A security model with biometric components for e-learning systems

Sorin SOVIANY, Cristina-Gabriela GHEORGHE, Maria GHEORGHE-MOISII

National Institute for Research & Development in Informatics – ICI Bucharest

sorin.soviany@ici.ro

Abstract: *The paper presents an innovative security architecture with multimodal biometrics for e-Learning systems. The biometric data fusion is approached using a hierarchical methodology for feature-level fusion with 2 layers, local (intra-modal) and global (inter-modal) fusion. Some design options are proposed to be explored and evaluated in order to establish their feasibility for e-Learning platforms. This proposal belongs to an ongoing research with focus on improving the security in applications from various areas and in which the multimodal biometrics should be used.*

Keywords: biometric, multimodal, e-Learning.

1. Introduction

The e-Learning platforms and systems are evolving very fast, significantly changing the educational systems. Through the integration of the most advanced technologies and innovative teaching strategies, this educational framework provides sustainable and effective solutions to contemporary training challenges. The expansion of technological platforms for distance learning and e-Learning requires the integration of effective security mechanisms. The design of security mechanisms for e-Learning should consider the optimization in respect to the technical requirements of those applications, but ensuring a proper level of security and reliability. These requirements are enabled by the actual trend to enlarge the spectrum of cybersecurity threats against the hardware/software platforms for a wide variety of applications.

The biometric technologies provide a reliable approach to develop efficient authentication mechanisms that can be integrated into multi-factor schemes. The advances in biometric systems, either for desktop but also for mobile use-cases, are key factors enabling to improve their integration in applications for many domains, including e-Learning.

The paper proposes a security model for e-Learning platforms. The architectural model addresses the problem of the secure user authentication; it includes multimodal biometric components. The design specifies the client-side

https://doi.org/10.58503/icvl-v20y202509

and server-side components. The biometric data fusion is approached with a hierarchical methodology for feature-level fusion with 2 layers, local (intra-modal) and global (inter-modal) fusion. Some design options are proposed to be explored and evaluated to further establish their feasibility for e-Learning platforms. This proposal belongs to an ongoing research with focus on improving the security in various applications and in which the multimodal biometrics should be used.The remainder of the paper is structured as follows: Section 2 - recent related works; Section 3 - the proposed security architectural model, and potential future improvements; Section 4 that concludes this work, with steps towards a software implementation.

2. Related works and current developments

Given the technological advances, the adoption of e-Learning systems and platforms significantly increased, becoming an essential component of the educational landscape. e-Learning is highly adaptable and accessible, providing an efficient modality for various learning activities (Zogas et al., 2016).

According to (Al-Fraihat et al., 2020), e-Learning offers fast and personalized learning strategies with high efficiency in the educational process. An important challenge for the online learning is the quality assurance (Gheorghe-Moisii &Tîrziu, 2015) and integrity of the online educational processes.

The biometric technologies provide a reliable way to validate the student identity and to prevent the security breaches in the online education. The use of fingerprints and other biometrics has proven to be reliable in strengthening the educational processes security (Ivanova et al, 2019). A biometric system extracts and matches features of the human body such as fingerprint, iris, and face to identify individuals (Soviany et al., 2023).

The state of the art in the biometrics'usage for the individual's authentication in online learning environments is presented in (Curran & Curran, 2021), followed by a detailed investigation of the authentication systems with face and iris for the learner authentication. The user authentication is a key factor for the e-Learning systems security. In (Luu, Nguyen, Pham, & Huynh-Tuong, 2020) a brief description of the authentication methods for online systems was made: ID/password, biometrics and the user behaviour. Shen et al. proposed a real-presence detection system called IriTrack, which relies on iris tracking to prevent facial spoofing attacks. By asking users to move their eyes according to a randomly generated trajectory, the system analyses iris movements as evidence of real presence (Shen et al., 2018). Afolabi & Adagunodo described a secure multimedia e-Learning system based on facial recognition and data encryption; the implementation of the system was carried out in three main stages (Afolabi & Adagunodo, 2018): a) Facial recognition, b) Data encryption, c) Implementing the multimedia-focused e-learning.

The multi-biometric systems have been developed as reliable solutions for authentication. Many researchers have proved their effectiveness, showing that in multi-biometric (multimodal) systems, the various biometric traits can overcome the limitations of the single-modal systems. Although the biometrics can be combined at different levels (feature, score, or decision), the matching score-level fusion is commonly applied because of its low complexity. Herbadji et al. propose a multi-biometric system based on the fusion of 2 different techniques: triangular norms and rule-based classifiers such as SVM (Support Vector Machine) (Herbadji et al., 2020). (Daza et al., 2022) present edBB-Demo - a research platform that integrates biometric authentication and behavioural analytics for the student monitoring in the distance education. The feature fusion remains a hot topic because of its major challenges: the curse-of-dimensionality (if the features are concatenated); the issue of finding relationships among the original feature spaces, together with the potential incompatibility among the feature sets generated by different feature extractors (Jain, 2005); the unavailability of the feature vector structure to prevent potential security breaches. The feature-level fusion can be applied on several feature sets either extracted from the same biometric (intra-modal fusion, like textural and structural features extracted from the same input face image) or from different human traits or modalities (inter-modal fusion) (Singh et al, 2019).

The feature fusion has promising usage cases such as indexing and retrieval of biometric data allowing to develop computationally efficient, accurate, and privacy-preserving data storage and retrieval tools (Drozdowski, 2021). This is why there are ongoing research efforts to develop innovative feature fusion methods, basically looking to overcome the main drawback of the concatenation. The feature-level fusion can be addressed with techniques like clustering and indexing (Sasikala, 2018). Some simple fusion techniques like the weighted sum are applied for different use-cases (Atenco, 2023). The concatenation-based fusion is typically used with normalized features (Harakannanavar, 2022). More complex feature-level fusion methods include procedures like the Canonical Correlation Analysis (CCA) with a SVM classifier to get a highly discriminant fused feature vector (Kamlaskar, 2022); in this case a procedure with Principal Component Analysis (PCA) + CCA subspace is applied to achieve a reliable dimensionality reduction within the feature fusion framework.

3. The security architectural model with multimodal biometrics for an e-Learning platform

3.1 Basic architecture (model)

The security architecture for the e-Learning use-cases is depicted in Figure 1. It includes a multimodal biometric authentication component to be used by the e-Learning platform end-users. The client-side component includes the biometric data processing together with the data fusion. The data processing module performs

the feature generation. The server-side component includes the matcher (data classifier) within an access control module; the matching process is applied to a Key Generator allowing that individual to have access to the e-Learning platform functionalities. The design specifies: the feature generation, the data fusion, the biometric data classifier and some improvement/optimization options.

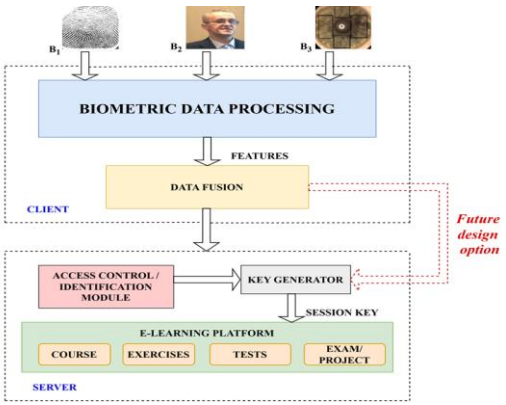

Figure 1. Security Architecture for e-Learning

3.2 Feature generation/extraction process

The feature generation process (Figure 2) is based on a regional approach in which several regions of interest (ROIs) are manually selected and extracted from the original images to get the informative features. The 3 biometrics are fingerprint (B_1), face (B_2) and iris (B_3). The main steps are as follows:

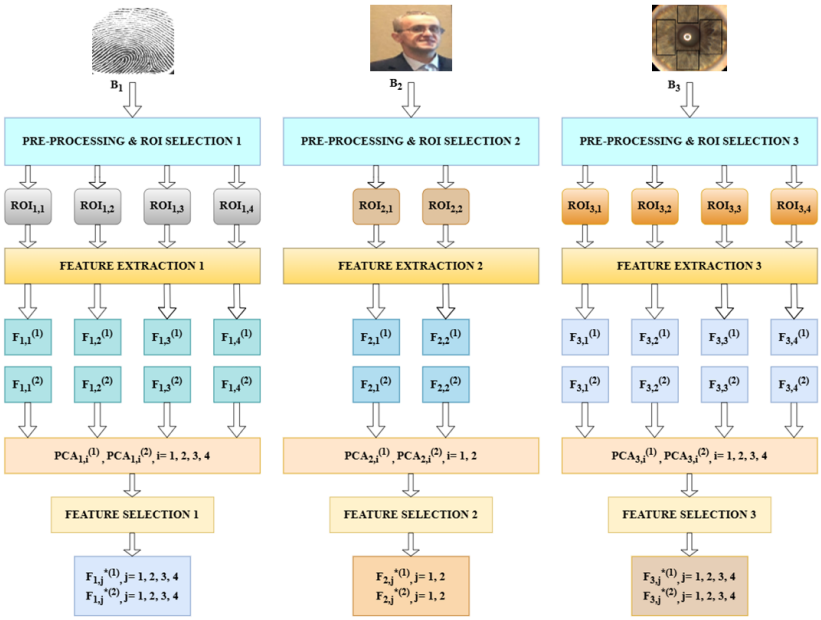

Figure 2. Feature Generation (client-side)

The pre-processing and ROI selection/extraction, in which the original images are pre-processed to enhance their quality. The pre-processing step will perform operations like image clipping, noise removing and thresholding. The main operation is the manual selection and extraction of a specified number of ROIs from every pre-processed image. The ROIs will be used for the feature generation (feature extraction, dimensionality reduction, optionally Feature Engineering and feature selection). For the specified biometrics the number of ROIs is as follows: $n_{ROI_{B_1}} = 4$, $n_{ROI_{B_2}} = 2$ and $n_{ROI_{B_3}} = 4$;

The feature extraction from the selected ROI, using an approach with textural features (Haralick). The same Feature Extractor model is applied for all biometrics: regional process with several ROIs, textural 1st and 2nd order statistical features. The extracted features evaluate the gray-level distribution within the selected ROI: per pixel (1st order statistical features) and per pair of neighboring pixels with a certain displacement (2nd order statistical features). The co-occurrence matrices are used to derive 2nd order statistical features (Theodoridis, 2009), (Lofstedt, 2019), (Mansour, 2023). The feature extractor uses as the main parameter the number of gray-level bins (GLB). For each selected ROI from the original image there will be 2 feature vectors containing the 1st and 2nd order textural features. The 1st order features include the mean value of GL (gray-levels) and the central moments: variance, skewness and kurtosis. These amounts are evaluated based on the 1st order histogram - the ratio between the number of pixels with the given GL and the total number of pixels within the selected ROI, and for a certain number of possible gray-levels. The resulting feature vectors are $F^{(1)}_{B_{k,j}}, B_k \in \{B_1, B_2, B_3\}, j = \overline{1, n_{ROI_{B_k}}}$ The 2nd order statistical features are based on the co-occurrence matrix (CM) with elements computed as the ratio between the number of pixels with a certain displacement between them having the specified gray-levels and the total number of possible pairs (Theodoridis, 2009). The total number of CM elements is $(GLB)^2$. The CM-based feature extractor parameters are fixed to maximize the number of non-null (informative) CM elements. The 1st parameter (GLB) ensures a proper adjustment of the feature space size in respect to the performance vs. complexity trade-off. The 2nd parameter (offset) is used to adjust the spacing between the pixels pairs. After the CM generation, additional variables are computed based on the CM elements: Angular Second Moment (ASM), Contrast (CON), Inverse Difference moment (IDF), Entropy, Correlation (Mansour, 2023), Autocorrelation, Dissimilarity (Lofstedt, 2019), Variance. These texture features are concatenated to the vector containing the CM elements. The resulting feature vectors are $F^{(2)}_{B_{k,j}}, B_k \in \{B_1, B_2, B_3\}, j = \overline{1, n_{ROI_{B_k}}}$;

The dimensionality adjustment through PCA. PCA (unsupervised process) retains the features having the highest variance and the lowest correlation but with the potential drawback of not preserving the class separation among the samples within the datapoints space. A supervised PCA version could be a design option to

improve the process, for example by using a weighted covariance matrix. The weighted covariance matrix could be computed based on the class covariance matrices while taking as weigths the priors (occurrence frequencies) of the classes (target and non-target identities) within the training biometric data;

The feature selection and Feature Engineering (FE) (optionally). The feature design/generation process for the biometric recognition of the e-Learning platform users could include a feature selection stage looking to search for and to retain the most useful features to be applied in the advanced data processing (data fusion in the client-side and data matching/classification in the server-side). For the feature selection one can apply typical techniques that are already known for pattern recognition use-cases (Theodoridis, 2009), but avoiding those methods evaluating the discriminant power per individual feature. For the feature generation step one can take in account the almost inherent correlation among the different features. Suboptimal searching techniques are considered for the feature selection: sequential forward selection. The feature selection ensures a common dimensionality for the vectors containing the same order textural features from different ROIs and for the same biometric. This ensures the homogeneity required for the functional feature fusion (intra-modal fusion). An optional process should be to derive new features from the original ones through FE. FE allows to enrich the initial feature space with new variables ensuring potentially higher discriminant value. This process assumes the cost of a certain dimensionality increasing. The improved feature space may reveal hidden data patterns that cannot be observed within the original space. The following FE techniques are considered (Heaton, 2016):

- counts, in which the new features are computed by fixing a certain thresholding and counting the cases where the specified original features exceed or are below the given threshold. One can take the number of non-null CM elements, or can specify a certain interval for the textural features values;
- differences and ratios, in which the new features are engineered by taking the differences and rations between the maximum and minumum values of the given original features.

The resulted dimensionality (feature space size) for the 2 feature sets per ROI and per biometric is $d^{*(z)}_{B_k,j}, j=\overline{1,n_{ROI_{B_k}}}, B_k \in \{B_1, B_2, B_3\}, z \in \{1,2\}$.

3.3 Biometric data fusion scheme design

The biometric data fusion process is addressed with a pre-classification (feature-level) fusion methodology. The reason is the capability to exploit the informative properties of the raw samples, before any advanced processing that could generate a certain loss of information, as in the post-classification fusion – score-level, ranking-level, decision-level. The proposed feature-level biometric data fusion methodology uses a hierarchical approach with 2 layers, local and

global. This is justified by the regional approach of the feature extraction with several ROIs per biometric providing the corresponding feature sets to be fused. The 2 fusion layers are as follows:

The local biometric feature-level fusion is the process in which the extracted features per ROI are combined for every biometric (an *intra-modal* fusion). The local fusion is performed such as the 1st order textural statistical features provided by the all ROIs for the same biometric ($F^{*(1)}_{B_{k,j}}$) are combined with a functional rule f (1), and the same proceeding for the 2nd order statistical features ($F^{*(2)}_{B_{k,j}}$) (2). The 2 fused feature sets ($F^{*(1)}_{B_k}$), ($F^{*(2)}_{B_k}$) are then concatenated (3) to achieve the final feature vector for each biometric ($F^{*}_{B_k}$), where $B_k \in \{B_1, B_2, B_3\}$, and $n_{ROI_{B_k}}$ is the number of ROIs specified to extract the features from the input images, per biometric.

$$F^{*(1)}_{B_k} = f\left(F^{*(1)}_{B_{k,j}}\right), j = \overline{1, n_{ROI_{B_k}}} \tag{1}$$

$$F^{*(2)}_{B_k} = f\left(F^{*(2)}_{B_{k,j}}\right), j = \overline{1, n_{ROI_{B_k}}} \tag{2}$$

$$F^{*}_{B_k} = \begin{bmatrix} F^{*(1)}_{B_k} \\ F^{*(2)}_{B_k} \end{bmatrix} \tag{3}$$

The functional fusion requires homogeneous input feature vectors. A certain compatibility among the fused feature sets is ensured by using the same basic feature extractor for each biometric. The compatibility is another requirement for a reliable functional fusion. In this way the concatenation can be avoid for the fusion of the same order statistical features originating from the selected ROI. The concatenation is only appplied to combine the 1st and 2nd order feature sets, according to (3), with a resulted feature space dimensionality

$$d^{*}_{B_k} = d^{*(1)}_{B_k} + d^{*(2)}_{B_k}, B_k \in \{B_1, B_2, B_3\} \tag{4}$$

The following methods are considered for the functional feature fusion scheme:

1. *Weighted Average (Sum) Fusion* (Chen et al., 2021), given by

$$F^{*(1)}_{B_k} = \sum_{j=1}^{n_{ROI_{B_k}}} w_j \cdot F^{*(1)}_{B_{k,j}} \tag{5}$$

$$F^{*(2)}_{B_k} = \sum_{j=1}^{n_{ROI_{B_k}}} w_j \cdot F^{*(2)}_{B_{k,j}} \tag{6}$$

where the weights w_j are normalized such as $\sum_{j=1}^{n_{ROI_{B_k}}} w_j = 1$. The weighting is done based on the recognition performance per ROI. During the development process, the recognition performance will be separately evaluated with features sets extracted per ROI, before the data fusion. The performance will be evaluated using TPR (True Positive Rate) and FPR (False Positive Rate) on the target class (the identity to be recognized). Actually the weighting for the fusion rules is applied for all features per set. A modified version of the rule should assign weights per individual features according to their discriminant power, but with the cost of an increased complexity. The equations are quite similar, excepting the assigned weights per feature.

2. *Weighted Fusion for normalized features*, in which a weighted sum is applied on normalized 1st and 2nd order statistic textural features (Haralick). The defining equations for the local fusion rules remain quite similar to the previous case, but their application concerns the transformed features based on a sigmoid function (for both 1st and 2nd order feature vectors per ROI). The features to be fused can be normalized with the sigmoid function having as parameters the scaling and translation factors α, β like in (Han, 2020):

$$f(x) = \frac{1}{1+\exp\left(-\alpha \cdot (x-\beta)\right)} \tag{7}$$

in which the input variable x is an individual feature as extracted from the selected ROIs within the original images with the local feature space size $d_{B_{k,j}}^{*(z)}$, $x = F_{B_{k,j}}^{*(z)}[i]$, $z \in \{1,2\}$, $j = \overline{1, n_{ROI_{B_k}}}$, $i = \overline{1, d_{B_{k,j}}^{*(z)}}$. The parameters should be fixed based on experimental data or using an empirical approach. A particular case of this function (with parameters the mean m_x and standard deviation σ_x of the input variable) is

$$f(x) = \frac{1}{1+\exp\left(-\frac{(x-m_x)}{\sigma_x}\right)} \tag{8}$$

One can consider a double sigmoid function quite similar to one specified in (Jain, 2005) by:

$$f(x) = \begin{cases} \dfrac{1}{1+\lambda \cdot \exp\left(-\alpha \cdot \dfrac{(x-\theta)}{\gamma_1}\right)}, x < \theta \\ \dfrac{1}{1+\lambda \cdot \exp\left(-\alpha \cdot \dfrac{(x-\theta)}{\gamma_2}\right)}, x > \theta \end{cases} \tag{9}$$

where: the amounts λ and α are the shape parameters of the sigmoid function (that

should be provided based on the available data); θ is a threshold that is selected such as to fall into the overlapping region between the distributions of the scores for the target vs. non-target classes (enrolled identities for the biometric recognition); γ_1 and γ_2 are the boundaries of the region in which the sigmoid function behavior is almost linear. The last 2 amounts are selected such as to ensure an equal extension of the 2 distributions towards the left and the right around the threshold.

The global biometric feature-level fusion is the process in which the features from each biometric modality are combined into a single feature vector (an *inter-modal* fusion). The global fusion scheme concatenates the feature vectors previously resulted from the local fusion (10).

$$\boldsymbol{F} = \begin{bmatrix} \boldsymbol{F}_{B_1}^{*} \\ \boldsymbol{F}_{B_2}^{*} \\ \boldsymbol{F}_{B_3}^{*} \end{bmatrix} \tag{10}$$

3.4 Biometric data classifier design

The classifier design addresses the identification task. The classification with a Machine Learning (ML) model follows a multi-class approach in which each of the enrolled identities represents a class. The identification is a process in which the subject only provides his/her biometric credential and the system just guess his/her true identity without any username. The identification needs to explore a large searching space of the possibile identities, therefore a multi-class design is required. For this design a conventional ML modeling is specified. Currently methods based on Deep Learning and particularly Convolutional Neural Network are used in many cases requiring image classification with advantages for feature representation and data classification. This research is still looking to explore the performance of conventional ML models (like SVM) on various biometric datasets, especially while making certain improvements of the original data space with FE techniques.

For the basic model one take the SVM classifier with a polynomial kernel (that is frequently used in image processing). The size of the training set will be fixed according to the condition specified in (Theodoridis, 2009), looking to ensure the best trade-off training set size (N_{tr}) vs. feature space size (N_{feat}) such as to prevent or to minimize the peaking and curse-of-dimensionality: $2 \le \frac{N_{tr}}{N_{feat}} \le 10$, where:

$$N_{feat} = d_{F_{B_1}^{*}} + d_{F_{B_2}^{*}} + d_{F_{B_3}^{*}} \tag{11}$$

$$d_{F_{B_k}^{*}} = d_{B_k}^{*}, B_k \in \{B_1, B_2, B_3\} \tag{12}$$

SVM is a binary classifier by default, therefore to properly manage the

identification as a multi-class problem one should apply a multi-class extension. For this design, the model is trained as a detector for a single target class (the enrolled identity) and the process will design several classifiers, one per identity.

3.5 Server-side: authentication and access control

The server-side component of the security architecture is depicted in Figure 3. This component includes the biometric matcher that basically performs the identification (biometric recognition) of the person providing the testing samples without any username. The biometric recognition output could be an ID (class membership) or a normalized score, depending on the design option for the classifier.

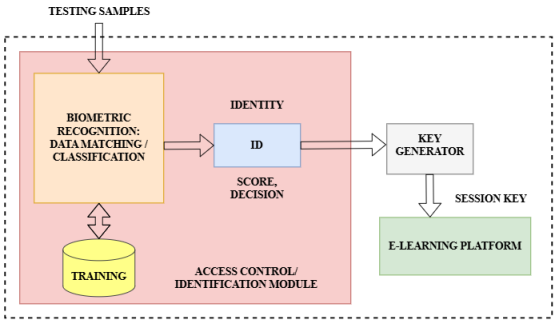

Figure 3. Feature Generation (server-side)

The key could be generated either based on the results of the biometric data matching but also one can take in account to directly use the fused features for this step. For example, one can consider methods like one presented in (Wang, 2021).

3.6 Various design options to be evaluated

Several design options will be further explored to develop a reliable and optimal security solution for e-Learning platforms:

- for the client-side components: feature selection and/or FE before or after feature-level fusion, an improved supervised PCA;
- for the server-side components: the mechanism for the key generation (based on the matcher ouputs or on the fused feature);
- for the mobile devices (Android): the feature fusion could by applied between face and iris, as the developer cannot have full access to the fingerprint feature vector.

4. Conclusions

The current advances in algorithms, hardware, software and communications enabled a significant evolution towards the adoption of e-Learning. However, the security still remains a major challenge for many existing e-Learning platforms.

This justifies the efforts to develop and integrate advanced solutions able to enhance the security degree but also to meet the applications constraints (resources, complexity, costs, performance).

In this paper a security model for e-Learning was proposed, based on a multimodal biometric approach with feature fusion. In this ongoing research several data fusion methods are explored. The proposed security model addresses the problem of biometric identification, looking to design a reliable system able to accurately guess the true identity of the e-Learning platform users. The steps towards a software implementation include: the enhancement of the model with optimized fusion rules and several FE methods, the implementation of the client-side components with the functionalities for feature generation, the implementation of the server-side component including the key generator (based on the identification output or on the fused features), the integration of the developed modules. For the experimental tasks, the recognition algorithms (based on ML) will be tested using Python libraries like scikit-learn. The performances ensured by the proposed data fusion method will be evaluated measuring the execution time on several datasets.

Acknowledgement

The work presented in this paper is supported by the Core Program within the National Research Development and Innovation Plan 2022-2027, carried out with the support of MCID, project no. 23380601, "Advanced research in the Metaverse and emerging technologies for the digital transformation of society".

REFERENCES

Afolabi, A.O., & Adagunodo, E. R. (2018) Securing E-Learning System with Crypto – Biometric Multimedia. *Biostatics and Biometrics Open Access Journal*. 7(2). https://juniperpublishers.com/bboaj/BBOAJ.MS.ID.555710.php [Accessed 20 th January 2025].

Al-Fraihat, D., Joy, M., & Sinclair, J. (2020) Evaluating E-Learning Systems Success: An Empirical Study. *Computers in Human Behavior*. doi: 10.1016/j.chb.2019.08.004.

Atenco, J. C., Moreno, J. C. & Ramirez, J. M. (2023) Audiovisual Biometric Network with Deep Feature Fusion for Identification and Text Prompted Verification. *Algorithms*. 16(2). doi: 10.3390/a1602 0066.

Chen, G., Liu, Z., Yu, G., Liang, J. (2021) A New View of Multisensor Data Fusion: Research on Generalized Fusion. *Mathematical Problems in Engineering.* doi: 10.1155/2021/5471242.

Curran, J. & Curran, K. (2021) Biometric Authentication Techniques in Online Learning Environments, IGI Global. doi: 10.4018/978-1-7998-8047-9.ch042.

Daza, R., Morales, A., Tolosana, R., Gomez, L. F., Fierrez, J. & Ortega-Garcia, J. (2022) edBB-Demo: Biometrics and Behavior Analysis for Online Educational Platforms. *arXiv* [preprint] arXiv:2211.09210. [Accessed: 23 th January 2025]

Drozdowski, P., Stockhardt, F., Rathgeb, C., Osorio-Roig, D. & Busch, C. (2021) Feature fusion methods for indexing and retrieval of biometric data: Application to face recognition with privacy protection. *IEEE Access*. 9.

Gheorghe-Moisii, M. & Tîrziu, E. (2015) Quality of applications in m-learning, *Romanian Journal of Computer Science and Automation*, vol. 25(1).

Han, W., Wang, R., Huang, D. & Xu, C. (2020) Large-Scale ALS Data Semantic Classification Integrating Location-Context-Semantics Cues by Higher-Order CRF. *Sensors*. 20(6), doi: 10.3390/s20061700.

Harakannanavar, S. S., Ramachandra, A. C., Pramodhini, R., Surekha, M., Puranikmath, V. I., Prashanth, C. R. (2022) Performance Evaluation of Feature Level Fusion for Multimodal Biometric Systems. *Mathematical Statistician and Engineering Applications*. 71(4). doi: 10.17762/msea.v71i4.836.

Heaton, J. (2016) An empirical analysis of feature engineering for predictive modeling. *SoutheastCon 2016*. https://arxiv.org/pdf/1701.07852 [Accessed 23th January 2025].

Herbadji, A., Guermat, N., Ziet, L., Akhtar, Z., Cheniti, M. & Herbadji, D. (2020) Contactless Multi-biometric System Using Fingerprint and Palmprint Selfies. *Signal Processing*. 37(6).

Ivanova, M., Bhattacharjee, S., Marcel, S., Rozeva, A. & Durcheva, M. (2019) Enhancing Trust in eAssessment - the TeSLA System Solution. *arXiv* [preprint] https://arxiv.org/abs/1905.04985 [Accessed 23th January 2025].

Jain, A., Nandakumar, K. & Ross, A. (2005) Score normalization in multimodal biometric systems. *Pattern Recognition.* 38, 12. doi:10.1016/ j.patcog.2005.01.012.

Kamlaskar, C. & Abhyankar, A. (2022) Feature level fusion framework for multimodal biometric system based on CCA with SVM classifier and cosine similarity measure. *Australian Journal of Electrical and Electronics Engineering*. 20(2). doi: 10.1080/1448837X.2022.2129147.

Lőfstedt, T., Brynolfsson, P., Asklund, T., Nyholm T. & Garpebring, A. (2019) Gray-level invariant Haralick texture features. *PLOS ONE*. 14(2):e0212110, https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0212110. [Accessed 28 th January 2025].

Luu, Q., Nguyen, D., Pham, H. & Huynh-Tuong, N. (2020) Authentication in E-learning systems: Challenges and Solutions. *Sci. Tech. Dev. J. – Engineering and Technology*. 3(SI1):SI95-SI101. doi: 10.32508/stdjet.v3iSI1.516.

Mansour, I. R. & Thomson, R. M. (2023) Haralick texture feature analysis for characterization of specific energy and absorbed dose distributions across cellular to patient length scales. *Physics in Medicine & Biology*. 68(7). https:// iopscience.iop.org/article/10.1088/1361-6560/acb885 [Accessed 23th January 2025].

Sasikala, T. S. & Sivasankar, K. (2018) Minutiae Based Feature Level Fusion for Multimodal Biometrics. *International Journal of Applied Engineering Research*. 1.

Shen, M., Liao, Z., Zhu, L., Mijumbi, R., Du, X. & Hu, J. (2018) IriTrack: Liveness Detection Using Irises Tracking for Preventing Face Spoofing Attacks. *arXiv* [preprint] arXiv:1810.03323. [Accessed 23 th January 2025].

Singh, M., Singh, R. & Ross, A. (2019) A Comprehensive Overview of Biometric Fusion. *ArXi.* abs/1902.02919. [Accessed 23 th January 2025]

Soviany, S., Gheorghe, C., & Dumitrache, M. (2023) A Multimodal Biometric System for the e-Health applications security. Proceedings of *24th International Conference on Control Systems and Computer Science (CSCS), Bucharest, Romania, May 24 - 26, 2023*. pp. 586 – 593.

Theodoridis, S. & Koutroumbas, K. (2009) *Pattern Recognition*. 4th edition, Academic Press Elsevier.

Wang, Y., Li, B., Zhang, Y., Wu, J. & Ma, Q. (2021) A Secure Biometric Key Generation Mechanism via Deep Learning and Its Application. *Applied Sciences*. 11(18). doi: 10.3390/app11188497.

Zogas, S., Kolokathi, A., Birbas, K., Chondrocoukis, G. & Mantas, J. (2016) The e-Learning Effectiveness Versus Traditional Learning on a Health Informatics Laboratory Course. *Studies in health technology and informatics.* 226, 109-12.