Applying Benford's Law as an Efficient and Low-cost Solution for Verifying the Authenticity of Users' Video Streams in Learning Management Systems

Argyris Constantinides
University of Cyprus & Cognitive UX LTD, Cyprus
aconst12@cs.ucy.ac.cy

Christodoulos Constantinides
Columbia University, United States
cc4718@columbia.edu

Marios Belk
Cognitive UX GmbH, Germany
belk@cognitiveux.de

Christos Fidas
University of Patras, Greece
fidas@upatras.gr

Andreas Pitsillides
University of Cyprus, Cyprus
cspitsil@cs.ucy.ac.cy

ABSTRACT

An important challenge of online learning management systems (LMS) relates to continuously verifying the identity of students even after they have successfully authenticated. Although various continuous user identification solutions exist, they are rather focused on complex examination proctoring systems. Challenges further increase within large-scale online courses, which require a strong infrastructure to support numerous real-time video streams for verifying the identity of students. Considering that the students' input video stream is an important factor for verifying their identity, and given that naturally generated data streams have been found to adhere to a pre-defined behavior as indicated by the Benford's law, in this work we investigate whether Benford's law can be applied as a reliable, efficient and cost-effective method for the detection of authentic vs. pre-recorded input video streams during continuous students' identity verification within online LMS. In doing so, we suggest a prediction model based on the distribution of the first digits of image Discrete Cosine Transform (DCT) coefficients from the students' input video stream. We found that the input video stream type (authentic vs. pre-recorded) can be inferred within a few seconds in real-time. A system performance evaluation indicates that the suggested model can support up to 1000 concurrent online students using a conventional and low-cost server setup and architecture.

CCS CONCEPTS

• **Human-centered computing** → Human computer interaction (HCI); • **Applied computing** → Education; Distance learning.

KEYWORDS

Continuous User Identification, Benford's Law, Learning Management Systems, Distance Learning, Image Forensics

WI-IAT '21, December 14–17, 2021, ESSENDON, VIC, Australia

ACM ISBN 978-1-4503-9115-3/21/12…$15.00
https://doi.org/10.1145/3486622.3493993

ACM Reference Format:
Argyris Constantinides, Christodoulos Constantinides, Marios Belk, Christos Fidas, and Andreas Pitsillides. 2021. Applying Benford's Law as an Efficient and Low-cost Solution for Verifying the Authenticity of Users' Video Streams in Learning Management Systems. In *IEEE/WIC/ACM International Conference on Web Intelligence (WI-IAT '21), December 14–17, 2021, ESSENDON, VIC, Australia.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3486622.3493993

1 INTRODUCTION

Recent days have created notable challenges for online Learning Management Systems (LMS) in higher education, and consequently higher education institutions, which ought to sustain their educational and academic quality and reputation during the urgent transition towards an online teaching and learning paradigm. Although in-person educational and academic activities have been limited due to movement restrictions and social distancing guidelines, a vast number of higher education institutions across the globe increased the availability of online courses in an attempt to maintain their educational and academic quality [22]. Nevertheless, the urgent need to shift from the traditional in-person educational model to a completely online teaching and learning environment could be problematic in various aspects, such as, verification of students' identity, classroom attendance, and adequate performance assessment [1, 2].

Focusing on the *verification of students' identity*, a key issue in the majority of the recently online-transitioned education systems relates to the fact that they usually define a single entry-point authentication mechanism as a prerequisite to allowing access to protected resources and services. Hence, these systems are often inadequate in detecting fraudulent users after the authentication step is performed successfully [3]. To alleviate the single entry-point problem, continuous or implicit authentication methods have been proposed as an additional non-intrusive security countermeasure [3, 4, 13, 23]. Being able to continuously verify student's presence and attendance is of major importance in several educational activities, such as, laboratories' quizzes, online examinations, collaborative learning contexts [19, 25, 26], in order to tackle the threat of impostors intentionally pretending someone else's identity.

Nevertheless, existing solutions are usually designed as proctoring tools only during online examinations with a person monitoring

students remotely (*e.g.*, Kryterion[1], Respondus[2], ProctorU[3], tend to not consider the rest of the course participation, and are not scalable [2]. With these considerations in mind, we believe that the verification of the students' identity within LMS environments can be improved by solutions that target to deliver trustworthy and credible academic and e-learning activities.

1.1 Research Motivation

A good indicator for continuously verifying a student's identity is the input video stream used during presence and attendance in online classes and/or examinations [30]. Hence, this work aims to investigate whether the type of the input video stream (*i.e.*, authentic vs. pre-recorded) could be predicted in real-time for the student interacting with the LMS. Previous works revealed that, on digital images from naturally generated data streams, the probability distribution of specific variables usually follows a pre-defined behavior that proves to be completely altered whenever the stream is modified [6, 7]. Such an example is the distribution of the first significant digit of quantized Discrete Cosine Transform (DCT) coefficients that follow Benford's law [6], which indicates that in many naturally occurring collections of numbers, the leading digit is more likely to be small. Therefore, we investigate whether Benford's law can be applied for the detection of pre-recorded input video streams during continuous students' identity verification within LMS environments. We envision that such knowledge will assist continuous identity management and authentication scheme designers with the design of low-cost assistive mechanisms that detect impostors within a few seconds in real-time.

2 RELATED WORK

Several works on LMS have provided evidence that the verification of students' identity should be continuous [2, 8, 30]. In fact, authentication solutions that rely only on something that the student knows (*e.g.*, passwords) or has in possession (*e.g.*, devices), are based on the assumption that the student will not provide them to other people. Moreover, the use of authentication solutions at the entry-point based on something that the student is or does (*e.g.*, biometrics) is not adequate for scenarios in which the legitimate student is first verified and then allows an impostor to carry on. Additionally, student verification methods should also operate in a non-intrusive way, without affecting the students' learning and examination activities [2, 30]. As a result, numerous works proposed various continuous and transparent verification solutions. For example, Atoum et al. [9] proposed a uni-biometric system that integrates both face and body cues.

However, systems that simply monitor face and/or body cues are not adequate to stop cheating in examinations, since they lack students' interactions and are not able to capture cases in which the camera is switched to other video sources [2]. Other works focused on combining multiple biometrics. Examples include face with fingerprint [10], fingerprint with vocal traits [11], and fingerprint with mouse patterns [12]. Nevertheless, multiple-biometric solutions often interfere with students' activities, as well as require the use of additional devices [12]. With regards to transparent authentication, prior works investigated the use of behavioral biometrics by analyzing keystroke and mouse patterns while students take online examinations [8, 14]. However, behavioral-based approaches are often unreliable without the combination of a physical biometric trait and are usually limited to particular types of interaction (*e.g.*, recognizing keystroke patterns is effective only when the student is typing) [2].

Taking into consideration that the verification of students' identity usually occurs in Web-based LMS environments, the detection of impostors and fraudulent students is highly related to the multimedia forensics' research community. In this context, numerous forensics' detectors suggested the effective use of the Benford's law, such as, detection of JPEG compression [16, 31], synthetic images [17], face morphing [18], and images produced through Generative Adversarial Networks [7]. One of the most widely used applications of Benford's law in forensics relates to the study of traces left from JPEG compression, aiming to verify whether an image has been JPEG compressed once or twice [24]. To detect multiple JPEG compressions, Milani et al. [31] exploited features based on the statistics of the first digits to train Support Vector Machine classifiers, while Pasquini et al. [16] proposed the statistical analysis of Benford-Fourier coefficients. In another work by Pasquini et al. [27], Benford-Fourier coefficients were also used for a forensics detector of JPEG compression traces on images stored in uncompressed formats.

Although numerous works exist for the detection of computer-generated and manipulated video input streams, to the best of the authors' knowledge, no research attempts have been made to investigate whether Benford's law can be used for the detection of pre-recorded video input streams in the context of continuous student verification within LMS environments.

3 USER STUDY

3.1 Research Questions

We formed the following research questions:

RQ1: Can we build a prediction model for detecting authentic vs. pre-recorded videos from users' input streams by considering the distribution of the first digits of image DCT coefficients?

RQ2: How well does the prediction model for detecting authentic vs. pre-recorded videos perform when a large number of users (*e.g.*, 1000 users) are concurrently streaming videos?

3.2 Study Instruments and Metrics

3.2.1 Web-based LMS. We implemented a Web-based LMS in which students could engage in e-learning activities, such as, watch educational videos. Since we were interested on the detection of authentic vs. non-authentic input video streams, the system was designed to simulate a continuous identification approach by allowing the students to either use their laptop's Web camera (*i.e.*, authentic input video stream), or upload a pre-recorded input video (*i.e.*, non-authentic input video stream).

3.2.2 Metrics. Following common practices from prior works on Benford's law [6, 7, 31], we measure the probability distributions of the first digits (ranging from 1 to 9) of the block DCT coefficients.

[1] *https://www.kryteriononline.com*
[2] *https://web.respondus.com*
[3] *https://www.proctoru.com*)

To extract the block-DCT coefficients, we first capture frames from both the students' Web camera and the pre-recorded video every 1 second, for a total duration of 20 seconds. Then, each frame is divided into distinct 8x8 blocks and the two-dimensional DCT is applied to each block [6].

3.3 Classification Setup

We treated the prediction of the authentic vs. pre-recorded input video stream as a classification task using the discussed metrics. To build our prediction model, we used the publicly available dataset GI4E[4] [21], which consists of 1339 authentic Web camera images that correspond to 103 different individuals. We used 669 images as-is (*i.e.*, uncompressed), which represented the frames of the authentic video type. The rest 670 images, which represented the frames of the pre-recorded video type, were JPEG-compressed with quality factors ranging between 80%-99% [6] to improve the generalization ability of the classifier.

3.4 Sampling and Procedure

3.4.1 Participants. A total of 18 individuals participated in the study, ranging in age between 20-32 years old (m=24, sd=3.1). Participants were split evenly into two groups, and the access type (authentic vs. pre-recorded) varied across all users. To increase the internal validity of the study, we recruited participants that had no prior experience with continuous identification mechanisms, as assessed by a post-study online discussion.

3.4.2 Experimental Design and Procedure. All participants performed the task remotely. To avoid any bias effects, no details regarding the research objectives were revealed to the participants. The study involved the following steps: first, participants were informed that the collected data would be stored anonymously and would be used only for research purposes, and they digitally signed a consent form. Then, they completed a questionnaire on demographics and they familiarized themselves with the process of authenticating into the system. Half of the participants were requested to access the system using their laptop's Web camera by recording their face in real-time for 20 seconds, and the other half were requested to use a pre-recorded single-compressed video stream of 20 seconds, which we provided to them. To control the type of accessing the system, we provided each user a unique random ID, which either prompted them to use their Web camera or redirected them to a screen for uploading the pre-recorded video.

4 ANALYSIS OF RESULTS

4.1 Effectiveness of the Prediction Model (RQ_1)

To investigate RQ_1, we used Python scikit-learn[5] module. In order to avoid overfitting, we used a 10-fold cross-validation. We tested various classifiers (Support Vector Machines, Logistic Regression, and Naïve Bayes) to predict the correctly classified instances, with Naïve Bayes providing the best accuracy. Results (**Table 1**) revealed that the highest accuracy achieved was 81%. The high prediction accuracy observed by the analysis of video frames with duration of 20 seconds is of major importance for the current work, considering that the aim is to identify the type of the input video stream (authentic vs. pre-recorded) at early stages of continuous verification of students' identity.

Table 1: Accuracy across classifiers

Classifier	Quality Factor	Accuracy
Support Vector Machines	80%-99% [6]	0.791666
Logistic Regression	80%-99% [6]	0.787037
Naïve Bayes	80%-99% [6]	**0.819444**

As shown in **Figure 1 (left)**, the distribution of the first digit DCT coefficients for the authentic input video streams follows the generalized Benford's (logarithmic) law perfectly [6]. In the case of the pre-recorded input video streams, which included multiple JPEG compressed frames, the generalized Benford's law is violated, as shown in **Figure 1 (right)**. These findings can be attributed to the fact that naturally generated real-time data streams are being compressed once, and then they are further processed for the extraction of the DCT coefficients for calculating the first digit distributions. Therefore, they adhere to the Benford's law since no traces are left from a single compression [6, 24]. On the other hand, pre-recorded videos, although they might have been compressed once (or more times) during the actual capture of the video, they will be regarded as two (or more) times compressed. As a result, traces left from the multiple compressions lead to violation of the Benford's law [16, 31].

4.2 System Performance Evaluation (RQ_2)

Challenges of applying continuous student identification mechanisms further increase within large-scale online courses, since higher education institutions require a strong infrastructure to support numerous real-time video streams for identifying and verifying the identity of students. Hence, we have further conducted a system performance evaluation (RQ_2) aiming to investigate how the proposed model behaves with a larger number of users. We consider that a regular university may have approximately 1000 concurrent students taking online examinations. Hence, we conducted a simulation of an online examination with up to 1000 online students using a conventional and low-cost server setup and architecture.

4.2.1 Examination Simulation Scenario. We consider the following examination scenario for the simulation: examination takers log in to a proctoring platform and the platform takes periodically a picture using the user's Web camera. In case the examination takers circumvent their Web camera and use a pre-recorded video to bypass the identity and authentication system, the system will recognize it from the analysis of the frequency of the first digits of the DCT coefficients of the picture. Then the proctor is notified about the incident.

For the system performance evaluation, we set up an Apache server to process the requests and forward them to Django with mod_wsgi. In Django, we exposed an endpoint that inputs an image, applies Benford's law and responds whether the image is valid or not. We used a conventional and low-cost server setup that had 32GB DDR3 RAM, an Intel Xeon E5-2603V4 processor, and

[4] *https://www.unavarra.es/gi4e/databases/gi4e*
[5] *https://scikit-learn.org*

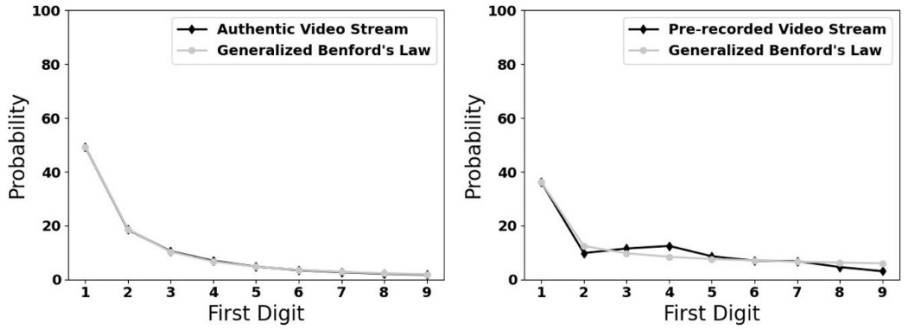

Figure 1: The distribution of the first digit DCT coefficients for the authentic input video streams follows perfectly the generalized Benford's law (left); The distribution of the first digit DCT coefficients for the pre-recorded input video streams violates the generalized Benford's law (right).

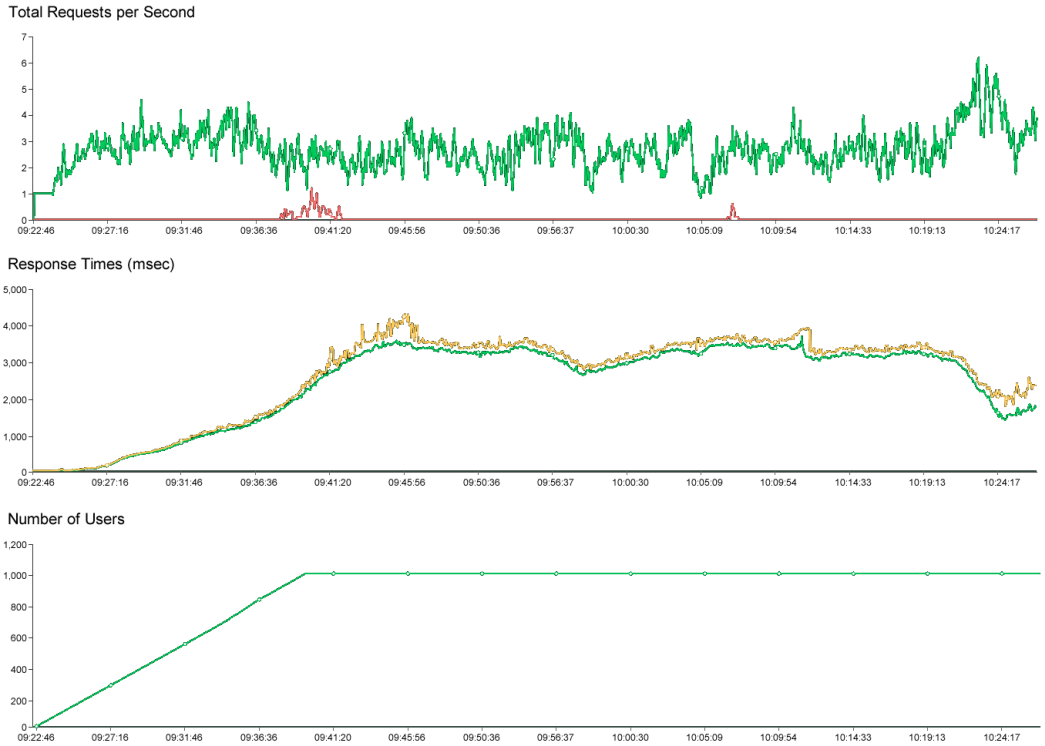

Figure 2: Total requests per second (green) and failures per second (red) – *top figure*; maximum response time (ms) in the particular second (yellow) and the median response time (ms) (green) – *middle figure*; number of users that are active (total 1000 users) – *bottom figure*

was running on a Linux Operating System. To simulate a real-world scenario with multiple concurrent users, Locust[6] has been used, which is a widely applied open-source load testing tool. The simulated users were distributed across 10 different machines on a different network from that of the server. The images sent from the simulated users were taken from a Web camera with a size of 200 KB.

[6] *https://locust.io*

The simulation starts with zero users and linearly increases the number of users by 1 until it reaches the desired number of concurrent users. When a new user is spawned, it posts the image to the exposed endpoint and waits for the response. When the server responds, it repeats the same action after a random amount of time distributed evenly between 60 and 90 seconds. The simulation was running for one hour, each time with a different number of users. **Figure 2** illustrates the total requests made per second (green) and failures per second (red); the maximum response time (ms)

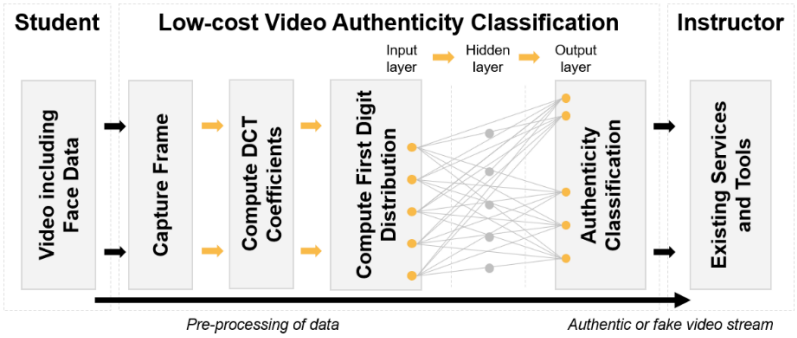

Figure 3: The proposed classifier could be used as a low-cost assistive mechanism during continuous student identification in combination with face recognition tools

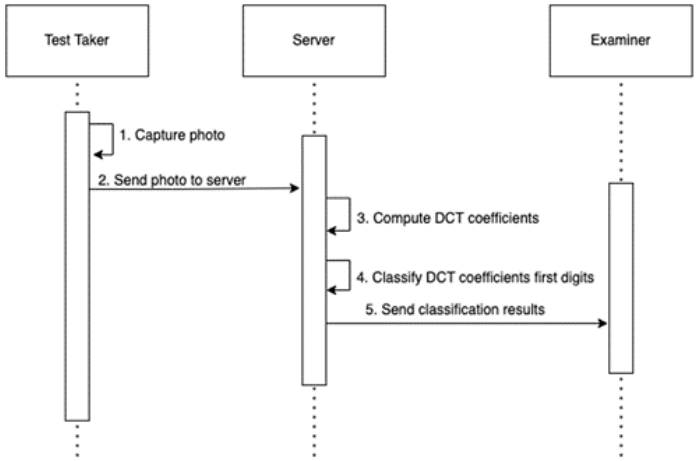

Figure 4: Main steps of the assistive mechanism's procedure

in the particular second (yellow) and the median response time (ms) (green); and the number of users that are active (total 1000 users) respectively. Accordingly, as the number of concurrent users increase, the response time increases too. The first spawned user waited for 200ms for the first request, while the 1000th spawned user waited for 3.5 seconds. When all users have been spawned, the response time fluctuates between 1.5 and 3.5 seconds. The request failure rate was 1%.

5 DISCUSSION

The analysis of results revealed that the input video stream type (authentic vs. pre-recorded) based on our prediction model can be inferred within a few seconds in real-time (RQ_1). In addition, the system performance evaluation (RQ_2) indicates that the suggested prediction model can support up to 1000 concurrent online students using a conventional and low-cost server setup and architecture.

Considering the need for continuous and transparent verification of students' identity, such knowledge is important and could drive the design of intelligent assistive mechanisms for improving the security and credibility in higher education Learning Management Systems (LMS). We envision that our classifier could be easily adopted with low cost, and used in a continuous manner complementary with face recognition technologies, to provide further insights in cases where the face recognition is not adequate or it is tricked by fraudulent users (*e.g.*, a student modifies the Web camera stream to display a pre-recorded video of himself/herself).

Figure 3 illustrates the video authenticity classification procedure in which the proposed classifier could be used as a low-cost assistive mechanism during continuous student identification in combination with face recognition tools. **Figure 4** further illustrates the main steps of the assistive mechanism's procedure.

Accordingly, for the pre-processing, the captured frame is divided into 8x8 blocks and the DCT coefficients for each block are computed. Then, for each of the coefficients, the first digit distribution is calculated. The frequency of the digits 1 to 9 are given as input to a pre-trained binary classifier (*e.g.*, Support Vector Machines, Logistic Regression, Naïve Bayes). This classifier is trained on first digit distributions of frames from a live camera stream and pre-recorded frames. Finally, it responds to the proctoring services whether or not the video stream is authentic.

Furthermore, one important challenge for deploying such assistive mechanisms relates to architectural design decisions and whether the image analysis should be conducted at the client's side or at

Table 2: Comparison between client-side vs. server-side image analysis based on the proposed approach

	Client-side Analysis	Server-side Analysis
Privacy-preserving	Yes	No
Server Load	Less	More
Network Load	Less	More
Bypass the Analysis	Possible	Unlikely

the server's side. **Table 2** summarizes a comparison when running the prediction model at the client's side vs. at the server's side. Accordingly, one important advantage of conducting the analysis at the client's side relates to the fact that such an approach would increase privacy preservation of the users' data as no photos of the users would be sent over the network and/or stored at the server. In addition, the servers would need less computing power as processing would be conducted at the client, while the network load would be less as the photos would not be sent to the server. On the counter side, such an architectural design would increase possibilities for attackers to circumvent the image analysis mechanisms and models at the client's side in an attempt to bypass the system.

Limitations of this work relate to the fact that some Web camera drivers may further compress/process (double compress) the captured picture, even when the video stream is not pre-recorded, which might affect the identification of authentic vs. pre-recorded videos based on the suggested approach. Furthermore, we conducted a system performance evaluation with up to 1000 concurrent users, which represents a typical online examination scenario within a regular university nowadays. However, for supporting a higher number of concurrent users for large universities, this can be supported with a distributed system approach by distributing the image analysis to various computing machines. In addition, even with a smaller number of users, a distributed system approach is suggested aiming to avoid single points of failure.

6 CONCLUSIONS

In this paper, we investigated whether Benford's law can be applied for the detection of authentic vs. pre-recorded input video streams during continuous students' identity verification within online Learning Management Systems (LMS). For this purpose, we have developed and evaluated a classifier that predicts the type of the input video stream of students interacting with a Web-based LMS, after extracting and analyzing the first digit distributions of the Discrete Cosine Transform (DCT) coefficients during continuous verification of their identity.

Initial results are encouraging for further investigating various experimental designs for improving the accuracy of real-time classifiers within LMS environments. We have shown that our classifier (based on Naïve Bayes) achieved an accuracy of 81% in which the authenticity of each of 1000 concurrent users was performed within a few seconds in real-time. In addition, we have shown that our model can run and support up to 1000 online students using a conventional and low-cost server setup and architecture as proven from the setup in our case study.

Future work entails the combination and evaluation of the proposed system with existing proctoring algorithms and systems, such as, user face identification, gaze estimation, voice detection, and active window detection, as well as implicit user modelling mechanisms based on user interaction and eye gaze analysis [20, 28], and personalized human interaction proof mechanisms [5, 15, 29].

ACKNOWLEDGMENTS

The work has been partially supported by the European project TRUSTID - Intelligent and Continuous Online Student Identity Management for Improving Security and Trust in European Higher Education Institutions (Grant Agreement No: 2020-1-EL01-KA226-HE-094869), which is funded by the European Commission within the Erasmus+ 2020 Programme and the Greek State Scholarships Foundation I.K.Y., and the EU Horizon 2020 Grant 826278 "Securing Medical Data in Smart Patient-Centric Healthcare Systems" (Serums).

REFERENCES

[1] Fidas, C., Belk, M., Portugal, D., & Pitsillides, A. (2021). Privacy-preserving Biometric-driven Data for Student Identity Management: Challenges and Approaches. ACM UMAP 2021, ACM Press, 368-370.
[2] Fenu, G., Marras, M., & Boratto, L. (2018). A multi-biometric system for continuous student authentication in e-learning platforms. Pattern Recognition Letters, 113, 83-92.
[3] Frank, M., Biedert, R., Ma, E., Martinovic, I., & Song, D. (2012). 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.
[4] Shahzad, M., & Singh, M. P. (2017). Continuous authentication and authorization for the internet of things. IEEE Internet Computing, 21(2), 86-90.
[5] Belk M., Fidas C., Germanakos P., Samaras G. (2012). Do Cognitive Styles of Users affect Preference and Performance related to CAPTCHA?. In Proceedings of Extended Abstracts on Human Factors in Computing Systems (CHI 2012), ACM Press, 1487-1492.
[6] Fu, D., Shi, Y. Q., & Su, W. (2007). A generalized Benford's law for JPEG coefficients and its applications in image forensics. Security, Steganography, and Watermarking of Multimedia Contents, 6505, 65051L.
[7] Bonettini, N., Bestagini, P., Milani, S., & Tubaro, S. (2020). On the use of Benford's law to detect GAN-generated images. In 2020 25th International Conference on Pattern Recognition (ICPR) (pp. 5495-5502). IEEE.
[8] Flior, E., & Kowalski, K. (2010). Continuous biometric user authentication in online examinations. In 2010 Seventh International Conference on Information Technology: New Generations (pp. 488-492). IEEE.
[9] Atoum, Yousef, Liping Chen, Alex X. Liu, Stephen DH Hsu, & Xiaoming Liu (2017). Automated online exam proctoring. IEEE Transactions on Multimedia 19, no. 7, 1609-1624.
[10] Moini, A., & Madni, A. M. (2009). Leveraging biometrics for user authentication in online learning: a systems perspective. IEEE Systems Journal, 3(4), 469-476.
[11] Agulla, E. G., Rúa, E. A., Castro, J. L. A., Jiménez, D. G., & Rifón, L. A. (2009). Multimodal biometrics-based student attendance measurement in learning management systems. In 2009 11th IEEE International Symposium on Multimedia (pp. 699-704). IEEE.
[12] Asha, S., & Chellappan, C. (2008). Authentication of e-learners using multimodal biometric technology. In 2008 International Symposium on Biometrics and Security Technologies (pp. 1-6). IEEE.
[13] Constantinides, A., Belk, M., Fidas, C. & Pitsillides, A., (2020). An eye gaze-driven metric for estimating the strength of graphical passwords based on image hotspots. In Proceedings of the 25th International Conference on Intelligent User

Interfaces. ACM IUI 2020, ACM Press, 33-37.
[14] Morales, A., & Fierrez, J. (2015). Keystroke biometrics for student authentication: A case study. In Proceedings of the 2015 ACM Conference on Innovation and Technology in Computer Science Education (pp. 337-337).
[15] Fidas, C., Voyiatzis, A., Avouris, N. (2011). On the Necessity of User-Friendly CAPTCHA. In Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI 2011), ACM Press, 2623-2626.
[16] Pasquini, C., Boato, G., & Pérez-González, F. (2014). Multiple JPEG compression detection by means of Benford-Fourier coefficients. In 2014 IEEE International Workshop on Information Forensics and Security (WIFS) (pp. 113-118). IEEE.
[17] Acebo, E., & Sbert, M. (2005). Benford's law for natural and synthetic images. In Proceedings of the First Eurographics conference on Computational Aesthetics in Graphics, Visualization and Imaging (pp. 169-176).
[18] Makrushin, A., Kraetzer, C., Neubert, T., & Dittmann, J. (2018). Generalized Benford's Law for Blind Detection of Morphed Face Images. In Proceedings of the 6th ACM Workshop on Information Hiding and Multimedia Security (pp. 49-54).
[19] Fidas, C., Komis, V., Avouris, N., Dimitracopoulou, A. (2002). Collaborative Problem Solving using an Open Modeling Environment. In Proceedings of Computer Support For Collaborative Learning: Foundations For A CSCL Community (CSCL 2002), Lawrence Erlbaum Associates, 654-655
[20] Belk, M., Papatheocharous, E., Germanakos, P., Samaras G. (2013). Modeling Users on the World Wide Web based on Cognitive Factors, Navigation Behavior and Clustering Techniques. Journal of Systems and Software, Special Issue on Web 2.0 Engineering: New Practices and Emerging Challenges, 86(12), 2995-3012.
[21] Villanueva, A., Ponz, V., Sesma-Sanchez, L., Ariz, M., Porta, S., & Cabeza, R. (2013). Hybrid method based on topography for robust detection of iris center and eye corners. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 9(4), 1-20.
[22] Crawford, J., Butler-Henderson, K., Rudolph, J., Malkawi, B., Glowatz, M., Burton, R., Magni, P. & Lam, S. (2020). COVID-19: 20 countries' higher education intra-period digital pedagogy responses. Journal of Applied Learning & Teaching, 3(1), 1-20.
[23] Constantinides, C., Constantinides, A., Belk, M., Fidas, C., & Pitsillides, A. (2021). A Comparative Study among Different Computer Vision Algorithms for Assisting Users in Picture Password Composition. ACM UMAP 2021, ACM Press, 357-362.
[24] Pevny, T., & Fridrich, J. (2008). Detection of double-compression in JPEG images for applications in steganography. IEEE Transactions on information forensics and security, 3(2), 247-258.
[25] Margaritis, M., Fidas, C., Avouris, N., Komis, V. (2003). A peer-to-peer architecture for synchronous collaboration over low-bandwidth networks. In Proceedings of the Panhellenic Conference on Informatics (PCI 2003), ACM Press, 231-242.
[26] Komis, V., Avouris, N., Fidas, C. (2002). Computer-Supported Collaborative Concept Mapping: Study of Synchronous Peer Interaction. Education and Information Technologies, 7, 169-188.
[27] Pasquini, C., Boato, G., & Pérez-González, F. (2017). Statistical detection of JPEG traces in digital images in uncompressed formats. IEEE Transactions on Information Forensics and Security, 12(12), 2890-2905.
[28] Leonidou, P., Constantinides, A., Belk, M., Fidas, C., Pitsillides, A. (2021). Eye Gaze and Interaction Differences of Holistic Versus Analytic Users in Image-Recognition Human Interaction Proof Schemes. In Proceedings of the HCI International 2021 (HCII 2021), 27, 66-75.
[29] Fidas C., Hussmann H., Belk M., Samaras G. (2015). iHIP: Towards a User Centric Individual Human Interaction Proof Framework. Proceedings of the Extended Abstracts on Human Factors in Computing Systems (CHI 2015), Seoul, South Korea, ACM Press, 2235-2240.
[30] Traoré, I., Nakkabi, Y., Saad, S., Sayed, B., Ardigo, J. D., & de Faria Quinan, P. M. (2017). Ensuring online exam integrity through continuous biometric authentication. In Information Security Practices (pp. 73-81). Springer, Cham.
[31] Milani, S., Tagliasacchi, M., & Tubaro, S. (2014). Discriminating multiple JPEG compressions using first digit features. APSIPA Transactions on Signal and Information Processing, 3.