteristics and requirements of the use case scenarios for face spoof detection, (ii) collect a large and representative database that considers the user demographics (age, gender, and race) and ambient illumination in the use case scenario of interest, (iii) develop robust, effective, and efficient features (e.g., through feature transformations for the selected use case scenario, and (iv) consider user-specific training for face spoof detection.

REFERENCES

[1] A. Rattani, N. Poh, and A. Ross, "Analysis of user-specific score characteristics for spoof biometric attacks," in *Proc. IEEE Comput. Soc.Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, Jun. 2012,pp. 124–129.

[2] Z. Wu, N. Evans, T. Kinnunen, J. Yamagishi, F. Alegre, and H. Li,"Spoofing and countermeasures for speaker verification: A survey," *Speech Commun.*, vol. 66, pp. 130–153, Feb. 2015.

[3] L. Best-Rowden, H. Han, C. Otto, B. F. Klare, and A. K. Jain,"Unconstrained face recognition: Identifying a person of interest from a media collection," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 12,pp. 2144–2157, Dec. 2014.

[4] H. K. Ekenel and R. Stiefelhagen, "Why is facial occlusion a challengingproblem?" in *Proc. IAPR 3rd Int. Conf. Biometrics (ICB)*, 2009,pp. 299–308.M. Storer, M. Urschler, and H. Bischof, "Occlusion detection forICAO compliant facial photographs," in *Proc. IEEE Comput. Soc.Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, Jun. 2010,pp. 122–129.[6] D. Lin and X. Tang, "Quality-driven face occlusion detection andrecovery," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*,Jun. 2007, pp. 1–7.