CONTENT

• NEWS
• SPOTLIGHT
• COTS
• INTERVIEW: Prof. Matti Pietikäinen
• PAPER SUMMARY
• CALL FOR PAPER
• DATA SET
• SOURCE CODE
• EMERGING BIOMETRICS
NEWS

IDEMIA introduces new biometric tech to combat identity spoofing

Following an 18-month collaboration effort by Télécom SudParis and IDEMIA, the design of a contactless biometric reader based on a patent filed by two Télécom SudParis researchers has been finalized and the transfer of the technology to IDEMIA is now completed.

The technology involves a next-generation digital fingerprint reader known as BioDigital. According to the announcement, it provides an effective defence against identity spoofing and also offers improved recognition of damaged fingerprint surfaces and has a fingerprint matching success rate bordering on 100%.

This contactless technology recognizes the fingerprint and the subcutaneous print and the network of sweat pores. It relies on optical coherence tomography (OCT), a technique that produces 3D images from “echoes” of backscattered light, offering access to fingerprints without direct contact with the reader. This innovative new feature is also accompanied by outstanding image reconstruction quality.


FIDO Alliance launches biometrics certificate programme

The FIDO Alliance has announced its Biometric Component Certification Programme – calling it the first such Programme for the industry at large. FIDO said the Programme utilizes accredited independent labs to certify that biometric subcomponents meet globally recognized performance standards for biometric recognition performance and Presentation Attack Detection (PAD) and are fit for commercial use. The FIDO Alliance aims to deliver several benefits to providers and users of biometric recognition systems through the new Biometric Component Certification Programme. Until now, due diligence was performed by enterprise customers who had the capacity to conduct such reviews.

This required biometric vendors to repeatedly prove performance for each customer. The FIDO Alliance Programme allows vendors to test and certify only once to validate their system’s performance and re-use that third-party validation across their potential and existing customer base, resulting in substantial time and cost savings. For customers, such as regulated online service providers, OEM’s and enterprises, it provides a standardized way to trust that the biometric systems they are relying upon for fingerprint, iris, face and/or voice recognition can reliably identify users and detect presentation attacks.


NIST announces International Face Performance Conference (IFPC)

Following the IBPC-conference series, the US National Institute of Standards and Technology (NIST) has announced the International Face Performance Conference (IFPC) 2018, which will take place in Gaithersburg from November 27 to 29. EAB will support the conference as co-organizer.

The conference is focused on all technical factors affecting the deployment and use of high performance face recognition applications, including applications, standards, advanced and rapid capture, quality assessment, age and ageing effects, demographic effects, presentation attack detection, non-cooperative uses, accuracy measurement and performance tests.

Cutting-edge face recognition technology reaches the mobile consumer market

Maria De Marsico

Looking at the tremendous advances in the possibilities provided by biometric recognition on consumer devices, one may ask what is left to do on mobiles. In particular, mobile devices are continuously empowered following the last technological findings. Three recent news can illustrate the point.

From the press release of IDEMIA on 10 of September: “IDEMIA presents IDEMIA 3D Face, the cutting-edge facial recognition technology - IDEMIA, the global leader in Augmented Identity, is bringing electronic device makers its expertise in biometric security with IDEMIA 3D Face, software that uses 3D facial recognition to unlock smartphones quickly and easily.”


As other technological proposals in the market, IDEMIA 3D Face can accurately calculate face geometry in three Another recent frontier in biometric research is the use of deep learning on the smartphones. Beyond proprietary solutions like those implemented by Panasonic, the Kneron facial recognition software is worth mentioning, that is claimed to unlocks entry-level and mid-range smartphones in 0.2 seconds, with an error rate lower than one in ten thousand. The technology can be adopted on any device with a front-facing camera with high resolution (more than a million pixels). The underlying approach uses a deep learning algorithm which can recognize multiple faces from a single device. Moreover, antispooing is also enforced using the three most popular approaches: optical sensing analysis processes the lighting variations on the face to assess its three-dimensionality; biological behavior recognition detects cues such as eye blinking, which is another typical strategy to recognize areal face; finally, the background depth detection solution, recently adopted in literature, can be used if the autofocus function is available by studying the image differences at different focal distances, to analyze the scene depth of field and intercept a fake two-dimensional image. Until a few years ago it was unthinkable that it was possible to perform operations of this kind on a mobile device.

dimensions using the invisible light beams of an infrared camera. In March IDEMIA had announced to have won the top ranking as the most accurate 1:1 algorithm out of 33 competitors in the SELFIE and WEBCAM categories of the widely esteemed NIST’s Face Recognition Vendor Test (FTRVT) [1]. While the technology exploited by Apple Face ID is a proprietary one, IDEMIA proposes its technology for any smartphone having the needed hardware. In fact, the solution requires an infrared camera, which is not available on most present smartphones. But this hardware would allow a higher level of security than 2D selfies, and a more robust anti-spoofing ability. Moreover, an infrared camera would allow to further enforce security by the best (at present) available algorithms for iris recognition, that exploit infrared capture. This would allow to implement a robust multimodal system on a consumer device. What is really amazing is the possibility to run such sophisticated biometric recognition procedures on a smartphone.

More details can be found at: https://www.biometricupdate.com/201803/kneron-facial-recognition-software-unlocks-entry-level-smartphones-in-0-2-seconds

Cutting-edge face recognition technology reaches the mobile consumer market

One element that may still hinder facial recognition on smartphones can still be represented by adverse illumination conditions. A news by U.S. Army Research Laboratory may represent the next future mobile add-on. The announcement regards an artificial intelligence and machine learning technique that produces a visible face image from a thermal image of a person's face captured in low-light or nighttime conditions. Such image can then be matched with a stored one through conventional single-modality techniques. The approach exploits advanced domain adaptation techniques based on deep neural networks. A non-linear regression model maps a given thermal image into a corresponding visible latent representation. Afterwards, an optimization problem projects the latent projection back into the image space.

More details can be read at https://www.sciencedaily.com/releases/2018/04/180416142443.htm and in the paper

"Thermal to Visible Synthesis of Face Images using Multiple Regions "presented at the IEEE Winter Conference on Applications of Computer Vision, or WACV, in Lake Tahoe, Nevada[2]. At present, thermal sensor are still quite expensive, but … who can say?

Notwithstanding the progress, the direction to continue research in mobile biometrics field is clear. Mobiles are almost always used in uncontrolled settings, therefore it is important to support both technical and non-technical users through more and more robust systems. These systems should both be able to guide the users in capturing good quality samples, and be resilient to sample distortions caused by poor capture quality.

Panasonic facial recognition technology FacePRO

Panasonic's FacePRO Facial Recognition Solution has been named the winner of the site protection software category in the Benchmark magazine's Innovation Awards 2018. The software had also previously ranked in top-2 in the IJB-A Face Identification Challenge organized by NIST in 2017 with a Cumulative Match Characteristic of 0.96 at rank 1 and 0.99 at rank 10.

FacePRO matches a person's face using live or recorded video from Panasonic i-PRO cameras to a database of enrolled faces (up to 30,000 faces). The deep learning technology used in the new software was jointly developed with the National University of Singapore (NUS) and is used in conjunction with a similarity calculation method that aims to reduce errors and enable recognition in situations that are difficult with conventional facial recognition technology (e.g. when the face is angled or partially hidden with sunglasses). It is reported to have a 90% accuracy rate when detecting faces partially hidden by sunglasses or facemasks.

The software automatically adjusts settings for the camera to capture optimal images that are best suited for facial recognition, by detecting the moving objects, movement speed, faces, and light intensity (day/night/headlights). It also automatically selects the best images for facial recognition from the multiple face images captured when a person passes in front of the camera, and sends only those selected images to the server to reduce the load on the server.

Read more at: https://tinyurl.com/y9viaglv about the award and at https://tinyurl.com/yca5aaq2 about the technology.

**Matti Pietikäinen** is one of the researchers that developed Local Binary Pattern (LBP) theory. This operator and its variations are extensively used as texture descriptors, and are also exploited in biometric research, both related to recognition and to spoofing detection. He is the winner of the 2018 edition of King-Sun Fu prize, that has been presented at the 24th International Conference on Pattern Recognition (ICPR) held in Beijing, China.

**Question:** What is a critical area/application, possibly related to safety, where face sentiment analysis could be used successfully and reliably at present? And what about the future?

**Matti:** Currently most successfully in applications in which high reliability is not necessary, eg. monitoring how people react when seeing different products or advertisements. Detecting the mood and alertness of car drivers should be coming soon, as well as developing advanced tools for health monitoring, diagnostics and therapy. In security area, for example border control or police investigations, face sentiment analysis can be helpful when used as an aid for human made analysis.

**Question:** Do you think there is still room to improve micro-expression recognition? Which are the problems to address?

**Matti:** There is much room to improve. Current methods and databases are for near-frontal images of relatively high quality with limited number of subjects. To make micro-expression detection and recognition to work in the real world is a major challenge. This includes also collecting and annotating databases in realistic conditions.

**Question:** May hand crafted and learned features coexist?

**Matti:** Why not? This may also be a computational efficiency issue. If hand-crafted features enable operating at higher frame rate with same energy, they might actually provide for better emotion recognition performance. A proper combination of these approaches would be often desirable, for example with limited data in applications such as micro-expressions. See also my answer to the next question.

**Question:** Local textural descriptors such as LBP, LPQ and BSIF have to face new challenges when working on images acquired by mobile devices, and especially in less controlled conditions. Which are in your opinion the main elements to consider and to take into account, and which are the best strategies to perform domain adaptation?

**Matti:** The higher the speed of operation and frame rate, the faster can the adaptation to changes in varying conditions become. A proper combination of local descriptors and learned features may often be needed to address these challenges, and depends on the given application. As well, how to efficiently use the unlabeled data acquired in the wild in unsupervised learning should be considered. The final solution is typically a compromise between classification accuracy, robustness to image degradations, compactness and efficiency, number of training data available, and cost and power consumption of implementations.

**Question:** Which are the most important/unsolved issues to be solved in visual emotion/expression recognition, i.e. that will occupy research in the forthcoming years?

**Matti:** Emotion recognition in the wild when no frontal images are available, also detecting minor variations of emotions, eg. between minor hesitation and confidence. Multimodal data would be often needed to improve the performance of emotion recognition, including head, eye and body movements, speech, and some physiological signals. Continuous and dynamic emotion changes together with context would need consideration. Due to the great variability of emotional face data, large enough databases should be collected and annotated for learning reliable emotion models.
**Interview**

Matti Pietikäinen is one of the researchers that developed Local Binary Pattern (LBP) theory. This operator and its variations are extensively used as texture descriptors, and are also exploited in biometric research, both related to recognition and to spoofing detection. He is the winner of the 2018 edition of King-Sun Fu prize, that has been presented at the 24th International Conference on Pattern Recognition (ICPR) held in Beijing, China.

**Question:** What would you suggest to a young researcher approaching biometrics-related topics?

**Matti:** Future biometrics research offers interesting opportunities and challenges. Good skills in mathematics, computer vision & pattern recognition, machine learning, and programming provide a solid basis for biometrics-related research. Even though deep learning has been very popular and shown impressive capability in different tasks, researchers should not just know and just focus on deep learning. They need to know different types of technologies to use and propose new methods to new problems flexibly. Biometric systems can be a part of different types of security solutions, so it could be helpful have also a little broader view of the security field.

Matti Pietikäinen received his Doctor of Science in Technology degree from the University of Oulu, Finland. He is currently Professor (emer.) and Senior Research Advisor at the Center for Machine Vision and Signal Analysis, University of Oulu. From 1980 to 1981 and from 1984 to 1985, he visited the Computer Vision Laboratory at the University of Maryland. He has made fundamental contributions, e.g. to local binary pattern (LBP) methodology, texture-based image and video analysis, and facial image analysis. He has authored about 350 refereed papers in international journals, books and conferences. His papers have over 51,000 citations in Google Scholar (h-index 76), and eight of these have over 1,300 citations. He was Associate Editor of IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI), Pattern Recognition and IEEE Transactions on Forensics and Security journals. Currently he serves as Associate Editor of IEEE Transactions on Biometrics, Behavior and Identity Science and Image and Vision Computing journals, and Guest Editor for special issues of IEEE TPAMI and International Journal of Computer Vision. He was President of the Pattern Recognition Society of Finland from 1989 to 1992, and was named its Honorary Member in 2014. From 1989 to 2007 he served as Member of the Governing Board of International Association for Pattern Recognition (IAPR), and became one of the founding fellows of the IAPR in 1994. He is IEEE Fellow for contributions to texture and facial image analysis for machine vision. In 2014, his research on LBP-based face description was awarded the Koenderink Prize for Fundamental Contributions in Computer Vision that stood the test of time. In August 2018, he received the prestigious IAPR King-Sun Fu Prize for fundamental contributions to texture analysis and facial image analysis.
I. INTRODUCTION

With the growing popularity of mobile devices, much attention has been paid to the protection of security and privacy of user information, especially when it comes to sensitive transactions, such as financial or e-payment applications [1]. The widely adopted knowledge-based authentication methods are vulnerable to hackers and it is cumbersome to remember complex passwords. Owing to the convenience and reliability, biometrics has become the new favorite of mobile access control. Iris is one of the most reliable, robust and distinctive modalities [2]. Irises are taken from an appropriate distance with little intrusiveness, making iris recognition user-friendly. Hence, iris recognition is a promising alternative to protect the security of user information on mobile devices.

Iris recognition on mobile devices faces some new challenges. Firstly, due to the limitations of space, power and heat dissipation, camera sensors on mobile devices are much smaller than traditional iris sensors, and the intensity of NIR light is much weaker than that on traditional iris imaging devices. Therefore, intensive noise is introduced in the imaging process on mobile devices, which impairs the sharpness and contrast of iris texture. Secondly, both camera sensor size and focal length are small on mobile devices, causing radiiuses of captured irises to be less than 80 pixels, which do not satisfy the requirement described in the international standard ISO/IEC 29794-6:2015. Moreover, iris radius decreases rapidly as the stand-off distance increases. Concretely, the diameter of the iris decreases from 200 pixels to 135 pixels when the stand-off distance increases for only 10 cm. Lastly, fast iris recognition algorithms with compact models are required as computational and storage resources on mobile devices are limited.

Degenerated image data captured by mobile devices damages the identification accuracy of iris recognition modules, posing serious threats to the security of mobile devices. To effectively handle the challenges, more robust and distinctive iris features should be extracted. Compared with traditional handcrafted iris features, deep learning models, especially convolutional neural networks (CNNs), have shown incomparable advantages. In addition, multimodal fusion strategy is also a good choice to alleviate the performance drop. Most previous biometrics fusion approaches utilize simple score level fusion based on weighted sum rule [3], [4], where weights are manually set without optimization. Other methods such as feature level fusion have not been explored thoroughly [5]. Some works directly concatenate various feature vectors [6] without considering the weights of different modalities.

II. PROPOSED APPROACH

This work [7] proposes a deep feature fusion network that exploits the complementary information presented in iris and periocular regions. The proposed method first integrates maxout units into CNNs to generate a compact representation for each modality. Afterwards, discriminative features of two modalities are concatenated. We employ prior modality information constraints via multiplying various weights for feature vectors of different modalities. In this way, the deep fusion network will treat iris and periocular modality separately and will assign a larger weight if one modality makes more contribution to the correct recognition result. In this way, we can emphasize the relatively more important modality in the feature fusing step. Concretely, the adaptive weight layer is added to each modality, as shown in Fig. 1. The parameters of convolutional filters and fusion weights are simultaneously learned to optimize the joint representation of iris and periocular biometrics.

Fig.1: An overview of the proposed deep feature fusion with adaptive weights method.

To evaluate the actual performance of the proposed approach and promote the iris recognition research on mobile devices under near-infrared (NIR) illumination, we construct and publicly release the CASIA-Iris-Mobile-V1.0 database*, which includes 11000 NIR iris images of both eyes from 630 Asians in total. To the best of our knowledge, this is the largest NIR mobile iris database so far[1].

III. Results

The proposed approach, deep feature fusion with adaptive weights, is compared with two other methods, direct feature concatenation fusion without weights and score level fusion based on the weighted sum rule. Fig. 2 shows DET curves of iris and periocular fusion at the feature level, where ‘Feature fusion–FC’ denotes deep feature concatenation fusion without weights and ‘Feature fusion–AW’ represents deep feature fusion with adaptive weights. Fig. 3 shows DET curves of iris and periocular fusion at the score level based on the weighted sum rule, where ‘Iw + Pw score fusion’ denotes the weight for iris is wi and that for periocular modality is wp. The best result is achieved at ‘10.6-0.4 score fusion’. We further draw the best DET curve of score level fusion together with that of the deep feature fusion using adaptive weights in the same figure, as shown in Fig. 4.

In conclusion, the proposed deep feature fusion approach

![Fig. 2: DET curves of iris and periocular fusion at the feature level.](image1)

![Fig. 3: DET curves of iris and periocular fusion at the score level.](image2)

![Fig. 4: DET curves of the best result of score level fusion and deep feature fusion with adaptive weights.](image3)

### Table 1: Storage space and computational costs

<table>
<thead>
<tr>
<th>Method</th>
<th>Storage Space</th>
<th>Computational Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>AlexNet [8]</td>
<td>232MB</td>
<td>109.4ms</td>
</tr>
<tr>
<td>VGG-16 [9]</td>
<td>528MB</td>
<td>91.9ms</td>
</tr>
<tr>
<td>Iris maxout CNNs</td>
<td>16MB</td>
<td>5.8ms</td>
</tr>
<tr>
<td>Periocular maxout CNNs</td>
<td>15.9MB</td>
<td>6.4ms</td>
</tr>
<tr>
<td>Deep feature fusion CNNs</td>
<td>31.9MB</td>
<td>12.5ms</td>
</tr>
</tbody>
</table>

IV. References


CALL FOR PAPER

International Conference on Biometrics

http://www.icb2019.org/
Submission deadline: Dec 15, 2018

IAPR/IEEE International Workshop on Biometrics and Forensics 2019

https://warwick.ac.uk/fac/sci/dcs/people/victor_sanchez/iwbf2019/
Submission deadline: Dec 10, 2018

IWBF 2019

BIOSIGNALS 2019

12th International Conference on Bio-inspired Systems and Signal Processing

http://www.biosignals.biostec.org/
Submission deadline: Oct 22, 2018

SPECIAL ISSUES

Domain Adaptation for Visual Understanding - Special Issue in Pattern Recognition

https://www.journals.elsevier.com/pattern-recognition/call-for-papers/domain-adaptation-for-visual-understanding
Submission deadline: Nov 30, 2018


Submission deadline: Mar 31, 2019
Sokoto Coventry Fingerprint Dataset

The SOCOFing dataset is a biometric fingerprint database designed for academic research purposes. It contains 6,000 fingerprints belonging to 600 African subjects. There are 10 fingerprints per subject and all subjects are 18 years or older. Labels for gender, hand and finger name are also available as well as synthetically altered versions of these fingerprints. In particular, three different levels of alteration for obliteration, central rotation, and z-cut are provided. The STRANGE toolbox was used for the generation of realistic synthetic alterations on fingerprint images. Alterations were done using easy, medium and hard parameter settings over 500 dpi resolution images. Therefore, the database contains a total of 17,934 altered images with easy parameter settings, 17,067 with medium settings, and 14,272 with hard parameter settings. Note that in some cases some images did not meet the criteria for alteration of STRANGE toolbox, hence the unequal number of altered images across all the three alteration categories. The original images were acquired based on impressions collected with Hamster plus (HSDU03P TM) and SecuGen SDU03P TM sensor scanners. SOCOFing consists of a total of 55,273 fingerprint images combined. All file images have a resolution of $1 \times 96 \times 103$ (gray × width × height). Figure 1 below shows some samples of the original fingerprints.

![Sample Illustration of Five Left Hand Fingerprints Belonging to the Same Subject.](image)

**Usage**

The dataset is freely available for noncommercial research purposes at: https://www.kaggle.com/ruizgara/socofing. Any publications arising from the use of this database must cite the following work:

SOURCE CODE

DENSEPOSE

As you surely know the COCO dataset has been designed to focus on challenging large-scale object detection and recognition tasks in the context of scene understanding. Within the context of ECCV, this year four challenges have been announced and their respective results presented at the Joint COCO and Mapillary Recognition ECCV workshop [1]. This letter reviews the COCO DensePose Challenge, whose task “requires localization of dense person keypoints in challenging, uncontrolled conditions”. With this objective in mind, the task aim goes beyond people and their respective keypoints detection in RGB images, i.e. without any depth sensor, in fact any human pixel is mapped to a 3D human body surface.

A little bit earlier this year a RCNN based system, see [2], was made available to researchers through the Facebook AI team github [3] to serve as baseline in the DensePose Challenge. The approach, developed by Riza Alp Guler, Natalia Neverova and Iasonas Kokkinos, has served not just as baseline in the DensePose Challenge within the ECCV workshop, but also in the PoseTrack Challenge. Even if DensePose served as baseline in both challenges, it ranked fifth and third respectively in the overall results. For those interested, the workshop challenge final rankings are available at [4]. In relation to the DensePose Challenge, a team from Beijing University of Posts and Telecommunications (BUPT) ranked first.

Even if the baseline approach was beaten by other teams according to DensePose Challenge results site [5], the available resulting videos and code availability makes it an interesting solution with a Creative Commons Attribution -NonCommercial 4.0 International license. The installation requires the Detectron framework [6] and therefore Caffe2 [7], circumstance that may make installation challenging, than other available codes such as openpose. In any case, DensePose output differs, as it is not providing the planar landmark detection, i.e. a limited number of 2D skeleton joints, but the pixel correspondence to a set of body parts segmentation in the wild, see Fig. 2. For this aim, the authors have gathered a “ground-truth dataset with image-to-surface correspondences manually annotated” on 50K COCO images. The body parts include head, torso, lower/upper arms, lower/upper legs, hands and feet, making a total of 24 body parts. The approach can handle occlusion, scale and pose variation (even unusual poses), successfully estimating the body behind the clothes. The processing speed depends on the image resolution, DensePose can process 240x320 images at 25 fps, whilst 800x1100 images at 4-5 fps, using a GTX 1080 GPU.

The code availability will soon serve to explore the domain of applications. So far, the approach authors have already proposed its use for Avatar creation [8]. Some preliminary results have been reported by the community, mainly art coders such as Mario Klingemann, Daito Manabe, Robbie Barrat or Kyle McDonald, confirming the processing rates provided by the authors.. Given these facts, may DensePose be also applied for biometric applications?

References:
Exploiting Linguistic Style as a Cognitive Biometric for Continuous Verification

In the last years, the continuous verification has become a quite trendy topic within the biometric field; such ever growing interest arises from the fact that it allows setting up and controlling a safe and secure session in which only the authenticated user is allowed to act. A module is in charge of continuously updating a matching score related to the identity of the user and: if it decreases below a given threshold, the session is locked.

Regarding this branch, at the last ICB (International Conference on Biometrics) 2018, held in February in Australia, a work has been presented which analyses the linguistic style of an individual, as well as the quality of the written text, as a biometric trait to be used for continuous verification applications.

The linguistic style can be considered an emerging biometric trait, since a feasibility study published at the beginning of the 2017 on IEEE Transactions on Information Forensics and Security [1] analysed the language-usage of an individual for cognitive systems automation purposes, showing quite promising results. Also in stylometry, the authorship verification is a quite open challenge, if we aim at using the linguistic written style for recognizing/verifying the author of a written text, whether it is a blog, a newspaper or a scientific article.

In the paper, text samples from the CASIS corpus (Center for Advanced Study in Identity Science) are used, which consists of 4000 blog samples; each sample, in turn, consists on average of more than 1600 characters, 300 words and 13 sentences. Each sample is divided according to a window function where (ranging from 1 to the number of total characters) and , respectively denote the beginning and the of a block and defines the length of a block (usually fixed to 50 or 100). From each window a set of linguistic features, both at character-level and at lexical level are extracted, resulting in a 671-dimension vector. The features extracted are shown in Figure 1.

Hence, the training is achieved in a continuous fashion: the blocks from the first to the fifth are used for training and the sixth for testing, then the blocks form the second to the sixth for training and the seventh for testing and so on. In Figure 2 an example of features extraction process is shown over a sample.

A 50-tree Isolation Forest classifier has been employed for this one-class verification problem. For assessing the accuracy regarding the continuous authentication the True Positive Rate and the False Positive Rate are reported. Results show that for n=50 and n=100, a TPR value of about 99.33% and 98.5% respectively, has been obtained. Also, an analysis of the computed features is reported, consisting of a value depicting the importance of each feature. In Table 1, such values are shown.

For each feature, the chi-square test is applied in order to measure the dependencies between each feature and the corresponding class: the lower the value the more independent the feature.
Exploiting Linguistic Style as a Cognitive Biometric for Continuous Verification

<table>
<thead>
<tr>
<th>Character Level Features</th>
<th>$\chi^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td># of characters</td>
<td>0.00000</td>
</tr>
<tr>
<td># of alphabets</td>
<td>0.00000</td>
</tr>
<tr>
<td># of uppercase alphabets</td>
<td>0.000494</td>
</tr>
<tr>
<td># of digits</td>
<td>0.003865</td>
</tr>
<tr>
<td># of tab spaces</td>
<td>0.000344</td>
</tr>
<tr>
<td>Freq. of alphabets</td>
<td>0.032433</td>
</tr>
<tr>
<td>Freq. of special characters</td>
<td>0.005962</td>
</tr>
<tr>
<td>Freq. of digits</td>
<td>0.040584</td>
</tr>
<tr>
<td>Freq. of character bigrams</td>
<td>0.918544</td>
</tr>
<tr>
<td>Freq. of character trigrams</td>
<td>1.00000</td>
</tr>
<tr>
<td>Freq. of character 4-grams</td>
<td>0.629513</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Lexical Level Features</th>
<th>$\chi^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td># of words</td>
<td>0.00000</td>
</tr>
<tr>
<td>Frac. of short words</td>
<td>0.00000</td>
</tr>
<tr>
<td>Avg. word length</td>
<td>0.00000</td>
</tr>
<tr>
<td># of unique words</td>
<td>0.00000</td>
</tr>
<tr>
<td>Frac. of capitalized words</td>
<td>0.000479</td>
</tr>
<tr>
<td>Frac. of uppercase words</td>
<td>0.004182</td>
</tr>
<tr>
<td>Frac. of lowercase words</td>
<td>0.000000</td>
</tr>
<tr>
<td>Frac. of camelcase words</td>
<td>0.000280</td>
</tr>
<tr>
<td>Frac. of othercase words</td>
<td>0.000157</td>
</tr>
</tbody>
</table>

Table 1: The importance for each feature, computed with the chi-square test.

Reference: