Survey on Image Authentication and Privacy in Public Networks

A. Parimala[1*], Y. Vijayalata[2], Ashlin Deepa R N[3]
[1,2,3]Dept of Computer Science and Engineering
Gokaraju Rangaraju Institute of Engineering and Technology
Hyderabad, Telangana, India
*parimalaamudalapally@gmail.com

2022 6th International Conference on Trends in Electronics and Informatics (ICOEI) | 978-1-6654-8328-5/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICOEI53556.2022.9776842

Abstract— **The number of people using social networking sites such as Facebook, Twitter, Instagram, and LinkedIn over the last couple of years has increased dramatically. On the one hand, these online communication sites have offered a lot of options for users to communicate and interact with each other. On the other hand, social networks raise concerns about privacy and security among internet users. In gaining an understanding of the unknown risks associated with the exposure of their content and information in this space as a result of its unchecked publication and sharing, users can better protect themselves against various forms of online attacks and be able to moderate its influence and adapt to evolving technologies. As people have become more dependent on social media and the Internet, they have developed negative traits that have led some to commit crimes. Due to multiple shortcomings, information security has become a major issue in today's society. While classifying the images, the main obstacles will be on achieving intra-class variation, size variation, occlusion, lighting, and background clutter. This research paper intends to present a detailed survey about various methodology implementations by previous researches for OSN privacy management and control using AI algorithms.**

Keywords— Online Social Network (OSN); Artificial Intelligence (AI); social media.

I. INTRODUCTION

One of the greatest advancements in 21st-century technology is social networking platforms. User profiles on social networking platforms generally come with numerous privacy policies users are not aware of. By posting personal information online, users risk making themselves vulnerable to online predators. They sell their data to others, and in some cases, sites take credit for everything a person puts on their profile page. Communication on social media platforms has become so popular and fashionable [1]. As a result, it is imperatively crucial for young people to maintain their social status among their friends by sending them social messages. Due to this, young people are particularly prone to indulge themselves. This is because there is virtually no understanding of what might happen to the information, photographs, and postings they post on their profile pages or those of their friends [1].

There are a number of different social media platforms that differ in terms of their objectives and characteristics, and they may be grouped according to their objectives, for example:

A. Communication platforms

This website's main objective is to let users' exchange data and communicate with one another, as well as to extend the number of users with similar interests. One example of a social networking site is LinkedIn, a platform for connecting colleagues and classmates. This can help users advance their careers

B. Social Networking Platforms

There are many types of sites available, but this type of site's primary objective is finding friends and participating in their virtual lives. Sites like Facebook, Twitter, and WhatsApp are some of the most popular examples of this type of site. There are many institutions that have started now using and exploiting such sites for professional and commercial purposes, despite the fact that these sites were first established in order to cater to the needs of private individuals.

C. Visual Data Posting Platforms

Users of these platforms are able to upload videos and personal photos as part of their day-to-day activities. In addition to videos and photos, also allowed to post, movies and television shows etc. It is generally accepted that YouTube, TikTok, Dub smash, Theek Thaak, Vigo Video, etc., are the most important of these video sharing sites.

Social media platforms have unquestionably brought a lot of advantages to individuals utilizing them. However, in addition to these benefits, there have been a lot of pitfalls connected with these advances in technology. In addition to these advantages, there are precautions regarding the protection and security of the data that are traded and stored on each of those social media platforms. There are a lot of social networks out there which provide access to a great deal of data, some of which can be sensitive and even basic. Some of these include details about the customers, such as their particulars, addresses, financial information, where they originate from, their preferences, educational background, and a great many others. Having the ability to gather a great deal of data regarding certain individuals and their activities across a wide range of social networks might hold any significance for particular individuals as well as groups.

As IT has become a more significant part of people's lives, it has become more difficult to control. These factors disrupt innovation and prevent full oversight of information. It is increasingly difficult to stop noxious projects that are spreading and becoming more complex, making them more difficult to stop. It has been reported that information robbery is expanding on a large scale at the institutional level. While using interpersonal organization services, individuals encounter different difficulties with regard to their personal data, for example, utilizing unapproved programs, abusing corporate computers, and accessing unapproved organizations. In addition, they promote sensitive material on unstable websites. Recent years have seen a significant increase in the number of interpersonal organizations being used on a global scale. The fact that Facebook has overtaken 2.25 billion monthly dynamic clients, for example, makes securing client information and the privacy of such information critically imperative [3]. By one estimate, more than 1.8 billion photos are posted to popular social media systems each day. Many of these images are shared despite the presence of private elements within the photo (e.g., an embarrassing facial expression or sensitive information visible on a computer screen), while other images may not be shared because of sensitive content that people prefer to keep hidden.

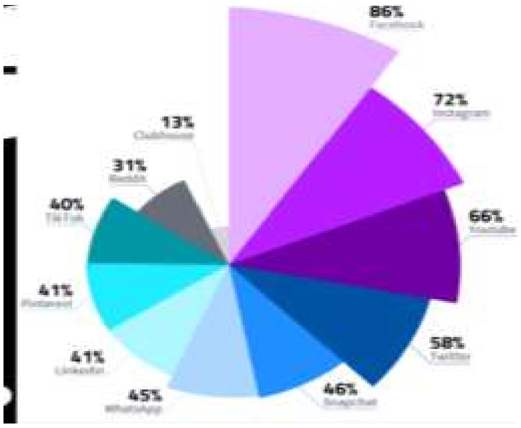


Fig. 1. Most popular social media platforms in 2021 [2]

Several social networks around the world that are used for online networking are stated in this research. These include the privacy problems in Australia, Brazil, the USA, Korea, Japan, and India. In order to bring to light the issues relating to privacy and security that individuals may encounter when creating their web-based personas, we anticipate that individuals, as well as companies, will take more consideration of these points [1]. In this paper we are focusing on surveying the image pixel degradation techniques of different authors. The paper navigation as follows: Section-1 represents the introduction of social networks and privacy issues. Section-2 discusses about the survey of different types of threats involved through online social networking. Section-3 survey of different research works done on image pixel degradation. Section-4 discusses about Future work and conclusion.

II. LITERATURE SURVEY ON PRIVACY THREATS THROUGH SOCIAL NETWORKING

Typically, social networking sites are a source of these threats. The purpose of this is to obtain both the personal information of the users as well as information from their friends. The privacy settings of users of social networks such as Facebook and Myspace are targeted by intruders as they are crucial to their identity. An attacker will have access to this information if all personal information has been made public; otherwise, an attacker has the ability to send friend requests to targeted users who have customized their Facebook profile settings. As a result, a target user's personal information is revealed after they accept a friendship request from a user. In the age of technology, there are several types of threats that are prevalent today, including Surveillance, Cyberstalking, Inference Attacks, User Profiling, Identity Clone Attacks, Information Privacy Leakage, Fake Profiles, De-Anonymization, Location Privacy Leakage, and Clickjacking Attacks.

TABLE I. TYPES OF PRIVACY THREATS THROUGH SOCIAL MEDIA

Type of Threat	Type of Data
Surveillance	Social, Political Governance, Environment, and E-Commerce,
Cyberstalking	Intimidation and Harassment
Inference Attacks	Prediction Sensitive, Political, Religious & Information about Education
User Profiling	Behavior and activities of individual characteristics
Identity Clone Attacks	Fake profiles
Information Privacy leakage	Property, Credit cards, Banking, Operational Infrastructure, Health Issues, Recent Purchases, etc.
Fake Profiles	User Information
De-Anonymization	Health Services, E-Commerce Trades, social media, etc.,

A. surveillance

A study on social networking platform surveillance, also referred to as posting and estimation, is another form of observation that is used to observe and acquire the data of clients, whether those clients be people, gatherings, associations, or even organizations. OSN surveillance can be characterized as innovative surveillance where the online activities of the onlookers are monitored via social media platforms [4]. A good example is how Facebook allowed Cambridge Analytica to access an enormous number of user profiles without obtaining the clients' informed consent of how the information gathered could be utilized for political campaigning. There is a belief that the organization has located social media appearances plausibly used by a large number of people and an analysis was then used to create individual mental profiles that were then used for an influencer campaign. Observations that are more intense and intentional are frequently conducted in an adversarial and inquisitive setting following the use of gradually more sophisticated means to gather and investigate information, and is used to administer social, natural, monetary, or political affairs [4].

B. Cyberstalking

This is referred to as e-stalking or web-based stalking and can be viewed at times as another name for cyberstalking. When the offender bothers or undermines different clients across long distances through informal communication, such as texting, email, or even a mix of texting and emailing, it is a crime. An example of badgering conduct would include provocation and terrorizing, as well as checking up on or following up on the victim. Cyberstalking is classified into four basic types; the created digital stalker, the aggregate digital stalker or the close digital stalker, and finally the pernicious digital stalker. When cyberstalking occurs, the aggressor relies on secrecy to follow up with their victim without being discovered by either them or others. Researchers used a mysterious electronic survey in order to discover what the opinions of American ladies were regarding digital provocation. 293 women were selected from different OSN destinations to take part in the study, in which the respondents were randomly selected. There were 58.5% of members who attended school or college as understudies. Approximately 20 percent of ladies have repeatedly received an unexpected physically revolting message or sexual request online. Over ten percent of respondents saw explicit messages from someone they had no clue who sent them, more than three-quarters experienced digital badgering and experienced symptoms of restlessness, and over one-fifth noticed changes in their sleeping and eating habits [5]. According to a few Research Center surveys conducted in July 2017, 4.248 U.S. adults were surveyed about their online encounters with provocations. As a consequence, 41% of American adults have already seen irritating behavior online, while 66% have witnessed annoying behavior coordinated by others. Often, these practices cannot be considered disruptive of online life simply because they are limited to specific perspectives. Despite this, almost one out of five Americans (18%) has been subjected to especially extreme forms of online harassment, such as physical injuries, threats sustained over extended periods, or lewd behavior [5].

C. *Inference Attacks*

Inference Attack is one of the technique used for data mining where information is examined to obtain the oldest information about a subject or a person. Machine learning models are probed with various input data and the output is weighted to reveal secret information. A foe's ability to infer its real worth with high certainty can be considered as spilling a subject's sensitive information. These attacks involve the exploitation of various information mining strategies to anticipate valuable data by gaining access to clients' data. It is probably not a good idea for clients to reveal their sensitive details such as political affiliations, home addresses, training, inclinations, ages, or orientations. As a result, the attacker may include any party (e.g., cybercriminals, suppliers of online social organizations, sponsors, information agents, and surveillance offices) with an interest in clients' private information. The attacker only needs to gather public information from online social networks to launch such security attacks. There is a need to protect the data contained in web-based social networking sites. Despite this, the attacker is still capable of predicting private information using data mining methods. In order to find the neighbour of any two clients using a shared companion-based attack, the shared companions of both clients must be known [6]. A principal component analysis (PCA) is a method utilized in order to deduce a client's traits based on their other public credit accounts that can be found online. Using Facebook, PCA was able to find out different client identifying factors, like area and educational background, while assessing PCA's procedures [6].

D. *User Profiling*

User profiling is a collection of settings and data related to the individual. It consists of basic information that can be used to categorize individuals, such as their name, age, picture, and any individual qualities they possess such as knowledge or mastery. The purpose was to not only record and analyze a user's exercise regimen to be comparable with both mental and conduct attributes. It was also to do so using a variety of strategies, including neural networks, genetic algorithms, and association rules. Unlike typical profiles of users, user profiles contain data that is not only a summary, but also the user's interests, abilities, objectives, and practices [7]. It may be crucial to establish age, orientation, and character attributes of users in order to create personalized forms of assistance, viral advertising, recommendation frameworks, and custom commercials. In addition, the user profiling is being conducted by specialized organizations for business purposes, but this can open the door for security fears to come to fruition [8].

E. *Identity Profile Cloning*

In our daily lives, one of the most common ways to steal information is through identity theft. Identity profile cloning refers to the method of creating a fake profile taking pictures, recordings, and other private data from a specific user's real profile. In some cases, the attacker may copy the profile of a user that looks very much like the profile of the target. That is especially true if a large part of the user profile appears to be open in the vast majority of cases. The cloning of profiles is carried out in two ways, one being the cross-site cloning and the other being the similar site cloning. The process of cross-website cloning involves the capture of the user's personal data from another website on the Internet that provides social networking services. However, when cloning a similar web-based social networking site, user private information is taken from that site as well. Furthermore, it should be possible to copy or reproduce a profile through natural means. In addition, if it was to be executed in social networking systems such as LinkedIn and Facebook, it would require the approval of a composed content code and to have the content code executed. Basically, an attacker uses the manual technique to duplicate the data of a victim and create a fake profile [9]. There are different approaches to identifying profile cloning but the common way of identifying is to find the key information of the user's current profile in which the identity of the individual should be apparent from the attributes of each profile. The query used for finding similar profiles may be narrowed by using only these attributes rather than others such as home, city, nationality, age, mutual friends, etc. In a later step, all similar profiles across various social networks are located using the gathered information. The list of profiles is then passed on to the algorithm, which compares the similarity and displays them to the user so that they are able to determine which profiles are legitimate and which ones are clones. Ideally, this is an approach that works for all social networks.

F. Information Privacy Leakage

In the context of information privacy leakage, the term refers to the situation where sensitive information is exposed to unapproved individuals. A user generally offers and exchanges their information with companions and other users on social media platforms through internet-based social networking services. By using social networking through the internet, information can be injected into the internet in four distinct ways: foundational information (for example, specialization choices), client information (for example, health information), functional information (for example, securing), and licensed information (for example, reports). There was a study conducted in which gave an indication that (95.8%) of (n=166) members of the social media online community shared any information related to their overall health. Likewise, leakage of such information can have a negative impact on online social networks users who are exposed to such sensitive and private information. For example, insurance companies might be utilizing online social network information in order to distinguish between customers who are safe and those who are not [10]. Leaking personal information is one way to harm the reputation of your business. It should be obvious by now that potential customers would feel anxious about doing business with you or divulging personal information to your company in the future. In order to prevent data leakage, there are a variety of possible explanations, such as using phishing tricks, utilizing instruments that are not secure, taking data, and sending them to users that are unacceptable [10].

G. Fake Profiles

Generally, a fake profile attack refers to the creation of a profile by an attacker with counterfeit credentials. For instance, the fake entry contains the attacker's name, interests, social security number, photos, and other information on a social network. It also sends messages to those users. False profiles are created in order to gather as much information as possible about the users. Despite the lack of bandwidth in this organization, counterfeit profiles have an impact on the general standing of the organization [11]. Reports indicate that a method was created in for displaying a fictitious Facebook profile and to be prepared to send an estimated 8,570 requests to online associations. The strategy recorded all data related to the expected covertness of users and correlated this information with the actual behavior of users. This information was compared with the profile information of all open users. As another example, during the latter half of the year and into the beginning of this year, Facebook exposed and suspended some (1.3) billion phony records. There are, however, just as many - or even more - phony profiles out there that haven't yet identified, which range spans from (66) million to (88) million. A similar measure has been taken to assess whether between 9 percent and 15 percent of Twitter's (336 million) records are fake [12].

H. De-anonymization

An anonymous deanonymization attack makes use of cross-referencing between unidentified information and other public sources in order to re-identify the unknown source of information to identify a specific individual or group of people. Anonymization refers to the process of concealing whatever information can be identified with users of various areas, for example, web-based business markets, well-being administrations, social media, and others. Considering the fact that the information shared by networking sites based on the Internet is publicly available, it makes them an easy target for de-anonymization attacks to re-identify an individual as a result of the information in such networks. The re-identification rates of a Bumblebee, which is an original social de-anonymization attack is planned and assessed in [13] and the results show a high rate of re-identification with reasonable accuracy, resistance to disorder and as well as better control of blundering. There is a proposal in [14] to propose a de-anonymization attack based on original design that does not require the attacker to have prior knowledge of the attack. Taking advantage of the upgraded AI strategies proposed in this paper, the proposed attack strategy makes use of neighborhood information collected for a multi-jump attack and streamlines the process of de-anonymization. De-anonymization effectiveness of the decrypted file was greatly improved, with a 10* increase in accuracy. It also beat the most advanced decryption attacks in the market by a wide margin.

III. Literature Survey On Image Pixel Degradation Techniques

As mentioned in the Section- I about different types of OSN threats. We observed most of the problems like Cyberstalking, User profiling, Fake profile, De-anonymization, Profile cloning problems caused due to the availability of image data to an anonymous people. Even in a website like google anyone can search any individual and get an image of desired person which fetches from the connected websites. So, we believe an Image Pixel Degradation (IPD) is one of the best approaches to hide the faces of individual in a social networking platform. In this section we are reviewing different IPD research techniques published by different authors.

In 2005, Elaine M. Newton et al., proposed the k-Same algorithm, which is geared toward ensuring de-identified faces cannot be reliably recognized even when other features are preserved, allows face recognition software to be anonymous [15]. In this algorithm, a distance metric determines if two faces are similar and creates the matching faces by averaging image components, which may be pixels or eigenvectors from the initial image (k-Same-Pixel). Putting a person's face set into smaller sets of faces or "clusters" of at least k faces helps protect privacy since members of each cluster are portrayed as aggregate faces instead of their original images. By aggregating homogeneous original faces, each aggregate face minimizes information loss. Finding the most homogeneous clusters-those with the least number of faces-is one concern. This can be done by measuring distance. If one views the vector as a tuple, a face image can also be conceptualized as a point in N-dimensional space. By computing Euclidean distance among points, you can find clusters of nearest neighbors (or faces) by computing the distance between them. If clusters are identified with minimal distance, aggregate face images should be constructed with minimal information loss in mind. Various strategies can be employed. Using N-dimensional (or pixel-wise) "averages," this work constructs an aggregate face from the cluster. The purpose of this process is to test ad hoc techniques in which the identity of a subject is masked through the use of face images. A masking of a face image may appear sufficiently de-identifiable to the human eye. In the experiment, k-Same-Eigen and k-Same-Pixel protected de-identified faces from face recognition software by providing K-anonymity methods. In terms of achieving no better than 50% correct recognition (based on random guessing), K-Same, Blackout, and additive random noise provided equally effective results [15].

In 2006, Ralph Gross et al., proposed a K-Same-M algorithm for privacy protection: to blur facial images similar to previous method [16]. The method works by combining a formal privacy protection model with a model-based face image parameterization. This proposed method includes using the Active Appearance Models (AAMs) as a background model to produce parameterized models, in order to model an individual's face and capture its location in space. In the later stages of the k-Same-M algorithm, the subjected images are used in conjunction with the AAM models to generate a face image described by the models with high accuracy. This means that the related face image generated using the model parameters shows a very closely related appearance to the original face image. k-Same-M algorithm was applied to AAM model parameter vectors to carry out face de-identification in the space of the model parameters instead of the image space. K-Same-M, as the name implies, applies the method of calculating the average of k AAM parameter vectors computed from a set of faces and replacing the vectors with the average of the k vectors. In this paper, a classifier based on Support Vector Machines and Radial Basis Kernels was employed, implemented within LIBSMV algorithm. Further, in their retrospective study, the authors performed 5-fold cross-validation by partitioning the dataset into five subsets not exceeding the same size, training each set independently on four subsets, and testing each set empirically on the fifth subset. The accuracy of classification reported in this study is based on an average of five experiments. They found that the recognition rates p = 2 and p = 4 stay virtually the same in their experimentation. A rank-1 recognition of 40% is also achieved at the relatively high pixelation level of p = 8 despite the relatively high pixelation level. The authors showed how privacy protection and data utility are preserved by using two large-scale datasets [16].

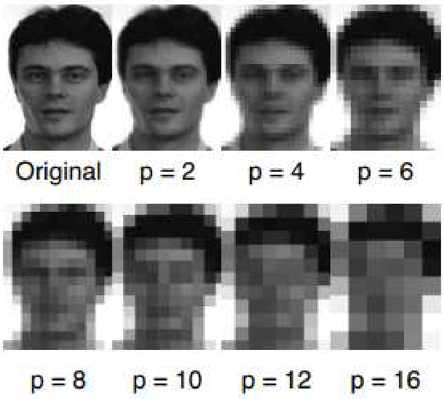


Fig. 2. Pixelated images using K-Same-M from [16]

In 2007, Xiaoyi Yu and Noboru Babaguchi proposed a detailed framework for the implementation of privacy-preserving techniques in real-time video surveillance systems [17]. To accomplish this, a fictitious face (fake face obtained for secrecy) is produced to hide a face (Real face and protected data). This framework proposes an Active Appearance Model (AAM), which enables protected data extraction and recovery, which effectively addresses the enormous payload problem of stowing away security data. To conceal the protected data, an information concealing plan based on quantized record regulations is employed. To prepare the statistical AAM model, the authors analyzed the privacy data. A model is built by combining a lot of face photos and using the training module. A decoded and encoded cycle is followed in this process. During the encoding process, AAM model parameters (privacy data) are acquired by examining an inconspicuous data outline coupled with a facial picture in conjunction with an AAM model which is computed instantly. It is then necessary to save a copy of the model boundaries for possible use later on when stowing away the model. Based on the AAM model boundaries calculated in accordance with the assessment, it is possible to create a veiled face, which is unique with regards to the original face. Finally, a mystery key is used to insert the security data into an unknown edge by using QIM. The data is subsequently retrieved for basic use. To unravel the AAM parameters, the QIM information concealing strategy is first extracted from the QIM parameters. After extracting the parameters and creating an AAM model, the first face can be integrated, and then pressed onto the protective covering edge to recover the outline. Three analyses were performed to evaluate the framework. The main objective of the test was to detect specific annoying AAM parameters related to personality secrecy. Next, we will analyze the presentation of age-related features based on face highlights for nameless data. The last step will be to evaluate the proposed framework [17].

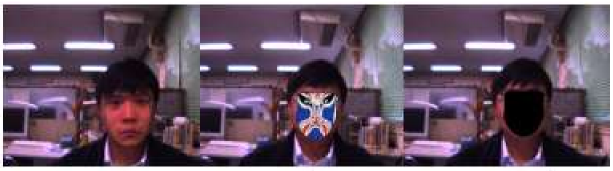


Fig.3. Different types of masked images proposed by [17]

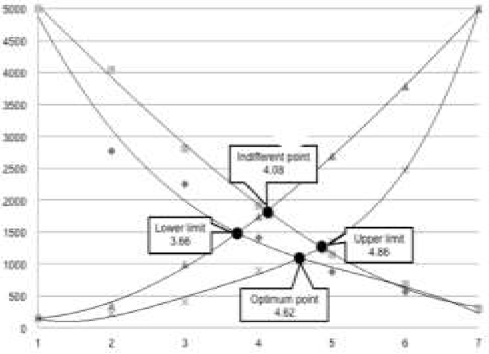
In 2013, Suman Jana et al., proposed a method called DARKLY for managing perceptions of 20 perceptual tasks, such as image recognition, object tracking, surveillance of perimeters, and facial recognition [18]. Applications like this run on DARKLY a modified or only modified version of OpenCV with a minimal performance overhead when compared with native OpenCV. The system has been developed using the Darkly server which combines with OpenCV, the IBC virtual machine, and the GUI. In terms of how DARKLY works, it has two elements, a trusted server that operates locally and a trusted client that is hosted remotely. DARKLY's privacy service uses a novel approach that consists of multiple layers of security: access control, algorithmic transformation, and user auditing. On the one hand it permits applications to manipulate perceptual inputs without directly interacting with them, on the other hand it replaces raw perceptual inputs with opaque references. Two other considerations arise from the fact that certain applications, such as surveillance cameras and object trackers, require access to the perceptual inputs at a high level. OpenCV functions are designed to capture the minutiae surrounding image processing as a whole, freeing applications from the problem of requiring access to raw image data. Additionally, this helps DARKLY to integrate privacy protection in a natural and secure manner. In order to prevent applications from directly accessing raw images, DARKLY replaces pointers to raw data with opaque references that cannot be decoded or redirected by applications. Analyzed on the Color FERET database, the proposed cluster–morph algorithm groups the "closest" images of an image in a cluster by k * 1 based on eigenfaces. De-identified versions of faces from the input database are the averages of all faces from their cluster [18].

In 2014, Liang Du et al., proposed a simple and effective framework, named GARP-Face, that balances utility preservation in face de-identification [19]. The authors of this model employed modern facial analysis techniques to analyze facial images and to determine the Gender, Age, and Race attributes of the images, while preserving these attributes by searching for representations of these attributes from an existing gallery dataset. Face de-identification is a transformation that is used in the facial recognition process to convert a normal image into a blurred image in order to enhance the accuracy of the algorithm. Furthermore, privacy gain and utility loss parameters were used to evaluate the algorithm. Later they used the proposed GARP De-identification algorithm which consists of Utility determination, Utility-specific AAM model and diverse face gallery. A utility-specific model is applied to a query face based on the training of classifiers for selected attributes. Rather than using a general face model to capture faces and utility characteristics, authors proposed to use AAM (Active Appearance Model) for building an attribute-specific model of faces. It is used both to train the AAM models and to train the attribute classifiers, both of which use a large and diverse face gallery. A further consideration is that the surfaces are generated from G as far as is possible, depending on which utility class should be used to de-identify the face [19]. The proposed approach is evaluated using the MORPH dataset, with a comparison to several state-of-the-art de-identification solutions of the time. Below are the results of three different de-identification algorithms and their comparison.

TABLE II. COMPARISON BETWEEN THREE DIFFERENT ALGORITHMS

I	k-same	Gen. AAM	GARP-Face
Race	0.4818	0.3727	0.0897
Gender	0.1469	0.3139	0.1372
Age	0.3606	0.4056	0.0878
Combined	0.4897	0.5106	0.1173

n 2015, Yasuhiro TANAKA et al Proposed a PSM (Price Sensitivity Measurement) system to find a relationship between willingness to share photos and preferred level of photo blurring for privacy protection. Using the PSM, the upper and lower levels of the price range is defined [20]. A lower price limit which is considered to be the point at which consumers are not likely to consider a purchase. This is because they doubt that the product or service is of acceptable quality. A price that would be considered too high by a consumer and prevent him or her from making a purchase is the upper price limit. Similarly, to what was initially mentioned, the authors experimented with finding the right balance point between revealing private information and ensuring their photographs were blurred to a preferred degree using PSM. Using two types of social media services, with and without access restrictions by PSM, the authors analyzed the relationship between willingness of blur photos and desired level of blurring photos. Media that has restricted access to social media is defined as media that can only be accessed by a few select colleagues or friends. Unlike the "Social Media Services without Access Restriction" described above, "Social Media Services without Access Restriction" are media that are shared completely publicly.



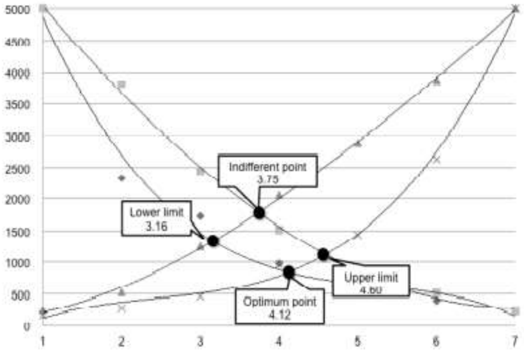


Fig.4. With and without access limitation using polynomial curves [20]

Four intersecting points were considered in the study: a sensitive point representing the individual's willingness to share their data, an indifferent point, which represents the freedom of sharing, a lower limit that affects the target person's privacy to an extent, and finally, an upper limit regarding how distorted the data is. They used polynomial approximate curves to calculate these intersecting points in order to clarify them. It can be concluded from a comparison of the upper limits of each intersection between the social media with/without access limitations (=0.26) that the difference is smaller than the difference between optimum points (=0.50) and lower limits (=0.5). There was only a small difference of upper limits regardless of whether access limitations were used or not. Meanwhile, privacy concerns could be affected by access limitations, which might have an impact on privacy concerns. Thus, depending on the audience to whom you wish to share your photos on social media, you may prefer a different degree of blurring of the photos. As shown in fig4, the comparison between social media types can be seen below [20].

TABLE III. COMPARISON BETWEEN WITH AND WITHOUT ACCESS LIMITATION VALUES

	With access restrictions	Without access restrictions	difference
Lower limit	3.16	3.66	0.50
Indifferent point	3.75	4.08	0.33
Optimum point	4.12	4.62	0.50
Upper limit	4.60	4.86	0.26
Acceptable range	3.16=<W=<4.16 1.44	3.66=<W=<4.86 1.20	0.24

In 2016, Jun Yu et al., proposed a system called iPrivacy which automates the privacy setting process and releases the burden from users [21]. Specifically, this framework involves the following stages: (a) a huge dataset of social photographs and their protection settings are analyzed to understand object security relatedness in a valuable way, and to automatically categorize a large number of privacy-sensitive objects. (b)The second concept is the development of hierarchical deep multi-task learning, which jointly learns more representative deep CNNs and a more discriminative tree classifier over visual data. (c) automatic security system settings recommendation, and (d) automatic obscuration of privacy-sensitive objects provides image security assurance. Using conditional random fields and deep CNN models, they segmented every image into semantic objects. The CNN was trained to enable pixel-level expectations and arrangements [21]. Next, they utilized a CRF model to determine how to produce semantic article locales based on neighbor pixels for a similar item class. A picture security setting is allocated unequivocally to each of the picture classes after division. Using a similar group of pictures, the security settings were combined into a short summary of default security settings. This is based on the frequency of events that were shown in the pictures. In that case, the security settings are adjusted for the entire group of users based on the events that occur more frequently. A second stage is proposed in which the framework is to give the protection-sensitive classes obtained during the first stage a powerful association. To achieve this, a visual tree T = (V, E) is constructed, which contains a bunch of hubs V and a bunch of edges E. In addition, for each non-leaf hub C * V there are a bunch of security touchy item classes L(c) * [1, 2, 3, . . . M] which are subsets of the parent hub. By arranging the protection-sensitive items into coarse-to-fine categories, this tree facilitates the learning of discriminative tree classifiers through deep multi-task learning (HD-MTL). To accomplish quick and precise detection of huge quantities of vulnerable articles, the third stage in this framework is to apply both the tree classifier and the deep CNNs in tandem to the visual tree [21]. Eventually, in the fourth stage of this framework, it is to identify the security sensitive content from the pictures that are being shared, perceive their categories, and identify their privacy settings for sharing pictures. Once the tree classifier and the deep CNNs have been developed, they are then used to predict the identification of items (object classes) in a picture, i.e., figuring out the best-matching security sensitive article class associated with the image. HD-MTL and HD-CNN calculations achieved accuracy of 92% and 87%, respectively [21].

This research was published in 2018 by Zhongzheng Ren et al., who proposed a new principal approach for learning a video face anonymizer [22]. They used an adversarial training scenario in which two competing frameworks battled each other: (1) a video anonymizer that adjusted the first video to eliminate privacy sensitive data while still trying to increase spatial activity identification performance, and (2) a discriminator that attempted to remove privacy sensitive data from the anonymized recordings. They used a dataset which consists of videos and photos for training purpose to train face modifier and simultaneously they trained an action detector to persons actions then it is formulated for multi task learning. In this formulation process for action detection loss authors used four different losses are added and fed to Fast-RCNN for classification and regression. For face classification they used adversial classification. For face detection the have used a SSH face detection on video dataset and observed more false positives in order to mitigate the false positives they increased the probability to 0.8 and fed the rest to MTCNN algorithm which uses a binary classifier. For face modification they used 256x256 resized images and fed through Perceptual losses for real-time style transfer feed forward networks. The authors used Faster-RCNN with ResNet-101 for spatial action detection and train the network from the beginning to the end, after which the images were again resized to 600 x 800. Sphere network was later used to classify faces. This classification algorithm produced a 95.75 percent accuracy rating. When modified LFW faces are used, the accuracy is only 66.35%. Despite being "fooled" by the modified faces, the classifier is still able to accurately identify the original images [22].

This paper presented Chih-Hsueh Lin et al., a method to de-identify images of faces using thermal features extracted from thousands of images using Deep Learning [23]. To enhance the fine-tuning of expectation precision and deidentification of crude faces, this study aims to develop a thermographic-based face recognition strategy. Convolution neural networks, together with vector machines that perform supporting calculations, are at the heart of this engineering. During this exploration, the dataset was further divided into 3 sections, namely the validation, training, and test dataset sections. The 3 expectation models are composed for different purposes, as shown by the information that is provided. Having defined the crude RGB picture and the warm picture, the next step would be to describe the component picture derived from the propose include extraction technique, and the third step would be to describe the element network. A total of 7500 warm images were collected first from a variety of subjects using the FLIR One warm camera. Further, they resized and cropped the image, and extracted the component framework, which offered two features consisting of the picture and element. There is one RGB picture among those four, and the rest are resized to 240x240 to facilitate deep learning using picture handling methods. On the basis of resized photographs, later milestone work identifies and marks the focus of facial components (C. - H. Lin, 2020). The NVIDIA Deep Learning GPU Training System (DIGITS) is utilized for executing a profound learning all-inclusive profound learning improvement stage. For example, DIGITS oversees information concerning multi-GPU frameworks and plans and integrates neural organizations according to normal profound learning undertakings. For the purpose of this analysis, arbitrary backwoods are utilized in order to determine the face recognition of the members based on the quality of the woods. As a result of the tests, RGB pictures had a precision of 0.834, component pictures had 0.953, and include lattice had 0.967 [23]. Highlight extraction technique can be used to deliver element pictures and component grids that can be used to execute better forecasts [23].

After all the research, it can be identified that there is a problem in achieving high recognition accuracy which leads to produce best results. Using of more effective algorithms to achieve high accuracy in image recognition as well as in image degradation can produce better results.

CONCLUSION

Privacy and security of data are some of the main concerns of this research. There are various types of threats OSN users face. The proliferation of social networking sites has led to an increase in information sharing. Nowadays even though various online social networks use proactive security monitoring technology to ensure the safety of their users against cyber-attacks, cyber criminals continue to find new methods to engage in malicious activities. This includes hacking computer systems, phishing, identity theft, and cyber bullying to name a few. When it comes to determining how to combat potential data protection threats, it is of the utmost importance to understand their impact on any aspect of our lives. In order to do this, you need to understand why, how, and who are the perpetrators. Additionally, we examined different image pixel degradation/blurring techniques proposed by different researchers for the anonymization of private photos and videos in the study.

REFERENCES

[1] "Adhikari, Abhijit, and Shital D. Bachpalle. "Survey: evaluation study of privacy conflicts in osns." International Journal of Emerging Technology and Advanced Engineering 3.11 (2013).".

[2] "Almarabeh, Hilal, and Amjad Sulieman. "The impact of cyber threats on social networking sites." International Journal of Advanced Research in Computer Science 10.2 (2019).".

[3] A. Ahmed, "digitalinformationworld," 02 06 2021. [Online]. Available: https://www.digitalinformationworld.com/2021/06/new-report-shows-most-used-social-media.html.

[4] "Fuchs, Christian, and Daniel Trottier. "Towards a theoretical model of social media surveillance in contemporary society." (2015): 113-135.".

[5] "Burke WinkelmAn, Sloane, et al. "Exploring cyber harassment among women who use social media." Universal journal of public health 3.5 (2015): 194.".

[6] "Heatherly, Raymond, Murat Kantarcioglu, and Bhavani Thuraisingham. "Preventing private information inference attacks on social networks." IEEE Transactions on Knowledge and Data Engineering 25.8 (2012): 1849-1862.".

[7] "Nowson, Scott, and Jon Oberlander. "The Identity of Bloggers: Openness and Gender in Personal Weblogs." AAAI spring symposium: Computational approaches to analyzing weblogs. 2006.".

[8] "Ali, S., et al. "User profiling: a privacy issue in online public network." Sindh University Research Journal-SURJ (Science Series) 49.1 (2017).".

[9] "Bolton, Richard J., and David J. Hand. "Statistical fraud detection: A review." Statistical science 17.3 (2002): 235-255.".

[10] "Torabi, Sadegh, and Konstantin Beznosov. "Privacy aspects of health related information sharing in online social networks." 2013 USENIX Workshop on Health Information Technologies (HealthTech 13). 2013.".

[11] "Wani, Mudasir Ahmad, and Suraiya Jabin. "A sneak into the Devil's Colony-Fake Profiles in Online Social Networks." arXiv preprint arXiv:1705.09929 (2017).".

[12] "Vishwanath, Arun "Why do so many people fall for fake profiles online." The Conversation (2018).," [Online]. Available: https://phys.org/news/2018-09-people-fall-fake-profiles-online.html.

[13] "Gulyás, Gábor György, Benedek Simon, and Sándor Imre. "An efficient and robust social network de-anonymization attack." Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society. 2016, pp. 1-11".".

[14] "Lee, Wei-Han, et al. "Blind de-anonymization attacks using social networks." Proceedings of the 2017 on Workshop on Privacy in the Electronic Society. 2017.".

[15] "Newton, Elaine M., Latanya Sweeney, and Bradley Malin. "Preserving privacy by de-identifying face images." IEEE transactions on Knowledge and Data Engineering 17.2 (2005): 232-243.".

[16] "R. Gross, L. Sweeney, F. de la Torre and S. Baker, "Model-Based Face De-Identification", Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06), 2006, pp. 161-161, doi: 10.1109/CVPRW.2006.125.," 2006.

[17] Yu, Xiaoyi, and Noboru Babaguchi. "Privacy preserving: hiding a face in a face." Asian Conference on Computer Vision. Springer, Berlin, Heidelberg, 2007..

[18] "S. Jana, A. Narayanan and V. Shmatikov, "A Scanner Darkly: Protecting User Privacy from Perceptual Applications," IEEE Symposium on Security and Privacy, 2013, pp. 349-363, doi: 10.1109/SP.2013.31.," 2013.

[19] "L. Du, M. Yi, E. Blasch and H. Ling, "GARP-face: Balancing privacy protection and utility preservation in face de-identification," IEEE International Joint Conference on Biometrics, 2014, pp. 1-8, doi: 10.1109/BTAS.2014.6996249.".

[20] "Tanaka, Yasuhiro, et al. "Relationship between willingness to share photos and preferred level of photo blurring for privacy protection." Proceedings of the ASE BigData & SocialInformatics 2015. 2015. 1-5.".

[21] "J. Yu, B. Zhang, Z. Kuang, D. Lin and J. Fan, "iPrivacy: Image Privacy Protection by Identifying Sensitive Objects via Deep Multi-Task Learning," in IEEE Transactions on Information Forensics and Security, vol. 12, no. 5, pp. 1005-1016, May 2017, doi: 10.".

[22] "Ren, Zhongzheng, Yong Jae Lee, and Michael S. Ryoo. "Learning to anonymize faces for privacy preserving action detection." Proceedings of the european conference on computer vision (ECCV). 2018.".

[23] "Lin, Chih-Hsueh, Zhi-Hao Wang, and Gwo-Jia Jong. "A de-identification face recognition using extracted thermal features based on deep learning." IEEE Sensors Journal 20.16 (2020): 9510-9517.".