applied sciences

MDPI

Article

Evaluating Secure Methodology for Photo Sharing in Online Social Networks

Athar A. Alwabel and Suliman A. Alsuhibany *

Department of Computer Science, College of Computer, Qassim University, P.O. Box 6688,
Buraidah 51452, Saudi Arabia

* Correspondence: salsuhibany@qu.edu.sa

Abstract: Social media has now become a part of people's lives. That is, today people interact on social media in a way that never happened before, and its important feature is to share photos and events with friends and family. However, there are risks associated with posting pictures on social media by unauthorized users. One of these risks is the privacy violation, where the published pictures can reveal more details and personal information. Since this issue has not yet investigated, this paper thus evaluates a methodology to address this issue, which is a precedent of its kind. In particular, our methodology relies on effective systems for detecting faces and recognizing faces in published images using facial recognition techniques. To evaluate the proposed idea, we developed an application using convolutional neural network (CNN) and the results showed that the proposed methodology can protect privacy and reduce its violation on online social networks.

Keywords: online social networking; protecting privacy; facial recognition; convolutional neural network; photo sharing; machine learning; face detection

check for updates

Citation: Alwabel, A.A.; Alsuhibany, S.A. Evaluating Secure Methodology for Photo Sharing in Online Social Networks. *Appl. Sci.* **2022**, *12*, 11889. https://doi.org/10.3390/app122311889

Academic Editor: Howon Kim

Received: 28 September 2022
Accepted: 4 November 2022
Published: 22 November 2022

1. Introduction

Over the years, people used to search for beautiful memories in their photo albums, and with the advancement of technology and the emergence of smart devices, a person opens his phone and sees the videos he recorded and the photos he took. Some consider that capturing and recording beautiful moments and sharing them on Online Social Networking (OSN) with family and friends simulates experiencing them with them [1]; because it is the archive that we turn to whenever we want to know the news and events of important people, especially when it is with loved ones and friends who are far from the eye or busy in their lives.

The OSN is defined as means of communication through which the user creates an account that enables him to communicate via the Internet with other people electronically [2]. To share information, ideas, opinions, messages, and other written, visual, audio, and file content. Examples of these platforms are Facebook, Twitter, Snapchat, and Instagram. For many people, posting a tweet on Twitter, creating a Facebook page, choosing the best hashtags to attach to their Instagram photos, or posting a cute video on YouTube has become a very easy and normal activity. If a person is an expert, then they may do the above four activities at the same time.

However, with the constantly flowing development in the OSN and the emergence of many new sites and applications, we can notice the development of the lifestyle of users based on what is happening within these sites. The spread of the OSN imposed by technological development has led to the explosion of a new conflict that is raging vigorously, both sides of which are clinging to their personal freedoms, and violators of privacy who do not hesitate to exploit every opportunity to benefit from them and expose the private lives of others [3–7].

Sharing photos by unauthorized individuals is considered a privacy breach [8]. Every person has the right to permit posting a picture of himself or his children, whether it is a single or shared picture, on social media. This controls the nature of the posted photos and helps increase privacy protection. Developing a feature added to OSN that would first seek permission before posting any photo may reduce such cases of cyberbullying and breach of privacy. Accordingly, this paper evaluates empirically our proposed methodology in [9].

In particular, this paper introduces an implementation of our proposed methodology in [9] as an application that works on smart device systems for both platforms IOS and Android. It is designed to allow people to know the photos posted for them and decide during the publishing process. By recognizing the people in the photos and determining their identity through facial recognition, the facial recognition technique can identify and verify a person in pictures in real-time. After completing the identification process, the application returns to the database to send a prior notice to the people to take permission to publish the photos or not. The application is written in Flutter language. This language is a toolkit that helps create mobile, web, and desktop applications from a single code base [10]. For facial recognition, we employ the deep learning technique, which is a branch of machine learning, with machine learning itself being a branch of artificial intelligence [11]. To be more precise, the convolutional neural network (CNN), which is one of the main categories of computer vision, will be used to perform image recognition and image classifications [12]. This CNN is used in the application to detect the faces in the image and then identify people's identity.

Our principal contribution is to prevent the publication of any photo without the permission of the owner of the photo. To the best of our knowledge, this has not been discussed before. Then, we carried out a real study to demonstrate the effectiveness of the proposed system. The results demonstrate that our proposal ensures a high level of privacy protection. The OSN can leverage our proposed system and add it as an option such as Public Accounts or Private Accounts. Facebook recently asked for an account holder video to be uploaded in which the face was taken from all parties to complete the registration process, and that can help Facebook implement our system with them.

The remainder of the paper is organized as follows sections: The research gap is highlighted in Section 2. Section 3 discusses related works. Section 4 describes problem definition. The proposed methodology is explained in Section 5. Section 6 explains implementation steps. Section 7 displays the feature of the proposed methodology. Section 8 presents the Experimental Studies. Section 9 demonstrates the outcomes of our experiment. Finally, Section 10 concludes the paper and presents the future works.

2. The Research Gap

Cyberbullying did not come out of nowhere; it came out of an explicit violation of privacy through photography and publication. Practices have increased lately; the phenomenon of privacy violations has intensified with mobile cameras. Where people's victims are photographed during weddings and events and during shopping and subsequently broadcast. The violation of privacy caused some people to abuse, ridicule, bullying, slander, and spread rumors. As a result, the display and sharing of images with unauthorized individuals constitute a privacy breach [5,6].

Lately, we have seen a significant increase in the number of users on OSN, and users are attached to them, as users spend a lot of time switching from one app to another. The latest statistics for the Statista website show that the average person spends 147 min per day on OSN [7]. The daily tracking of OSN made it possible to match and simulate what a person can publish to increase his interaction rate. Social media platforms provide their services in an easy, fun, and freeway, but this is in exchange for the huge amount of data that governments and companies can benefit from. In this paper, therefore, we seek to develop OSN from its advantages in protecting the privacy of individuals by adding optional features that help in using them with ease and safety.

3. Related Work

Previous studies have dealt with roles of social media; to inform, to influence, and to share data and information among individuals, businesses, corporations, and states. However, most of these studies have felt short of addressing the possible prevention mechanism particularly on sharing photos via social media platforms. Sharing of photos online is the transfer of users' digital images to the third parties with intended objectives. The term 'sharing' means that third parties may decide to view photos, but not necessarily download while the owner can have different copyright options to maintain the authority over the images [13]. Digital platforms offer features that allow hosting, sharing, and uploading of photos for either public or private viewing. Digital platform refers to the online businesses that allow interaction among different groups to share ideas, data, and information. Many people post their photos on various social media platforms such as Twitter, Facebook, Instagram, etc., oblivious of the consequences that come afterwards. Studies show that increased urge for people to post their photos on the online sites poses confidential risks that could private and sensitive information to the hackers or fraudsters. Hackers or fraudsters use their skills and computer expertise achieves certain goals-possibly to cause harm to others. Therefore, unless there are certain measures to control and prevent such activities, exposing personal information through online platforms may create a soft landing for thieves to locate and cause harm. We found that there was very little related work associated with the prevention of photo sharing on OSN.

Captured entities' privacy-preserving photo sharing methodologies are receiving massive attention, which has been handed-down privacy computing. It is critical to note that privacy-preserving photo sharing is a sibling are privacy computing. Nevertheless, attaining data sharing goals of attaining the lowest time and effort cost per data-sharing session and preserving privacy are antagonists. But there is usually tremendous privacy loss on granting data-sharing freedom to the data-sharing medium or platform. Hu et al. [14] finding a perfect balance of data privacy preservation and low-cost data sharing is a goal that all entities must strive to achieve.

Photo-sharing platforms are finding themselves at the center of multiple privacy conflicts that result from individuals' unconsented uploading/sharing in those platforms' multi-faced photos. Many entities whose faces appear in shared multi-face photos are constantly agitating for only consented sharing of such photos, with their demand being each individual whose face is cognizable in the photos being asked to consent to the sharing before it becomes public. Ilia et al. [15] offer a comprehensive discussion of a photo-sharing privacy conflicts solution which detail how dropping down to finer granularity levels where implementation of privacy gets to the face-level instead of the popular photo-level methods can speed addressing the privacy problem.

Ilia et al. in [15] stated that privacy conflicts solution received a new lease of life through the improvements proposed by Vishwamitra et al. [16] In the improvement, Vishwamitra et al. extensively discuss techniques for controlling privacy in multi objects photos. In Vishwamitra et al. research paper, the authors inform the readers that they should realign their privacy control focus to cover inappropriate objects that appear in a photo for the old way of focusing only on faces seems not adequate for achieving photo-sharing privacy preservation goals.

According to Tonge and Caragea [17] discussed that photo sharing in social media create significant unwanted discussion and unimaginable privacy violations. The two authors go ahead to explain how social networks keep off configuring privacy preferences to improve their privacy and security and prevent violations of their security and privacy because they regard the activity as a daunting and tiring one. Tonge and Caragea offer a vivid description of social media-based image-sharing privacy preservation automating the deep CNN prediction model. The authors discuss in detail how sensitive information that is in a given image can be automatically discovered with ease using a deep CNN model that has been trained accordingly. The Discovery of private pieces of data present in a particular photo can be done with a lot of success and effectiveness on employing well-trained deep CNN models that can get at their various layers extracts of "deep" visual features and generate "deep" image tags.

In Ghazinour and Ponchak [4] discussed that the authors make available a lot of information that details the ever-increasing complexity of achieving desired data privacy levels in social media's multimedia content sharing as the risk of exposure of those multimedia metadata to increase setting stage for a new violation; hidden privacy violations. According to the authors, information of high sensitivity is usually stored in pictures and images metadata with the location of taking the images/pictures, camera identifier number being some of such information, which image/picture reconstruction can make public. They also suggest a model for diffusing the privacy risks or issues that emerge sensitive metadata containing multimedia contents sharing. The focus of the model is on the removal of metadata from multimedia content when sharing them on social media to heighten the involved parties' security and privacy.

Social media is a huge engine for applications, as millions of people use it to communicate and share their information and data with others. This huge amount of information requires high-security measures to maintain privacy. Sushama et al. [18] report that the reliability of social media platforms is being compromised and that protection controls need to be raised further. Sushama analyzed some applications in a number of security areas of these applications and found that they failed to provide the highest protection reserves.

Over the last few years, social media have spread. The major reason for its release is its ability to provide a platform for communication and sharing for users with their families and friends. instant and fast, and the qualitative leap in the development of its features make it an attractive factor for users. However, the significant issue is the extent of the privacy and confidentiality of social media platforms. Jain et al. [19] conducted an extensive review of the security and privacy threats affecting social media platforms and discuss many solutions and ideas to ensure the security and privacy of social media users.

Social media contain a massive amount of information. These networks aim to improve the level of privacy protection by made the user the decision in some respects, while at the same time constantly seeking to develop privacy policies. Unfortunately, there are many privacy issues that arise from social media. Alemany et al. [20] reviewed the privacy mechanisms and solutions currently available on social media platforms and analyzed them, examined user sub-decisions and identified privacy requirements and the extent to which the user is allowed to make the decision.

An update to "Terms of Service" that YouTube made in November 2020 stated the company's commitment to privacy preservation as it stated that it was restricting the identification of persons via its facial recognition programs [21]. It further made public its restriction of the use of the same programs in its videos for users' identification. YouTube, just like other major social network platforms owners, including Twitter, Facebook, Venmo, and LinkedIn, filed a lawsuit against Clearview AI demanding deletion of all their images that they have in their storage [22].

These works are summarized in Table 1 and compared with our work.

Table 1. Summarizing related works.

Study	Approach
[14]	Hu et al. Found the perfect balance between maintaining data confidentiality and sharing data at low cost is a goal that all entities must strive to achieve. They therefore proposed a solution for shared data within the OSN by developing a multi-party access control model (MPAC). The MPAC model works in parallel with a multiparty policy and the corresponding policy evaluation mechanism.
[15]	Ilia et al. Presented a thorough discussion aimed at resolving the issue of privacy by sharing images by reducing the image's accuracy at the facial level only. This makes it impossible to identify the owner of the face in the publication process.

Table 1. *Cont.*

Study	Approach
[16]	Vishwamitra et al. suggested that the level of control within shared imagery should focus on individual elements as well as policy specifications and policy implementation mechanisms. The model is based on the identification of personal identity, then the identification of identifiable information elements to control multilateral access.
[17]	This study highlited that sharing photos on social media creates large, unwanted discussions and unthinkable privacy breaches. In the discussion of Tonge and Caragea, they suggest using the CNN model that was formed to find sensitive information in the photos. Then inform the photo publisher about the photosensitivity level prior to publication.
[4]	This study focused on that very sensitive information is stored in images and image metadata with the location of the captured image, and the camera identification number is part of that information. The authors propose a model based on the removal of metadata from multimedia content when shared on social media to increase the security and confidentiality of the parties concerned.
[18]	Auothrs of this study assessed the level of security and privacy in social networking sites, and the outcome was the inability of applications to provide the highest levels of security and protection reserves.
[19]	Jain et al. took a comprehensive look at the security and privacy threats to social media platform models and discussed a range of ideas to ensure the security and privacy of social media users.
[20]	Alemany et al. represented and analyzed the mechanisms and solutions for the protection of personal information available through social media. They then reviewed user sub-decisions and identified confidentiality requirements and the extent to which the user was authorized to make the decision.
Our work	We suggest using a deep convolutional neural network to detect people in photos, send them a message and take their permission to finish the publication process. This is empirically evalauted.

4. Problem Definition

Many social networking applications have proliferated, and perhaps sharing photos and videos are one of these applications' main features. Sharing photos have a lot of fun and entertainment for social media users. It contributes to knowing their families' conditions, knowing their latest news, and having fun with them with funny things [1,2]. The numbers of pictures published daily on social media platforms invite surprise, exclamation, and fear. This leads us to ask: is what on social media is authorized to publish or not?

Most children play with their parents' devices, and they can take and download pictures without their knowledge. People take pictures to document the beautiful moments on holidays or wedding celebrations, and the photos may be shared on social media. In festivals and on ordinary days, people are photographed intentionally and unintentionally, and photos are shared without their knowledge. Moreover, it also happens that these photos are reposted. These examples highlight the problem of posting photos on social media without the owners' knowledge. This leads to myriad privacy problems [3,4].

People like to maintain their privacy, e.g., know what is published about them, and control it. By analyzing research papers published between 2010 and 2021 it indicates that there has been an increasing interest in protecting privacy via social media.

Very recently, YouTube has updated terms of service to prevent the use of facial recognition technology in its videos. As stated previously, the main problem is posting pictures on social media without the knowledge of their owners. Therefore, this paper evaluates a solution to this problem proposed in [9] by developing an application for smart devices through which the published images of people are controlled by using face recognition technology to protect the privacy of people as a kind of security protection.

5. The Methodology

We have designed a new technique proposed in [9] in which the basic concept of the proposal, as shown in Figure 1, and will be explained in more detail in this section.

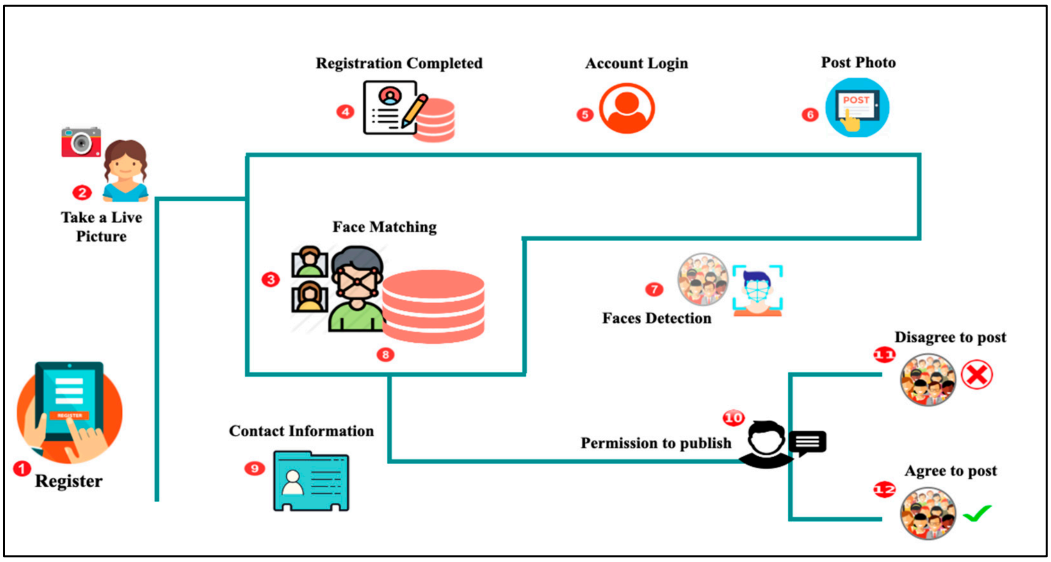


Figure 1. An Abstract System Model.

5.1. The Proposed System Design

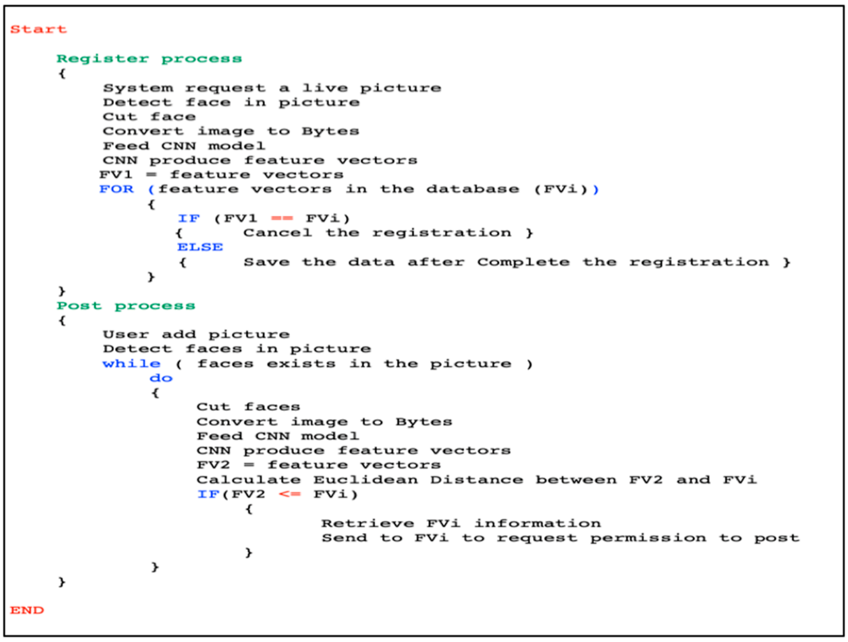
We used a new approach and present an abstract system model to accurately describe the proposed system.

The first step is the registration to the application request for the user to create an account, where they are asked to fill in their details like name, gender, date of birth, email and password as shown in Figure 1 step (1). All of these data will be automatically stored in the Firebase datastore. The second step (2), where the person should take Live Photos. The system detects the face in the uploaded images. Followed by cutting the images on the borders of the face, then converting this image into byte format. This format is then fed to CNN model with bytes. To produce feature vectors that describe these face features. The system compares the resulting features with the features stored in the database by using evaluation measures that calculating the distance between the parameters step (3), to prevent impersonation or identity theft. The registration process is completed when the results of an image match in the data store are negative step (4).

A person can log in and then post photos that represent the step (5) (6). Before publishing the photo, the step (7) is to scan the uploaded photo to verify that there are no unauthorized people in the photo. This is done by using face detection model. The publishing process will be completed if the result of detecting the face is negative; if the opposite is proven (i.e., positive result), the process of detecting the faces of the people in the photo is done.

In the step (8), as we explained previously in the registration process, the faces in image will be carve, followed by converting the images into bytes, and then feeding them to the CNN model. The CNN produces feature vectors, and then the features are matched with the rest of the features in the database. This matching is by calculating the distance between the parameters, the face owner will be deduced, and then his information will be retrieved from the database which represents the step (9).

In the step (10), a notification is sent to the owner of the face that a person wants to publish a photo that belongs to him. Based on this notification, the owner can decide whether the photo can be released (12) or not (11). Figure 2 shows the pseudocode of the proposed system.



```
Start

    Register process
    {
        System request a live picture
        Detect face in picture
        Cut face
        Convert image to Bytes
        Feed CNN model
        CNN produce feature vectors
        FV1 = feature vectors
        FOR (feature vectors in the database (FVi))
            {
                IF (FV1 == FVi)
                {       Cancel the registration }
                ELSE
                {       Save the data after Complete the registration }
            }
    }
    Post process
    {
        User add picture
        Detect faces in picture
        while ( faces exists in the picture )
            do
            {
                Cut faces
                Convert image to Bytes
                Feed CNN model
                CNN produce feature vectors
                FV2 = feature vectors
                Calculate Euclidean Distance between FV2 and FVi
                IF(FV2 <= FVi)
                    {
                            Retrieve FVi information
                            Send to FVi to request permission to post
                    }
            }
    }
END
```

Figure 2. The Pseudo code for the proposed system.

5.2. Face-Recognition Library in Python

The proposed system aims, as we stated previously, to prevent the publication of photos on social networking sites without prior permission. In this section, we describe this system in which detecting people in the photo, identifying them, and then obtaining permission to publish are detailed in the following sections.

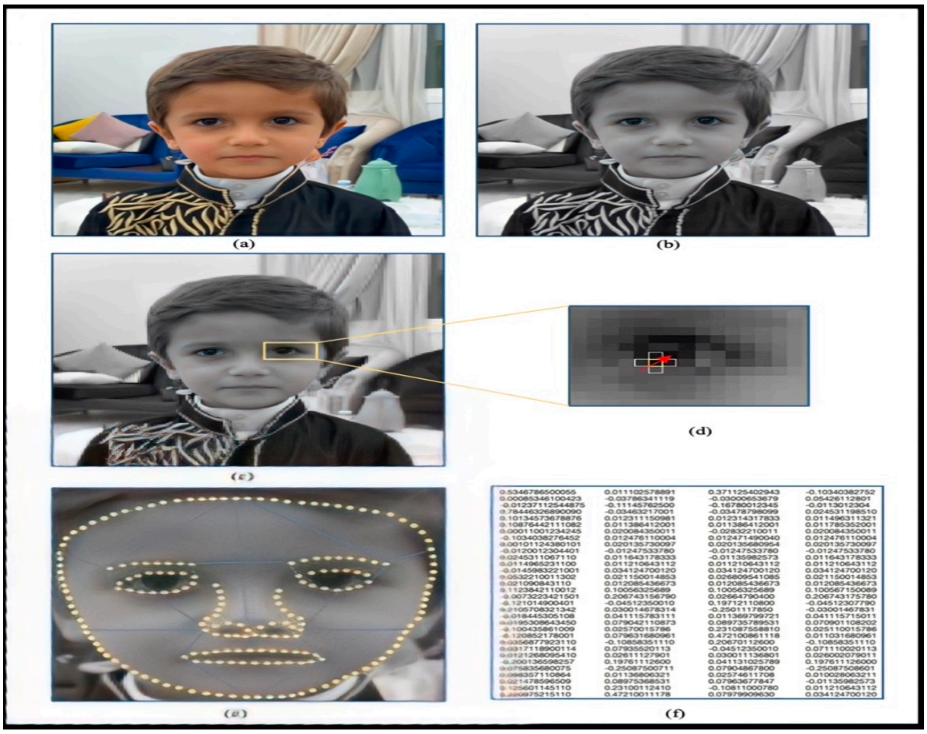
We decided to use a Flutter language to build both the smartphone applications, as this language supports building smartphone applications with a single code for Apple and Android [10]. Afterward, Firebase was chosen as Backend-as-a-Service (BaaS), which includes datastore, real-time database, authentication, hosting, and machine learning [23].

The face-recognition library is recognized and handled faces from Python or the command line using dlib's and CNN models [24]. Dlib Library is one of the most widely used packages in the facial recognition [25]. There are two integrated face detection procedures. The first one is the Histograms of Oriented Gradients (HOG) + linear Support Vector Machine (SVM) Face detector [26]. This is an accurate and effective face detection algorithm. The second one is the Max-Margin Object Detection (MMOD) CNN Face detector [27]. This is a very accurate and very robust, from different viewpoints Face detection in lighting and occlusion conditions.

Figures 1 and 2 describe how to address the mentioned issues to demonstrate the proposed system design. Each step of the proposed methodology is explained as follows:

- The first step (1) is the application request for the user to create an account, where they are asked to fill in their details like name, family, gender, date of birth, email, username, and password. All of these data will be automatically stored in the Firebase datastore.
- The second step (2) where the person should take Live Photos.
- The third step (3): our system detects and recognizes the face in the uploaded photos using Face-recognition Library in Python. We used the Google cloud platform as a local machine for run Python code. The Python code includes the basic operations of our application. We have two operations face detection in images and the face recognizing. Additionally, we used Google Cloud as a server for connecting the local machine with the flutter app. We can simplify this library's work by proceeding as shown in Figure 3. The image is initially received Figure 3a and then converted to a black and white image Figure 3b. Each pixel of the image is watched and gradations of brightness in Figure 3c,d, that is from light to dark, are deduced for the whole

image. Afterward, the pictures will be divided into small squares, each containing 16 × 16 pixels and color gradations will be calculated for each pixel in any direction, then replace the square with stronger pixel directions. At last, we will obtain a simple representation of the basic structure of the face as in Figure 3e.



0.5346786500055	0.0111102578891	0.371125402943	-0.10340382752
0.00085346100423	-0.03786341119	-0.03000653679	0.05426112801
-0.01237112544875	-0.11145762500	-0.16780012345	-0.0113012304
0.78446326890090	-0.03463217001	-0.03478798099	0.024531198510
0.10134573678876	0.0123111150981	0.012314317833	0.011496311321
0.10876442111082	0.011386412001	0.011386412001	0.011785352001
0.00011001234245	0.020084350011	-0.02832210011	0.020084350011
-0.1034038276452	0.012476110004	0.012471490040	0.012476110004
0.00101124380101	0.020135730097	0.020135680954	0.020135730097
-0.0120012304401	-0.01247533780	-0.01247533780	-0.01247533780
0.0245311067110	0.011643178333	-0.01135982573	0.011643178333
0.0114965231100	0.011210643112	0.011210643112	0.011210643112
-0.0145983221001	0.034124700120	0.034124700120	0.034124700120
0.0532210011302	0.021150014853	0.026809541085	0.021150014853
0.021090843110	0.012085436673	0.012085436673	0.012085436673
0.1123842110012	0.10056325689	0.10056325689	0.100567150089
-0.0073223421501	0.206743156790	0.02664790400	0.206743175780
-0.121014900401	-0.04512350010	0.19712110800	-0.04512307790
0.2105708321342	0.030014678314	-0.2501117850	-0.03001467831
-0.018445305108	0.041115783111	0.011369799721	0.041115715011
0.0195308643450	0.079042110873	0.089735789531	0.070901108202
-0.100435861009	0.02570015786	0.231087558810	0.025110015786
-0.120852178001	0.079631680961	0.472100861118	0.011031680961
0.0356877923110	-0.10858351110	0.20670112600	-0.10858351110
0.0317118900114	0.07935520113	-0.04512350010	0.071110020113
0.0121268095410	0.02611127901	0.030011136801	0.026002079011
-0.200136598257	0.19761112600	0.041131025789	0.197611126000
0.075835680075	-0.25087500711	0.07904867800	-0.25087508601
0.098357110864	0.01136806321	0.02574611708	0.010028063211
0.021478596509	0.08975368531	0.07963677847	-0.01135982573
0.125601145110	0.23100112410	-0.10811000780	0.011210643112
0.220975215110	0.47210011178	0.07979909630	0.034124700120

Figure 3. Face-recognition Library procedures (**a**) represents The library received image, (**b**) represents converting the image to a black and white, (**c**,**d**) represent that each pixel of the image is watched and gradations of brightness, (**e**) represents the basic structure of the face, and (**f**) represents 128 facial features.

The outcome is that we convert the original image into a very simple representation that captures the basic facial structure in a simple way. We will emphasize the eyes and lips are centered. This image will be taken and passed across a neural network to measure facial features, and these 128 measurements will be recorded as in Figure 3f. Our system compares the resulting features with the features stored in the database by using evaluation measures that calculate the distance between the parameters, to prevent impersonation or identity theft. The registration process is completed when the results of an image match in the Firebase data store are negative.

- In the fourth step (4), the new user data and image are added to the Firebase database used for our application.
- In the fifth step (5), a person can log in and then post photos that represent the sixth step (6).
- Before publishing the photo, the seventh step (7) is to scan the uploaded photo to verify that there are no unauthorized people in the photo. This is done by using the previous Face-recognition Library in Python, the publishing process will be completed if the result of detecting the face is negative; if the opposite is proven (i.e., positive result), the process of detecting the faces of the people in the photo is done.
- In the eighth step (8), as we explained previously in the registration process, the photo will be sent to Face-recognition Library to measure facial features. Then the features are matched with the rest of the features in the database. This matching is by calculating the distance between the parameters, the face owner will be deduced, and

then his information will be retrieved from the database which represents the ninth step (9).
- In the tenth step (10), a notification is sent to the owner of the face that a person wants to publish a photo that belongs to him. Based on this notification, the owner can decide whether the photo can be released (12) or not (11). Figure 4 summarizes these steps in their entirety.

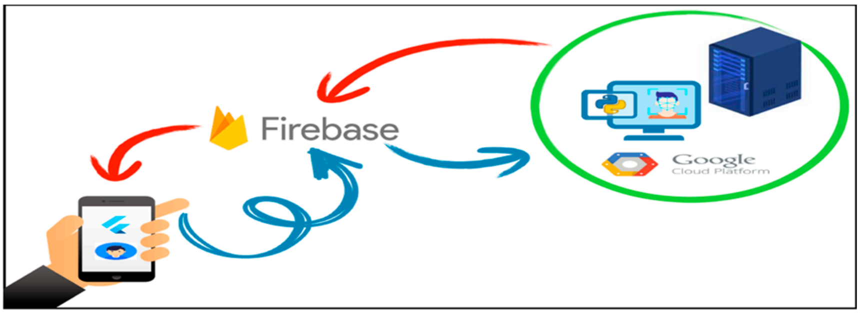


Figure 4. Describe the use of the Google Cloud platform and firebase on our app.

6. Implementation

There are two phases for our system: the registration phase and posting phase, as explained previously in Section 4. In this section, we describe the implementation of our application.

Firstly, the registration page was designed in flutter language, in which general data such as name, age and gender will be recorded. This is followed by a live picture of the person. When the user presses the sign-up button, it checks that all information has been filled in and that the photo has been taken. The live picture will be sent to be input into a code written in Python and uploaded to a Google cloud server for execution. Python code contains two operations for registration process the first is to verify that there is a face in the image, followed by the second step. It will compare the face in the image with the faces stored in the firebase when the output from the comparison process is 0 which mean no face similar. Then all this information will be passed on and kept in the firebase and the recording process is completed.

Second, the photo posting page was designed in flutter language. Two options were added, either by taking a photo from the camera or choosing from the photo library. The selection is carried out by clicking on one of the two buttons. The image will be sent as input to Python function that uploaded to the Google cloud server for execution. Python function has two operations, the first is to check whether there is a face in the image and the number of faces in the image. Afterwards, the faces of the image will be compared to the faces stored in Firebase. When the result of the comparison process is 0 which mean no face similar, the image is saved to the firebase database and posted. However, if the result of the comparison process showed that the face matches one of the faces stored in the firebase, the information of the corresponding face will be restored, the image will be saved in the firebase. Then send a notification to the owner of the corresponding face containing the image and about the possibility of publishing or not.

Thirdly, the notifications are shown to the user if an image contains their face. The notification includes the image to be published, as well as two buttons for acceptance or rejection, Photo publisher name.

Fourthly, the profile page, that is, the person's personal page. It is designed to show the pictures he posted, and if the pictures contain other people, they do not appear until they have approved. Figure A1, which is added in the appendix, shows some screenshots of our application.

7. The Feature of The Proposed Methodology

The proposed methodology has a set of features that are listed as follows:

1. The proposal is conceived with a proactive mechanism that allows everyone in an image to be conscious of the publication Figure A2a.
2. The proposal helps prevent online bullying and physical humiliation, particularly against children Figure A2b.
3. The suggestion helps inform the people in the photo of the purpose of publishing the photo, for example, if it is a magazine, family, or friends Figure A2c.

8. Experimental Studies

We successfully performed a controlled laboratory experiment. The objective of this experiment is to verify the ability to control the process of publication of private images. This section provides an explanation of the experiments carried out to evaluate the proposed system.

8.1. Primary Experiment

We conducted a controlled laboratory experiment with four participants to test the application initially. The age of the participant ranges between 20 and 35 years. One participant had a technical background, while the other three had not a technical background.

Participants were asked to sign up and take a live photo and then press the sign-up button when the registration process is complete. The participants were divided into two teams, each one has two persons. Then, each team is asked to take a photo with the other team member and one member posts the photo the other member makes sure that s/he receives a notification containing the photo and a request to allow the sharing process. Cases of refusal of publication and acceptance of publication have been put on trial. We ran an experiment using an Android smartphone; the application was downloaded as a trial version.

The results, as estimated from the primary experiment the application was recognized faces of four participants very well. On the basis of these results, we have realized the real experiment which is detailed in the following section.

8.2. Real Experiment

We applied our experiment in a controlled environment. The experiment involves several users who are invited to use our app. The design of the experiment, the users, and the system are explained in the following sections.

8.2.1. Experiment Setup

In experiment design we have created several scenarios for the participants to try out. Initially, we divided the participants into two groups; the first group was pictures of one person, while the second group contained pictures of several people. The experiment was performed via the participants' smartphones as application. We wanted the images of the experiment to mimic the images usually published on social media. The following scenarios were applied:

- Take a face snapshot [front, right, left].
- The person on the photos is close and far away.
- Wear an accessory.
- Lighting and photo accuracy.
- Images from various age period.

For the participants we recruited 42 users who participated in this experiment over two weeks to evaluate the performance of our approach. The participants were divided into two groups: the first group consisted of one person in images, while the second group contained images of single people or more than one person, some participating in the experience and some not. The age of the participants varied between one and 60 years shown in Figure 5. Participants in the experiment of both genders: men and women. Figure 6 shows the percent of males and females in the experiment, carry different skin colors.

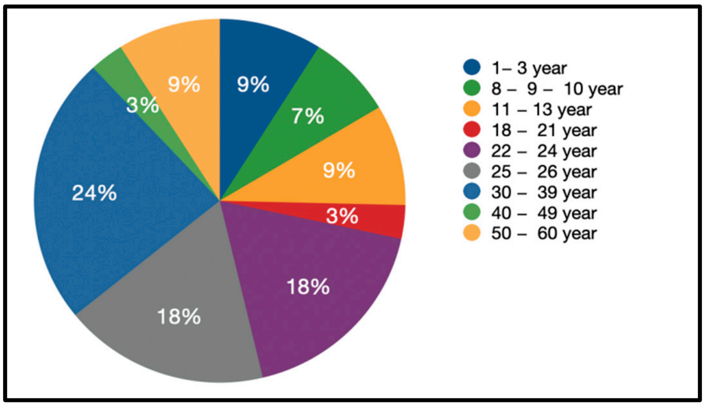


Figure 5. Age of experience participants.

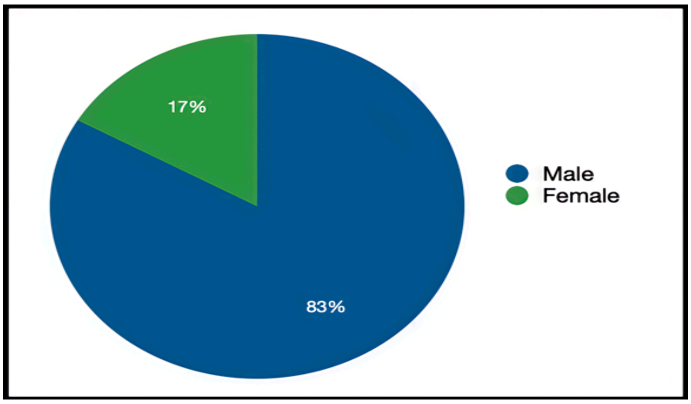


Figure 6. The ratio of males and females in the experiment.

Children participated in the experiment under the consent and supervision of their parents. All participants did not have technical backgrounds but were using social media platforms. All participants agreed to go ahead with the experiment and save their photos in the database.

The proposed system is represented in the form of a smartphone application available on Google Play console and the Test Flight, used to download the development and testing applications. We tested this application on an Android smartphone. We can access the application by entering the application name on the Test Flight and Google Play console or by using just their email address or by sharing a public link. Participants interacted with the application by posting photos to the application.

When the participant starts using the application, they complete their information and take a live photo through the registration process. The photo is then sent to the server and then to the local machine after pressing the sign up button to check whether it has already registered as shown in Figure A3a. In case the server replies that the photo has not already been registered, then the registration process is completed by sending the data to the firebase database to store it as shown in Figure A3b.

As we explained earlier, the system allows participants, after the registration process, to post photos as shown in Figure 7a. When the participant publishes photos, this picture is sent to the server and then to the local machine, where there are searches for faces in the picture, and then the process of identifying the owners of these faces. Once the previous process is completed, this information is sent with the image to be stored in the notification part in the database. A notification appears in the account of the people in the picture, bearing the image to be published, with two buttons of acceptance and rejection as shown in Figure 7b–e. If the approval process is completed, the image will be moved from the notification section to the post section of the database. Then it appears on the publisher's page as show in Figure 7f.

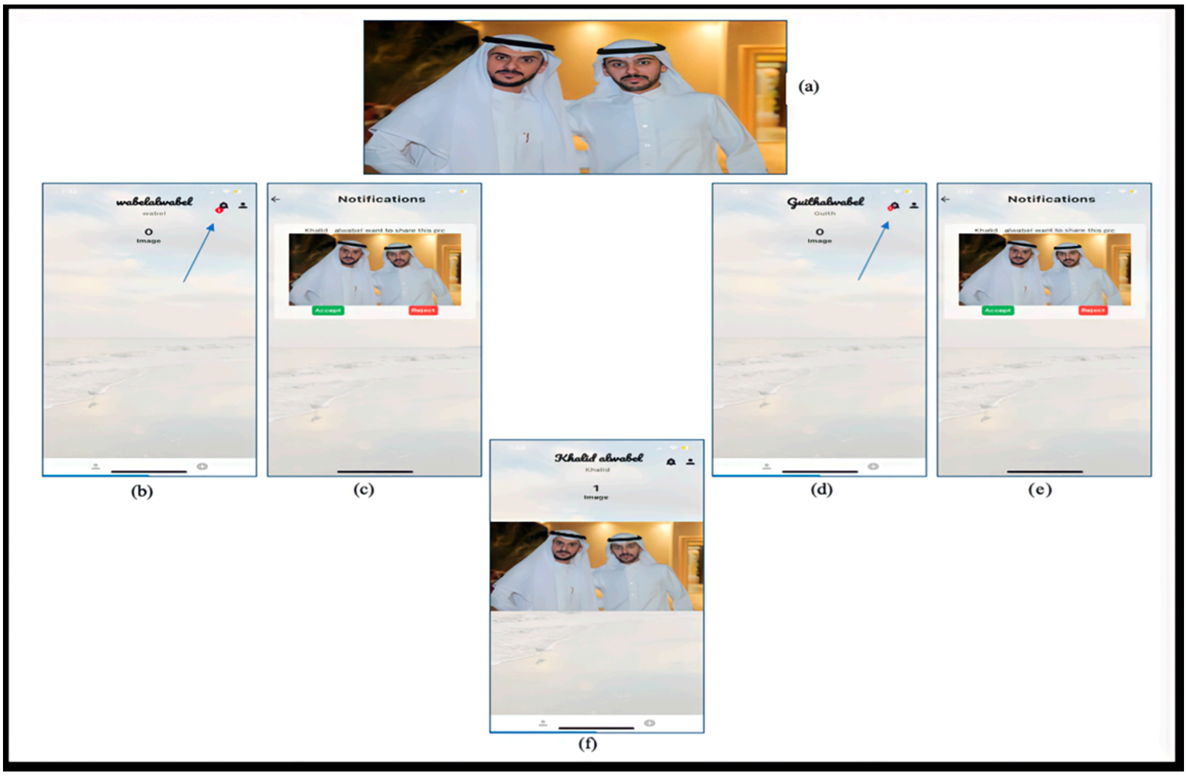


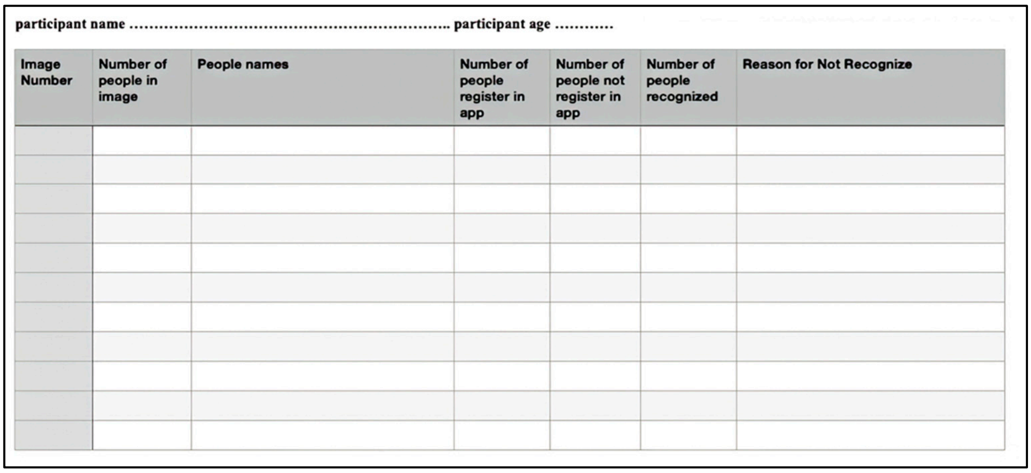
Figure 7. Post image and notifications in our app: (**a**) represents posting photos, (**b**,**d**) represent receiving a notification, (**c**,**e**) represent Image and publisher name with two buttons for acceptance and rejection, and (**f**) represents the image appears on the publisher page after accept.

8.2.2. Experiment Procedure

We describe how we carried out the experiment in terms of instructions to participants, procedures, and scenarios required in the following.

The participants were instructed that the aim of this experiment is to test whether our proposed system can protect user privacy by distinguishing between faces and controlling the process of image publishing. The instruction was given to the participants before the experiment is running. Participants were directed to use the application by registering and sharing photos as their usual method of social media platforms. Also, the participants were given some guidelines when using the app. For example, taking a photo of the full face without wearing any accessories. When taking the photo or choosing from the photo library for publication, choose different positions in the face, full face, or half-face from the right and left sides, or wear accessories such as sunglasses.

For the procedure, the experiment was conducted in a controlled environment to ensure that every participant was executing the required scenario. Each participant was asked to use the app to sign up first, then post a photo, and then accept or reject a photo posted them. At the same time as tracking database updates, we tracked manually by filling tables that contain the participant's name and age, photo number, the number and name of people in the photo, type of photo new or old, the number of registered and unregistered people, the number of people who were identified, and finally write the reason of not recognize people. Figure 8 shows a sample of the used table.



participant name .... participant age ....

Image Number	Number of people in image	People names	Number of people register in app	Number of people not register in app	Number of people recognized	Reason for Not Recognize

Figure 8. Tracking table for experience participants.

8.2.3. Measurement

We evaluated the performance of a face recognition model in our app using a confusion matrix. Figure 9 shows a sample of the confusion matrix for our app. In Figure 4 there are two faces A and B, face A is positive by positive we mean the attribute that we want while face B is negative by negative, we mean lack of attribute that we want. When feeding a model with face A and the result of predicting is face A this is called True Positive (TP), whereas when feeding a model with face B and the result of predicting is face A this is called False Positive (FP). And when feeding a model with face B and the result of predicting is face A this is called False Negative (FN). Finally, when feeding a model with face B and the result of predicting is face B this is called True Negative (TN).

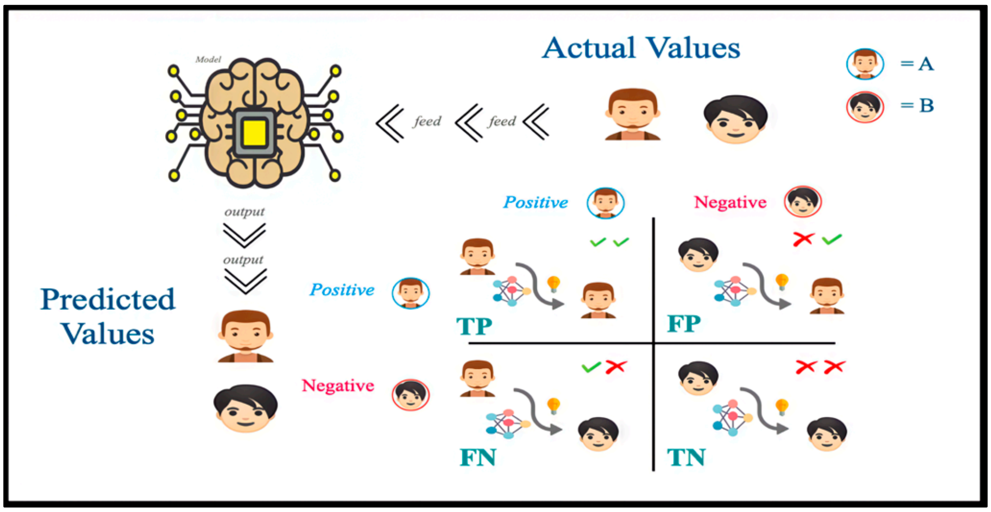


Figure 9. The Confusion Matrix for face recognition.

9. Results and Discussion

All participants completed the experiment successfully. In particular, the developed application has been downloaded, utilized, and published photos. Participants posted 475 photos which have different characteristics. Details of these results are explained in the following sections.

9.1. Results

9.1.1. Result of The Number of Images Uploaded per User, Number of People per Image

As shown in Figure 10 the number of images uploaded by user. Figure 11 shows the number of people.

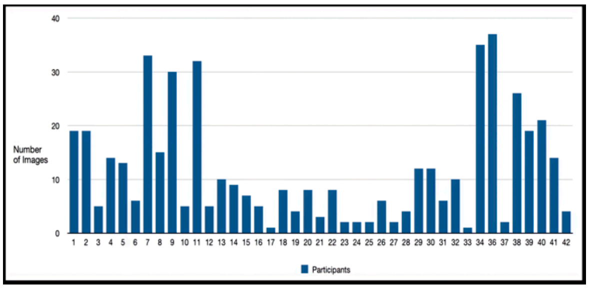


Figure 10. Number of images uploaded by user.

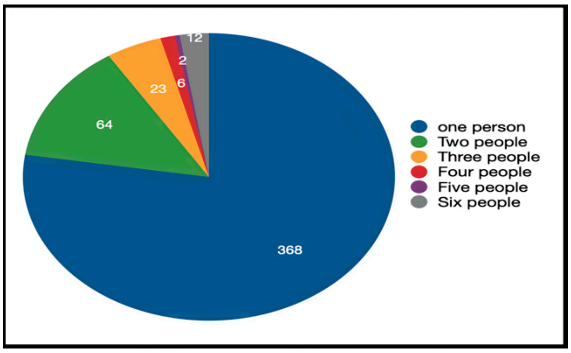


Figure 11. Number of people per image.

9.1.2. Results of Face Recognition in the Application

475 pictures of the participants were published during the performance of the experiment. Figure 12 indicates the percentage of identifying persons in the published photos.

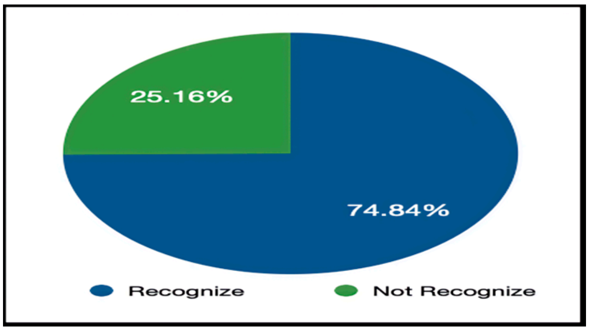


Figure 12. Face recognition percentage in the published photos.

9.1.3. Results of the Type of Images Posted by Every User

The published photo is different from when the pictures were taken. Figure 13 presents the numbers of photos published by each participant, whether it is a recent or an old photo.

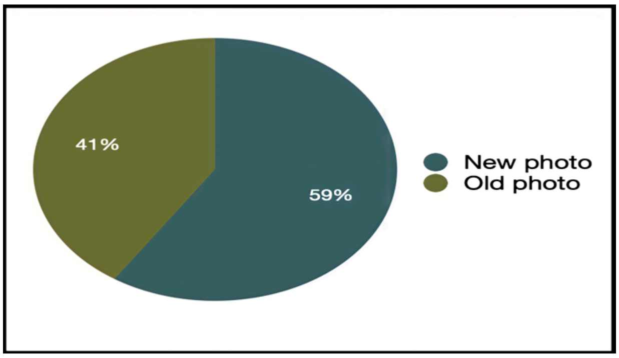


Figure 13. Image Type.

9.1.4. Number of States Incorrectly Predicted Face Recognition

Figure 14 shows the number of cases for which the model failed to predict identity people.

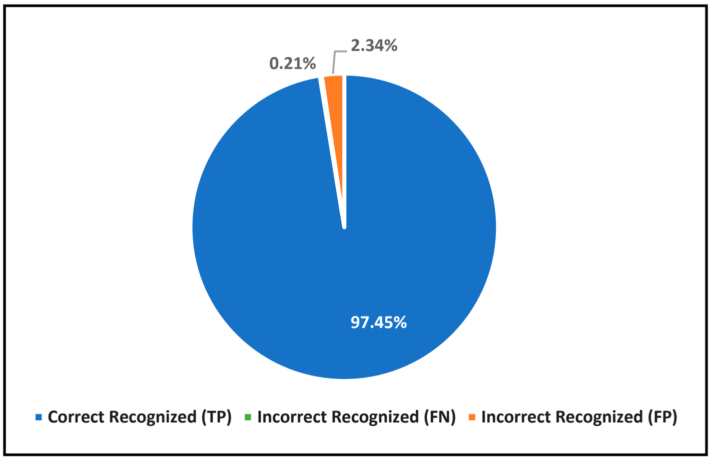


Figure 14. TP, FN and FP of face recognition in app.

9.1.5. The Number of Cases That Did Not Recognize the Face

The images published during the experiment, 73 pictures in which people were not identified. Figure 15 shows the state of the face on the image.

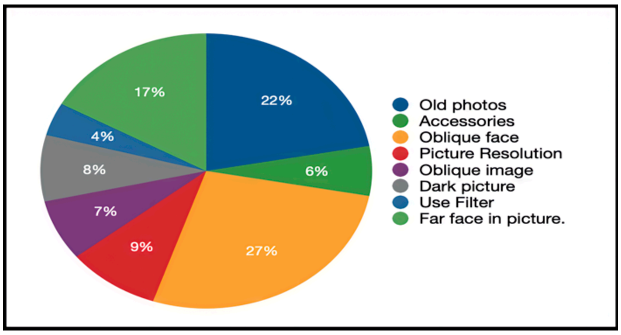
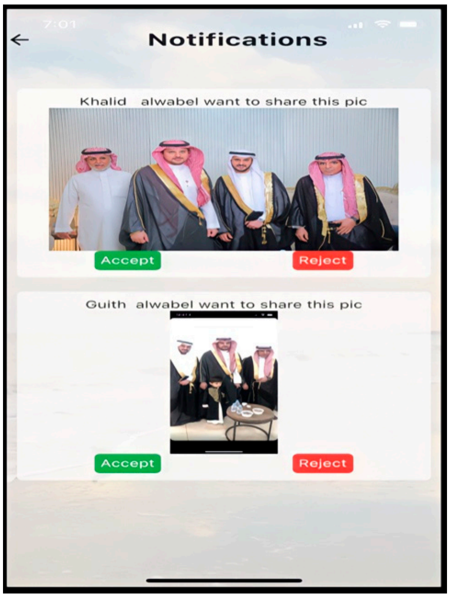


Figure 15. Reason behind not recognize the faces.

9.2. Discussion

According to our experiment, we have 42 participants as users of apps and each participant has an account. As shown in Figure 10, the number of images posted by every user. The photos posted by users varied, with some relating to the participant himself and others relating to the participants in the experiment and others not participated. Images of some of the participants were from different ages and scenarios, as mentioned in Section 7. Figure 16 show's some participants posted photos of people, the application was able to identify people and send them notifications.



7:01

Notifications

Khalid alwabel want to share this pic

Guith alwabel want to share this pic

Figure 16. Recognized multiple persons.

It is clear from the results that our proposed system has been able to recognize people as shown in Figure 12 that represents the percent of recognition and non-recognition cases. 74.84% of photos were identified successfully, while 25.16% could not be recognized. We asked users to enter pictures of different age stages, some pictures of them in the case of tilting the face, pictures from far and near, and pictures with different resolutions. Figure 17 shows samples of posted photos, some of them recognize their owners and some of which are not. We have looked at the results of Figure 16 that indicates the number of recent and old photos released per user. CNN model had errors in the prediction process, since it classifies people to people other than what they belong to. This is illustrated in Figure 14.

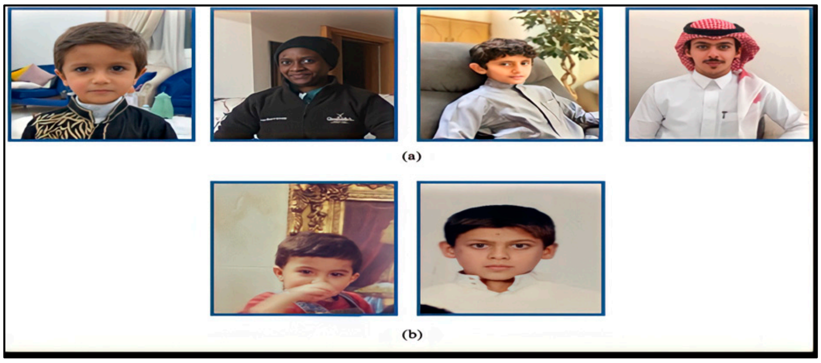


Figure 17. Samples of recognized and not recognized faces: (**a**) represents recognised faces and (**b**) represents unrecognised faces.

It is observed that possibility of identifying persons in new photos are more likely than in old photos. The reason behind this might be that the new images have gained a high recognition rate due to the narrow period between our stored image and the released image, and also developing imaging precision in modern devices facilitate reading the face features, for example Figure 17a. On the other hand, some of the photos were difficult to be identified using old photos if the pictures are of an early age or the appears and not the complete face for example Figure 17b. accuracy of the pictures is not good enough, or part of the face.

It is observed also that photos were taken with the close different stages of the age can be recognized easily, while the pictures with far stages of the age cannot be recognized. An example of close different stages of the age is shown in Figure 18a. Moreover, an example of long stages of the age is shown in Figure 18b.

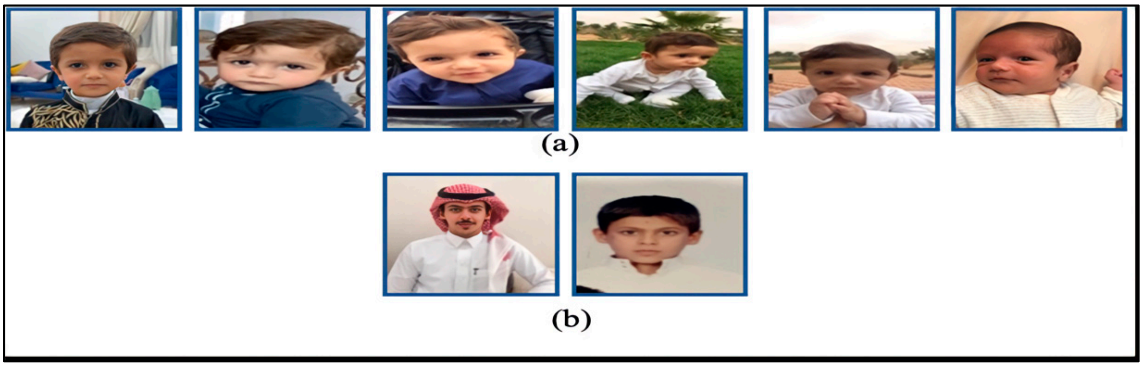


Figure 18. Samples of various age stages of the person: (**a**) represents early stages (**b**) later stages.

Additionally, it is observed that when we obtained at the time of registration a clear picture of the person in good lighting that shows the features of the face, we can identify him in different stages, provided that the face is completed and the accuracy of images is good, for example Figure 19.

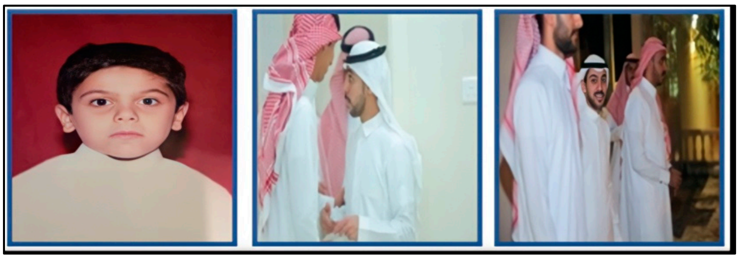


Figure 19. Samples of recognized different age stages of one person.

It is observed there was a challenge in the faces that do not appear completely, it was showing half the face, the face far away, or people who wear accessories. The success of recognition is due to the quality of the image captured in the registration. For example, in Figure 20a, a person was wearing sunglasses; in Figure 20b, a person was far; in Figure 20c,d, a person was looking left or right which means just have half of the face is appeared; therefore, the app was able to identify all of them.

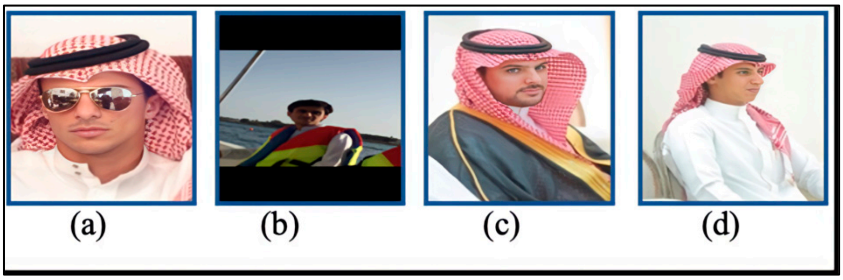


Figure 20. Samples of success recognized in different shape: (**a**) represents wearing sunglasses, while (**b**) represents so far shap and (**c**,**d**) represent half of the face is shown.

As shown in Figure 12, 25.16% of faces are not recognized. The reasons for not recognizing people have varied over the course of our monitoring of the performance of the experience. It is observed that several reasons prevent the model from identifying the person. First, the photograph is old; that is, different ages are there as shown in Figure 21a. Second, the person wears an accessory such as sunglasses or a mask as shown in Figure 21b. Third, the person uses a filter while taking the photo as shown in Figure 21c. Forth, the face capture angle to the right or left side as shown in Figure 21d,e and face capture angle from down as shown in Figure 21f. Fifth, a person was in dark photos as shown in Figure 21j. Sixth, the image is flipped left or right for example Figure 21h. Seventh, the photo accuracy was also a factor in the model's inability to predict an individual's identity, for example Figure 21i. Eight, when the location of the person is so far when taking a picture, this causes face features to be blurred, for example Figure 21k. Figure 15 illustrates the distribution of these reasons for the photos whose owners are unknown. Face looking right or left photos were the largest in our experiment, accounting for 27% of faces not recognized. 22% were for old photos. 17% for pictures of people wearing an accessory such as glasses or a mask. 9% for medium resolution photos or poor quality. 8% for dark photos. 7% for tilted photos where the app could not identify the face. 6% The location of people on the photos was too far away and the application could not extract the features. 4% of people publish photos using a filter whose characteristics have changed compared to the original.

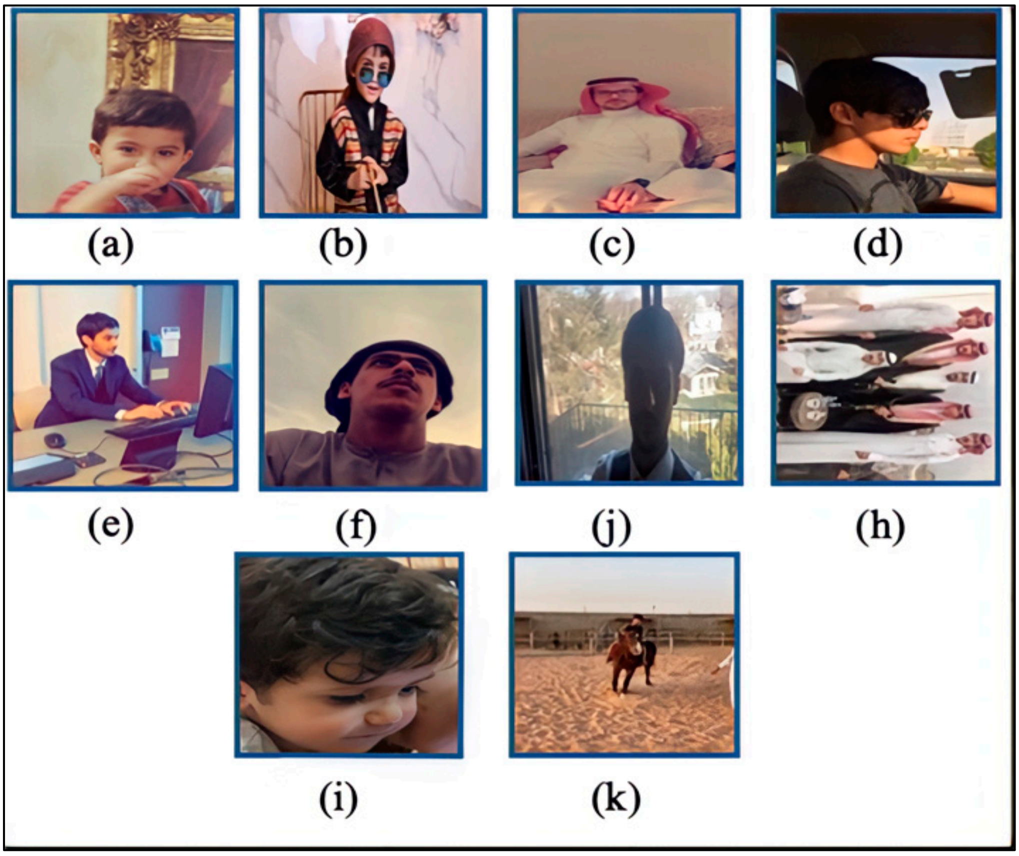


Figure 21. Samples of face not recognized: (**a**) represents the Photograph is old, (**b**) represents wears an accessory, (**c**) represents using a filter, (**d**–**f**) represents face capture angle to the right or left or down, (**j**) represents dark photos, (**h**) represents the image is flipped left or right, (**i**) represents photo accuracy and (**k**) represents the person is so far.

An issue in our application is observed that is the mistakes in prediction process. This has been defined in Section 7. The TP, FN and FP percentage is illustrated in Figure 14. Figure 22 shows sample in which there are errors in the identity of the predicted persons in the model.

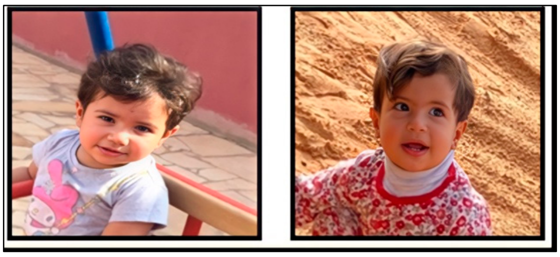


Figure 22. Samples of False prediction (FN).

Based on our result, we could conclude some registration restrictions. For example, once the face photo is taken the face should be adjusted directly to the camera and the lighting is clear. If the image has clear face features, we can get accurate results, especially with new images.

10. Conclusions

The proposed methodology in this paper for obtaining permission from the owners of images before sharing them appears promising. This methodology is based on facial recognition as a secure method of authentication of a person who posts a photo. Such an application can also be used to identify a cyberbully and report it to the authorities. The purpose of the automated image control system is to provide immediate notification. The developed application identified and informed individuals for permission to post and share before posting to social media accounts. This can prevent the potential leakage of image privacy and enhance the privacy protection aspect of social media. Face recognitions are used to check if the posted image matches any face image in the database. This helps to control the nature of images posted online and may reduce instances of cyberbullying. The results of our experiment indicated that our proposed system could identify the owners of images and not publish images without obtaining prior permission. As a result, our proposed system helps to give a good security level in terms of preventing potential leakage of image privacy and enhances the aspect of privacy protection. Based on the outcome, OSN may benefit from our proposal as a new OSN feature, as we are not in the process of releasing a new social networking application. However, we simply tried to simulate social networking programs to prove our concept.

In our future research, we intend to concentrate on taking more than one photo of the faces at the registration stage, and in different positions, this may produce good and accurate results. We will consider the published photo of people, where the system cuts the face of a person appearing in the post and adds it to his file in the database. This can feed the database and then give more accurate results. We will encrypt the pictures before uploading them to the database for better privacy protection. Also, we will improve the proposed methodology to include privacy protections in videos.

Author Contributions: Conceptualization, A.A.A. and S.A.A.; methodology, A.A.A.; software, A.A.A.; validation, A.A.A.; formal analysis, A.A.A.; investigation, A.A.A.; resources, A.A.A.; data curation, A.A.A.; writing—original draft preparation, A.A.A.; writing—review and editing, S.A.A.; visualization, A.A.A.; supervision, S.A.A.; project administration, S.A.A.; funding acquisition, S.A.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: The study was conducted in accordance with the Declaration of deanship of higher education, and approved by the Institutional Review Board of Computer Science Department and date of approval June 2020.

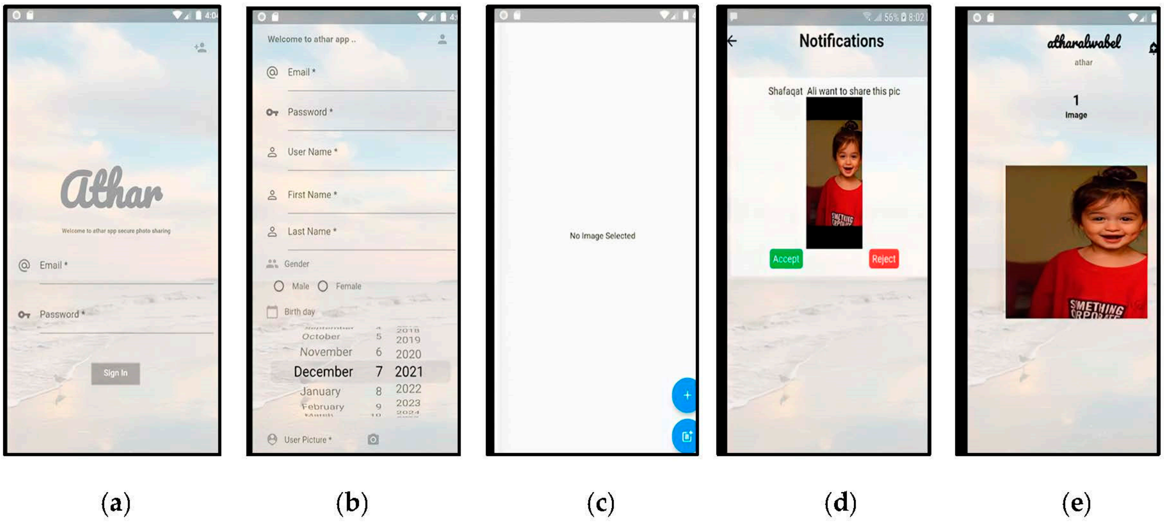
Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Acknowledgments: The researchers would like to thank the Deanship of Scientific Research, Qassim University for funding the publication of this project.

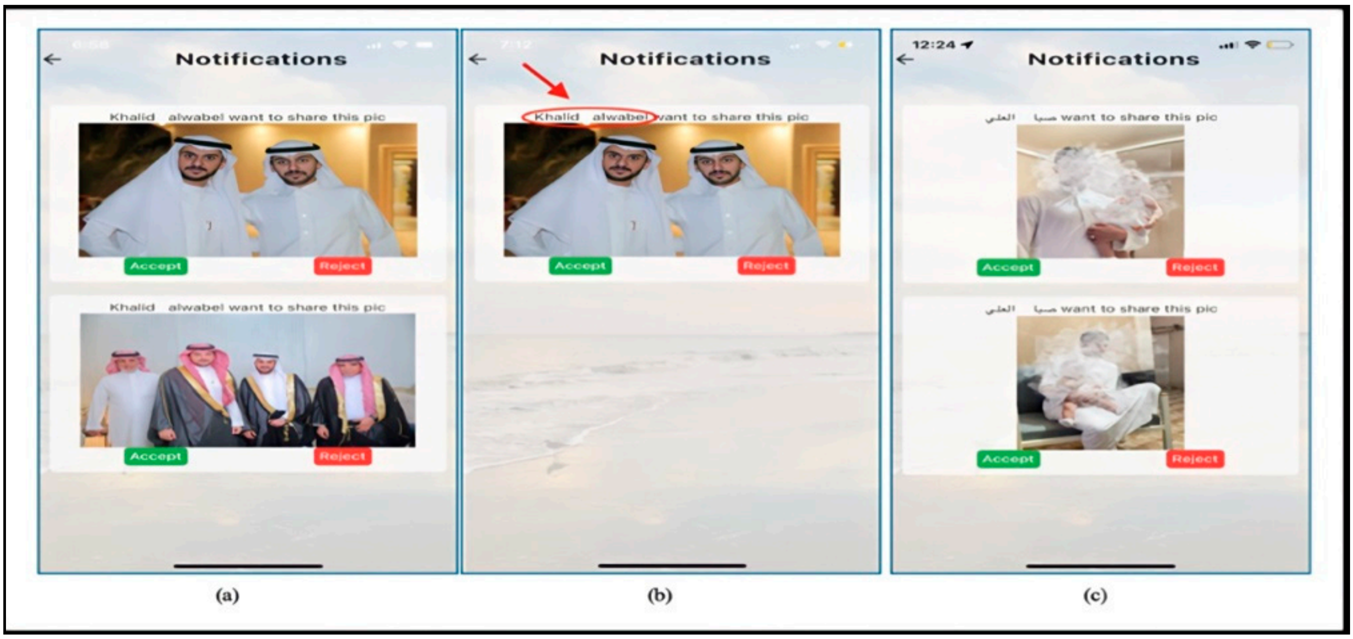
Conflicts of Interest: The authors declare no conflict of interest.

Appendix A



Shafaqat Ali want to share this pic

Figure A1. Screenshots of our mobile application. (**a**) refers to sign in page. (**b**) refers to sign up page. (**c**) refers to post images from the gallery or camera. (**d**) refers to the notifications the user received for accepting or rejecting. (**e**)refers to the image publish after accept.



Khalid alwabel want to share this pic

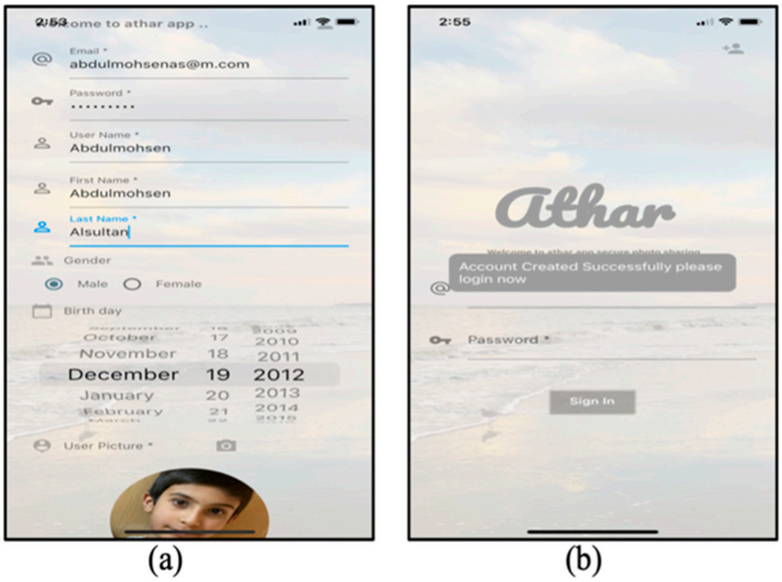
Khalid alwabel want to share this pic

Khalid alwabel want to share this pic

العلي صبا want to share this pic

العلي صبا want to share this pic

Figure A2. Screenshots of the Feature of The Proposed Methodology in application: (**a**) represents everybody in the image receive a notification, (**b**) represents the publisher name and (**c**) represents even account holder will receive a notification if he/she publish photo for here self we consider case of children play with pedant devices.


2:53 Welcome to athar app ..

Email *
abdulmohsenas@m.com

Password *
•••••••••

User Name *
Abdulmohsen

First Name *
Abdulmohsen

Last Name *
Alsultan

Gender
● Male ○ Female

Birth day
December 19 2012

User Picture *

2:55

Welcome to athar app secure photo sharing

Account Created Successfully please login now

Password *

Figure A3. Registration process: (**a**) refers to sign up page, while (**b**) refers to sign in page.

References

1. Ferdowsi, A.; Houston, D.; Ying, J.; Bartelma, J. File Sharing via Link Generation. U.S. Patent 9716742, 25 July 2017.
2. Amichai-Hamburger, Y.; Hayat, T. Social networking. In *The International Encyclopedia of Media Effects*; John Wiley & Sons: Hoboken, NJ, USA, 2017; pp. 1–12.
3. Mushtaq, A. Privacy in Online Social Networks. Seminar on Internetworking. 28 April 2008. Available online: http://www.cse.tkk.fi/en/publications/B/1/papers/Mushtaq_final.pdf (accessed on 5 February 2020).
4. Ghazinour, K.; Ponchak, J. Hidden privacy risks in sharing pictures on social media. *Procedia Comput. Sci.* **2017**, *113*, 267–272. [CrossRef]
5. Xu, J.-M.; Jun, K.S.; Zhu, X.; Bellmore, A. Learning from bullying traces in social media. In Proceedings of the 2012 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Montreal, QC, Canada, 3–8 June 2012.
6. Kumari, K.; Singh, J.P.; Dwivedi, Y.K.; Rana, N.P. Towards cyberbullying-free social media in smart cities: A unified multi-modal approach. *Soft Comput.* **2020**, *24*, 11059–11070. [CrossRef]
7. Dixon, S. Daily Social Media Usage Worldwide 2012–2022. 2022. Available online: https://www.statista.com/statistics/433871/daily-social-media-usage-worldwide/ (accessed on 5 February 2020).
8. Heravi, A.; Sameera, M.; Kim-Kwang, R.C. Information privacy in online social networks: Uses and gratification perspective. *Comput. Hum. Behav.* **2018**, *84*, 441–459. [CrossRef]
9. Alsuhibany, S.A.; Alwabel, A.A. Proposing a Novel Secure Methodology for Photo Sharing in Online Social Networks. In Proceedings of the 2022 2nd International Conference on Computing and Information Technology (ICCIT), Tabuk, Saudi Arabia, 25–27 January 2022.
10. Flutter. Available online: https://flutter.dev/ (accessed on 5 February 2020).
11. Albawi, S.; Mohammed, T.A.; Al-Zawi, S. Understanding of a convolutional neural network. In Proceedings of the 2017 International Conference on Engineering and Technology (ICET), Antalya, Turkey, 21–23 August 2017; pp. 1–6.
12. Deffo, L.L.S.; Fute, E.T.; Tonye, E. CNNSFR: A convolutional neural network system for face detection and recognition. *Int. J. Adv. Comput. Sci. Appl.* **2018**, *9*, 12. [CrossRef]
13. Farooqi, S.; Musa, M.; Shafiq, Z.; Zaffar, F. Canarytrap: Detecting data misuse by third-party apps on online social networks. *arXiv* **2020**, arXiv:2006.15794. [CrossRef]
14. Hu, H.; Ahn, G.J.; Jorgensen, J. Multiparty access control for online social networks: Model and mechanisms. *IEEE Trans. Knowl. Data Eng.* **2012**, *25*, 1614–1627. [CrossRef]
15. Ilia, P.; Polakis, I.; Athanasopoulos, E.; Maggi, F.; Ioannidis, S. Face/off: Preventing privacy leakage from photos in social networks. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, 12–16 October 2015.
16. Vishwamitra, N.; Li, Y.; Wang, K.; Hu, H.; Caine, K.; Ahn, G.J. Towards pii-based multiparty access control for photo sharing in online social networks. In Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies, Indianapolis, IN, USA, 21–23 June 2017.
17. Tonge, A.; Caragea, C. On the use of "deep" features for online image sharing. In Proceedings of the Web Conference 2018, Lyon, France, 23–27 April 2018.

18. Sushama, C.; Sunil Kumar, M.; Neelima, P. Privacy and security issues in the future: A social media. *Mater. Today Proc.* **2021**, *49*, 3488–3496. [CrossRef]
19. Jain, A.K.; Sahoo, S.R.; Kaubiyal, J. Online social networks security and privacy: Comprehensive review and analysis. *Complex Intell. Syst.* **2021**, *7*, 2157–2177. [CrossRef]
20. Del Val Alemany, J.E.; García-Fornes, A. A Review of Privacy Decision-making Mechanisms in Online Social Networks. *ACM Comput. Surv.* **2022**, *55*, 1–32. [CrossRef]
21. YouTube. Updated Terms of Service. Available online: https://support.google.com/youtube/answer/10090902?hl=en (accessed on 18 November 2020).
22. CBS NEWS. Google, YouTube, Venmo and LinkedIn Send Cease-and-Desist Letters to Facial Recognition App that Helps Law Enforcement. Available online: https://www.cbsnews.com/news/clearview-ai-google-youtube-send-cease-and-desist-letter-to-facial-recognition-app/ (accessed on 5 February 2020).
23. Firebase. Available online: https://firebase.google.com (accessed on 5 February 2020).
24. Geitgey, A. Face Recognition Documentation. *Release 1.2* **2019**, *3*, 3–37.
25. Boyko, N.; Basystiuk, O.; Shakhovska, N. Performance evaluation and comparison of software for face recognition, based on dlib and opencv library. In Proceedings of the 2018 IEEE Second International Conference on Data Stream Mining & Processing (DSMP), Lviv, Ukraine, 21–25 August 2018; pp. 478–482.
26. Dadi, H.S.; Pillutla, G.M. Improved face recognition rate using HOG features and SVM classifier. *IOSR J. Electron. Commun. Eng.* **2016**, *11*, 34–44. [CrossRef]
27. Khamket, T.; Surinta, O. Feature Extraction Efficient for Face Verification Based on Residual Network Architecture. In *International Conference on Multi-Disciplinary Trends in Artificial Intelligence*; Springer: Cham, Switzerland, 2021; pp. 71–80.