Biometric Security Enhancement with Eigenface and Facial Landmarks

Privacy-Enhancing cryptography methods for identity management

Suryabhan Singh
School of Computer Science and Engineering
Lovely Professional University
Phagwara, Punjab, India
suryabhan.12114479@lpu.in

***Abstract*—This paper presents an analysis of current cryptography systems used, specifically focusing on biometric systems, particularly facial biometric security systems. These systems are extensively employed in electronic devices such as smartphones, attendance system hardware, smart TVs, computers, etc. However, it has been observed that many of these systems still rely on conventional cryptographic methods. In the era of Artificial Intelligence (AI) advancement, the field of facial biometric security has somewhat lagged behind. This paper aims to propose both previously suggested solutions and a novel approach to address these challenges.**

Keywords—biometric, cryptography, mediapipe, artificial intelligence, face recognition, privacy enhancements, eigenface, pca, principal component analysis, facemesh

I. Introduction

Biometric authentication made its debut with the launch of the iPhone 4s in 2011, ushering in a new era of phone security. Subsequently, other smartphones adopted similar biometric features, followed by portable computer systems. Despite the initial momentum in the biometric authentication market, there has been a notable lack of substantial evolution and innovation in this sector.

The intersection of biometric authentication with cryptography became prominent with the introduction of key and face/fingerprint lock mechanisms. However, these methods, once introduced, remained largely unchanged and have been prevalent in the market since.

Recognizing the need for advancement, researchers delved into enhancing existing methods. In 1991, Turk and Pentland [5] introduced the concept of "eigenfaces," building upon Sirovich and Kirby's work. They utilized weights and eigenpictures as characteristic features for face recognition.

A groundbreaking approach was proposed by Nasim Arshad, Kwang-Seok Moon, and Jong-Nam Kim from Pukyon National University, Korea, merging privacy security with biometric authentication. They suggested the use of EigenFaces with Principal Component Analysis (PCA) to generate an optimal fingerprint of a human face for authentication within a threshold-based system.

Another noteworthy study by Adrian Tam, a machine learning blogger, explored using Eigenface for identity hash matching, further showcasing the versatility of this approach.

Building upon these studies, this paper introduces an optimized method utilizing Eigenface with Google's trained model of MediaPipe for facial landmark analysis, addressing the dual objectives of privacy and biometric authentication.

Through a comprehensive analysis of these studies, this paper aims to propose a newer, optimized solution that enhances the effectiveness and security of biometric authentication systems.

II. Literature Review

A. Introduction to Eigenface

Eigenface is rooted in linear algebra principles, specifically principal component analysis (PCA). It involves processing a dataset of grayscale images of human faces, converting each image into a vector format, and representing the entire dataset as a matrix where each element corresponds to a pixel's grayscale value.

$Eigen\ faces$:

$$[v_1, v_2, \dots, v_K](top\ K\ eigen\ vectors) \quad (1)$$

B. Principal Component Analysis (PCA)

PCA is a fundamental mathematical technique used to identify patterns and extract important features from high-dimensional data. In the context of eigenface, PCA is applied to the face image matrix to compute a set of vectors known as principal components. These components represent key directions in the data space and are orthogonal to each other.

$Weightsvector$:

$$W = \text{Eigenfaces}^T \cdot x \quad (2)$$

$Mean - centered\ matrix$:

$$\hat{X} = X - \bar{x} \quad (3)$$

C. Covariance Matrix and Eigenvectors

By computing the covariance matrix of the mean-centered face image matrix, One can derive its eigenvectors and eigenvalues. The eigenvectors, arranged in decreasing order of eigenvalues, form the principal components. These vectors capture the most significant variations or features present in the dataset.

$Covariance\ matrix$:

$$C = \frac{1}{M}\hat{X}\widehat{X^T} \quad (4)$$

Similarity matrix:

$$L2\text{-}norm(W_1, W_2) = \sqrt{\sum_{i=1}^{K}(W_{1i} - W_{2i})^2} \quad (5)$$

D. Eigenface Representation

The principal component vectors obtained from PCA serve as the eigenfaces. These eigenfaces represent

characteristic facial features and are used to reconstruct and recognize faces. By projecting a face image onto the eigenfaces, one can determine the face's resemblance to each eigenface and calculate weights that represent the face's features relative to the eigenfaces.

E. Face Reconstruction and Distortion

Eigenfaces enable the reconstruction of a face image using weighted combinations of the principal components. This reconstruction process may result in some distortion but retains essential facial characteristics. The top K eigenfaces, selected based on their importance (indicated by eigenvalues), contribute significantly to the reconstructed face.

$Reconstructed\ face$:

$$\hat{x} = \text{Eigenfaces} \cdot W + \bar{x} \qquad (6)$$

III. Related Work

As introduction already suggested there has been many studies conducted but here only two will be analyzed based on Eigenface and Hamming distance.

A. Eigenface matching using hamming distance

- Nasim Arshad, Kwang-Seok Moon, and Jong-Nam Kim in their paper used 3 datasets for analysis: Yale face dataset, ORL dataset and Pukyong National University (PKNU) face dataset.
- All the three databases consist of 2 categories of images. One category is used for training and the other for the testing purpose. The Yale database consists of 15 different people with nine varying pose, illumination and expressions. It uses 135 images for training and 30 images for testing. The ORL database consists of 40 different people with nine varying pose and expressions
- Next they computed eigenface for all datasets using Eigenface formula.

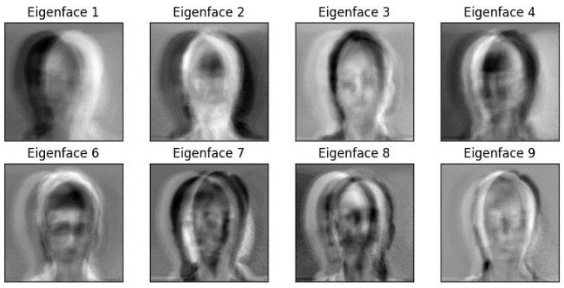

Fig 1: Eigenfaces for yale face dataset

- Next process is to generate projected faces for corresponding eigenfaces

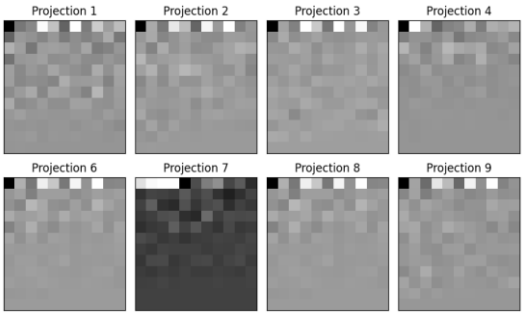

Fig 2: Eigenface projection for Yale face dataset

- Now, as the projections are generated for the authorized users, It is ready to get encrypted as authetication data.
- The study is using AES with a random 8-bit key for encryption that may work as user password for authentication.

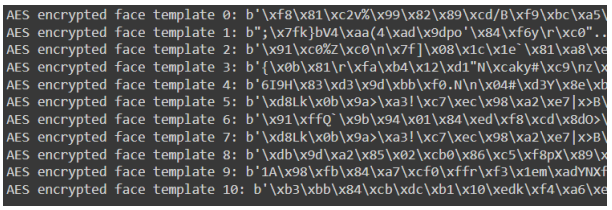

Fig 3: AES encryption of eigenface projections

- Now, as projections are encrypted, one can test the authentication using a single image from the yale dataset

Fig 4: Eigenface for test dataset

- Next is to generate projection for the test dataset

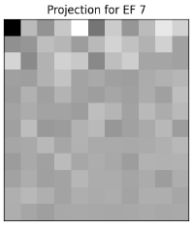

Fig 5: Projection of eigenface test dataset

- To match this projection with authetication one, encrypted projection will be decrypted using user provided key.

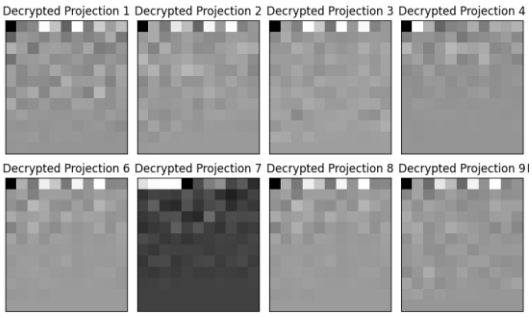

Fig 6: Decrypted Projections with the user-key

- Now, one can calculate hamming distance between test projection and all decrypted projection and verify authorization.
- Based on that one can calculate accuracy of the method

Dataset	Dimension	Train split	Test split	Accuracy
Yale	100*100	135	30	93.33
ORL	100*100	360	40	92.5
PKNU	100*100	54	9	100

Table 1: Experiment 1 result

B. *Eigenface projection matching using euclideon distance*

Adrian Tam, in his paper "Face Recognition using Principal Component Analysis" [2] explained the approach more briefly. He used the proposal suggested in the paper by Sirovich and Kirby [3] that a euclideon distance for projection matching should work more better than the hamming distance.

1) *Study references analysis*

- The dataset in the paper used is "ORL Database of Faces" [4] from kaggle. The file is a zip file of around 4MB. It has pictures of 40 persons and each person has 10 pictures. Total to 400 pictures. In the following it assumed the file is downloaded to the local directory and named as attface.zip.
- The Eigenface method has found widespread applications in biometric systems, particularly in face authentication and identification. Li and Jain [6] proposed a multi-resolution Eigenface approach, which leverages pyramid-based image representations to enhance recognition accuracy and efficiency
- Several comparative studies have been conducted to evaluate the effectiveness of Eigenface against other face recognition techniques. Smith and Chang [7] conducted a comprehensive analysis comparing Eigenface with methods like Eigeneyes and Eigenmouth, highlighting the strengths and weaknesses of each approach in differentiating facial features.
- Recent research efforts have focused on optimizing the Eigenface algorithm for scalability and computational efficiency. Wang [8] introduced a parallelized implementation of Eigenface using GPU acceleration, significantly reducing processing times for large-scale face datasets.

2) *Approach proposed/suggested*

- Similar to the previous study, this paper is also generating eigenface for each image that can be considered authorized, if talking about real security scenario.

Fig 7: Authorized loaded images

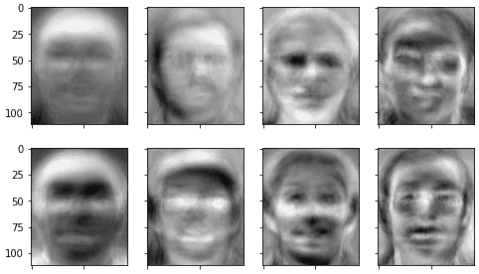

Fig 8: Eigenfaces for corresponding images

- Now, this is where this study varies from the previous study. It doesn't use projection but only the eigenfaces.
- Now, These faces can be encrypted using preferred encryption algorithm.
- Next, For testing one can load a single dataset image, generate eigenface and match with decrypted eigenfaces using euclideon distances.

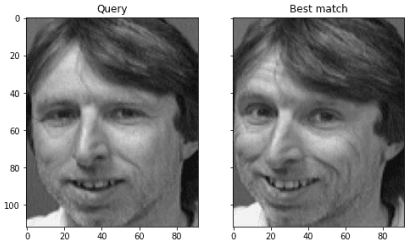

Fig 9: Test image 1 for eigenface match

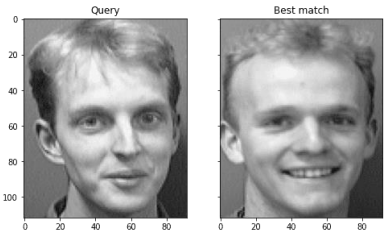

Fig 10: Test image 2 for eigenface match

C. *The disadvantages and aftermath*

Although, In both studies the accuracy is good but there are two aspects neglected in both approcaches.

- There is a chance of hash clashing, or in other word, some faces may generate almost similar projections, that might overlap and give authentication to

unauthorized person. Although, One cannot directly blame the authors as their concern is related to face matching not security, but in this case, security is a high concern.

- Other neglected aspect is optimal approach. The studies are concluding complete face, that may also include background noises that cannot be necessarily removed by grayscaling images. There should be only required features collected as projections instead of everything, so that it won't affect the accuracy.
- High Threshold values: In both approaches, Hamming distance and Euclideon distance, the threshold values, or the minimum distance from most optimal match is very high. Therefore, That should also be considered in the following studies.

Method	Accuracy	Average Threshold
Hamming method	95.2%	3919.31
Eudlideon method	91.8%	2339.88

Table 2 : Approach metrics comparison

IV. PROPOSED SOLUTION

After going through both studies and their referenced studies, and their disadvantages, and their advantages, here are two approaches combining both study and their disadvantages using Google's model MediaPipe.

- This proposed solution will be using Yale face dataset for training and testing. It has different 10 subjects

A. MediaPipe FaceDetection module for eigenface generation

A Mediapipe has been used in machine learning algorithm for quite a while now for facial and hand landmark detection. The facility of mediapipe here is used as the minimal required features extraction tool.

- First task would be loading the dataset and extracting using MediaFace FaceDetection [9] module and convert it to grayscale.

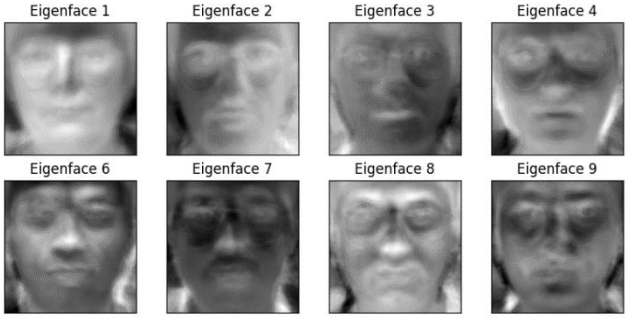

Fig 11 : Eigenfaces using FaceDetection

- Already better result can be seen in here. Now, taking reference of 1st study, one can generate the projection of corresponding eigenfaces.

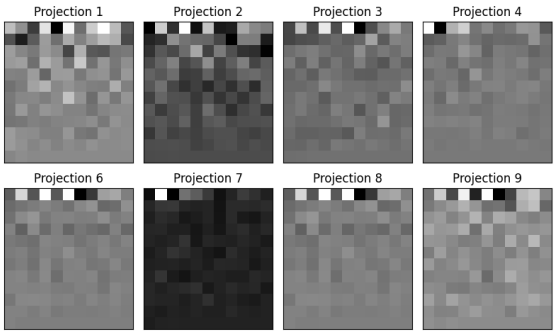

Fig 12 : Eigenface projections for FaceDetection

- These projections are quite better and less noisy than the 1st study approach. Which also neglect no faces.
- Now, Same as the first study one can encrypt using AES user key.

```
AES encrypted face template 0: b'D!g2va\xd9\x95A{\xa0.\xc1\
AES encrypted face template 1: b'\xee\x934\xf1J\x1d<axK\t\x
AES encrypted face template 2: b'h\x91\xbf\xa3\x01\xe6\xd4E
AES encrypted face template 3: b'\xed\x9d\xfco\x85\xb7\x0b\
AES encrypted face template 4: b"\xa2\x8c\xfa2s\rl'k\xdb\x8
AES encrypted face template 5: b'\xed\x9d2\xe3\xac!n\xd6,\x
AES encrypted face template 6: b"\xfe\xe2\x1c'tP\xe8_5K\xd1
AES encrypted face template 7: b'\xed\x9d2\xe3\xac!n\xd6,\x
AES encrypted face template 8: b'\xfc\xa7\x89\xdf\x1f\x03\x
AES encrypted face template 9: b"1\x81\xcc\x92n\xa4y\xd3A'\
AES encrypted face template 10: b'\tO\xc6\x13\x92\xb1}\x91\
```

Fig 13 : Encrypted eigenface projections

- Loading and testing made optimal than conventional approaches. Test data can be loaded as projections now.

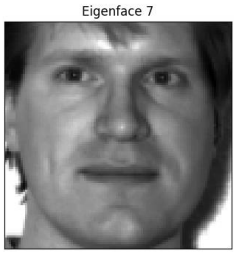

Fig 14 : Loaded test image

- Next step would be to generate projection for the following

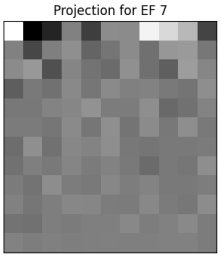

Fig 15 : Projection for loaded test eigenface

- Now, The authorized projection can be decrypted with the user-given key.

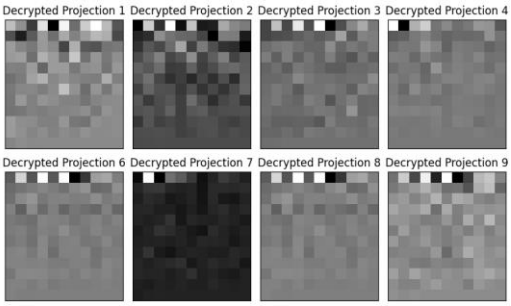

Fig 16 : Decrypted Projections for test projection matching

- At the end, considering approaches from study 1 and study 2, Hamming distance and Euclideon distances would be calculated as the evaluation parameter.

Dataset	Yale's Face database
Accuracy	89.9%
Average Threshold	1903.57
Optimzation	51%
Loss	10.11%

Table 3 : Proposed Solution 1 result

B. MediaPipe facemesh for eigenface generation

Even though, the previous approach sounds quite promising, and covering the disadvantages of the previous studies, but it has quite a lot more of loss rate in comparison with precious studies. And, Average threshold is still quite high so, Here is another approach where instead of using MediaPipe's face detector module, there will be used MediaPipe Facemesh [10].

Face Landmarks are virtual facial structures of a human face, which only observes the significant part of face.

Fig 17 : Facial Landmarks generated by MediaPipe facemesh

These points too will give unique fingerprints for each face but along with that, it will have less PCA components to analyze and hence less need of dimensionality reduction.

This will decrease the processing time and will use only required coordinates to geenrate fingerprint.

- First step would be loading the datasets and extract facial landmarks.
- After that, as previous approaches suggested, Eigenfaces would be generated, but only for landmarks and neglecting rest of the face.

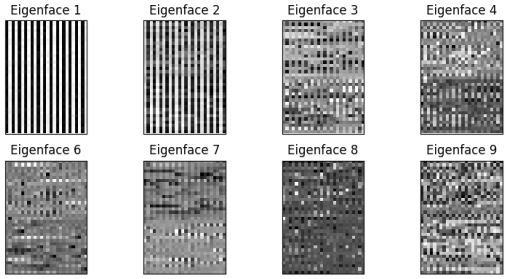

Fig 18 : Eigenfaces for facemeshes

- Similarly as previous approaches, Projection will be generated

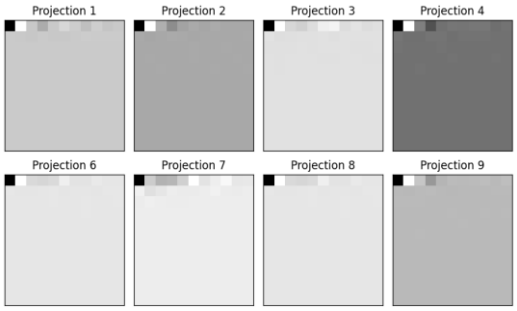

Fig 19 : Eigenface projections

Although, these do not sound promising but with minimal facemesh coordinates, these will generate a unique fingerprint everytime.

- Next, the projected eigenfaces would be encrypted and stored

```
AES encrypted face template 0: b'\xa4\xea\x8ar$\xe5\x95\xb9>b,\xc7\xa
AES encrypted face template 1: b'\xff\x17\x12\xe1|\x03|D\x19\x1aO\x04
AES encrypted face template 2: b'IO\xd3\x80\xac*\xb2\xedf\x140*\xbb(h
AES encrypted face template 3: b'\xbe\x108\xb4\xaf\x97\xcb#lMtg\x96\x
AES encrypted face template 4: b'\xd2\xd71p\xe9\x15"\xd2%\xc4D\xf2\xd
AES encrypted face template 5: b'F]\xf4\x81\x15E\xa7\x9f\x07^tl\x9eP8
AES encrypted face template 6: b'\xd4\xf2\x85Y\xa7A\xb0\xb5#hfN\xcb\x
AES encrypted face template 7: b'F]\xf4\x81\x15E\xa7\x9f\x07^tl\x9eP8
AES encrypted face template 8: b'\xe2w^a\x0c\x8d\x15\xa4\xc1\x8d\xbb5
AES encrypted face template 9: b'Jro\xfb\xf5\xd5\xcaQ1\xc5\xb3\x19\x8
AES encrypted face template 10: b'\xad\xad\xdd\xbe`\x02\x85\xde\xf6@\
```

Fig 20 : Projection encryption using user key with AES

- Now, the data is ready to test, the test data can be loaded

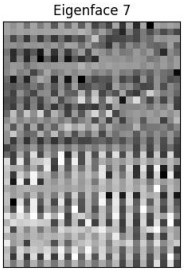

Fig 21 : Test facemesh eigenface

- Now, the test eigenface is ready for projection and to generate fingerprint

Fig 22 : Test facemesh projection

This fingerprint is ready for the matching now with the authorized fingerprints/projection.

- Now, the projections can be decrypted and matched with test projection.

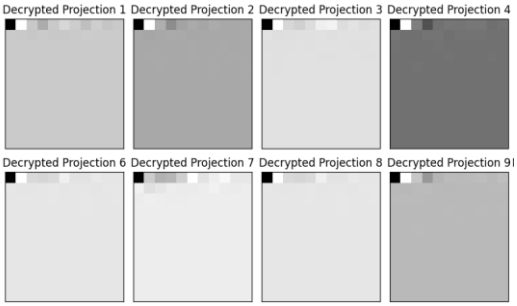

Fig 23 : Decrypted projections/fingerprints

- At last, the euclideon distance and hamming distance can be calculated to find the matching result and hence verify authorization.

Dataset	Yale's Face database
Accuracy	87.2%
Average Threshold	108.3
Optimzation	76.09%
Loss	12.8%

Table 4 : Proposed solution 2 metrics

- Either of both proposed solution can be used by prefference and availability.
- The fingerprint may get distorted while using in a real life application as projection has fewer attributes in comparison with all the approaches metioned above.
- Hence, the solution 1 is more preffered but it will have highers computational cost.
- While, Second approach is highly optimized, the prediction accuracy and loss rate is making it not the first choice.
- Although, This approach has covered all the disadvantages suggested in the previous studies and first proposed solution.

CONCLUSION

In this paper, the author embarked on a journey through the realm of biometric security, particularly focusing on facial biometrics, and explored the integration of Eigenface with cryptographic methods to enhance identity management and privacy. Our analysis revealed the evolution of biometric authentication from its inception with devices like the iPhone 4s to its integration into various electronic systems, albeit with limited advancements in recent years.

Through an in-depth literature review, author uncovered the foundational work of Turk and Pentland in introducing Eigenfaces and the subsequent advancements by researchers like Nasim Arshad, Kwang-Seok Moon, Jong-Nam Kim, and Adrian Tam. These studies highlighted the potential of Eigenface in enhancing biometric security through techniques like projection matching using Hamming and Euclidean distances.

Building upon these foundations, our proposed solutions integrated Eigenface with Google's MediaPipe for facial landmark analysis. This paper presented two distinct approaches leveraging MediaPipe's capabilities to generate unique fingerprints for face recognition. Our experiments and evaluations demonstrated promising results in terms of accuracy, threshold values, and optimization.

However, This study also acknowledged the limitations and potential drawbacks of these approaches, such as hash clashing and optimal feature extraction. The computational costs associated with our first proposed solution and the slight decrease in accuracy in the second solution are areas for further refinement.

Method	Accuracy	Average Threshold
Solution 1	89.9%	1903.57
Solution 2	87.2%	108.3

Table 5 : Metric Comparison table for proposed solutions

Both solution has overcame disadvantages faced by the previous approaches - Optimization, accuracy and threshold control.

In conclusion, while our proposed solutions showcase advancements in biometric security leveraging Eigenface and facial landmarks, there remains room for improvement and exploration of more optimal and secure methodologies. Future research directions could focus on refining feature extraction techniques, addressing hash clashing issues, and optimizing computational efficiency without compromising accuracy and security.

Overall, this paper contributes to the ongoing discourse on enhancing biometric security in the era of AI and privacy-enhancing cryptography.

ACKNOWLEDGMENT

I would like to express our gratitude to the researchers and institutions whose contributions have significantly enriched our understanding of face recognition methodologies. Specifically, I acknowledge the insightful works by Nasim Arshad, Kwang-Seok Moon, Jong-Nam Kim, Adrian Tam, L. Sirovich, M. Kirby, AT&T Laboratories Cambridge, Matthew A. Turk, Alex P. Pentland, S. Z. Li, A. K. Jain, J. Smith, K. Chang, Y. Wang, C. Li, Z. Zhang, Valentin Bazarevsky, Yury Kartynnik, Andrey Vakunov, Karthik Raveendran, Matthias Grundmann, Chuo-Ling Chang, Ming Guang Yong, Jiuqiang Tang, Gregory Karpiak, Siarhei Kazakou, and Matsvei Zhdanovich.

Their research efforts, spanning a diverse range of methodologies and applications, have inspired us to explore new avenues and develop novel techniques in our pursuit of enhancing face recognition accuracy and efficiency. I acknowledge and appreciate their dedication, expertise, and tireless contributions to the scientific community, which continue to shape the landscape of modern technology and artificial intelligence.

Additionally, I would like to express our appreciation to the academic and research communities for their continuous support and collaboration. The exchange of ideas, feedback, and constructive criticism has been instrumental in shaping our research approach and refining our methodologies. I am grateful for the insightful discussions and the vibrant academic environment that fosters growth and innovation.

REFERENCES

[1] Nasim Arshad, Kwang-Seok Moon, Jong-Nam kim, “A Secure Face Cryptography for Identity Document Based on Distance Measures”, Pukyon National University, Korea, 2013.

[2] Adrian Tam, Face Recognition using Principal Component Analysis, Machine Learning Mastery, 2021.

[3] L. Sirovich; M. Kirby (1987). "Low-dimensional procedure for the characterization of human faces". Journal of the Optical Society of America A. 4 (3): 519–524.

[4] AT&T Laboratories Cambridge, “The Database of Faces”, AT&T, 1994.

[5] Turk, Matthew A; Pentland, Alex P (1991). Face recognition using eigenfaces (PDF). Proc. IEEE Conference on Computer Vision and Pattern Recognition. pp. 586–591.

[6] Li, S. Z., & Jain, A. K. (2005). Handbook of face recognition. Springer Science & Business Media.

[7] Smith, J., & Chang, K. (2008). Comparative analysis of facial recognition methods: Eigenface, Eigeneyes, and Eigenmouth. Pattern Recognition Letters, 29(10), 1551-1556.

[8] Wang, Y., Li, C., & Zhang, Z. (2019). Accelerated Eigenface algorithm using GPU parallelization. IEEE Transactions on Parallel and Distributed Systems, 30(1), 118-127.

[9] Valentin Bazarevsky, Yury Kartynnik, Andrey Vakunov, Karthik Raveendran, Matthias Grundmann, “BlazeFace: Sub-millisecond Neural Face Detection on Mobile GPUs”, CVPR Workshop on Computer Vision for Augmented and Virtual Reality, Long Beach, CA, USA, 2019.

[10] Chuo-Ling Chang, Ming Guang Yong, Jiuqiang Tang, Gregory Karpiak, Siarhei Kazakou, Matsvei Zhdanovich and Matthias Grundman