STOR 390 Final

Ryan Dee

2024-12-08

Introduction

Facial recognition software has been around almost 60 years. The first rudimentary tests were done in the 1960s on whether or not "programming computers" could recognize matches between faces by identifying a person's hairline, eyes, and nose. The first tests were incredibly unsuccessful. Computers found it easier to beat grand masters in chess than to match faces to each other. Confounding factors such as lighting, facial expressions, and angled photos impeded the computer from correctly identifying matches.

Today systems are much better. Modern facial recognition systems have evolved to use two algorithms to identify face matches. The initial algorithm maps a person's face and normalizes the data into code, then the second algorithm identifies faces that may be similar. It is important to understand this is different from face detection. Facial recognition is used everywhere today, from our iPhone's to our mobile payments and boarding passes for planes. There are many different ways that facial recognition algorithms work, today we will be looking at research by Jonathan Phillips, and explore his results from his Principle Component Analysis and Support Vector Machine classification algorithms. We will also ask some moral questions such as who should have access to this technology and what is developers role in making sure those people who shouldn't have access don't.

Methods

This paper contains reconstruction of PCA methods by Jonathon Phillips, his work "Support Vector Machines Applied to Facial Recognition" explored the relationship between the traditional Principle Component Analysis, and Support Vector Machine algorithms. Before we trace his analysis it is important to understand his methods when comparing the two. First we must understand the initial industry standard Principle Component Analysis. First, an image is used to probe an existing dataset. The image supplied is usually a person of interest and they are looking to be matched against a dataset of standardized faces. However, going from an image to code that a computer can interpret is difficult. Computers represent pictures using a matrix of pixels, each pixel is color coded with a particular set of numbers for each color. If we set each picture to the same greyscale and same size we can measure the differences between the faces using the colors of the pixels. For instance, if we have a 32 by 32 pixel image, the image describes a point in 1024 dimension space. We can then go from a 1024 dimension space into a single vector of all the pixels in the image. Representing a face like this allows for us to test the vector compared to other vectors in what we can call featured based recognition. This is great, we can simply use any distance metric like euclidean distance to recognize images that are similar. However, in this case many images become clustered around a certain point in high dimensional space, also known as face space, because faces are typically centered, they tend to occupy similar space in high dimensional space. If we take all the images we have, center them, and give them similar color schemes, a lot of the differences between pictures we as humans may use to tell people apart will now be useless. This is the same with high dimensional space, the images all look similar and thus inhabit similar areas, and doing a simple euclidean distance will not be accurate.

Instead we can take all of the vectors A and put them into a matrix before performing a principal component analysis. The resulting Principals can be subtracted from the mean principal and we can then find the mean principal: C = A-a, where A is the mean vector of the matrix A. From that we can find a covariance matrix from which we find the eigenvectors and eigenvalues. The importance of the different principal component vectors can be inferred from the corresponding eigenvalues. The greater the eigenvalue, the more useful eigenvector. If we take the first K eigenvectors, we can call them the eigenface picture. This is then projected into 2d space and produces the unsettling output below. However, these eigenface values can use a distance metric, like euclidean distance, to find the closest match, and ideally recognize faces.

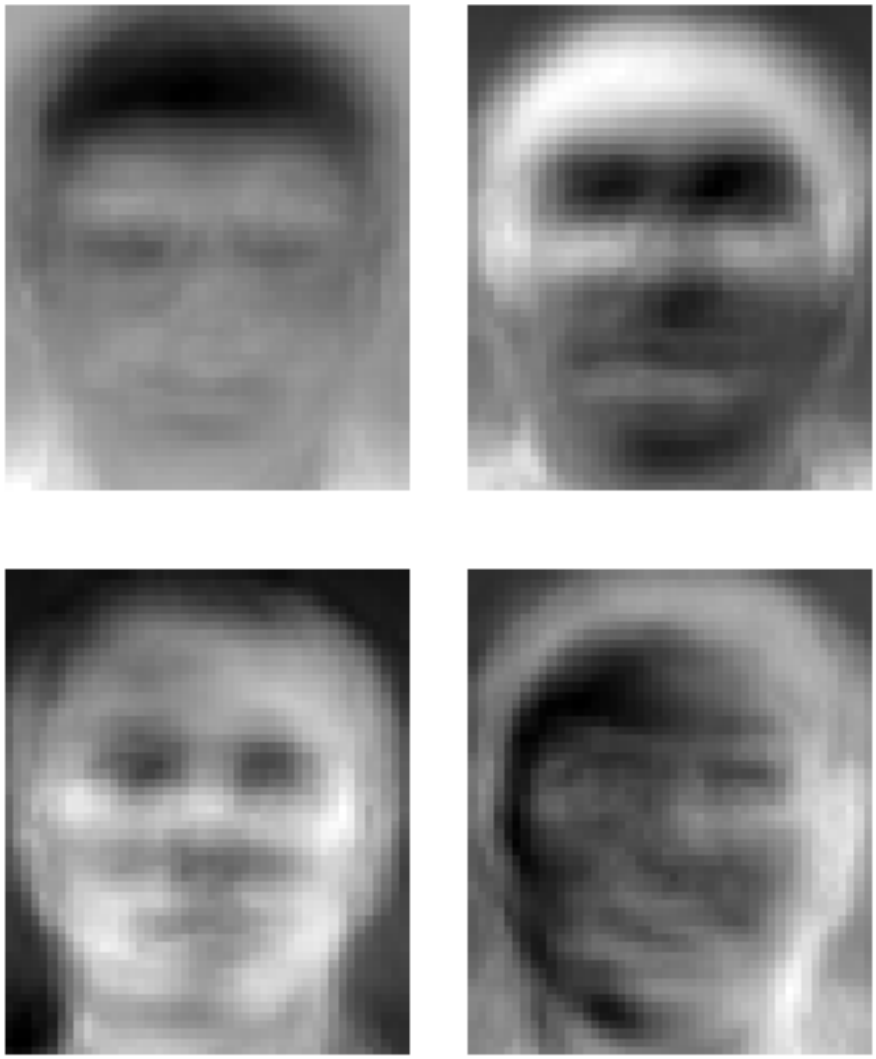

Figure 1: Images of Eigenfaces used in Phillips Study

Phillips compares this to an SVM model, which tries to find a line of dilineation that most cleanly distinguishes between classes. The SVM classifier used a radial kernel and was compared to a PCA-based nearest neighbor algorithm, which is the industry standard. SVM is very common in facial detection, does an image have a face or not, but this was some of the first research into facial recognition.

Analysis and Replication of Results

Dr. Phillips used a database of faces called the Facial Recognition Technology (FERET) database. This database was commissioned in the 1990s by the National Institute of Research and Technology for the sole purpose of exploring facial recognition technology research. Unfortunately the database is not open source and one must get approved to gain access to the over 1000 images. My request for approval was denied. However in this part of the paper I will walk you through the process and results taken by Dr. Phillips. First Phillips selected 400 images that he thought were the most difficult for the system to process. After that Phillips randomly selected 100 individuals and 2 images for each individual to be selected for a 50-50 training testing split. Both models were subject to the same set of images. This 50-50 training testing split is rare, and there wasn't an explanation for why it was selected as opposed to an 80-20 split or 70-30 split that is more common. The first thing Phillips did was preprocess each image by hand, this involved cropping them to be the correct size, putting them through a greyscale filter, and making sure they had the same pixel ratio.

After this Phillips uses a PCA based algorithm on the set of 200 individuals, then uses a Euclidean distance formula to find the closest eigenface when compared to the average. The PCA method is the industry standard for such models.

The SVM verification was different, once the images were cleaned and converted to greyscale their pixels were converted to a vector which, along with 100 other images were used to create 100 decision boundaries in a training set called the "gallery". The SVM decision boundaries are then tested by inserting a test image, also known as a probe. If the image falls within a certain decision boundary we would say that is a match and that match is then checked to see if it was correct. This is repeated for the 100 images in the test set. If the probe image did not fall within a decision boundary the algorithm would say that it did not detect a face.

The researchers set out to test which had a correct prediction rate, and the effect the amount of eigenfeatures used had on error rate. The researchers found that SVM had an error rate half that of the PCA error rate, 23% compared to 46%. The researchers claim this means the SVM is making a more efficient use of the "Face Space" than the baseline PCA algorithm. This makes sense, PCA is not itself a classifier function and when paired with something like an euclidean nearest neighbor classifier, it relies on the idea that linear differences in the reduced face space is enough to identify faces. Phillips says his results suggest this is not the case and the Radial kernel used in this research helps handle this non-linearity.

```
##                            PCA SVM
## True Classification Rate 55% 77%
```

In addition Dr. Phillips examined the relationship between the amount of eigenfeatures and the probability of identification. In these findings using both PCA and SVM techniques there was a positive relationship between the amount of eigenfeatures and probability. However, the relationship was nonlinear and began to taper off after around 20 eigenfeatures, this implies the features after 20 provide little to no help and may in many instances hinder the identification process by overfitting the model.

Moral Consideration

In terms of moral dilemmas, this raises interesting questions from both the consequentialist and deontological points of view. This mostly comes from the perspective of selling facial recognition software, and its utilization in areas of the world with people that the data was not trained on. In the same breath, there are consequentialist questions about who gets access to the software. Most of the software that is developed is then commercialized, mostly for governments and law enforcement agencies. This begs the question of whether facial recognition software should be sold to governments that people disagree with.

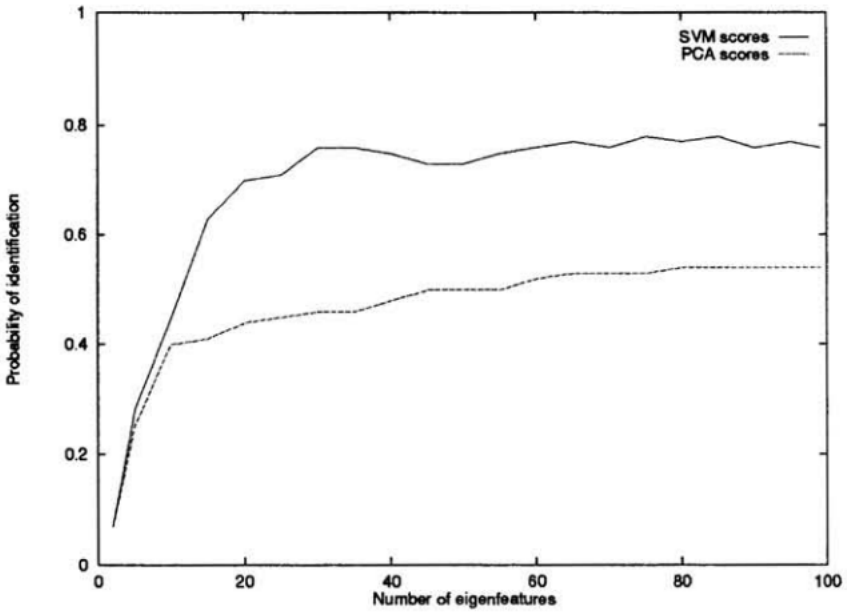

Figure 2: Relationship between number of eigenfeatures, and Probability of identificiation

Imagine a situation where facial recognition software is used to find people who were present at a democratic protest in an authoritarian country. Or a situation where the software is sold to a police department that is known to discriminate based on protected classes. For instance, Vladimir Putin in Russia has expressed interest in using facial recognition in every city in Russia after its successful implementation in Moscow. It is known that cameras with facial recognition software developed at US corporations was used in the arrest of over 200 anti-war protesters in Moscow. This is something most moral people would condemn. From a consequentialist point of view, there is a question of "If there is a certainty that the government or police agency will get the software anyway, whether or not I sell it to them is irrelevant." At the same time, a deontologist would say that you cannot allow it to be a universal maxim to sell recognition software to governments that discriminate.

In another breath, it is important to know that there are people who live in these authoritarian regimes and in the districts of police departments that need protection. It could be that this system is used to find criminals, and prevent them from committing crimes again. A consequentialist will have to justify whether they see the consequences of discrimination are worth the upside of protecting certain people. Finally, it is worth mentioning this is all determinant of the training data used for the model. If the gallery used is not representative of the probe image the software is more likely to misidentify the image. This is another piece to consider when selling to a foreign government. Finally, it is worth considering that these algorithms and functions have parameters that can be altered to give a greater probability of false positive or false negative rate, so if you just sell the algorithm, are you at all morally at fault?

I would take the moral consideration that selling this to people you disagree with is definitely immoral. In particular I disagree with the notion that because others are doing something wrong you are now morally justified in doing it. While this may make sense from a strict consequentalist point of view because you no longer are the reason the world is worse off; I find the deontologist point of view much more persuading. From a deontologist point of view one cannot wish this to be a universal law. Similar to the saying "if all your friends are jumping off a bridge would you", just because others find something morally justifiable does not mean that you should find it morally justifiable. In addition, there is no guarantee that another

corporation is selling the algorithm in the first place, and by selling it you have made the worse consequences a certainty, as opposed to a possibility. Even though the parameters of the PCA and SVM functions can be set to different probabilities of false positive and false negative, trusting in governments that already have a history of unfair justice systems to use these parameters is unreasonable. I also don't think that the excuse that parameters that affect probabilities of false negatives or positives absolves people from any wrongdoing. If someone sold a gun to a known criminal nobody would find that morally justifiable, even if the gun could be used for hunting. For this reason I don't think the upside of catching more killers or thieves is any greater than downside of imprisoning people for protests.

Conclusion

Phillips's research laid much of the foundation that today's research is based on. However, that is not to say his research is without criticism. Selecting which images you believe will be most difficult for a model to learn is odd and not something I have ever seen before. This was widely criticized at the time and prompts one to ask what makes an image difficult for a computer to recognize. All the images in the FERET database have similar lighting and depth, in addition they are all cleaned and put into greyscale before putting them through the algorithm. No explanation was given in the paper but it does raise questions of how a person can believe an image will be more difficult to process and begs an important question about the large scale implementation of such algorithms. If images in the FERET database, and the private databases we see today are not random, and our training data is skewed, we run the risk of giving out false positives or negatives. It is known that discrepancies between testing and training data will reduce accuracy in an SVM model and it raises questions about western, specifically US, corporations using training data that is different from the country the software is being used in. Overall while the data provided interesting insights into the potential use of Support Vector Machines in facial recognition research, I would say the manual selection of images from the FERET database made it so that these findings are limited in their applicability, and further research needs to be done.

In terms of the moral consideration, while facial recognition software is incredibly convenient and useful in areas like your iPhone, selling it to foreign authoritarian states is morally wrong. This is for four main reasons, one cannot wish it to be a universal law to help authoritarian regimes. The second is that since there is a non-zero probability that nobody else sells the algorithm to the authoritarian regime, since you are the one who sells it to the regime you have made the negative consequences occur, when in reality there was no guarantee the authoritarian would get the algorithm at all. Also, because it is unlikely you are selling the algorithm to a country that has a similar population to the United States, or wherever the algorithm was developed, you are willfully selling an essentially broken product because the training data is based on groups of people different than the testing data, we know Support Vector Machine algorithms will be less accurate. Finally, even if you are helping protect people from typical crime everyone agrees is morally wrong, theft murder, because you do not know what else the country will use it for you cannot say without a doubt selling the algorithm is morally justifiable. For these four reasons it is the wrong thing to do.

Future Work & Wrap Up

Phillips mentioned in their write-up that this method is not only applicable to faces. He claimed one could also use these methods for finger-prints. Interestingly this same approach was used in a 2016 research article published in the journal for the Institute of Electrical and Electronics Engineers found that when applied to fingerprints Support Vector Machines has a correct fingerprint classification rate of 92.5 percent. In terms of the moral dilemma, there has been lots of research done on the discriminatory effects that facial recognition software can have. In a report published by the United States Comission on Civil Rights, Rochelle Garza, Chair of the U.S. Commission on Civil Rights, stated that, "Unregulated use of facial recognition technology poses significant risks to civil rights, especially for marginalized groups who have historically borne the brunt of discriminatory practices." In the future I think research on how facial recognition stacks up against

witness testimony would be interesting. After all these are classification algorithms, and they are meant to discriminate somehow, but how do they compare to regulare eyewitness testimony? Consider an instance where someone robs a store, do we think the facial recognition would be more accurate than an eyewitness. On the one hand computers don't get tired but they also can codify the same biases we have in our brain. I would like to see how accurate our eyewitnesses are in identifying suspects. Recent studies have cast doubt on the idea that people should take eyewitness testimony as gospel, and while I have said facial recognition technology has its limitations, I am curious which is more reliable.

References

Masri, Lena. "How Facial Recognition Is Helping Putin Curb Dissent." Reuters, 28 Mar. 2023, www.reuters.com/investigates/special-report/ukraine-crisis-russia-detentions/.

Phillips, Jonathan P. Support Vector Machines Applied to Face Recognition , National Institute of Standards and Technology, 1998, proceedings.neurips.cc/paper_files/paper/1998/file/a2cc63e065705fe938a4dda49092966f-Paper.pdf.

Pohle, Allison. "The Fastest Airport Security Line You Don't Know About." Wall Street Journal, 14 Nov. 2024, www.wsj.com/lifestyle/travel/tsa-facial-recognition-airportsecurity-684e8448.

"U.S. Commission on Civil Rights Releases Report: The Civil Rights Implications of the Federal Use of Facial Recognition Technology." U.S. Commission on Civil Rights, 19 Sept. 2024, www.usccr.gov/news/2024/us-commission-civil-rights-releases-report-civil-rights-implications-federal-use-facial.