Exploiting Linguistic Style as a Cognitive Biometric for Continuous Verification

Tempestt J. Neal, Kalaivani Sundararajan, Damon L. Woodard
University of Florida, Gainesville, FL 32611 USA
tempesn@ufl.edu, kalaivani.s@ufl.edu, dwoodard@ece.ufl.edu

Abstract

This paper presents an assessment of continuous verification using linguistic style as a cognitive biometric. In stylometry, it is widely known that linguistic style is highly characteristic of authorship using representations that capture authorial style at character, lexical, syntactic, and semantic levels. In this work, we provide a contrast to previous efforts by implementing a one-class classification problem using Isolation Forests. Our approach demonstrates the usefulness of this classifier for accurately verifying the genuine user, and yields recognition accuracy exceeding 98% using very small training samples of 50 and 100-character blocks.

1. Introduction

Continuous verification has become a hot research topic since the early 2000s. Its convenience has attracted many biometric researchers, resulting in a variety of approaches for maintaining secure login sessions [6, 19, 9]. In continuous verification, a user's activity is continuously monitored in a passive manner; an authentication score is frequently updated as the user is logged into a particular application. Given the event that this score drops below some threshold, it is deemed that the session has been hijacked in some way by an intruder. Thus, compared to passwords and other point-of-entry verification methods, continuous verification allows the ability to maintain a secure and user-friendly operating session. This work proposes the use of linguistic style, or the discriminative qualities of written text, as a cognitive biometric for continuous verification. Biosignals, such as EEG, ECG, and EDR signals, were first considered as cognitive biometric modalities [12, 17, 20, 16]. Pokhriyal *et al.* extends cognitive biometrics as "the process of identifying an individual through extracting and matching a characteristic signature based on the cognitive, affective, or conative state of that individual" [15, 14]. In their work, the authors assess cognitive verification using language use as a binary classification problem, along with cognitive identification, with 77% and 90% accuracy, respectively. In comparison, we explore a one-class classification problem for verifying the identity of an individual as text continues to become available.

In the general biometric verification protocol, it is assumed that there are examples of positive and negative classes upon which a classifier can be trained to distinguish between the two. Thus, when a test sample is compared, it is either classified as 1 or -1. However, in practical settings, it is very unlikely that negative samples will be available, particularly during continuous verification, which is likely most useful for private sessions. In other words, during continuous verification, it is expected that the user accessing the respective application is the user which is supposed to have access to this application. Hence, expecting negative examples upon which to build a binary verification model is illogical. Further, even if negative examples are available, it is not possible to model the space of *every* negative example as there will always exist some negative example that has not been found and accounted for. Thus, this paper explores verification accuracy using linguistic style given a forest of trees trained on the positive class.

Finally, we also intend to demonstrate the amount of data required for maintaining a positive verification, and aim to direct our efforts towards applications which yield small text samples, such as text messages and social media posts. Thus, we evaluate blocks of text with 50 and 100 characters. Because the average word length in the English language is approximately five characters, our evaluation corresponds with 10 and 20-word length text samples [1]. This is an incredibly difficult task for multiple reasons; first, authorship analysis is most successful when considering large samples (in regards to length), classifiers trained on a single class are not able to generalize their decision boundaries due to the lack of negative examples, and cognitive biometric recognition, particularly in the context of continuous verification, is subject to concept drift.

The main contributions of this work are to first, analyze the minimum amount of information required for continuous verification of the genuine class. Compared to previous works, this work assesses much smaller sample and training sizes. Second, this work provides a framework for continu-

0-7695-6403-8/18/31.00 ©2018 IEEE
DOI 10.1109/ICB2018.2018.00048

ous verification using a window function and a classification technique commonly used for anomaly detection for one-class learning. We pose the following research questions:

- Is linguistic style reliable as a cognitive biometric for continuous verification?
- Is one-class learning feasible for language use for the purpose of continuous verification?
- Do linguistic features satisfy the biometric property of permanence?

The paper is outlined as follows: Section 2 discusses related work, Section 3 details the methodology used in experimentation, Section 4 provides and discusses experimental results, Section 5 discusses advantages and limitations of our approach, and Section 6 summarizes the paper.

2. Background

The task of authorship verification has been widely explored in stylometry and within the community of natural language processing (NLP). There is little work, however, which addresses language use as a cognitive biometric. Besides the works of [15] and [22], we are unaware of any additional efforts which have leveraged language as a behavioral biometric modality. Further, in both NLP and biometric communities, there is currently very little exploration of continuous verification using linguistic style, while we present the first to consider continuous verification as a one-class classification problem. In the most related approach presented by Stolerman *et al.*, continuous verification is analyzed in a similar setting using data captured from 67 subjects [22]. Using the general binary classification approach, the authors report 0.5/0 FRRs/FARs. Our work improves drastically on this approach by considering lower level features, 1,000 subjects which allows better generalization of our results, and improved performance.

In stylometry, authorship verification is a binary classification problem where the goal is to determine if a text sample is written by a particular author. For instance, Brocardo *et al.* investigate authorship verification using e-mails and Twitter messages from 76 and 100 authors, respectively, separated into blocks of 140 to 500 characters [4, 3, 2]. The authors report EERs of 9.98% to 21.45% using support vector machines trained on both positive and negative samples. Meanwhile, Koppel *et al.* [7] present a technique known as *unmasking* in the stylometry community. The basis of this concept lies in the speed at which accuracy degrades as features are iteratively removed. If two documents are written by the same author, then the speed at which the accuracy decreases should be fast, signifying that the features extracted between the two documents are strongly correlated. A support vector machine is trained on a corpus of known documents after which the unknown document is predicted; during multiple runs of this process, features are removed and the degradation curves are assessed. An overall accuracy of 95.7% is reported. Our work, however, improves upon this approach is several ways. First, in Koppel's work, the training samples consists of at least 500 words taken from novels such that an analysis of their technique as content changes is not provided. Moreover, the iterative nature of this approach is likely not applicable for continuous verification, where a small verification time and minimum computational requirements are desired.

Beyond the unmasking technique, an additional method, referred to as the *Impostors Method*, is also applied for authorship verification in stylometrics [18]. Here, the unknown document is compared to several impostor models along with the known document. The likeness between the unknown and known documents is computed given the percentage of features for which the unknown and known document are more similar compared to the similarity between the unknown document and impostor samples.

In summary, the techniques presented in the stylometry and NLP domains are adapting the verification problem as an identification problem, where a document with an unknown author is compared to other samples of known authorship in some repetitious manner instead of the traditional binary verification problem. In any case, this paper presents a novel technique for continuously verifying the identity of an individual as text becomes available. We formulate the problem as a true one-class classification problem, and demonstrate the effectiveness of the proposed technique even when using text samples of only 50 characters. In the domain of stylometry, determining authorship is very challenging when text samples are less than 2,500 words [5]; thus, we greatly improve upon what is typically regarded as the standard in an alternative field, while leveraging linguistic style as a cognitive biometric modality. For verification in particular, our results strongly suggest the distinctiveness and permanence of linguistic style, which are two fundamental properties of biometric modalities.

3. Methodology

In this section, we describe the experimental procedure used to assess the feasibility of continuous verification using a classifier trained on a single class.

3.1. Dataset Description

In this study, text samples from the Center for Advanced Studies in Identity Science (CASIS) corpus are used. CASIS consists of 4,000 blog samples from 1,000 non-native English speakers (4 samples per author). Each sample is an average of 1,634 characters, 304 words, and 13 sentences. To evaluate the robustness of the proposed approach, all blogs are concatenated for each subject to create a dataset which consists of 1,000 text samples. Thus, this allows an assessment of the ability to continuously verify a subject's identity, even after the context of the text changes, as may occur as one blog transitions to another.

3.2. Feature Extraction

Traditionally, text samples are characterized from features stemming from six categories: character, lexical, syntactic, semantic, structural, and domain-specific [21]. Character features capture the most primitive characteristics of a text sample, such as n-grams, or the frequency of n consecutive characters. Lexical features capture the distinctive properties at the word level; vocabulary richness measures which attempt to provide a numerical quantifier for the vocabulary diversity of a text sample are a common lexical level feature representation. Typically, character and lexical level features are collectively referred to as *bag-of-word* (BoW) features, as they extract features which correspond with the representation of the document as a collection of words without regard for word order, grammar, and context. Syntactic features capture sentence-level structure, and often rely upon robust natural language processors, while semantic features attempt to capture meaning and connotation. Structural features reflect a document's organization, such as in the use of indentations, while domain-specific features represent the document's theme as a result of its content.

For feature extraction, each text sample is divided into blocks using a window function, $W(i, j, n)$. The parameters of W define where the block begins at character i and ends at character j, and the number of characters, n, between i and j. Results correspond with i ranging from one to the total number of characters in a sample, including white spaces, in increments of n, where n is set to either 50 or 100. Thus, this allows training to occur in a continuous fashion. For example, if feature vectors one through five are used for training (where each vector consists of linguistic features from non-overlapping, but consecutive, blocks of characters), then the sixth feature vector is used for testing. Next, vectors two through six are used for training, followed by testing on feature vector seven. From each block of text as defined by W, character and lexical-level features are extracted (refer to Table 1). Syntactic, semantic, structural, and domain-specific features are avoided as these features typically require larger text samples.

As a result of these settings, we are able to generalize our approach to applications which are generally limited in the amount of text produced, such as in text messages and social networking posts. Further, by using a sliding window function to define the parts of the text where features should be extracted, we are able to filter out older samples as new text becomes available. This is important due to the effect of concept drift, or a change in the interests and/or behavior of the user, that typically plays an important role in the processing of traits in cognitive and behavioral biometric recognition.

Table 1. Linguistic Features

Character-level features	**No. of dimensions**
No. of characters	1
No. of alphabets	1
No. of uppercase alphabets	1
No. of digits	1
No. of tab spaces	1
Frequency of alphabets	26
Frequency of special characters	21
Frequency of digits	10
Frequency of character bigrams	200
Frequency of character trigrams	200
Frequency of character 4-grams	200
Lexical-level features	**No. of dimensions**
No. of words	1
Fraction of short words	1
Average word length	1
No. of unique words	1
Fraction of capitalized words	1
Fraction of uppercase words	1
Fraction of lowercase words	1
Fraction of camelcase words	1
Fraction of othercase words	1
Total dimensions	**671**

3.3. Classification Approach

We employ a 50-tree Isolation Forest as the classifier as it is typically used for anomaly detection, and is thus applicable for one-class learning [10]. Similar to Random Forests, random features are selected from which a random splitting given the feature values is performed. An abnormal sample is determined based on its path length in the forest; the idea is that an abnormal sample should require less effort to separate it from the rest of the samples, leading to a shorter path length across the trees. For training the forests, the number of training samples is varied from 3 to 10. For instance, if the number of training samples is 5, we train the Isolation Forests on five consecutive samples, and test on the following sample.

4. Results

4.1. Continuous Verification

First, an assessment of accuracy regarding continuous verification is examined as a one-class classification problem. For this, the true positive rate (TPR) and false negative rate (FNR) are reported. Assuming TP is the number of true positives and FN is the number of false negatives,

$$TPR = \frac{TP}{TP + FN}$$

and

$$FNR = 1 - TPR$$

During these experiments, each window of samples is compared to the next available sample from the same user; this is the same protocol that would be followed in a practical scenario. After training the Isolation Forests on the training samples, the next available sample is classified as either a normal sample or an abnormal sample. Ideally, all test samples will be classified as normal, indicating that linguistic style is unique enough to serve as a cognitive biometric for continuous verification without the need to train a classifier on both positive and negative examples.

Figure 1 plots the average TPR across all subjects given a particular number of training samples. From this graph, it is observed that the TPR increases as the number of training sample increases. However, it is also observed the TPR tapers off with only five training samples for both 50 and 100-character block sample sizes at 99.35% and 98.5%, respectively. These rates correspond with a FNR of less than 0.65%. These are very promising results for several reasons. First, it demonstrates the consistency of the English language in regards to very primitive features which will ultimately result in reduced run-time for feature extraction and a verification decision. These results also indicate that a misclassification of a positive test sample is a rare occurrence, leading to a highly accurate and efficient verification system, even in the absence of negative examples from which decision boundaries can be more accurately learned. Finally, because blogs are concatenated for each subject and the topics of these blogs may differ from one another, results suggest that character and lexical-level features are sufficient at maintaining a secure operating session even if the context of the session changes. This could lead to continuously verifying the identity of an individual as they type essays, then blogs, and then post on social media.

Moreover, while in our preliminary experiments a false rejection is rare, because linguistic style is a behavioral biometric in this context, there are several options that can handle the situation where a genuine user is falsely rejected. One option is to combine linguistics with another modality, such that the weaknesses typically associated with behavioral biometrics can be addressed via a stronger, or more reliable, source of identification. Alternatively, an alert or password-based response could be triggered for the user to authenticate themselves. An additional option is to implement a score or confidence-based function, such that a rejection occurs once the score decreases below some threshold. This should address frequent rejections once the threshold is optimized.

Further, it is also observed that feature representations which correspond with 50-character blocks yield slightly better performance compared to the 100-character blocks. This is interesting given that in traditional authorship analysis studies, larger text samples typically correspond with improved performance. While the observed performance gains are not drastic improvements, it provides an operational benefit, particularly on behalf of the user. In other words, these results suggest that continuous verification can be carried out with a 96% probability of being classified correctly throughout active sessions with only three samples of consecutive 50-character blocks. Equivalently, a user can maintain a secure login session after only providing 150 characters of text. To our knowledge, these are the most promising results regarding continuous verification based on language use using one-class verification in the research literature to date.

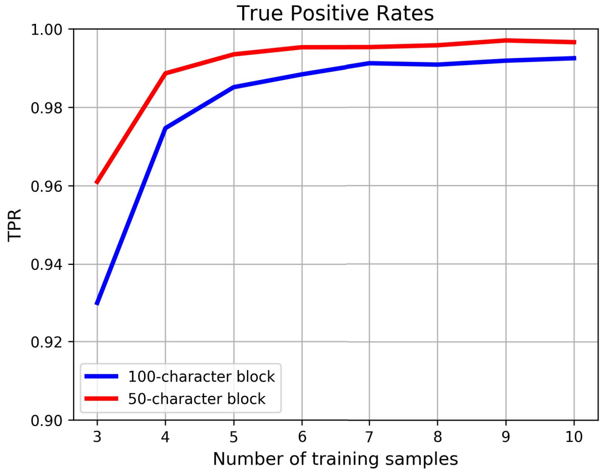

Figure 1. True Positive Rates

4.2. Permanence of Linguistic Style

Permanence is one of the fundamental biometric properties used to describe the stability of a modality. A biometric trait, rather physiological, behavioral, or cognitive, should be relatively unchanged over time for reliability. Otherwise, the biometric system must learn to handle the changes exhibited by the modality in order to provide an accurate classification in the future. In this section, we describe an experimental protocol to assess the permanence of linguistic style as a cognitive biometric. For this, we set n=50 in W and train using five samples. The 5^{th}, 10^{th}, 15^{th}, 20^{th}, 50^{th}, and 100^{th} samples from the last training sample are predicted as either normal or abnormal using the trained forests.

Figure 2 plots the TPR for each test sample. It is very obvious from this graph that linguistic style exhibits the property of permanence. Due to these results, it is inferred that individuals tend to maintain their linguistic style over time and across different writing samples. It is also assumed that due to the consistency of linguistic style, an intrusion should be detected with high accuracy; however, further experimentation is required to assess an attack scenario as this paper is purposely structured to mainly focus on verifying the genuine subject for multiple reasons. First, because this is the first application of one-class learning for continuous verification using linguistic style, there are many associated unknowns, such as how often the classification model should be trained/updated. Here, we direct our efforts towards maintaining an accurate identification.

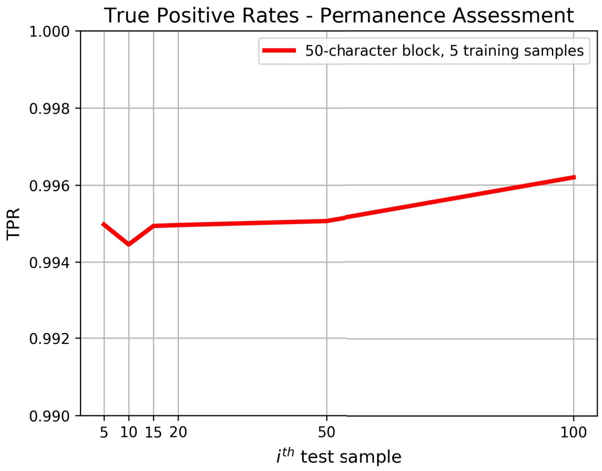

Figure 2. True Positive Rates - Permanence

4.3. Feature Analysis

In this section, we provide a further analysis of the features. Following feature selection, a common next step is to perform feature selection. This is especially important for continuous verification for reducing the amount of time required to make a verification decision as a more compact feature representation should reduce the time required to train the Isolation Forests. Therefore, we apply the chi-square (χ^2) test to measure the dependencies between each feature dimension and the corresponding class; features which tend to be independent of the class are less important for verification.

To learn the most important features for each user, we apply χ^2 tests to features repesenting 50-character blocks. For each user, we randomly assign binary labels to each feature vector and compute the χ^2 statistic. This is repeated for 20 iterations and the average χ^2 value is retained. In other words, we randomly assign feature vectors to a positive or negative class. While the features correspond with one true class, this methodology is necessary as there are no negative examples upon which to determine the salient feature dimensions. Hence, if a dimension is repetitively deemed as important over the 20 iterations, it is considered an overall salient dimension. Table 2 provides the average χ^2 value for each feature dimension across all subjects. It is observed that character level features are the most class-dependent, likely due to the small size of the text samples (i.e., 50/100-character blocks). Results also suggest the importance of consecutive characters as n-grams were regarded as the most representative of each class. In fact, results indicate that n-gram features may serve as standalone features.

Table 2. Feature Importance

Feature	χ^2
Frequency of character trigrams	1.000000
Frequency of character bigrams	0.918544
Frequency of character 4-grams	0.629513
Frequency of digits	0.040584
Frequency of alphabets	0.032433
Frequency of special characters	0.005962
Fraction of uppercase words	0.004182
No. of digits	0.003865
Fraction of camelcase words	0.002800
No. of uppercase alphabets	0.000494
Fraction of capitalized words	0.000479
Fraction of othercase words	0.000157
No. of tab spaces	0.000034
Fraction of lowercase words	0.000000
No. of words	0.000000
Fraction of short words	0.000000
No. of alphabets	0.000000
No. of characters	0.000000
No. of unique words	0.000000
Average word length	0.000000

The advantages of using one-class learning also yields author-specific feature sets following feature selection due to the consideration of each class separately. In Figure 3, the average between-class similarity between the salient feature dimensions is provided. We compute the similarity between two feature vectors, a and b, using the Jaccard similarity, J as

$$J = \frac{|a \cap b|}{|a \cup b|}$$

From this graph, it is observed that, for every salient feature set between two different subjects, the average similarity between these features is less than 0.5. In other words, there is less than 50% similarity between the feature dimensions deemed as the most important for each class between every pair of different subjects. Hence, analysis of these features implies that author-specific feature representations are available, which will likely provide performance advantages in regards to the robustness against circumvention and reduction in authentication delays.

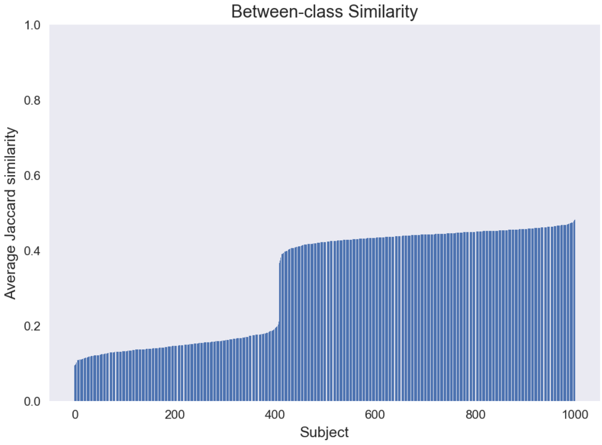

Figure 3. Between-class similarity of feature vectors.

5. Discussion

This paper approaches continuous verification using linguistic style as a one-class classification problem. Experimental results are very promising, and suggest that linguistic style has high potential to serve as a cognitive biometric. In this section, we provide additional advantages of our approach, while also discussing limitations.

Scalability

In several papers [8, 11], the inability of authorship analysis tasks, such as authorship attribution, authorship verification, and plagiarism detection, to scale seems to be regarded as a key stylometry-related issue. This is discouraging, especially considering the amount of communication that is now generated online as typed text. Most of this text will be short in length, grammatically incorrect, varied in content, cohesive thoughts, and themes, and multilingual. Yet, a solution to these issues remains an open research problem for researchers in stylometry and NLP. In the biometrics community, little work has been directed towards leveraging linguistic style for biometric recognition. While there are works in handwriting recognition [13], the core of this research lies in the ability to extract discriminating features about *how* text is written instead of *what* is written. This is where cognitive biometrics play an important role as relying upon linguistic style now yields more information compared to handwriting regarding the cognitive state of an individual.

In this paper, we have demonstrated the effectiveness of linguistic style for continuous verification, while clearly going beyond the constraints exhibited in stylometry. Our results show that a secure login session can be maintained with a probability of falsely verifying the genuine subject of less than 1%. Thus, our work suggests that, when considering a purely one-class classification problem, there is less required in regards to efficiently representing linguistic style, addressing the biometric property of *measurability* while not being limited by the scalability issue.

Limitations

While experimental results are very promising, this work is obviously limited to applications where continuous verification is desired. Such applications may include maintaining secure workstations in work and lab environments and improving upon current locking mechanisms on mobile devices by monitoring text provided by the device's owner. It is unclear whether this technique will generalize to applications which requires multiple legitimate authors. For instance, in scientific publications, it is common that multiple authors will contribute to the work. Our results suggest that implementing this approach to ensure that a shared paper is not hijacked by a malicious individual may yield a very inconvenient system as each author will likely be considered an impostor, particularly if considering author-specific feature sets.

A further limitation is the scalability of this approach to other languages. While we restrict our features to very low level representations, some languages differ significantly in regard to length of average words and the use of spaces. Thus, it would be interesting to explore this approach on multilingual samples.

6. Conclusion

This paper proposes the use of linguistic style as a cognitive biometric modality. Character and lexical-level features are extracted from 50 and 100-character blocks of text from 4,000 blogs written by 1,000 authors. An Isolation Forest, a common classifier used for anomaly detection, is trained for each user to create a one-class classification problem, yielding a worst-case true positive rate of 93%. Results also indicate that linguistic style is consistent over time as true positive rates continue to exceed 94% for all subjects as the time between the training and test samples increases.

Further, our results indicate that, compared to initial claims in previous assessments [22], linguistic style can potentially serve as a standalone cognitive biometric. While multimodal systems are generally considered more robust in the biometric community, the accuracy exhibited in this study suggests the robustness of language choice on its own. Further, the convenience of this approach as an unobtrusive and covert biometric is very appealing, particularly for applications that regard user convenience as a priority.

To our knowledge, this is the first assessment of continuous verification using linguistic style based on one-class learning. We expect this analysis to contribute greatly to the field of biometrics, especially considering the novelty of cognitive biometrics beyond biosignals. We envision this approach, along with additional continuous verification approaches, to significantly improve the convenience and strengthen the security of many user services as cognitive modalities can be captured covertly and unobtrusively. Future work will assess the generalization of our approach across multiple languages and document types, such as e-mails and social media posts. We will also consider the consistency of salient features over time, along with an evaluation of performance rates (e.g., false positives and true negatives) under an attack scenario.

References

[1] V. Bochkarev, A. Shevlyakova, and V. Solovyev. Average word length dynamics as indicator of cultural changes in society. arxiv preprint (2012). *arXiv preprint arXiv:1208.6109*.

[2] M. L. Brocardo and I. Traore. Continuous authentication using micro-messages. In *2014 Twelfth Annual International Conference on Privacy, Security and Trust*, pages 179–188, July 2014.

[3] M. L. Brocardo, I. Traore, and I. Woungang. Toward a framework for continuous authentication using stylometry. In *2014 IEEE 28th International Conference on Advanced Information Networking and Applications*, pages 106–115, May 2014.

[4] M. L. Brocardo, I. Traore, and I. Woungang. Authorship verification of e-mail and tweet messages applied for continuous authentication. *Journal of Computer and System Sciences*, 81(8):1429 – 1440, 2015.

[5] M. Eder. Does size matter? authorship attribution, small samples, big problem. *Proceedings of Digital Humanities*, pages 132–135, 2010.

[6] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *IEEE Transactions on Information Forensics and Security*, 8(1):136–148, Jan 2013.

[7] M. Koppel and J. Schler. Authorship verification as a one-class classification problem. In *Proceedings of the Twenty-first International Conference on Machine Learning*, ICML '04, pages 62–, New York, NY, USA, 2004. ACM.

[8] M. Koppel, J. Schler, and S. Argamon. Authorship attribution in the wild. *Language Resources and Evaluation*, 45(1):83–94, Mar 2011.

[9] S. Kumar, T. Sim, R. Janakiraman, and S. Zhang. Using continuous biometric verification to protect interactive login sessions. In *21st Annual Computer Security Applications Conference (ACSAC'05)*, pages 10 pp.–450, Dec 2005.

[10] F. T. Liu, K. M. Ting, and Z. H. Zhou. Isolation forest. In *2008 Eighth IEEE International Conference on Data Mining*, pages 413–422, Dec 2008.

[11] K. Luyckx and W. Daelemans. Authorship attribution and verification with many authors and limited data. In *Proceedings of the 22Nd International Conference on Computational Linguistics - Volume 1*, COLING '08, pages 513–520, Stroudsburg, PA, USA, 2008. Association for Computational Linguistics.

[12] E. Maiorana, D. L. Rocca, and P. Campisi. Cognitive biometric cryptosystems a case study on eeg. In *2015 International Conference on Systems, Signals and Image Processing (IWSSIP)*, pages 125–128, Sept 2015.

[13] R. Plamondon and S. N. Srihari. Online and off-line handwriting recognition: a comprehensive survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 22(1):63–84, Jan 2000.

[14] N. Pokhriyal, I. Nwogu, and V. Govindaraju. Use of language as a cognitive biometric trait. In *IEEE International Joint Conference on Biometrics*, pages 1–8, Sept 2014.

[15] N. Pokhriyal, K. Tayal, I. Nwogu, and V. Govindaraju. Cognitive-biometric recognition from language usage: A feasibility study. *IEEE Transactions on Information Forensics and Security*, 12(1):134–143, Jan 2017.

[16] K. Revett. Cognitive biometrics: A novel approach to person authentication. *International Journal of Cognitive Biometrics*, 1(1):1–9, 2012.

[17] K. Revett, F. Deravi, and K. Sirlantzis. Biosignals for user authentication - towards cognitive biometrics? In *2010 International Conference on Emerging Security Technologies*, pages 71–76, Sept 2010.

[18] S. Seidman. Authorship verification using the impostors method. In *CLEF 2013 Evaluation Labs and Workshop-Online Working Notes*, 2013.

[19] T. Shimshon, R. Moskovitch, L. Rokach, and Y. Elovici. Continuous verification using keystroke dynamics. In *2010 International Conference on Computational Intelligence and Security*, pages 411–415, Dec 2010.

[20] K. Song, S. M. Lee, and S. Nam. Combined biometrics for e-learning security. *ISA 2-13, ASTL*, 21:247–251, 2013.

[21] E. Stamatatos. A survey of modern authorship attribution methods. *Journal of the American Society for Information Science and Technology*, 60(3):538–556, 2009.

[22] A. Stolerman, A. Fridman, R. Greenstadt, P. Brennan, and P. Juola. Active linguistic authentication revisited: Real-time stylometric evaluation towards multi-modal decision fusion. In *Proc. IFIP WG*, volume 11, pages 1–11, 2014.