# Identifying Human Face under video surveillance using Machine Learning Technique

<sup>1</sup>Ashok R. Avachar, <sup>2</sup>Dr Shubhangi D. Sapkal, <sup>3</sup>N Dr. Ratnadeep R. Deshmukh

<sup>1</sup>ME. CSE Student, <sup>2, 3</sup>Professor <sup>1</sup>Computer Science and Engineering, <sup>1</sup>Government College of Engineering, Aurangabad, India

*Abstract*: Automatic Physiognomy recognition systems are now popularly used in various applications ranging from mobile payment verification to inbuild security access. The use of Physiognomy recognition has increased awareness about facial simulation attacks viz is also called as a biometric sensor presentation attack) that can use a picture or motion file of the Physiognomy of an known person with access to facilities or services. While the amount of Physiognomy identification methodologies that have been proposed do have the ability to place general implications however they are not adequately addressed that is why we offer a powerful and robust Physiognomy detection algorithm using image distortion analysis (IDA). Four different properties (Spectrum deflection, interval, color, and variety with colors) these can be separated to create an IDA class feature set vector, which consists of several SVM classifiers that have been trained for disguised Physiognomy forgery. (Eg printed photos and replayed videos) that are utilized to distinguish between true Physiognomy and pseudo-physiognomy. The method that is addressed here covers detecting multiple Physiognomy in a video using voting patterns.

# Index Terms: Component, formatting, style, styling, insert.

## I. INTRODUCTION (HEADING 1)

Physiognomy recognition attracts a lot of attention in various access control techniques, more over with unlocking of cellular phones. With the launch of the Physiognomy unlocking feature in mobile phones for Android platform, Physiognomy recognition has become a distinct biometric authentication feature for today's mobile phones, this feature is also needed as much as fingerprint identification technique that uses finger print signature of user to unlock the phone. In IOS system, facial feature identification does not need any additional sensors because every smartphone comes with a front camera. However, as with other biological radiation [1], [2], we are supposed to deal with issues such as Physiognomy-to-Physiognomy attacks in Physiognomy identification systems, especially in situations of unlimited awareness and non-cooperation. 3]. Obtaining a individual's Physiognomy (such as with a digital camera or social media) of video is quite easier then getting other biological features such as fingerprints, palm prints and iris. In addition, the process of activating Physiognomy forgery, such as printed photos, display images or videos that are replayed is relatively low in cost. The modern commercial Physiognomy recognition system is designed poorly to distinguish fake ones from real Physiognomy.

In this article, we intend to understand the problem of fake Physiognomy db counterfeiting detection and decide on fake facial attribute detection methods based on image distortion analysis (IDA). The contributions of this article can be summarized as follows:

i) Physiognomy identification algorithms using IDA, that is effective in capturing the true distortion of fake Physiognomy images related to real and original Physiognomy images.

## **II. LITERATURE**

According to our knowledge, one of the fastest studies on Physiognomy forgery detection was reported in 2004 by Li et al. [13] With the increasing popularity of using Physiognomy recognition for access control, topics This has attracted significant attention during the past five years [4], [7] - [12]. One of the main points of the project funded by the FP7 EU is TABULA RASA [14] is "Biometrics at Reliable under attack Counterfeit.

Here we have a brief summary of the Physiognomy detection algorithms published in literature, along with strengths and limitations in terms of:

(i) robustness and generalization ability, and

(ii) real-time response and usability. According to different types of cues used in Physiognomy spoof detection, published methods can be categorized into four groups:

- (i) motion based methods,
- (iii) texture based methods,

(iii) method based on image quality analysis, and

(iv) methods based on other cues

## Motion based methods

The strategies are made to counter assaults and the most significant picture is control: the intuitive development of organs and muscles in the Physiognomy of life, for example, squinting [10], development of the mouth [15] and turning the head [11] in light of the fact that movement is a relative property in the video outline. These strategies are relied upon to have a superior speculation capacity than this strategy. Utilize the surface to be examined underneath. In any case, the confinements of the strategy utilized are

clear. The regularity of facial developments is constrained by human physiological rhythms that range from 0.2 to 0.5 Hz [12], so it takes a significant long time (usually> 3 seconds) to gather stable vitality properties for Physiognomy fabrication discovery. Likewise, strategies that utilization movement can likewise be confounded by different developments, for example, foundation developments that don't include facial developments or reiteration in video assaults.

#### **Texture based methods**

In retaliation for the printed image and the video that has been played on another device, the surface presentation method was proposed to separate the artifacts of the image in a fake image. [18] The author argued that the surface characteristics (such as LBP, DoG or HOG can distinguish things) The invention of counterfeiting from genuine Physiognomy.

#### Methods based on image quality analysis

Ongoing work [22] offers techniques for recognizing biometric life forms for iris, fingerprints and Physiognomy pictures utilizing 25 picture quality estimations, including 21 full reference plans and estimations. Which does not reference 4 things contrasted with [22]. Our work is diverse in the accompanying territories: (1) while needing 25 properties in [22] for good outcomes, no Physiognomy information is considered in the structure Data highlights for fake Physiognomy location interestingly, four highlights are exceptionally intended for facial highlights in our strategy and we exhibit the viability of these highlights in identifying counterfeit Physiognomy. Despite what might be expected, the proposed technique is planned to improve general capacities in the circumstance of cross-database information that is seldom investigated in various networks.

#### Methods based on other cues

Adulterating by using prompts got from sources other than 2D power pictures, for instance, 3D significance [19], IR pictures [6], misrepresentation setting [20] and sound [21]. These are the additional essentials for customers or the game plan of physical affirmation and as needs be have a littler application go. For example, an IR sensor is required in [6]. Need to use a collector and talk analyzer in [21] and must use a lot of physical pictures taken from a substitute perspective in [19] The fake setting proposed in [20] can be kept up a vital good ways from by disguising fake media.

In the condition inside the database, acknowledged that fake media (Such as indicating photos and screens) cameras, normal factors, and even known sorts in the physical area structure. This theory isn't secured in the most veritable conditions. The efficiency of the inward database of physical disclosure structures is only the most extraordinary degree with respect to execution that can't be ordinary in genuine Ii applications). In a cross-database circumstance, we grant the usage of different sorts of media. Adulterating of cameras, cameras, circumstances and articles during the system headway strategy and structure association process. Appropriately, the introduction in this database reflects the certifiable display of the structure that can be typical in veritable applications. ii) Methods Available, especially the system that uses surface properties, ordinarily used properties, (for instance, LBP) that can record nuances, physiognomy and detachment Another refinement from the other.

Thusly, when using a comparative ability to perceive authentic physical substance from pseudopages, they may have some dreary data for development area or individual information. These two segments limit the ability to address existing strategies. To handle this issue, we have proposed a great deal of features subject to picture bending assessment (IDA) with ceaseless response.

## **III. PROPOSED SYSTEM**

When using a comparative ability to perceive authentic physical substance from pseudopages, they may have some dreary data for development area or individual information. These two segments limit the ability to address existing strategies. To handle this issue, we have proposed a great deal of features subject to picture bending assessment (IDA) with ceaseless response. (Disconnected from a singular picture with a suitable estimation) and improve all around execution in cross database conditions when diverged from existing systems, proposed strategies, taking the necessary steps not to perceive properties that catch physical physiological nuances But endeavoring to get the refinement in the idea of the physiognomy in light of the various reflecting properties of various materials, for instance, the base of the paper and the screen. The exploratory results exhibit that the proposed strategy can hypothesis.

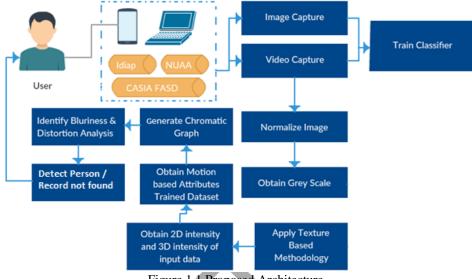


Figure 1.1 Proposed Architecture

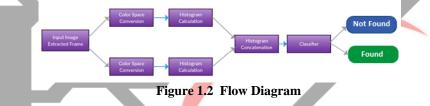
When considering the circumstance where real physicality is fashioned (Eg printed photographs or recordings that are played back on the screen) will be introduced to the camera in a similar shooting condition. The fundamental contrast between real physical and phony pictures is brought about by "The shape and presence of the outside of the body before the camera as per the Dichromatic reflector model [24] The impression of the article at a particular position x can be partitioned into diffuse reflection (Id) and specular reflection. (Is):

I(x) = Id + Is = wd(x)S(x)E(x) + ws(x)E(x) (1)

Whenever E(x) is the force of the occurrence light, wd (x) and ws (x) are geometric variables for light dispersion and reflection, individually, and S (x) is a diffuse reflection proportion because of the way 2-dimensional fake physical items that have been altered from the first physical picture. The production of the pseudo-face picture force (I) can be made as pursues.

I(x) = Id + Is = F(I(x)) + ws(x)E(x) (2)

It would be ideal if you note that the condition (1) and (2) are various reflections between veritable physical and counterfeit and don't consider the last picture quality after the camera catches in the condition (2. The diffuse impression of the pseudo-physical picture I d by F (I (x)) on the grounds that the diffuse reflection is controlled by the bending of the first physical picture I (x).



In this way, all twists in I (x) contrasted with I (x) comprise of two sections: I) Distortion in diffraction components (I d) and ii) Distortion in both intelligent components (I s) which are connected. With falsification The media, specifically, I identify with the conventional physical picture I (x) while I am free from me (x). What's more, it can likewise make a contortion capacity model F(x) in a diffuse reflection component.

$$F(I(x)) = H(GI(x))_{(3)}$$

Where G(x) is a low pass point dissemination work (Makes the first Physiognomy obscured) and H(x) as the histogram change work (Distortion of shading power) of G(x) and H(x).

In the assault, the printed photographs and assaults, replay recordings are point by point underneath. From this photographic model, we break down the significant contrasts between veritable physical and physical Two sorts of pseudo-physiognomys (printing photographs and recordings over and over, more than once playing or assaulting photographs).

Notwithstanding the diffuse impression of the particular impression of the pseudo-physiognomy, it is not quite the same as the real physical excitement brought about by the fake circle. Since the outside of the tablet/cell phone and the gleaming ink layer on the printed paper frequently show up around the pseudo-physiognomy picture, while the conventional 3D physical make-up is intelligent, it is In the precise position just (Such as the tip of the nose, glasses, temple, cheeks, and so forth.), so consolidating unique reflections from all face pictures can subsequently catch misshaped pictures as pseudo pictures

There might be different contortions that show up in physical pictures, for example, geometric mutilation. (For example, paper twisting) and counterfeit surface examples. Notwithstanding, these mutilations rely upon the camera and lighting. For instance, geometric contortion changes as indicated by splendor and example. Counterfeit surfaces must be seen with superb cameras. So we center around four normal wellsprings of picture contortion in pseudo-physical pictures.

There might be different bends that show up in physical pictures, for example, geometric twisting. (For example, paper distorting) and fake surface examples. In any case, these contortions rely upon the camera and lighting. For instance, geometric contortion differs as indicated by splendor and example. Counterfeit surfaces must be seen with astounding cameras. Along these lines, we center

around four basic wellsprings of picture twisting in pseudo-physiological pictures (specular reflection, foggy, power, shading and assortment of hues) and reliable structure highlights. Together for the recognition of physical parodying.

For transient satire assaults, physiognomy is regularly fooled into utilizing with cell phone cameras. The reason is fashioned media (The paper imprinted on the screen, tablet and cell phone screen) is for the most part of a restricted size and the assailant must be put close to the camera to cover the degree of the media utilized in the assault. Wow And obscured pictures because of absence of center can be utilized as another line for against falsifying. For transient assaults, faking physiognomy is regularly fooled into entering a cell phone camera. The reason is produced media (The paper imprinted on the screen, tablet and cell phone screen) is generally of a restricted size and the assaultant must be set near the camera to cover the degree of the media utilized in the assault. Duplicity Blurred pictures because of absence of center can be utilized as another line for hostile to duplicating.

#### **Chromatic Moment Features**

The physical picture of the shot is probably going to demonstrate an alternate shading conveyance contrasted with the shading in the veritable physical picture. This issue is brought about by inadequate shading creation highlights of print and show media. The disintegration of this shading has been investigated in [35] for identifying pictures taken. Be that as it may, did not know the viability of pseudo-identification in light of the fact that the precise shading circulation relies upon the splendor and decent variety of the camera. We propose to design includes that can't be changed to identify unordinary hues in the manner Hey produced That is, first, we convert the typical physical picture from the RGB region to the HSV region (Hue, Saturation and Value). At that point ascertain the mean, deviation and skewness of each channel as a shading property. Since these three properties are equivalent to three factual periods in each channel, called shading time properties notwithstanding these three properties, at that point the level of pixels in the littlest and most elevated histogram of each channel as it is utilized as two extra highlights.

#### **Color Diversity Features**

Another significant distinction between real Physiognomys and fakes is the assortment of hues, particularly real Physiognomys will in general have more hues. This assortment will in general blur away in the contorted physicality because of shading propagation vanishing during picture/video gathering. In this article, we pursue the strategy utilized in [35] to quantify the assortment of shades of Image First, measure the shading (there are 32 stages in the red, green and blue boxes, separately) in the ordinary physical picture. Two estimations consolidated from the shading conveyance: I) Histograms check the quantity of hues that seem most as often as possible, the main 100 and ii) the quantity of various hues that show up in the typical physical picture.

#### Classification

We propose to utilize the cover classifier model via preparing numerous beguiling classifiers in various gatherings of pseudoassault models. For explicit falsifying databases, we make separate preparing models as pursues: First, forging models are partitioned into K gatherings dependent on assault types. Furthermore, the particular preparing set was made by joining all the authentic examples and one phony example that happened in the K preparing set. K = 2) For two separate assaults, for example, composing assaults and rehashed assaults, picking a band is superior to preparing a solitary classifier in all databases.

During the vector test stage, the information highlight will be gone into all segment classifiers and the outcomes will be joined to get the last outcome. We assessed two sorts of consolidation grades: principles, entireties, and negligible guidelines.

Multi-picture combination on the grounds that the fake Physiognomy identification classifier works in a solitary picture, giving a multi-picture combination position that gives Physiognomy Detection execution to a progressively steady Physiognomy for video. The aftereffects of the characterization of each picture are consolidated by vote to acquire fake discovery scores for the video. The Physiognomy video is set to credible if over half of the pictures are delegated genuine Physiognomy pictures. Because of some distributed strategies for N video fake identification execution, the multi-picture blend augmentation enables us to analyze the exhibition of the proposed technique with present day video, giving a similar term in the video for test.

The significant disservice of these three fake databases is that they are altogether recorded by excellent web cameras or computerized cameras. There is no open space imitation database utilizing a cell phone camera as a catch gadget. The front camera of the cell phone displays the accompanying extra difficulties in recognizing misrepresentation Physiognomy: I) They as a rule have lower goals, thin powerful range, erroneous estimation capacities and auto center. Thus, recordings or pictures taken with these cameras are generally of low quality because of haze. Because of the crumbling in the nature of these pictures, both in the physiognomy of the real physiognomy and in the fakes, they will lessen the distinction among credible and false physiological pictures as far as subtleties of physiology and bending of physiology. picture. work increasingly troublesome, yet to all the more likely recreate the real circumstance, for example, the utilization of opening Physiognomy on the Android cell phone utilizing the front camera.

#### **IV. EXPERIMENTAL SETUP**

To assess the viability of satire recognition calculations, many distributed papers planned and tried their calculations on restrictive farce databases. We use three open space face

parody databases: NUAA Photograph Imposter database [8], Idiap REPLAY-ATTACK database [4] and CASIA Face Anti-Spoofing Database. The NUAA Photograph Imposter database [8], discharged in 2010, is one of the most punctual open space parody databases. It comprises of 12,614 pictures (extricated from 143 recordings) of real and assault endeavors of just 15 subjects. Also, just hand-held printed photograph assault is incorporated into the NUAA database.

The Idiap REPLAY-ATTACK database [4], discharged in 2012, comprises of 1,300 video chronicles of both genuine access and assault endeavors of 50 distinctive subjects.8 In a similar securing condition (controlled and antagonistic enlightenment), the face

parody assaults were produced by manufacturing live check endeavors of similar subjects by means of printed photographs, showed photographs/recordings on cell phone's screen, and showed photographs/recordings on HD screen.

Another perceptible property of these databases is the standoff separation utilized in propelling the parody assaults. We assessed three unique sorts of parody location highlight vectors: LBP highlights (as utilized in [49]), DoG-LBP highlights (as utilized in [50]), and IDA highlights characterized here. The Idiap REPLAY-ATTACK, CASIA FASD (H convention). A similar order design is received for looking at the IDA and different highlights.

Dataset	Precision	Recall	Specificity
CASIA	99.5025	99.5025	99.3333
IDIAP	99.5025	99.5025	99.3333
NUA	99.5025	99.5025	99.3333
Table 1.0 Kay Index Dependence			

Table 1.0 Key Index Parameters

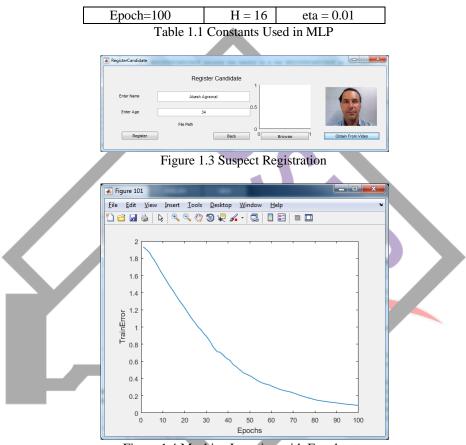


Figure 1.4 Machine Learning with Epoch rate

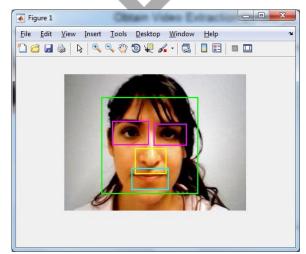


Figure 2.1 Preprocessing Output Voila Jones Face Detection

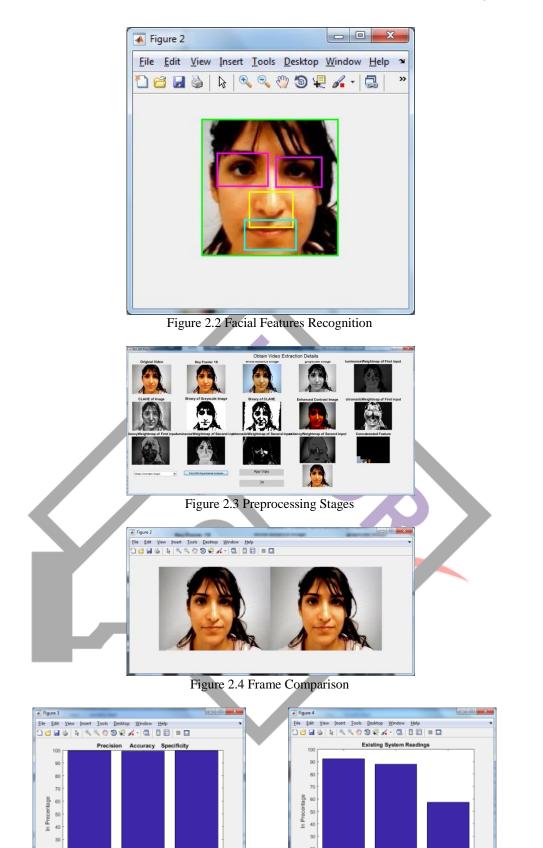


Figure 2.5 Comparison Between existing system and improved methodology.

Precision Accuracy Specificity

# V. CONCLUSION

In this article, we have tackled the issue of identifying Physiognomy misrepresentation, particularly in cross-database circumstances. Albeit most distributed strategies use movement or surface capacities, we propose to distinguish the misrepresentation

Precision Accuracy Specificity

of Physiognomy utilizing picture contortion examination (IDA). Four kinds of IDA capacities (unique reflectivity, diffraction obscure, time, shading, and shading assortment) are intended to catch picture twisting despite a machined picture. The four distinct qualities are connected together, giving an IDA highlight vector of 121 measurements. The gathering classifier comprises of two parts shaped to various mocking assaults, utilized for the distinguishing proof of genuine and misled Physiognomy.

#### **VI. FUTURE SCOPE**

Our proposals for future work on face recognition include: I) Understanding the highlights and necessities of reproductions, use instances of face fabrication discovery, ii) assembling enormous databases and specialists. considering the client populace (age, sexual orientation, light in intriguing use cases, and iii) growing ground-breaking and effective highlights (for instance, by changing over properties [51]) for situation situations. use and (iv) consider client explicit preparing for the discovery of fakes

#### REFERENCES

- [1] Di Wen, Member, IEEE, Hu Han, Member, IEEE and Anil K. Jain, Fellow, IEEE, "Physiognomy Spoof Detection with Image Distortion Analysis," in Proc. CVPR Workshops, 2012, pp. 124–129.
- [2] N. Evans, T. Kinnunen, and J. Yamagishi, "Spoofing and countermeasures for automatic speaker verification," in Proc. INTERSPEECH, 2013, pp. 925–929.
- [3] L. Best-Rowden, H. Han, C. Otto, B. Klare, and A. K. Jain, "Unconstrained Physiognomy 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] I. Chingovska, A. Anjos, and S. Marcel, "On the effectiveness of local binary patterns in Physiognomy anti-spoofing," in Proc. IEEE BIOSIG, 2012, pp. 1–7.
- [5] N. Erdogmus and S. Marcel, "Spoofing in 2D Physiognomy recognition with 3D masks and anti-spoofing with kinect," in Proc. IEEE BTAS, 2013, pp. 1–6.
- [6] Z. Zhang, D. Yi, Z. Lei, and S. Z. Li, "Physiognomy liveness detection by learning multispectral reflectance distributions," in Proc. FG, 2011, pp. 436–441.
- [7] A. Anjos and S. Marcel, "Counter-measures to photo attacks in Physiognomy recognition: A public database and a baseline," in Proc. IJCB, 2011, pp. 1–7.
- [8] X. Tan, Y. Li, J. Liu, and L. Jiang, "Physiognomy liveness detection from a single image with sparse low rank bilinear discriminative model," in Proc. ECCV, 2010, pp. 504–517.
- [9] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, "A Physiognomy antispoofing database with diverse attacks," in Proc. ICB, 2012, pp. 26–31.
- [10] L. Sun, G. Pan, Z. Wu, and S. Lao, "Blinking-based live Physiognomy detection using conditional random fields," in Proc. AIB, 2007, pp. 252–260.
- [11] W. Bao, H. Li, N. Li, and W. Jiang, "A liveness detection method for Physiognomy recognition based on optical flow field," in Proc. IASP, 2009, pp. 233–236.
- [12] S. Bharadwaj, T. I. Dhamecha, M. Vatsa, and R. Singh, "Computationally efficient Physiognomy spoofing detection with motion magnification," in Proc. CVPR Workshops, 2013, pp. 105–110.
- [13] J. Li, Y. Wang, T. Tan, and A. K. Jain, "Live Physiognomy detection based on the analysis of fourier spectra," in Proc. SPIE: Biometric Technology for Human Identification, 2004, pp. 296–303.
- [14] "The TABULA RASA project." [Online]. Available: http://www. tabularasa-euproject.org/
- [15] K. Kollreider, H. Fronthaler, M. I. Faraj, and J. Bigun, "Real-time Physiognomy detection and motion analysis with application in "liveness" assessment," IEEE Trans. Inf. Forensics Security, vol. 2, no. 3, pp. 548–558, 2007.
- [16] T. de Freitas Pereira, A. Anjos, J. M. De Martino, and S. Marcel, "LBP-TOP based countermeasure against Physiognomy spoofing attacks," in Proc. ACCV Workshops, 2012, pp. 121–132.
- [17] T. de Freitas Pereira, A. Anjos, J. De Martino, and S. Marcel, "Can Physiognomy anti-spoofing countermeasures work in a real world scenario?" in Proc. ICB, 2013, pp. 1–8.
- [18] J. Yang and S. Z. Li, "Physiognomy Liveness Detection with Component Dependent Descriptor," in Proc. IJCB, pp. 1–6, 2013.
- [19] T. Wang and S. Z. Li, "Physiognomy Liveness Detection Using 3D Structure Recovered from a Single Camera," in Proc. IJCB, 2013, pp. 1–6.
- [20] J. Komulainen, A. Hadid, and M. Pietikainen, "Context based Physiognomy Anti-" Spoofing," in Proc. BTAS, 2013, pp. 1-8.
- [21] G. Chetty, "Biometric liveness checking using multimodal fuzzy fusion," in Proc. IEEE FUZZ, 2010, pp. 1-8.
- [22] J. Galbally, S. Marcel, and J. Fierrez, "Image quality assessment for fake biometric detection: Application to iris, fingerprint, and Physiognomy recognition," IEEE Trans. Image Process., vol. 23, no. 2, pp. 710–724, 2014.
- [23] H.-Y. Wu, M. Rubinstein, E. Shih, J. Guttag, F. Durand, and W. T. Freeman, "Eulerian video magnification for revealing subtle changes in the world," ACM Trans. on Graphics, vol. 31, no. 4, 2012.
- [24] S. A. Shafer, "Using color to separate reflection components," Color Research and Application, vol. 10, no. 4, pp. 210– 218, 1985.
- [25] O. Bimber and D. Iwai, "Superimposing dynamic range," in Proc. ACM SIGGRAPH Asia, no. 150, 2008, pp. 1-8.
- [26] Pittsburgh Pattern Recognition (PittPatt), PittPatt Software Developer Kit (acquired by Google), http://www.pittpatt.com/. [27] Q. Yang, S. Wang, and N. Ahuja, "Real-time specular highlight removal using bilateral filtering," in Proc. ECCV, 2010,
- pp. 87–100.

- [28] V. Christlein, C. Riess, E. Angelopoulou, G. Evangelopoulos, and I. Kakadiaris, "The impact of specular highlights on 3D-2D Physiognomy recognition," in Proc. SPIE, 2013.
- [29] R. Tan and K. Ikeuchi, "Separating reflection components of textured surfacesusing a single image," IEEE Trans. Pattern Anal. Mach. Intell., vol. 27, no. 2, pp. 178–193, Feb. 2005.
- [30] J.-F. Lalonde, A. A. Efros, and S. G. Narasimhan, "Estimating the natural illumination conditions from a single outdoor image," Int. J. Comput. Vision, vol. 98, no. 2, pp. 123 145, 2011.

