Kids security on social networks by face blur technique

V Mladenovic¹, S Djukanovic¹, N Stefanovic¹, A Kar², M Jovanovic³, S Makov⁴

¹Faculty of Technical Sciences in Cacak, University of Kragujevac, Serbia
²Indian Institute of Information Technology, Design and Manufacturing, Kancheepuram, Chennai, India,
³Faculty of Electrical Engineering, University of Nis, Serbia
⁴Don State Technical University, Shakhty, Rostov region, Russia

Abstract. This article deals with increasing security and children protection under the age of 16 (underage) on social networks with photo content such as Facebook, Instagram, Twitter, and similar. Particularly, the emphasis is placed on the official sites of public institutions on Facebook, such as kindergartens, primary and secondary schools, and all institutions dealing with children. One of the source key issues is the ability to track these public pages by malicious visitors. The main point is the developed algorithm that analyzes any photo, recognizes kid(s), and blurs it during the upload photo onto the page of the social network. The complete procedure for processing is shown and performed testing, verification, and validation.

1. Introduction
Today, a large number of social networks exist where users can leave their photos without paying attention to where those photos may end up. Special attention is not paid to who can use these photos, and we can freely say - to misuse them. Typical examples of such social networks are 23snaps [1], Facebook [2], Instagram [3], Flickr [4], Fyuse [5], Tagged [6], Vingle [7], Virb [8]. Nowadays, many parents are too busy with jobs, and their children are left to the technologies that are available. Children still cannot distinguish between good and bad things, between good and bad intentions. Simply put, children are exposed to all the challenges on the Internet. On the way, children become like "digital natives" and begin to use the Internet at an early age and access it from various devices (computers, tablets, mobile phones). Usually, younger children use the Internet for entertainment (playing games, listening to music, watching videos, series, movies), while older children mostly use social networks [9]. Social networks have millions of users the number is increasing daily [10, 11]. Precise statistics on the number of children on the Internet have not yet been given precisely, but even that number is not negligible.

In the forest of social network users, one of the main dangers for children lurks from sexual predators. Their intentions are always with bad consequences for the children, and they use the methods that are various to get in touch with the child and turn him into a victim. For all activities that children perform on the Internet, such as surfing, chatting, using social networks, online games, child protection implies physical, mental, and moral safety of minors. This becomes one of the potential major threats to the child's identity, and perhaps to his life. In particular, this becomes more pronounced in a time of pandemic because few people pay attention to the activities of children who now spend much of their time in a closed environment. Despite ongoing commitments, it is easy to conclude that most of the time children spend in front of the computer.
This paper deals with one of the methods that can prevent child abuse on the Internet. The method involves preventing the possibility of a potential predator following a child through a social network through children's photos on the child's pages.

This paper is organized as follows. In section 2 the motivation for this paper is described. Section 3 provides what is problem statement and state-of-art. Complete algorithm, testing and results are presented in section 4.

2. Motivation

As already mentioned, the main goal of this paper is to develop a system that will increase the security of kids on social networks. The greatest aspiration of children on social networks is to be as visible as possible to the outside world, to present and popularize. Children do this by posting photos, videos, liking various information, and similarly. Getting in touch with other people is the next step in using social networks. Social networks allow you to connect with other people so that the child can get in touch even with an unknown person. There is a possibility that a malicious person or an internet predator is hiding behind that unknown person, who may have the profile of another child. By coming into contact with such a person, the child is introduced into a conversation, and ignorance of behavioral control mechanisms [12] can lead to challenges that can be fatal. On the other hand, an unknown person can make contact with the child on his/her own by making the first contact by praising the photos previously posted by the child, which makes the communication scenario similar. In this sense, this paper presents a model and algorithm to perform prevention for posting photos on social networks by a child by blurring photos. Then an unknown person will be able to see the photos, but the faces of children under the age of 16 will automatically be hidden (blurred). In order to see the full format of the photo, the algorithm identifies the location from which the child's profiles are accessed and asks the visitor to reveal their identity.

3. Problem statement and related work

3.1. How internet predators work?

There is no one and unique single method in which online predators work. But there are several methods that can have been identified as how online predators locate their victims and get them to do what they want, whether it is meeting them in person or simply engaging in some kind of online/on the phone sexual activity [13]. These are some typical methods online predators use: Find kids through social networking, blogs, chat rooms (even monitored, kids chat rooms), instant messaging, e-mail, and other Web sites, often using information in their targets’ personal profiles. Seduce their targets through attention, flattery, affection, kindness, and even gifts. These types of manipulation will cause kids to lose their sense of awareness, and help the predators to get from bad intentions to sexual exploitation (this is called “grooming”, and may continue over extended time periods). Are familiar with the latest music, hobbies, fashion, etc. that are likely to interest kids. Look for children that are emotionally vulnerable due to problems at school or home. Listen to and sympathize with kids’ problems, while building a pseudo friendship, taking the kids side vis-à-vis their parents or teachers. Gradually introduce sexual content into conversations or show sexually explicit material that may even involve children engaging in sexual activity – in order to convince kids that this type of behavior is acceptable. If the victim tries to cut off communication, predators scare the victim into continuing the relationship by convincing them that they will tell their parents what they have been doing online and that they have viewed pornographic pictures, etc. May impersonate other youths in order to convince minors to meet with them [13].

3.2. Age recognition based on faces

One of the key phases of this algorithm is a method for identifying a person’s age based on a photograph. There are currently several methods that give results with some accuracy. For each of them, a certain database of photographs is used in order to perform an age assessment. A longitudinal study of automatic face recognition uses two large databases of photos, PCSO LS with 147784 images of 18007 subjects, average 8 images per subject over average 8.5 years, and LEO LS with 31852 images of 5636 subjects,
average 6 images per subject over average 5.8 years). Each subject has at least four faces [14]. Paper [15] proposes a 3D facial aging model and simulation method for age-invariant face recognition. This method models from 2D to 3D domain and gives the additional capability of compensating for pose and, potentially, lighting variations. In paper [16] a wavelet transform is proposed to extract the face features and an Adaptive Resonance Theory for classifying age groups. The authors were trained neural networks with FG-NET images of different age groups and about 94.28% of images were grouped correctly. The study in [17] emphasis the significance of face recognition on social networks and addresses to development of techniques based on big data analytics, machine learning, etc.

In this paper, we use The Wolfram Neural Net Repository [18]. This is a public resource that can be used for evaluation, training, visualization, transfer learning, and more. More precision, we use the trained neural network in the model of “Age Estimation VGG-16 Trained on IMDB-WIKI Data”. The neural network is trained using the concept of deep learning. The convolutional neural network (CNN) uses VGG-16 architecture and The IMDB-WIKI dataset is used with 460723 images in IMDb, and 62328 images in Wikipedia [19].

3.3. Face blur technique

Blur technique is an integral part of well-known commercial professional software packages such as Adobe Photoshop, Premiere or After Effects, YouTube's face blurring tool, Wondershare Filmora, Skitch, Blur and Mosaic, Movavi, KineMaster. The Blur Technique blurs the pixels so that the image begins to lose detail. In this way, the image becomes blurred and it is not possible to recognize details in the parts covered by blur. Some of the most famous blur techniques are Gaussian Blur, Lens Blur, Motion Blur, and Blur Filter. In this paper, we use the blur technique to blur children's faces.

4. The algorithm development, testing and results

The complete algorithm’s roadmap is shown in Figure 1. In order to perform operations, it is necessary to fulfill the condition that there must be at least 3 people in each photo, one of whom must be younger than 16 years. On the other hand, the tested images are not of the same resolution, but the lowest resolution is 320×320. The algorithm starts by uploading a photo (a). The next step is to detect faces in the picture and put them in a frame, ie. to separate from the photo (b). After detecting and extracting faces, they are sent to an artificial neural network that has been pre-trained with a photo dataset where comparisons are made with other faces (c). As a result of this phase (c), an age is identified for each person sent. Thus, persons in the phase (d) were identified as having 45, 41, 7, and 10 years of age. U istoj fazi provera se vrsi koje je lice ima 16 godina ili je mladje. Kada se to uradi takvim licima se vrsi automatsko zamagljivanje lica. At the same phase, the check is performed on which person is 16 years old or younger. When this is done, such faces are automatically blurred (e). Finally, the processed photo is automatically uploaded and placed on the user's page, ie the child's page.

Figure 1. Algorithm’s roadmap of face blur technique
Figure 2 shows the distributions with which the probability of age identification was performed for each person in the photo.

5. Discussion
Many algorithms, developed as tools or toolboxes, aim to prevent children's activities by blocking their requests on the Internet. Basically, these add-ons are installed on user accounts, in this case these are kids, and block access to certain content or introduce parental controls. Such add-ons have been developed by companies such as Kaspersky [20]. For now, the world's greatest focus is to educate, which aims to guide children to all the challenges on the Internet and warn parents of the possible consequences [21]. With our method, we exclude the participation of parents, the child can work freely on the Internet, post their photos and content, and for that get protection from malicious visitors. Of course, all this includes mechanisms that record the attempt to access the content that children previously set, the content is protected automatically during upload, and in order to fully access the visitor must be personally identified and automatically revealed via the Internet location from which he accesses.

6. Conclusion
This paper deals with an algorithm that should prevent unwanted visitors from children and endanger their safety through social networks. This prevention is done by protecting the image, which the child places on his page, by blurring the faces of all persons aged 16 and younger. Modules that perform face isolation, face identification, and age assessment were tested.

References

[1]  https://www.23snaps.com
[2]  www.facebook.com
[3]  https://www.instagram.com/
[4]  https://www.flickr.com/
[5]  http://fyu.se/
[6]  https://secure.tagged.com/
[7]  https://www.vingle.net/users/sign_up
[8]  http://www.virb.com/
[9]  M. Stevanović, A. Mitovski, D. Živković, S. Živković, A. Mladenović, S. Vasković, “Internet habits of school-age children in some villages of Bor municipality,” Sinteza 2014 - Impact of
the Internet on Business Activities in Serbia and Worldwide, Belgrade, Singidunum University, Serbia, 2014, pp. 351-355, doi:10.15308/sinteza-2014-351-355

[10] https://www.socialmediatoday.com/news/facebook-reaches-238-billion-users-beats-revenue-estimates-in-latest-upda/553403/

[11] https://www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/

[12] Li L. (2017) Behavior Analysis in Social Networks. In: Alhajj R., Rokne J. (eds) Encyclopedia of Social Network Analysis and Mining. Springer, New York, NY. https://doi.org/10.1007/978-1-4614-7163-9_110198-1

[13] https://www.puresight.com/Pedophiles/Online-Predators/how-do-online-predators-operate.html

[14] L. Best-Rowden and A. K. Jain, "Longitudinal Study of Automatic Face Recognition," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 40, no. 1, pp. 148-162, 1 Jan. 2018, doi: 10.1109/TPAMI.2017.2652466.

[15] U. Park, Y. Tong and A. K. Jain, "Age-Invariant Face Recognition," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 32, no. 5, pp. 947-954, May 2010, doi: 10.1109/TPAMI.2010.14.

[16] J. Nithyashri and G. Kulanthaivel, "Classification of human age based on Neural Network using FG-NET Aging database and Wavelets," 2012 Fourth International Conference on Advanced Computing (ICoAC), Chennai, 2012, pp. 1-5, doi: 10.1109/ICoAC.2012.6416855.

[17] Shahabadkar R., Sai Satyanarayana Reddy S. (2019) An Integrated Schema for Efficient Face Recognition in Social Networking Platforms. In: Silhavy R. (eds) Software Engineering and Algorithms in Intelligent Systems. CSOC2018 2018. Advances in Intelligent Systems and Computing, vol 763. Springer, Cham. https://doi.org/10.1007/978-3-319-91186-1_9

[18] https://resources.wolframcloud.com/NeuralNetRepository

[19] R. Rothe, R. Timofte, L.V. Gool, Deep expectation of real and apparent age from a single image without facial landmarks, International Journal of Computer Vision, Vol. 126, number 2-4, pages 144-157, 2018, Springer

[20] https://www.kaspersky.com/safe-kids

[21] https://www.cyberwise.org/online-security-hub