International Journal of Scientific Research and Engineering Development-– Volume 5 Issue 5, Sep- Oct 2022
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

How Effective is Face Recognition as a Security Measure

Manisha Singh
Keraleeya Samajam's Model College, Dombivli East, Mumbai, Maharashtra, India
arya10112001@gmail.com

Abstract:

One of the security industries' fastest-growing technologies is face recognition. A rise in fraudulent activities has been caused by an increase in e-platforms and a lack of security. To deliver services to genuine and authorized users, the majority of systems, including e-business transactions, need a trustworthy recognition system. The answer to resolving security challenges in daily life is biometric recognition using facial features. Face recognition technology is used in our cell phones as well as in e-commerce, home security, and criminal identification.

This paper proposes the implementation of face recognition for security measures. Experimental results are provided to illustrate the effectiveness of the face recognition system.

Keywords- **Security, Smart Phones, E-platforms, Face Recognition**

I. INTRODUCTION

A subcategory of biometric security is facial recognition. Voice, fingerprint, and eye retina or iris recognition are examples of further biometric software types. Although there is growing interest in using the technology in other areas, security and law enforcement still account for the majority of its uses.

Face ID, which unlocks iPhones, has made face recognition technology widely known (however, this is only one application of face recognition). Typically, face recognition does not require a large collection of images to identify a person; rather, it merely recognizes one person as the device's owner and identifies them as such, denying others access to the device.

I. Literature Review

FacialRecognition are extensively studied within the past few years. With the pros and cons, people have been using this.Facial biometrics system has been used as a measure of security in the topmost institutions and workplaces to ensure that there is no scope for vandalism. This type of software leaves absolutely no room for human error and is a major helping hand. Just by a set of algorithms, the software does geometric and photometric recognition within seconds.
This facial biometrics system has emerged as the master of all recognition software due to its easy applicability and low-cost technology. Its non-contact nature is the best thing about it in the sense that a person through facial recognition, even in a crowded place can be recognized, given that his ../his images are saved in the database. Facial

recognition makes access to information more limited and restricted to those who own it. Facial recognition has made verification relatively easier, with nothing much to equip and a lot of information to access within minutes.

Beyond unlocking phones, facial recognition works by matching the faces of people walking past special cameras, to images of people on a watch list. The watch lists can contain pictures of anyone, including people who are not suspected of any wrongdoing, and the images can come from anywhere — even from our social media accounts. Facial technology systems can vary, but in general, they tend to operate as follows:

II. Algorithm of FaceRecognition

Step1: Identifying faces

In a crowd or by itself, the camera recognizes and pinpoints the image of a face. The subject in the picture may be seen either staring directly ahead or in profile.

Step 2: Assessing the face

The face is then photographed and examined. Your face's geometry is read by the software. The separation of your eyes, the depth of your eye sockets, the space between your forehead and chin, the form of your cheekbones, and the shape of your lips, ears, and chin are all important aspects. It's a goal to recognize the facial landmarks that are key to distinguishing your face.

Step 3: transforming the image into data Based on the subject's facial traits, the face capture procedure converts analog information (a face) into a collection of digital information (data). The examination of your face is basically reduced to a mathematical formula. The faceprint is a numerical code. Each person has a distinct faceprint, similar to how thumbprints are different from each other.

Step 4: Finding a match

Any image that is tagged with a name on Facebook is added to Facebook's database, which is also capable of facial recognition. Your faceprint's compatibility with a picture in a facial recognition database is determined.

The most natural biometric measurement is regarded to be facial recognition. This makes intuitive sense given that we usually recognize ourselves and other people by looking at their faces rather than their thumbprints or irises. According to estimates, facial recognition technology regularly interacts with more than half of the world's population.

IV. Methodologies & Approaches

A. Hybrid Research Model

As shown above, a specific model might include analytical and descriptive components, but it could also emphasize one or the other. It is possible to examine the logical connections in a descriptive model and draw conclusions about the system. However, a quantitative chemical examination of system parameters yields completely different conclusions than a logical analysis.

In order to get information regarding people's awareness, we first performed a survey of them using an online form builder and data collection service. After that, we arranged the existing code and ran experiments on it in accordance with past studies.

B. Research Approach

Firstly, we created a survey form using collect.chat an online form designing and data collection service which allows users to collect data from the research subjects and then the collected data can be exported into the .csv format.

V. Public Survey & Experiment

A. Public Survey

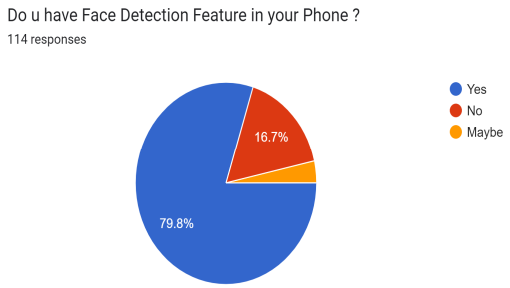
After creating our data collection utility or the survey bot we sent it to various people and collected data on How effective is face recognition as a security measure.

B. Questionnaire

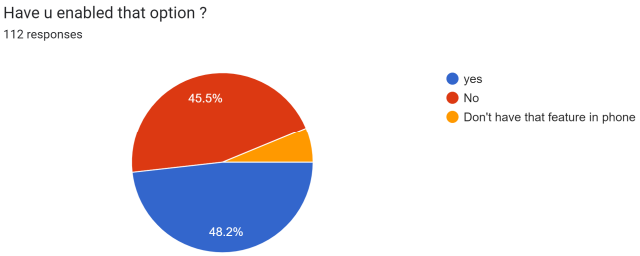
- Do u have Face Detection Feature on your Phone?
- Have u enabled that option?
- Does the use of facial recognitionincrease the risk of false authorization?
- Have you ever faced security problems because of face recognition?
- Are there Risks in using facial recognition for Banking Or Travelling purposes?
- Do facial recognition used by private companies or social platforms affect our privacy?
- Facial recognition is accurate enough for law enforcement use.

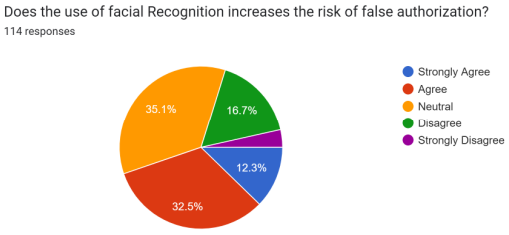
C. Results

When People were asked if they have face recognition features in their phones. Most people had that feature.The Below Graph will show you how many people are aware about this technology.

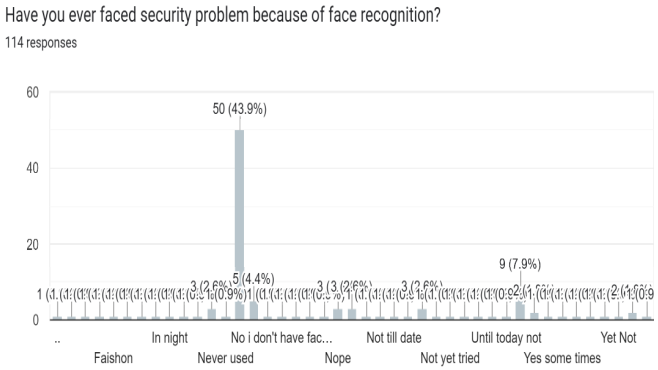


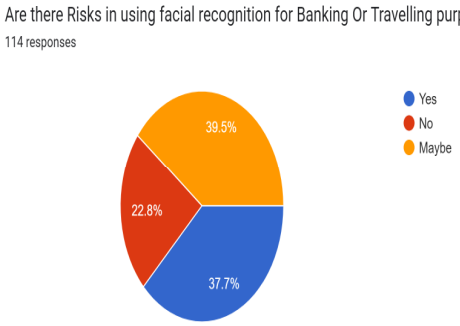
When people were asked that have they enabled that option 48% of people had enabled that option and 45%of people have not enabled it.



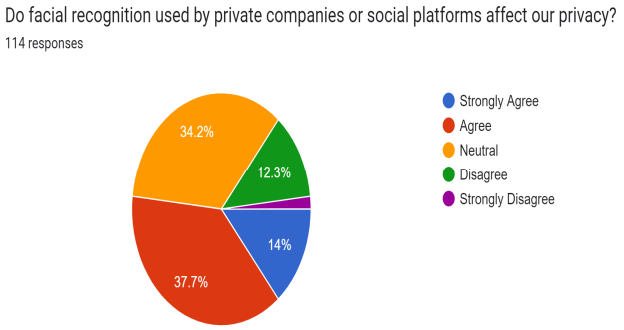


Face recognition can be used to grant false authorization. According to the New York Police Department, for instance, "No one has ever been arrested based purely on a positive facial recognition—it is a lead, not probable cause" in its investigations. The FBI "uses the technology to develop investigation leads, but nothing more," according to the Department of Justice.

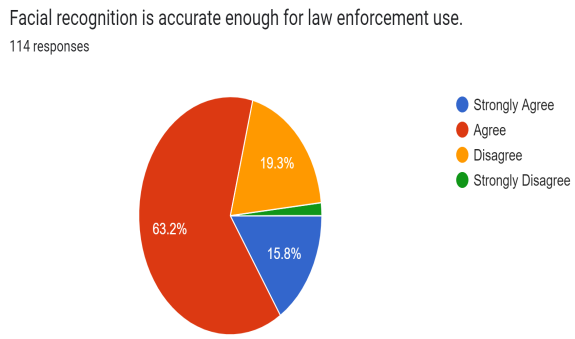




Face recognition can be used to grant false authorization. According to the New York Police Department, for instance, "No one has ever been arrested based purely on a positive facial recognition—it is a lead, not probable cause" in its investigations. The FBI "uses the technology to develop investigation leads, but nothing more," according to the Department of justice.



Businesses can use facial recognition technology's remote monitoring capabilities to gather a wealth of information about people's activities and actions without the subjects' knowledge and then share or sell that information. For instance, retail cameras may monitor what products a consumer browses and buys, sending personalized adverts to the unsure. Casinos currently make considerable use of face recognition technology to identify and categorize patrons according to risk and preferences, enabling them to bar patrons who are known to be problem gamblers or troublemakers from access while providing preferred patrons with exclusive benefits.



The answer to this issue depends on the intended usage and whether or not there are established

guidelines for that specific application of face recognition.

Over the past few years, facial recognition technology has advanced significantly. Facial recognition technology is very accurate under ideal circumstances. The most accurate face detection algorithm has a 0.1 percent mistake rate as of December 2020. The lighting and location of the photographs must be consistent, and the facial features of the subjects must be clearly visible and unobscured, in order to achieve this level of accuracy.

VI. Findings

- Technology can be really very useful to solve some real-world problems.
- Very Fewer People are aware of this technology
- People are Willing to Use This Technology.
- People are getting familiar with the modern concepts of face recognition.
- Technology is still an experimental technique and many people are working on it worldwide to make it better.

How facial recognition is used:

- A number of smartphones, notably the newest iPhones, employ face recognition tounlock the device.The technology provides a strong method to safeguard private information and makes sure that confidential information is inaccessible even if the phone is stolen. According to Apple, there is a one in one million chance that a random face will unlock your phone. To simulate and assess the performance of the face recognition system, the Python OpenCV package was employed.

- Law enforcement
- Airport & Border Control
- Finding Missing Person
- Reducing retail Crime
- Improving retail experiences
- Banking
- Marketing & Advertising
- Healthcare
- Recognizing drivers

VII. Conclusions

- People are working on thistechnology worldwide to make it more precise and useful.
- Very few people use this feature fortheir security.
- As the use of facial recognition becomes more widespread, thescopefor hackers to steal your facial data to commit fraud — increases.
- Facial recognition data is not free from error, which could lead to people being implicated for crimes they have not committed. For example, a slight change in camera angle or a change in appearance, such as a new hairstyle, could lead to an error.
- In 2018, Newsweek reported that Amazon'sfacial recognition technology had

falsely identified 28 members of the US Congress as people arrested for crimes.

References

I. https://www.kaspersky.com/resource-center/threats/hackers-and-your-online-privacy
II. https://ieeexplore.ieee.org/abstract/document/9873037
III. https://ethos.bl.uk/OrderDetails.do?uin=uk.bl.ethos.722632
IV. https://www.csis.org/analysis/questions-about-facial-recognition

