

# Information Retrieval on Enhanced Multiple Image Capture using Google Reverse Image Search Engine

**Dr. Manjunatha B N<sup>1</sup>, Dr. Manoj Kumar D P<sup>2</sup>, Dr. Ananda Babu J<sup>3</sup>, Lekhana S<sup>4</sup>,  
Manjula K<sup>4</sup>, Monika A<sup>4</sup>**

Associate Professor, Depart. of CSE, R. L. Jalappa Institute of Technology, Doddaballapur, India<sup>1</sup>

Associate Professor, Department of CSE, Kalpataru Institute of Technology, Tiptur, India<sup>2</sup>

Associate Professor, Department of Information Science & Engg, Malnad College of Engineering, Hassan, India<sup>3</sup>

UG Students, Department of CSE, R. L. Jalappa Institute of Technology, Doddaballapur, India<sup>4</sup>

manju.master@gmail.com, manojkumardp@gmail.com, abj@mcehassan.ac.in

**Abstract:** *The quick reception of facial recognition (FR) innovation in public and private self-employed has raised worries about common freedoms and security. Accordingly, a wide set-up of supposed "hostile to facial recognition" (AFR) apparatuses has been created to assist clients with keeping away from undesirable facial recognition. The arrangement of AFR apparatuses proposed over the most recent couple of years is wide-going and quickly advancing, requiring a stage for new AFR frameworks and much more difficulties. research means to fill the gap, gives the principal complete examination of the AFR research scene. Involving the functional phases of Facial Recognition frameworks as a beginning stage, make a precise structure for examining the advantages and utilities of various AFR approaches. We then, at that point, consider both specialized and public difficulties confronting AFR apparatuses and propose new facial recognition techniques for future exploration in image processing and restoration*

**Keywords:** facial recognition

## I. INTRODUCTION

In late years, facial identification frameworks have sped up their development in scale and turning into an inexorably pervasive piece of our regular routines. Most of residents on the planet's most crowded nations are signed up for at least one facial recognition frameworks. In the US Nations, almost 200 million Americans are signed up for the FBI facial recognition data set, which use admittance to driver permit photographs from most states [1]. In China, a notable observation framework utilizes facial recognition to screen non military personnel conduct and authorize the social FICO rating framework [2], [3].

Past public affairs use cases, facial identification frameworks are presently consistently utilized for validating explorers at air terminals and workers entering private workplaces. With moderate assets, an end-user or organization can now remove preparing information from web-based entrepreneurs to assemble facial identification models fit for perceiving enormous gatherings of clients. In US Nations, columnist Kashmir Hill showed the potential for facial identification abuse when benefit organization that scratched more than 3 billion pictures from "public sources" to construct a facial recognition framework that perceived countless private residents [5], without their insight or assent. Clear view and organizations like it could empower observation and following by anybody willing to pay 1. Not with standing pictures shared on the web, different reports have definite how photographs taken in surprising spots - air terminals, city roads, government structures, schools, colleges, private companies workplaces - can wind up in facial identification frameworks without subjects' information or assent.

In their place, a cabin industry of against facial recognition (AFR) instruments has arisen. These AFR devices are intended to target various pieces of facial recognition frameworks, from information assortment and model preparation to induction, with the brought together objective of forestalling effective acknowledgment by undesirable or unapproved

models. There is a need to more readily get their shared traits, to feature execution tradeoffs, and to distinguish neglected regions for future turn of events. More specifically, we introduce following earmarkings:

- **Hierarchy of targets in facial identification:** AFR frameworks focus on a wide scope of parts in the facial identification process. Utilizing a summed up adaptation of the facial identification information pipeline, we give the primary structure to reason comprehensively about existing and future work here.
- **Grouping and Examining of AFR systems:** We take the current assortment of work on AFR frameworks, sort and break down them utilizing our proposed system.
- **Planning design based on properties:** We distinguish a center arrangement of key attributes that future AFR frameworks could advance for the plan, and give a plan guide by examining and assuming such properties by AFR frameworks that focus oneach stage in our plan structure
- **Challenges:** We utilize our structure to distinguish huge difficulties confronting current AFR frameworks, as well as headings for expected arrangements

## II. FACIAL RECOGNITION

Facial Recognition workflow and breaking of Face Recognition into multiple stages are discussed below:

### 2.1 Run Time Facial Recognition Workflow

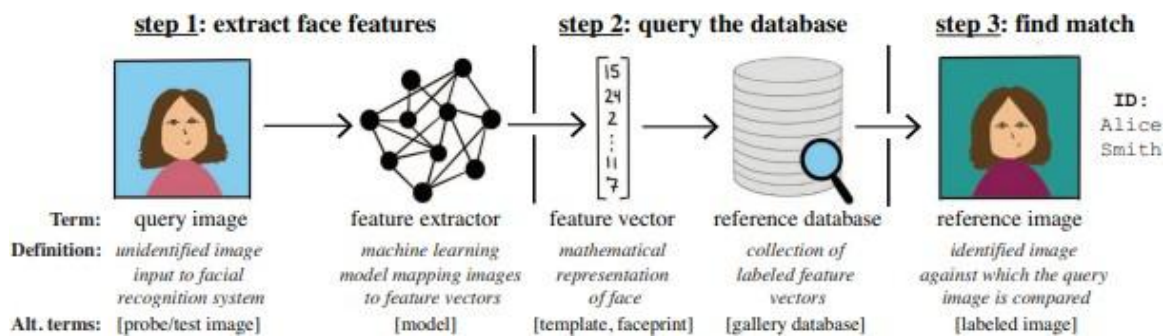


Fig. 1. Facial Recognition System identifying human face in an input image

Figure 1 describes up the run-time work process of Face Recognition frameworks distinguish a face from an info picture. Initial, an inquiry picture, for example a face picture to be recognized, is taken care of through an element, a Dense NeuralNetwork that changes over the picture into an element vector. Then, this include element vector is utilized to question a data set, an assortment of face pictures of different personalities. Search is finished by contrasting the info include element vector with the reference database image to highlight vectors put away in the data set to track down the nearest match. At last, assuming the question search observes a reference include vector in the information base adequately like the information, the FR framework pronounces that a face match has been found and results the relating character and the related reference picture.

### 2.2 Splitting Facial Recognition Stages:

We currently inspect the Facial identification functional pipeline and breaking it into abunch of functional stages that will outline our conversation of Facial Recognition and Anti Facial Recognition devices. These functional stages contains subtasks in Facial Recognition, incorporate the five basic places of direct cooperation among clients and Facial Recognition frameworks. Figure 2 describes the splitting up of facial recognition into five stages as given below

#### A. Image Assortment

Face recognition pictures principally come from two sources: Internet sources or actually snapping a picture of an individual [1], [8].

#### B. Image preprocessing

Crude pictures are regularly inadequately organized (e.g., face cropping, observers in foundation). To make downstream errands more straightforward, the Facial Recognition framework frequently preprocess pictures by applying face

recognition to eliminate the foundation and concentrate every individual face, trailed by an information standardization process.

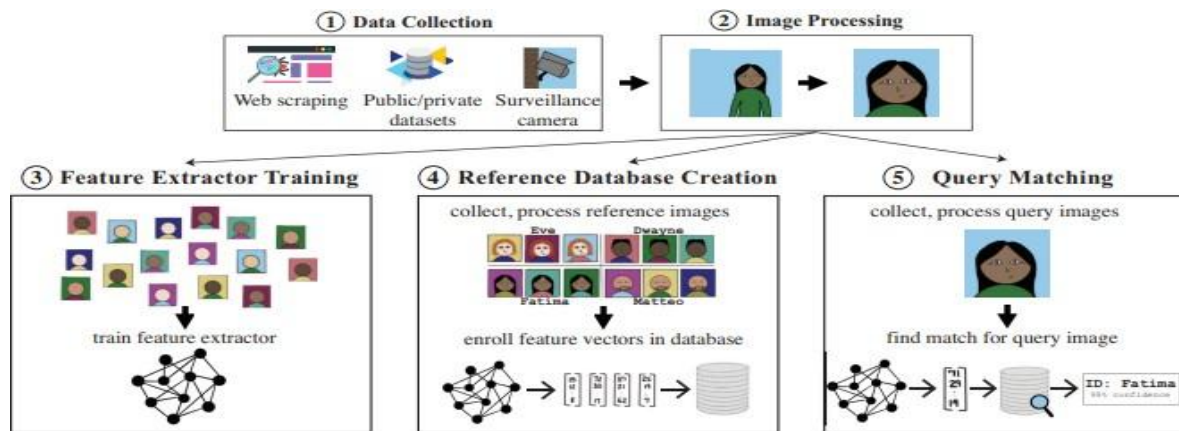


Fig.2: Five Operational Stages of Facial Recognition

### C. Feature Extraction

The essential component of DNN-based FR frameworks is the element extractor used to figure facial elements from a picture. To accomplish precise acknowledgment, the processed component vectors should be profoundly comparable for photographs of a similar individual, however adequately disparate across photographs of various individuals. Followup works investigate elective misfortune capacities and model structures to additionally work on the exactness of FR frameworks

To expand adequacy, the element extractor is by and large prepared on huge number of marked face pictures. Broad assets are expected to both gather and mark an enormous face dataset and to really prepare the model. Accordingly, numerous FR professionals, including enormous organizations and government offices pick to buy or permit a thoroughly prepared highlight extractor from tech organizations

### D. Reference database creation

FR frameworks need an enormous information base of known (or marked) faces to match obscure (unlabeled) countenances to their actual characters. Accordingly, FR frameworks fabricate a reference data set of individuals they need to perceive, by gathering and preprocessing named face pictures of different end users, and afterward passing them to the element extractor to acquire highlight vectors. The reference information base stores the comparing highlight vector.

### E. Query Processing

At execution, the Facial Recognition framework inputs an unidentified face picture, separates its element vector, then enquiry input with an reference data set to find a match.

### 2.3 Real World FR Deployment and Data collection

As of late, huge enterprises and government offices across the world have embraced Facial Recognition for different service oriented applications. This wide reception was set off by huge exactness upgrades of Facial Recognition frameworks, to a great extent because of new preparation techniques and all the more remarkable brain network structures. Beneath, we present some regularly realized FR use cases and talk about their effect on clients.

#### A. Service Oriented public sector use cases

Government organizations all over the earth use Facial Recognition for an assortment of purposes. For instance, the US Nation involves Facial Recognition frameworks for regulation requirement purposes, for example, line control and police operation.

**B. Private/ Entrepreneurship use cases**

Numerous organizations have incorporated Facial Recognition for security and trade pipelines. The most widely recognized Facial Recognition use cases are improving store or office security. Different organizations have utilized FR to screen corporate office access. Item based applications have arisen too, for example, vehicle organizations like Subaru utilizing FR to follow driver exhaustion or carriers utilizing FR to smooth out traveler checkins.

**C. Data Fetch of Face Images**

The conclusive wellspring of pictures for conveyed Facial Recognition models is regularly obscure. In view of private and public data, diagram a few known wellsprings of preparing, referencing and enquiring pictures utilized by the present Facial Recognition frameworks. Preparing pictures (used to prepare highlight extractors) regularly come from a blend of scholarly preparation datasets (for example restrictive information, and public information scratched from web-based media accounts, Reference pictures used to make the reference information base commonly come from the Internet (e.g., online media), or government data sets (e.g., identification and driver permit photographs).

Table 1: Private/Public Use cases of Facial Recognition

Type	Use Cases Reported	Countries/Companies
Government	On-street surveillance	Bahrain [36], China [2], England [15], France [37], Kenya [38], Myanmar [39], Russia [4], UAE [36], UK [40], US [9], Zimbabwe [41]
	Criminal suspect identification	Argentina [42], Belarus [39], Brazil [43], China [44], Greece [39], Malaysia [45], US [1]
	School monitoring	Brazil [46], China [47], India [11], Russia [46], US [46]
	Border security	Israel [48], Pakistan [49], US [50]
	COVID lockdown enforcement	China [51], India [52], South Korea [52], Russia [4]
Commercial	Catching shoplifters	Apple, Macy's, Lowe's [53], [54]
	Securing facility access	Alibaba [55], Intel [56]
	Tracking driver behavior	Hyundai [57], Subaru [58]
	Air passenger check-in	JetBlue [59], Delta [60]

**III. A STAGE-WISE FRAMEWORK FOR ANTI FACIAL RECOGNITION**

We currently talk about and dissect existing Anti Facial Recognition recommendations. To do as such, we propose and utilize a phase based structure to order Anti Facial Recognition procedures, incorporates the five basic stages among clients and Facial Recognition frameworks.

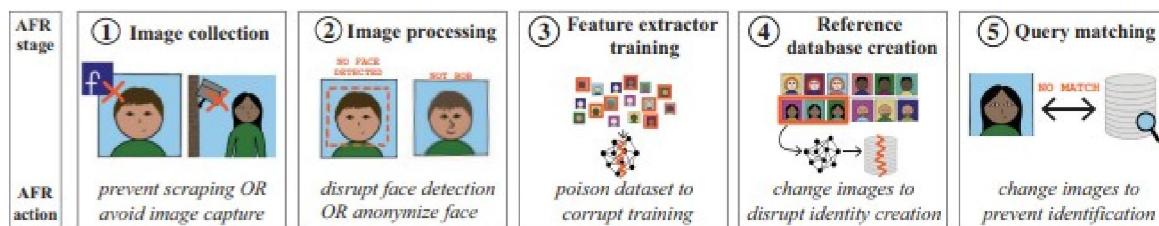


Fig. 3. Stage-based framework for analyzing Anti Facial Recognition proposals.

As shown in Figure 3, each of these basic focuses compares to a critical functional phase of FR frameworks. In view of this, we presently sum up the "assault" procedures utilized by Anti Facial Recognition devices to disturb the activity of every Facial Recognition stage and taxonomize current Anti Facial Recognition proposition.

**3.1 Anti facial recognition strategies per stage**

Since the five Facial Recognition stages 1 - 5 envelop the marks of direct collaboration among P and F, they normally cover the places of assault utilized by existing Anti Facial Recognition recommendations. Next we momentarily portray the overall procedures utilized by Anti Facial Recognition devices focusing on every Facial Recognition stage.

- Action1: In the image collection stage, as well as unlabeled pictures are gathered for use by F, either by actually taking photographs or scratching on the web pictures. While focusing on this stage, AFR instruments center around disturbing the information assortment cycle to keep F from obtaining usable face pictures of P.
- Action2: pre-processes gathered face pictures utilizing a progression of advanced changes, e.g., face recognition, foundation trimming, standardization. Anti Facial Recognition apparatuses sent will deliver the



handled pictures unusable, either by breaking the preprocessing capacities, infusing commotion and antiquities onto the pictures.

- Action3: Used for preparing face highlight extractors, Anti Facial Recognition devices focusing on this stage try to corrupt the exactness of the facial feature extractor by harming its preparation pictures.
- Action4: To make the data set, named reference pictures are gone through the element extractor to make their component vectors. Anti Facial Recognition instruments endeavour to ruin the element vectors made for P's reference images so the data set holds a "off-base" highlight vector of P.
- Action5: In the query matching stage, Anti Facial Recognition instruments try to forestall exact matching between a question picture's component vector and P's element vectors put away in F's reference data set.

#### IV. SYSTEM IMPLEMENTATION

Design cum implementation of above said proposed work consists of following software components:

Python 2/3 IDLE

Python Environment like Pycharm Community or Professional Edition or Anaconda Jupyter Notebook.

Python Libraries like OpenCV, Haar Classifier, Web browser and its dependencies.

Following commands to be given for proper execution of the proposed system

First clone this repo. Now, to install the dependencies and create the alias for Face Search, run the install.sh.

```
bash install.sh
```

Once it finishes, you can now use the following command on the terminal to detect and search for the faces in any image.

```
facesearch path/to/Image
```

Also, note that the path/to/Image can be an internet URL as well! (prefixed with http: or https:) So, you can just drag an image off the internet over the terminal to get its URL pasted over there and search for faces in it using FaceSearch. Really convenient.

Implementation Results: To implement the above said facesearch using google reverse engine model, we first select any image as input:

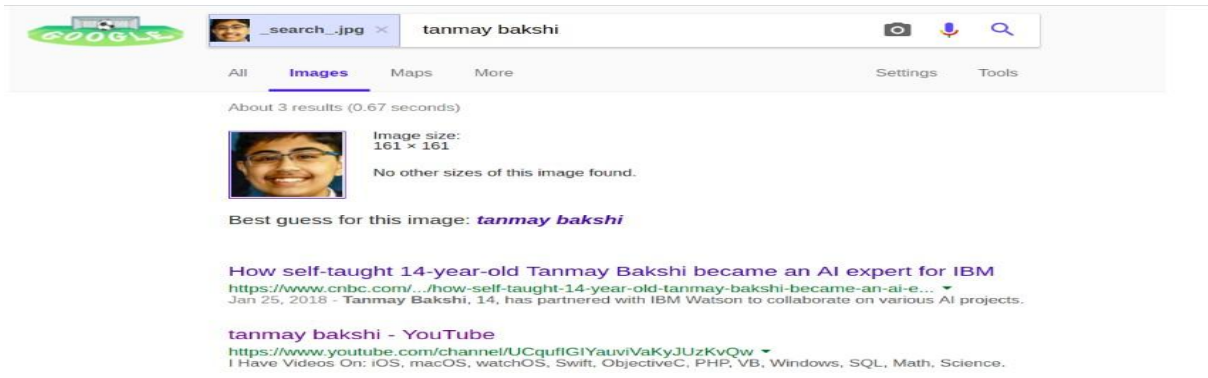
Test Image:



Output Window:



In the browser:



## V. CONCLUSION

As facial recognition keeps on filling in scale and pervasiveness, we anticipate that enemy of facial acknowledgments should ascend in prominence. There is a dire need to contemplate AFR devices, dissecting both their cutoff points and their true capacity. Our paper means to fill this hole by giving both a structure to talking about AFR recommendations and an appraisal of the current territory of AFR research. We observe that current AFR instruments have some, however not all, of the qualities expected to effectively overcome undesirable FR in reality. Many existing recommendations influence ill-disposed irritations to dodge FR models, either in the preprocessing - 2 or order 5 phases. Such annoyances, while frequently viable temporarily, need long haul ensures, and can't on a very basic level change FR framework conduct from now on.

## REFERENCES

- [1]. C. Garvie, A. Bedoya, and J. Frankle, "The perpetual lineup," Georgetown Law Center on Privacy and Technology, 2016.
- [2]. J. Chin and C. Burge, "Twelve days in xinjiang: How china's surveillance state overwhelms daily life," The Wall Street Journal, 2017.
- [3]. P. Mozur, "One month, 500,000 face scans: How china is using ai to profile a minority," The New York Times, vol. 14, 2019.
- [4]. P. Reeve, "How russia is using facial recognition to police its coronavirus lockdown," April 30, 2021. [Online]. Available: <https://abcnews.go.com/International/russia-facialrecognition-police-coronaviruslockdown/story?id=70299736>.
- [5]. K. Hill, "The secretive company that may end privacy as we know it," The New York Times, 2020.
- [6]. "Clearview ai's facial recognition app called illegal in canada," The New York Times, 2021.
- [7]. "Collection of biometric data from aliens upon entry to and departure from the united states." [Online]. Available: <https://www.regulations.gov/docket/USCBP-2020-0062/document>
- [8]. P. Grother, M. Ngan, and K. Hanaoka, "Ongoing face recognition vendor test (frvt)," NIST, 2018. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf>
- [9]. C. Garvie and L. Moy, "America under watch," Georgetown Law Center on Privacy and Technology, 2019.
- [10]. Y. Pan, Q. Feng, and C. Zhang, "Face recognition at the sales office," AI Outpost, 2020. [Online]. Available: <https://mp.weixin.qq.com/s/fWbQ3SD9vB-QdB51T097hw>
- [11]. "Fears for children's privacy as delhi schools install facial recognition," Reuters, 2021. [Online]. Available: <https://www.reuters.com/article/usindia-tech-facialrecognition-trfn-idUSKBN2AU0P5>
- [12]. D. Jeans, "Amazon extends moratorium on police use of facial recognition technology," Forbes, 2020.
- [13]. A. Krishna, "Ibm ceo's letter to congress on racial justice reform," 2020.
- [14]. "Ban dangerous facial recognition technology that amplifies racist policing," Amnesty International, 2021.
- [15]. "Stop facial recognition," Big Brother Watch, 2021. [Online]. Available: <https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/>

- [15]. S. Rodriguez, "Facebook plans to shut down its facial recognition program," 2021. [Online]. Available: <https://www.cnbc.com/2021/11/02/facebook-will-shut-down-program-that-automatically-recognizes-people-in-photos-and-videos-deletedata.html>
- [16]. T. Li and M. S. Choi, "Deepblur: A simple and effective method for natural image obfuscation," arXiv preprint arXiv:2104.02655, vol. 1, 2021.
- [17]. Y. Wen, L. Song, B. Liu, M. Ding, and R. Xie, "Identitydp: Differential private identification protection for face images," arXiv preprint arXiv:2103.01745, 2021.
- [18]. S. Shan, E. Wenger, J. Zhang, H. Li, H. Zheng, and B. Y. Zhao, "Fawkes: Protecting privacy against unauthorized deep learning models," in Proc. of USENIX Security, 2020.
- [19]. H. Huang, X. Ma, S. M. Erfani, J. Bailey, and Y. Wang, "Unlearnable examples: Making personal data unexploitable," in Proc. of ICLR, 2021.
- [20]. Evtimov, P. Sturmfels, and T. Kohno, "Foggysight: a scheme for facial lookup privacy," Proc. of PETS, 2021.
- [21]. V. Cherepanova, M. Goldblum, H. Foley, S. Duan, J. P. Dickerson, G. Taylor, and T. Goldstein, "Lowkey: Leveraging adversarial attacks to protect social media users from facial recognition," in Proc. of ICLR, 2021.
- [22]. T. Cilloni, W. Wang, C. Walter, and C. Fleming, "Preventing personal data theft in images with adversarial ml," arXiv preprint arXiv:2010.10242, 2020.
- [23]. Z. Wu, S.-N. Lim, L. S. Davis, and T. Goldstein, "Making an invisibility cloak: Real world adversarial attacks on object detectors," in Proc. Of ECCV, 2020.
- [24]. M. Treu, T.-N. Le, H. H. Nguyen, J. Yamagishi, and I. Echizen, "Fashion-guided adversarial attack on person segmentation," in Proc. of CVPR, 2021.
- [25]. K. Xu, G. Zhang, S. Liu, Q. Fan, M. Sun, H. Chen, P.-Y. Chen, Y. Wang, and X. Lin "Adversarial t-shirt! evading person detectors in a physical world," in Proc. of ECCV, 2020.
- [26]. V. Chandrasekaran, C. Gao, B. Tang, K. Fawaz, S. Jha, and S. Banerjee, "Face-off: Adversarial face obfuscation," Proc. of PETS, 2021.
- [27]. M. Xue, S. Sun, Z. Wu, C. He, J. Wang, and W. Liu, "Socialguard: An adversarial example based privacy-preserving technique for social images," arXiv preprint arXiv:2011.13560, 2020.
- [28]. D.-L. Nguyen, S. S. Arora, Y. Wu, and H. Yang, "Adversarial light projection attacks on face recognition systems: A feasibility study," in Proc. of CVPR, 2020.
- [29]. S. Komkov and A. Petiushko, "Advhat: Real-world adversarial attack on arcface face id system," in Proc. of ICPR. IEEE, 2021