Evaluating Iris, Face, and Fingerprint Authentication

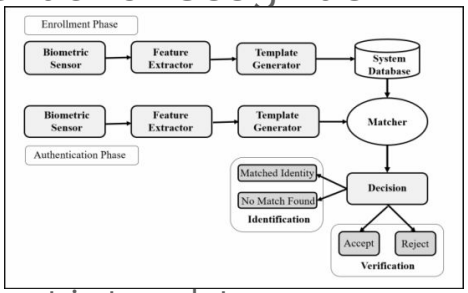
Amelie Ferrell, Griffin Danner-Doran, Ife Adetunji, Naif Alkaltham, Roneet Arora

Introduction - Roneet

- Passwords remain the most popular method of digital authentication
- In recent years, biometrics have been proposed as a supplement or complete alternative
- Fingerprint, 2D face, and iris recognition are the most promising alternatives for widespread deployment
  - lightweight algorithms that can be efficiently deployed on small devices (phones and laptops)
  - Shown to have high accuracy as well as fast run times - face and fingerprint already widespread, iris has promising methods
- Each have their own tradeoffs and weaknesses
- Goal: To evaluate each of the three biometric methods to determine the “best” for widespread use based on:
  - cost, accuracy, security, and usability,

Biometrics - Roneet

- 2 main phases of biometric authentication - enrollment and recognition
  - Consist of 4 modules
    - Enrollment:
      - sensor module
        - captures the users biometric data
      - feature extraction module
        - takes the target features and creates a biometric template
    - Recognition adds 2 additional modules:
      - matching module
        - new template is compared to the stored templates
      - decision module
        - matching results are used to accept or reject the user
  - Enrollment process is lengthy since it needs to be precise and make a detailed template
  - Recognition is where the authentication actually happens, so is much faster



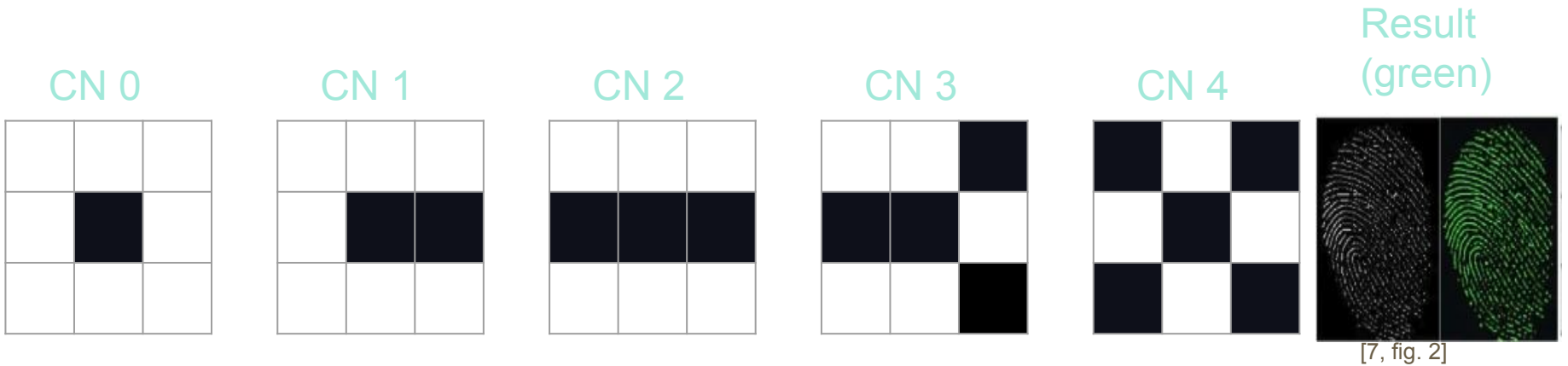
[6, fig 2]

Fingerprint Background - Roneet

- Oldest biometric:
  - discovered over 200 years ago and used as a form of identification for over 100
- Fingerprint biometrics comes from an analysis of ridges and valleys found on the human finger
- The patterns formed by ridges are called minutiae
- Before feature extraction, usually images are
  - Grayscaled then binarized to highlight ridges and valleys
  - Thinned to make it so each ridge is one pixel wide

Fingerprint Methods - Cross-Numbering[7] - Roneet

- In this method, after thinning the minutia is extracted by assigning each black pixel a value between 0-4
  - based on the sum of black neighbor pixels in its 3x3 area
- with each number corresponding to one of the 5 target properties:
  - isolated point, ending point, connecting point, bifurcation point



[7, fig. 2]

Fingerprint Methods - Mindtct[8] - Roneet

- In this algorithm, 2 x X slices of pixels are taken and analyzed to identify ridge endings and ridge bifurcations
  - These are the only 2 features looked at by this algorithm

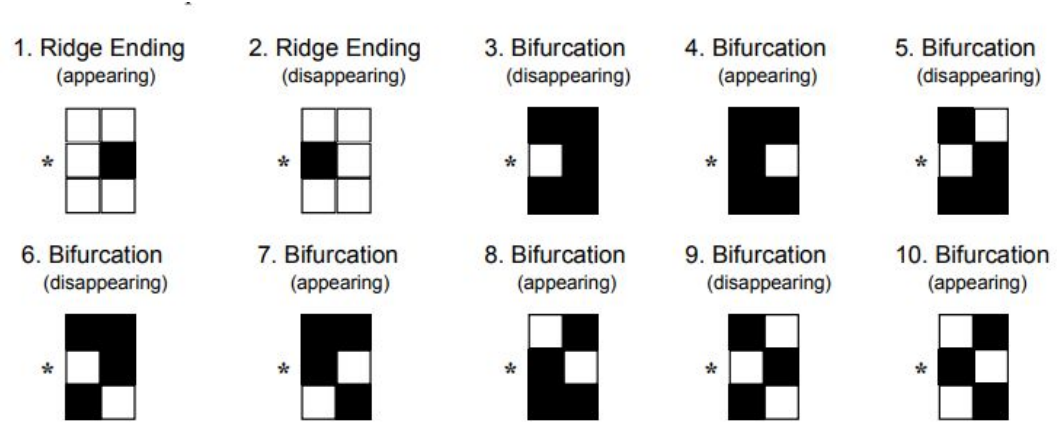


Figure 30. Pixel patterns used to detect minutiae.

[25, fig. 30]

Fingerprint Methods - Minutiae-pair[13] - Roneet

- After thinning, Verifinger SDK and a minutiae pair algorithm are used
  - All minutiae are paired to each other and have certain characters recorded into a short binary feature vector:
    - edge length
    - relative orientation
    - types
  - The vector is combined with the others to create a binary feature template vector

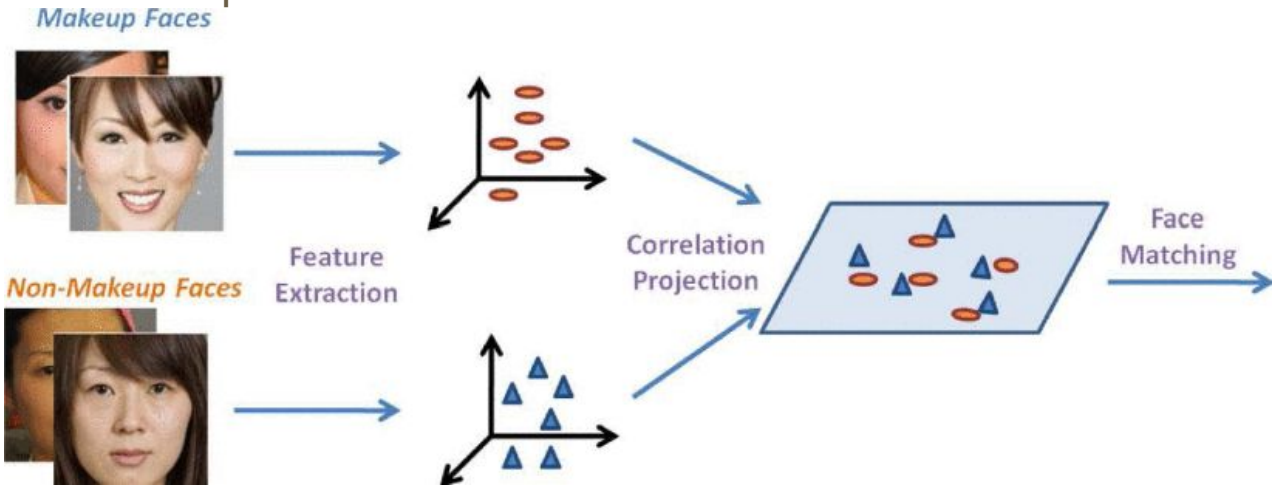
[13, fig. 2]

Face background - Amelie

- More recently developed method compared to fingerprint but has had a lot of growth over the past couple of years largely due to smartphones
- Face recognition uses the features of a user's face as its biometric marker
  - Face detection involves detecting an individual face from a live feed or an image
- Unlike fingerprint, there are many different features that can be analyzed which results in many different techniques for doing so
  - Most differences occur in the feature extraction and template encoding process

Face methods - Partial Least Squares[17] - Amelie

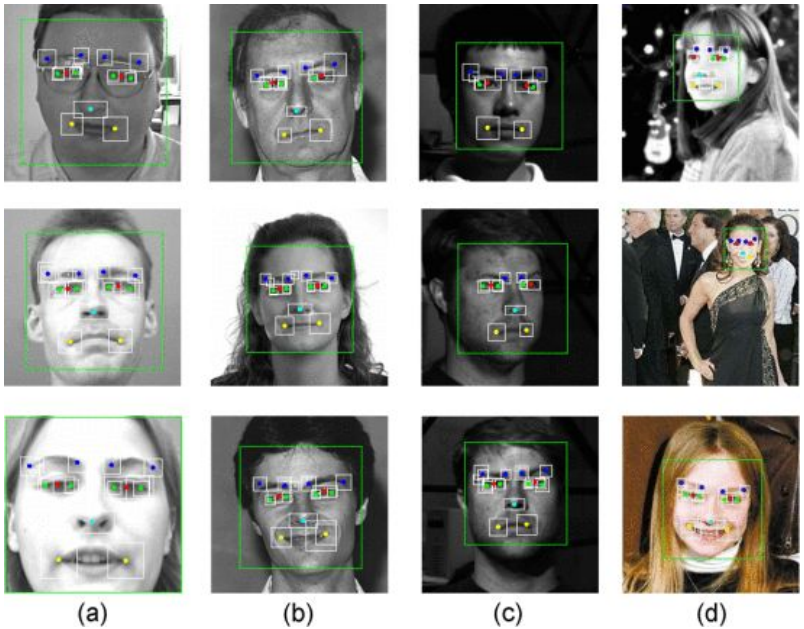
- This method uses a combination of a principal component analysis (PCA) algorithm, which is a form of eigenface feature extraction, and Partial Least Squares(PLS) algorithm to improve face accuracy when detecting makeup.



[17, fig. 2]

Face methods - Viola-Jones + LBP[18] - Amelie

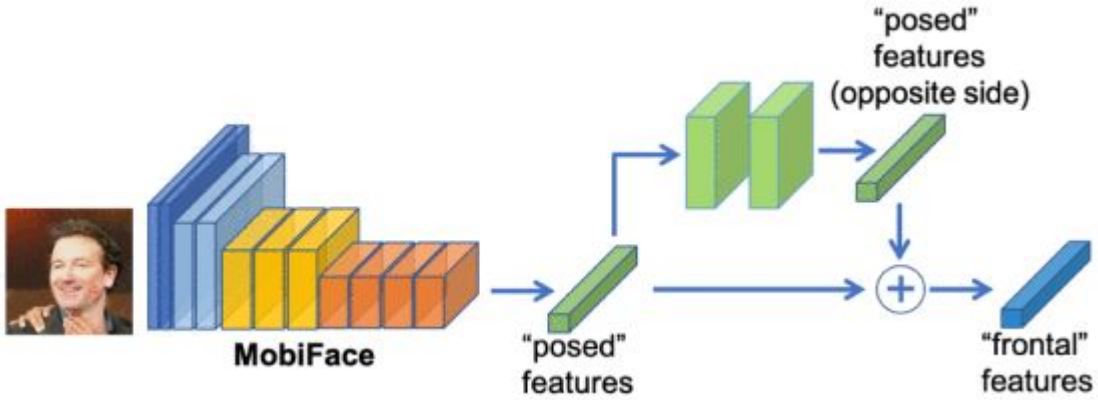
- This method uses the Viola-Jones pattern classification algorithm for face detection as well as feature extraction. It also uses LBP(Local Binary Pattern) to handle illumination normalization.



[18, fig. 6]

Face methods - Mobiface[23] - Amelie

- This algorithm uses lightweight deep learning. Mobiface algorithm uses bottleneck and residual bottleneck convolutional blocks for feature extraction. A fast downsampling strategy is also used to reduce computational complexity.



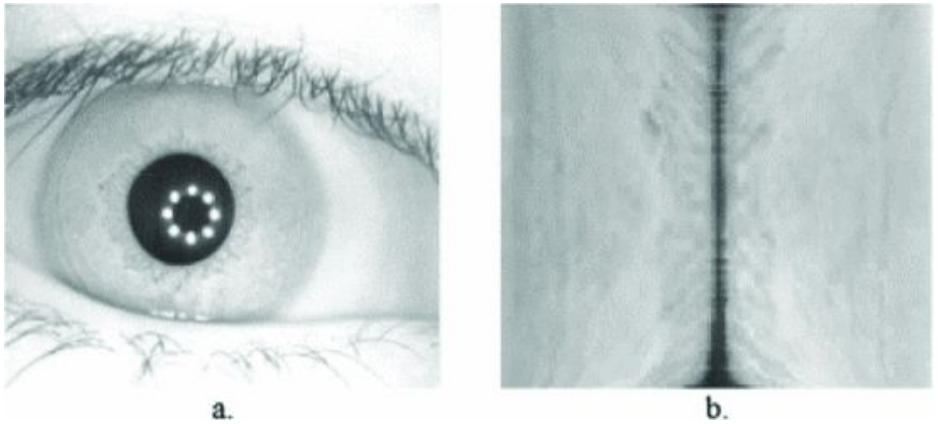
[23, fig. 1]

Iris background - Amelie

- Also more recently developed but is used less compared to Face recognition.
- Uses the unique colored ring around the pupil as its biometric feature.
  - The patterns of an iris form uniquely for each person, even among family members.
- There are a variety of different methods but all algorithms use iris segmentation and normalization to extract the iris from other features of the eye (e.g. sclera, pupil, eyelashes, etc).

Iris methods - CNN with softmax classifier[10] - Amelie

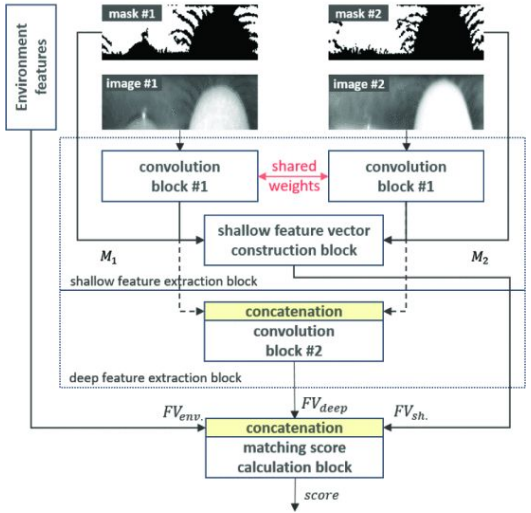
- This algorithm uses a thresholding algorithm to determine the iris boundary then goes through a normalization process to remove noise like eyelashes. Finally, features are classified and extracted using a layered Resnet CNN(Convolutional Neural Network) with a Softmax classifier.



[10, fig. 7]

Iris methods - Lightweight CNN[21] - Amelie

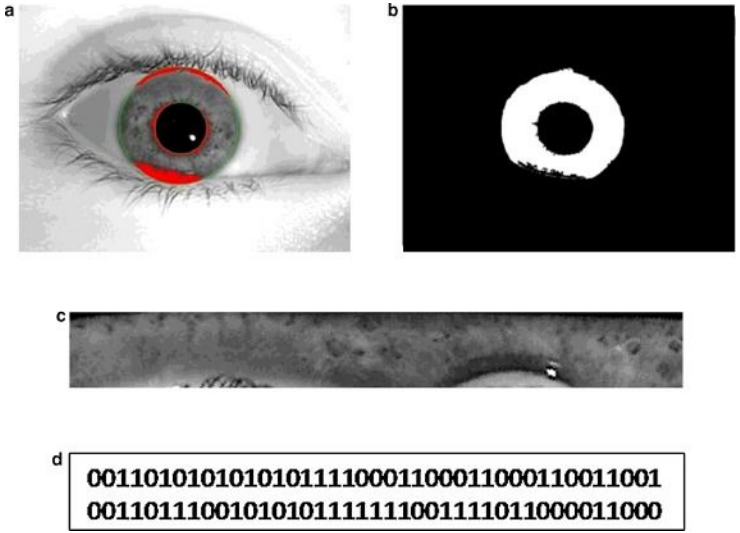
- This method uses a lightweight CNN that uses 2 convolutional blocks with 2 and 4 layers respectively. The first block extracts low level features to normalize and isolate the iris, then the second block extracts deep features for template generation and comparison.



[21, fig. 2]

Iris methods - NDBIris[11]- Amelie

- A Secure iris recognition scheme using a negative database storage technique on top of open source OSIRIS-V4.1
  - Algorithms used for recognition and extraction: OSIRIS-V4.1 uses least-squares for localization, Daugman's rubber sheet model for normalization, and 2D-Gabor filters for feature extraction



[26, fig. 1]

Research questions - Naif

- Security and accuracy are the most important elements of a biometric system, as they determine if a scheme is suitable for authenticating users correctly
  - R1:What are the security concerns (i.e. accuracy and resistance to impersonation) of each type?
- Because biometrics are meant to be permanent in order to accurately identity users over a long period of time, we wanted to see which of the 3 best fits this
  - R2: How do changes in an individual's physical features over time affect the reliability of iris, face, and fingerprint authentication? And among these, which method consistently delivers the most accurate results?
- Finally, widespread adoption will not occur if the method is hard to use or prohibitively expensive, so we wanted to examine these aspects
  - R3: What are the usability and cost propositions of each type? In other words, how viable is it to introduce this biometric type into everyday technology?

Outline/methods - Naif

- Literature Review: Investigated seminal papers on iris, face, and fingerprint biometrics, concentrating on:
  - Performance metrics: accuracy, security, cost, user experience.
  - Influence of environmental conditions (time, lighting).
  - Practical application of biometric methods.
- Outcome Synthesis:
  - Merged literature examination results
  - Ranked biometric methods for large-scale deployment suitability.
  - Produced final recommendation for ideal biometric practices in real-world use cases.

Findings - Griffin

- Overall, we found that despite its relatively high cost and somewhat cumbersome user experience, iris recognition's high accuracy and security make it the best choice for widespread, commercial biometric authentication

Each biometric method is rated on a scale of 1-5 where 1 = exceptional and 5 = substandard

X	**Accuracy**	**Accuracy over time**	**Security**	**Cost**	**Usability**
Finger	2	4	3	1	2
Face	3	3	5	1	1
Iris	1	1	1	4	3

Accuracy - Griffin

- Fingerprint had a variety of accuracies depending on the technique, but in the best cases it could get down to .94% EER
  - When taken correctly, fingerprint is very accurate
- 2D face authentication was a little less accurate, with the best method getting down to 2% EER
  - Much more potential features to analyze, can mix up those with similar faces
- As expected, iris was the most accurate, able to get down to an EER of .03% in the best case
  - Most detailed biometric features - provides the most distinguishing elements

Accuracy table - Griffin

- This table shows the best case accuracies of the various methods we explored

Technique	type	EER	GAR	FAR/FMR	FRR/FNMR
Blockchain-based cross numbering[7]	finger	-	82.55%	-	-
Mindtct[8]	finger	0.94%	-	1.53%	-
Minutiae-pair[13]	finger	8.25%	-	-	-
Partial least squares[17]	face	-	80.5%	-	-
Viola-Jones + LBP[18]	face	2%	-	-	-
MobiFace[23]	face	-	91.3%	-	-
CNN with softmax classifier[10]	iris	-	96.67%	-	-
NDBIris[11]	iris	0.6%	98.94%	0.01%	-
Lightweight CNN[21]	iris	0.03%	-	-	-

Security - Griffin

- Fingerprints have long been known to be copyable and are the our only studied biometric which requires contact, increasing the chance for biometric prints to be stolen
  - However, many software based solutions have been developed to detect false presentation attacks - one example was able to get down to an EER of just .97% when faced with picture-based presentation attacks
- 2D face has very low security
  - 2D face very vulnerable to image presentation attacks
  - Even with 3D depth added it, it still proves vulnerable - one study was able to achieve almost 60% success rate against 3D depth based systems with a static picture
- Iris is very secure - no contact, spoofed attacks lose details
  - Lightweight deep learning liveness check able to get EER of .33% against pictures, contact lenses, and even cadaver eyes

Accuracy over time - Ife

- Fingerprint recognition suffers very heavily from environmental factors like time, injury, or even dirtiness (scanner or finger)
  - Since most scanners just look at the grayscale ridges and valleys, very hard to account for such changes
- Face recognition also struggles with such changes like clothes, makeup, age, etc.
  - While some techniques try to use the increased information density of the face to account for these kinds of elements, like the makeup method discussed earlier, 2D face still has issues with feature changes
- Iris is fully unique over time and even between eyes, and suffers very little from environmental factors
  - Because users need to get close to camera, other factors tend to be less impactful

Cost - Ife

- Fingerprint authentication is very cheap to implement, scanners are cheap to buy or you can just use a phone camera like a scanner
- 2D face authentication costs almost nothing to implement on a modern phone
    - However, the 3D cameras that might be needed for proper liveness checks are not in all devices and could be potentially very expensive to add
- Iris has the highest cost since it needs much better quality compared to fingerprint and facial authentication
    - Although, as camera quality increases, this becomes less of a prohibitive factor

Usability - Ife

- Fingerprint authentication is very simple to use
  - Just touch finger to camera or scanner - however, is the only one of the 3 that requires physical contact
- 2D facial authentication easiest to use, just look at camera to authenticate
- Iris is hardest to use, requires you to get close to camera for a few seconds to let camera take high quality image of iris

Conclusion - Griffin

- Fingerprint authentication strikes a balance between cost, accuracy, ease of use and security but has weak accuracy over time
- 2D face authentication is incredibly cheap and easy to use while having decent accuracy, however it has very weak security and accuracy over time
- Iris has a relatively high cost and middling usability, but makes up for it with impressive security and overall accuracy
- Based on our research, we recommend iris as the best authentication method for widespread use

Future works - Naif

- We could include additional factors in our analysis
  - Efficiency - while all 3 methods are efficient enough for mobile devices, efficiency is an important factor in IoT devices
  - Privacy - we focused on security from an authentication perspective, but in the long term it is important to observe how secure template storage is
- We could also explore 3D face as an additional biometric method
  - While we did not include 3D since it generally requires additional hardware like an infrared scanner to implement, the cost of such hardware is going down
  - Though high end, apple with faceID shows that in the near future it can be cheaply implemented

References

[1] Z. V. Boriev, S. S. Sokolov, and A. P. Nyrkov, “Review of modern biometric user authentication and their development prospects,” *IOP Conference Series: Materials Science and Engineering*, vol. 91, p. 012063, Aug. 2015. doi:10.1088/1757-899x/91/1/012063.

[2]S. M. R. Bagwan, G. Gupta and S. B.Thigale, "Robust Multi-Bio-Metric Authentication Framework in Face and Iris recognition," 2023 2nd International Conference for Innovation in Technology (INOCON), Bangalore, India, 2023, pp. 1-10, doi: 10.1109/INOCON57975.2023.10100996.

[3]N. K. Shaydyuk and T. Cleland, "Biometric identification via retina scanning with liveness detection using speckle contrast imaging," 2016 IEEE International Carnahan Conference on Security Technology (ICCST), Orlando, FL, USA, 2016, pp. 1-5, doi: 10.1109/CCST.2016.7815706.

[4]Z. Wu, Y. Cheng, J. Yang, X. Ji and W. Xu, "DepthFake: Spoofing 3D Face Authentication with a 2D Photo," 2023 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2023, pp. 917-933, doi: 10.1109/SP46215.2023.10179429.

[5]H. Shahriar, H. Haddad and M. Islam, "An Iris-Based Authentication Framework to Prevent Presentation Attacks," 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC), Turin, Italy, 2017, pp. 504-509, doi: 10.1109/COMPSAC.2017.60.

[6]S. K. Choudhary and A. K. Naik, "Multimodal Biometric Authentication with Secured Templates — A Review," *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, Tirunelveli, India, 2019, pp. 1062-1069, doi: 10.1109/ICOEI.2019.8862563.

[7]D. Pawade, A. Sakhapara, M. Andrade, A. Badgujar and D. Adepu, “Implementation of Fingerprint-Based Authentication System Using Blockchain,” In Soft Computing and Signal Processing - Advances in Intelligent Systems and Computing, vol 900. pp. 233 -242, Jan 2019, doi:10.1007/978-981-13-3600-3_22.

[8]X. Yin, S. Wang, M. Shahzad and J. Hu, "An IoT-Oriented Privacy-Preserving Fingerprint Authentication System," in IEEE Internet of Things Journal, vol. 9, no. 14, pp. 11760-11771, 15 July 15, 2022, doi: 10.1109/JIOT.2021.3131956.

[9]S. Singh, S. C. K. Chintalacheruvu, S. Garg, Y. Giri and M. Kumar, "Efficient Face Identification and Authentication Tool for Biometric Attendance System," *2021 8th International Conference on Signal Processing and Integrated Networks (SPIN)*, Noida, India, 2021, pp. 379-383, doi: 10.1109/SPIN52536.2021.9565990.

[10]T. Le-Tien, H. Phan-Xuan, P. Nguyen-Duy and L. Le-Ba, "Iris-based Biometric Recognition using Modified Convolutional Neural Network," 2018 International Conference on Advanced Technologies for Communications (ATC), Ho Chi Minh City, Vietnam, 2018, pp. 184-188, doi: 10.1109/ATC.2018.8587560.

[11]D. Zhao, W. Luo, R. Liu and L. Yue, "Negative Iris Recognition," in IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 1, pp. 112-125, 1 Jan.-Feb. 2018, doi: 10.1109/TDSC.2015.2507133.

[12]I. Ahmed and A. Asghar, “Evaluating the Efficacy of Biometric Authentication Techniques in Healthcare”, IJRAI, vol. 13, no. 7, pp. 1–12, Jul. 2023.

[13]W. Yang, S. Wang, K. Yu, J. J. Kang and M. N. Johnstone, "Secure Fingerprint Authentication with Homomorphic Encryption," 2020 Digital Image Computing: Techniques and Applications (DICTA), Melbourne, Australia, 2020, pp. 1-6, doi: 10.1109/DICTA51227.2020.9363426.

References

[14]Y. Liu et al., "Secure and Efficient Online Fingerprint Authentication Scheme Based On Cloud Computing," in IEEE Transactions on Cloud Computing, vol. 11, no. 1, pp. 564-578, 1 Jan.-March 2023, doi: 10.1109/TCC.2021.3103546.

[15]A. A. Pawle and V. P. Pawar, “A study of different biometric authentication techniques in cloud computing,” *International Journal of Engineering Research and*, vol. V6, no. 05, pp. 944–951, May 2017. doi:10.17577/ijertv6is050575.

[16]S. M. R. Bagwan, S. Kumar and S. B.Thigale, "Face, Iris, and Fingerprint based Robust Biometric Authentication System," 2023 2nd International Conference for Innovation in Technology (INOCON), Bangalore, India, 2023, pp. 1-8, doi: 10.1109/INOCON57975.2023.10101122.

[17]G. Guo, L. Wen and S. Yan, "Face Authentication With Makeup Changes," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 24, no. 5, pp. 814-825, May 2014, doi: 10.1109/TCSVT.2013.2280076.

[18]Q. Tao and R. Veldhuis, "Biometric Authentication System on Mobile Personal Devices," in IEEE Transactions on Instrumentation and Measurement, vol. 59, no. 4, pp. 763-773, April 2010, doi: 10.1109/TIM.2009.2037873.

[19]C. Rathgeb, F. Breitinger, H. Baier and C. Busch, "Towards Bloom filter-based indexing of iris biometric data," 2015 International Conference on Biometrics (ICB), Phuket, Thailand, 2015, pp. 422-429, doi: 10.1109/ICB.2015.7139105.

[20]S. Joy, R. Baby Chithra, A. S. Bale, N. Ghorpade, S. N. Varsha and A. S. Naidu, "A Comparative Study on Recent Trends in Iris Recognition Techniques," 2022 International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, 2022, pp. 1521-1525, doi: 10.1109/ICEARS53579.2022.9752355.

[21]G. Odinokikh, M. Korobkin, I. Solomatin, I. Efimov and A. Fartukov, "Iris Feature Extraction and Matching Method for Mobile Biometric Applications," 2019 International Conference on Biometrics (ICB), Crete, Greece, 2019, pp. 1-6, doi: 10.1109/ICB45273.2019.8987379.

[22]J. E. Tapia, S. Gonzalez and C. Busch, "Iris Liveness Detection Using a Cascade of Dedicated Deep Learning Networks," in IEEE Transactions on Information Forensics and Security, vol. 17, pp. 42-52, 2022, doi: 10.1109/TIFS.2021.3132582.

[23]C. N. Duong, K. G. Quach, I. Jalata, N. Le and K. Luu, "MobiFace: A Lightweight Deep Learning Face Recognition on Mobile Devices," 2019 IEEE 10th International Conference on Biometrics Theory, Applications and Systems (BTAS), Tampa, FL, USA, 2019, pp. 1-6, doi: 10.1109/BTAS46853.2019.9185981.

[24]E. Marasco and A. Vurity, "Fingerphoto Presentation Attack Detection: Generalization in Smartphones," 2021 IEEE International Conference on Big Data (Big Data), Orlando, FL, USA, 2021, pp. 4518-4523, doi: 10.1109/BigData52589.2021.9672054.

[25]C. Watson et al., “User’s Guide to NIST Biometric Image Software (NBIS),” 2007,. https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7392.pdf.

[26]N. Othman, B. Dorizzi, and S. Garcia-Salicetti, “OSIRIS: An open source iris recognition software,” Pattern Recognition Letters, vol. 82, pp. 124–131, Oct. 2016, doi: https://doi.org/10.1016/j.patrec.2015.09.002.