Ethical and Technical Perspectives of Facial Recognition: CNN and Eigenfaces

Rick Kabuto

School of Computing, Binghamton University

CS 301: Ethical, Social, and Global Issues in Computing

Dr. George Weinschenk

December 2, 2024

Abstract

Technology in facial recognition drives advancements in security, law enforcement, and digital services. Industries depend on advanced algorithms to present enough accuracy in order to possess a strong sense of security. Convolutional Neural Networks (CNN's) excel in recognizing patterns and adapting to challenging conditions, such as low-light enviroments, through multi-layered architectures and massive datasets. However, reliance on heavy data collection poses ethical concerns in privacy and potential misuse. Eigenfaces, a data efficient method based on linear algebra, offers an alternative but presents a struggle with real world conditions. The weaker model remains adequate enough for tasks such as securing public spaces, however lacks the precision required for invasive government surveillance systems. This limitation reduces the potential for misuse in comprising fundamental rights. While CNN's demonstrate better performance, future development in safeguards needs to be implemented in the model in order to show true public trust. The responsibility lies with computer professionals to design systems that align with societal values while continuing to improve technology in facial recognition.

Ethical and Technical Perspectives of Facial Recognition: CNN and Eigenfaces

Facial recognition technology plays an important role in modern digital interactions, powering everything from security systems in banking, to personalized experiences on social media. A strong degree of accuracy with reliable performance requires dependable algorithms to ensure that consumers and organizations use facial technology applications with a sense of security. Eigenfaces and Convolutional Neural Network represent two effective approaches that illustrate the demand for accurate algorithms in facial recognition. These two approaches spark debate over the ethical implications of their functionalities, especially as the need for precision in technology increases. The Convolutional Neural Networks (CNNs) model delivers improved results as compared to Eigenfaces, which produces less accurate results in low light conditions for facial recognition. A comparison of these two algorithms reveals distinct advantages and trade-offs. Convolutional Neural Networks outperform in certain environments due to the pattern recognition of layered structures and learning patterns. The more accurate results stem from large datasets, leading to privacy concerns through data collection. In contrast, the Eigenfaces algorithm, while less accurate, provides an approach that raises less questions about the invasion of privacy.

Alternative Technology

While the approach provided by Eigenfaces, as implemented in Fisherfaces, offers improved performance, both Eigenfaces and Fisherfaces draw from linear algebra and statistical techniques. Meena Taneti, a researcher and faculty member at B.R.R & G.K.R Chambers Degree College, specializes in computer vision. An assistant professor of computer science, Taneti contributed to the field through multiple peer-reviewed journals and earned recognition in the International Conferences for Innovative Applications of Machine Learning Techniques in

Computer Vision. Taneti (2022) describes how Fisherfaces utilizes Linear Discriminant Analysis, which recognizes additional distinguishing facial features in different lighting conditions (Taneti, 2022, P.108). This method provides an additional and improved approach as compared to Eigenfaces which instead utilizes Principal Component Analysis, thereby maximizing the distance between classes while minimizing the variance within that class. Jevtic Dubravka, a researcher at the Innovation Center of the School of Electrical Engineering in Belgrade, focuses on image processing and machine learning. As a recognized senior researcher, Jevtic discusses dimensionality reduction applied to computer visions and biometric systems. The principal analysis approach provides effective outputs by distinguishing between the faces of different individuals while keeping the facial features of the images in a lower dimensional subspace retaining only the significant components of an individual (Jevtic et al. 2012, p.121). This approach also remains highly sensitive to environmental factors like lighting, treating all variations in data with equal importance**.** As a result, Eigenfaces can exhibit inconsistent performance in less controlled settings. The Linear Discriminant Analysis approach solves these separate classes by using Linear Algebra to create a linear combination of features that maximizes the inter-class differences. Fisherfaces emerged as a powerful contender to Eigenfaces' approach and dominated recognition research in the 1990s. To this day, Fisherfaces remains a practical choice in facial recognition, offering an effective option for applications with limited processing power. However, both techniques no longer represent the state-of-the-art technology, as Convolutional Neural Networks (CNNs) provide a more efficient and computational approach. Relying on Linear Discriminant Analysis, Fisherfaces addresses the shortcomings of Eigenfaces as an alternative approach to the resource-dependent, deep learning model required by Convolutional Neural Networks.

Support

Facial recognition technology advances with models such as Convolutional Neural Networks (CNNs) and Eigenfaces, each driving improvements in adaptability to environmental conditions. CNNs demonstrate stronger technical capabilities compared to Eigenfaces while also amplifying societal dilemmas. Beyond technical capabilities, facial recognition requires analysis of societal effects as well, since the reliance of high accuracy stems from extensive data collection. This leads to privacy concerns.

Technical Details

Convolutional Neural Networks (CNNs) excel in facial recognition applications due to their multi-layered architecture, designed for handling data images with high precision. CNNs operate by passing input data through a series of layers. These convolutional layers apply filters to extract spatial features to identify edges, textures, and complex patterns. Mathematical operations are performed on the input arguments, and the algorithm produces a feature map for reference. Pooling layers reduce the dimensions of the feature maps to retain the information while minimizing the complexity. The approach enables the algorithm to detect subtle facial variations in high dimensions, distinguishing key factors between individuals. Large datasets empower the algorithm's ability to generalize in unique conditions such as lighting.

Institute of Electrical and Electronic Engineers (IEEE) researches, who hold positions as senior engineers and have authored papers and magazines in journals such as *IEEE Transactions on Neural Networks and Learning Systems* on image processing and neural networks, focus specifically on the performance of five facial recognition algorithms in low light environments (IEEE, 2017, p.7). The IEEE researchers refer to CNN’s through a specialized term called LLCNN’s, or low light Convolutional Neural Networks because they possess the same functionality as a standard CNN. The study evaluated the algorithm's performance in enhancing degraded images under a gamma light of $\gamma = 3$. Convolutional Neural Networks consistently outperformed the alternative algorithms shown in Table 1, achieving significantly more accurate results in Peak Signal to Noise Ratio (PSNR), which measures the quality of reconstructed images. The algorithm excelled in Structural Similarity Index (SSIM), a metric that evaluates perceptual similarity between images (IEEE, 2017, p. 7). IEEE researchers recognized that this success stems from a specifically designed module within CNN's that enables a system to learn when images present specific changes in dark environments by dynamically adjusting

Table 1

LCCNN's Performance Compared with LLNet

PSNR/SSIM	Test	LLNet	LLCNN
Bird	12.27/0.18	18.43/0.60	29.95/0.87
Girl	9.50/0.51	22.45/0.80	36.29/0.99
House	12.12/0.32	21.10/0.64	29.15/0.85
Pepper	10.45/0.37	21.33/0.78	32.67/0.93
Town	10.17/0.36	22.47/0.81	33.90/0.96

the pictures through the extraction process. This causes the algorithm to identify patterns in low-light images by isolating essential features and suppressing noise, allowing the system to effectively recognize important elements in the image. Building on the foundational baseline performance of CNNs, Figure 1 demonstrates CNN's accuracy in facial recognition by presenting images that maintain the best representations of real lighting and individual features compared to other algorithms (IEEE, 2017, p. 9). Unlike competing methods, the LLCNN's output aligns closely with specific lightning conditions on a person's face, even with the lightning adjustments the researchers posed to the machine. While CNNs present impressive precision in facial recognition, alternative methods like Eigenfaces offer a simpler approach but face challenges specifically in environmental conditions.

Figure 1

Other Contrast Images Outputs Compared with LLCNN

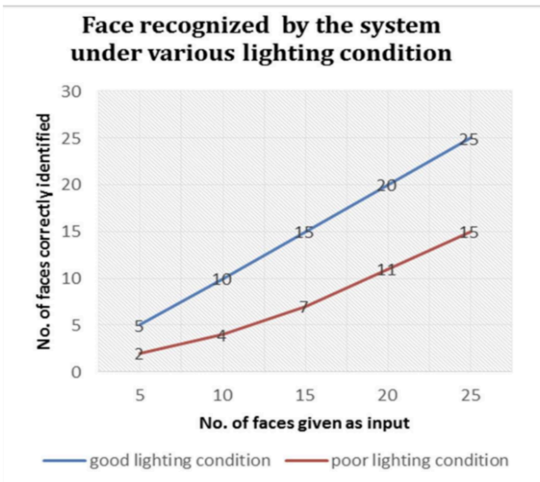
Eigenfaces, on the other hand, reduce dimensionality, condensing facial features into simplified representations through Eigenvectors. Eigenfaces convert each image into a vector by concatenating pixel rows of the image. The algorithm forms a matrix where each row corresponds to a specific image vector. Applying the computed eigenvectors and eigenvalues in the formula shown in (1) represents the most significant features across all images in the training set (Taneti, 110). Principal Component Analysis, a dimensionality reduction technique, identifies

$$\lambda i \text{ of S. } Svi = (TT^2)vi = \lambda ivi, \; i = 1,2, \ldots N. \quad (1)$$

features that show significance and sets the components to an orthogonal matrix. PCA presents a flaw by assuming uniformity in these subspaces by implying that all environmental conditions affect features in the same way. This assumption limits the algorithm's adaptability to variations in factors like lighting and angle, often reducing the accuracy of identifying individuals. A recent study by Taneti (2022) illustrates this limitation by testing an Eigenfaces system's efficiency under different shades of light. Designed to enhance security by recognizing faces from live video feeds, the system uses the Eigenface method to identify known individuals and alerts trusted contacts when unrecognized faces appear. The findings reveal that while the system

Figure 2

Eigenfaces in Certain Lighting Conditions



detects all faces in optimal lighting, the accuracy drops significantly as lightning conditions diminish (Taneti, 2022, p. 114). Figure 2 illustrates the decline in performance under poor lighting conditions (Taneti, 2022, p. 115). The system shows high accuracy in well-lit settings but significantly lowers accuracy in dimmer conditions. In real-world scenarios, this limitation causes the algorithm to misinterpret facial features, potentially compromising security and increasing risk to public safety. Analyzing these methods highlights the advantage of Convolutional Neural Networks in facial recognition tasks, as their adaptive architecture delivers significantly more accurate results compared to Eigenfaces. By dynamically enhancing image contrast and adjusting to real-life conditions, CNN's recognition of layered structures and learning patterns overcomes the limitations of environmental lighting for Eigenfaces. These consistently accurate outcomes indicate a strong preference for using the deep learning model.

Fully assessing the viability of this choice requires consideration of both technical reliability and impact on social values and ethical standards.

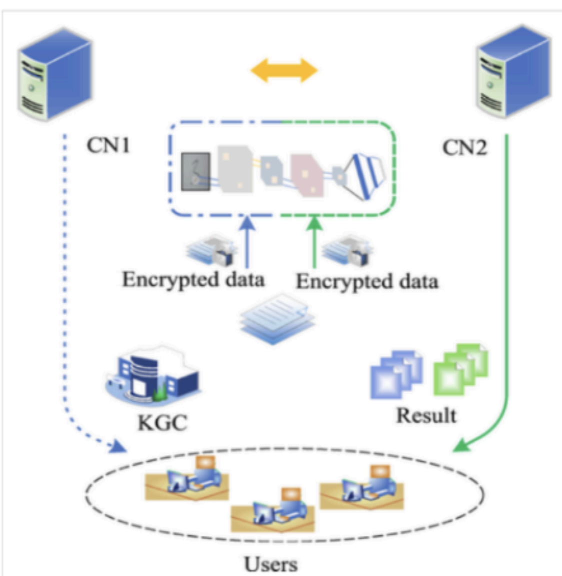
Social Impact

Improvements in facial recognition technology provide societal benefits such as increased security, streamlined identification processes, and a sense of safety to the public. With advancements in accuracy shown in Convolutional Neural Networks, facial recognition poses the ability to perform biometric authentication for banking transactions and to match faces from surveillance footage to criminal databases, aiding law enforcement. A study on population genomics published by the Association for Computing Machinery(ACM) highlights the positive benefits of CNNs. This approach allows for the processing of vast genetic datasets, ten times faster than the original hardware. The head researcher, Federico Corradi, an assistant professor in electrical engineering at Eindhoven University of Technology, leads the Neuromorphic Edge Computing Systems Lab and contributes to the EAISI Foundational program. The researchers analyzed occurrences of evolutionary sweeps and recombination hotspots on genomes and presented CNNs as a clear replacement for their old system (Corradi et al. 2024, p. 60). Improved analysis in population genomics provides quicker identification in human diseases, reducing health care costs and public health. Additonaltiy, CNNs emphasize the ability to estimate conservation efforts in climate strategies which can maintain our ecosystem and natural resources. Convolutional Neural Networks achieve significant accuracy improvements, particularly in low-light conditions through deep learning. Despite the benefits provided by CNNs across respective fields, the reliance on large-scale data collection raises concerns about confidentiality.

The general public often views large-scale data collection as an invasion of privacy. To address these concerns, privacy-preserving approaches such as encrypting data and managing data through a Key Generation Center (KGC) play a role in the algorithm. Furong Li, a researcher for Wuyi University in the school of computing, specializes in data processing through artificial intelligence. Her work developed recognition in cryptographic protocols and earned an award at the International Symposium on Information Security conference. Li explains the KGC distributes public and private keys, ensuring that only authorized decryption and controlled processing of facial data occur, enabling the model to deliver accurate results while maintaining privacy safeguards (Li, et al. 2021, p. 574). For example, Figure 3 displays a visual representation of the sculpture system(Li, et al. 2021, p. 574). Both networks contain encrypted model parameters, including kernel weights and biases,

Figure 3

Convolutional Neural Networks Model Overview



accessible only through notifications from the main service provider. This process enables both privacy and the controlled processing of information through encrypted channels. These privacy measures require recognition systems to incorporate built-in safeguards for personal data. Although CNN Developers aim to protect individual privacy through encrypted data handling, broader implications require careful consideration**.**

Holding recognition from organizations such as the Electronic Frontier Foundation, Kade Crockford's TED talk provides an important argument on how governments could use this technology. Crockford, a Director of the Technology for Liberty Program at American Civil Liberties Union (ACLU) of Massachusetts, advocates for privacy rights. Her work includes co-authoring reports on surveillance policy and testifying legislative bodies. Crokford warns the public that as facial recognition advances, governments worldwide could adopt these systems to track individuals solely through their facial features. Unlike mobile devices that individuals can leave behind, faces remain inescapable in public spaces. Crockford emphasizes that a lack of oversight surrounding facial recognition will eventually lead to facial surveillance (Crokford, 2020, 5:15). Without regulatory oversight, governments could exploit facial recognition systems to monitor the public, similar to China's use of technology to control minority groups. The lack of transparency enables the government to profile individuals, restrict freedoms, and misuse the data. While CNNs deliver enhanced performance and reliability in specific conditions, the social impact of widespread surveillance grows into consideration. Fundamentally, CNNs demonstrate greater strength as the preferred algorithm but introduce a social risk; advanced growth equips governments with a tool powerful enough to enable round-the-clock tracking. In this scenario, governments could control the surveillance technology and operate the system entirely in secret. This concern presents the need to explore alternative approaches, such as Eigenfaces which allow a simpler framework.

In contrast, Eigenfaces condenses facial features into mathematical concepts which minimizes the reliance on large amounts of data coming from the public. Eigenfaces offer less accurate results in certain conditions but provide a reliable approach for general use. The Principal Component Analysis approach strikes a careful balance, offering sufficient accuracy to support public safety measures without enabling the high precision needed for required government surveillance. Facial recognition technology, particularly Convolutional Neural Networks, enhances security by identifying threats with greater accuracy; however the implementation must comply with legal standards protecting privacy, such as outlined in frameworks in the U.S. Fourth Amendment. Without transparent and regulated deployment, facial recognition technology risks compromising fundamental rights and challenging the freedoms intended for protection, ultimately undermining social benefits.

Conclusion

Facial recognition technology continues to shape modern computing, with a demand for balance between ethical responsibility and technology. Convolutional Neural Networks present stronger precision with the ability to adapt under challenging conditions in specific shades of light. Though their reliance on extensive datasets raises ethical concerns regarding privacy and data security. In contrast, Eigenfaces demonstrates a mathematical approach with a simpler technique, but possesses limitations in environmental factors affecting real world applicability. The CNN model delivers improved results when compared to Eigenfaces, which produces less accurate results in low light conditions for facial recognition. Analysis emphasizes CNN’s ability to outperform Eigenfaces in accuracy, though concerns over mass surveillance continue to increase. Encrypted data handling, for example, provides a step towards a professional model that protects societal freedoms. Computer professionals hold the responsibility to design safeguards prioritizing privacy and compliance with ethical expectations. The priorities guiding programmer’s choices will not only shape the trajectory of future intelligent systems, but also will determine whether technology becomes a tool for societal empowerment.

References

Corradi, F., Shen, Z., Zhao, H., & Alachiotis, N. (2024). Accelerated spiking convolutional neural networks for scalable population genomics. In L. Josipović, P. Zhou, S. Shanker, J. MP. Cardoso, J. Anderson, & S. Yuichiro (Eds.), HEART '24: *Proceedings of the 14th International Symposium on Highly Efficient Accelerators and Reconfigurable Technologies* (pp. 53-62). Association for Computing Machinery, Inc. https://doi.org/10.1145/3665283.3665285

Jevtic, D. & Slavkovic, M. (2012). Face recognition using eigenface approach. *Serbian Journal of Electrical Engineering*, *9*(1), 121–130. https://doi.org/10.2298/SJEE1201121S

Li, F., Chen, Y., Duan, P., Zhang, B., Hong, Z., Hu, Y., & Wang, B. (2022). Privacy‐preserving convolutional neural network prediction with low latency and lightweight users. *International Journal of Intelligent Systems*, *37*(1), 568–595. https://doi.org/10.1002/int.22640

Taneti, M. (2022). Secure face recognition system based on eigenface and fisherface techniques. *International Journal of Multidisciplinary Educational Research*, *11*. https://ijmer.s3.amazonaws.com/pdf/volume11/volume11-issue1(7)/21.pdf

Tao, L., Zhu, C., Xiang, G., Li, Y., Jia, H., & Xie, X. (2017, December). *LLCNN: A convolutional neural network for low-light image enhancement.* In 2017 IEEE Visual Communications and Image Processing (VCIP) (pp. 1-4). IEEE. https://ieeexplore.ieee.org/abstract/document/8305143

TedxCambridgeSalon. (2021, September 8). Kade Crockford: Why face surveillance must be banned [Video]. TEDxCambridgeSalon. YouTube https://www.youtube.com/watch?v=Hg4qH7xK_2s

DraftBack Link

chrome-extension://nnajoiemfpldioamchanognpjmocgkbg/playback.html?docId=1191L-tFq2nuA
PZp8nueVppDFJ607EJ8ljVx_e9UiIyY