УДК 351.321

Tsomko Elena,
Ph.D, Assistant Professor,
Multimedia Department,
Namseoul University, Republic of Korea

A LOOK INTO A FUTURE: SMART CYBER COMMUNICATION, ON A PHOTO PRIVACY ISSUE

Annotation. Once the technologies started to develop rapidly, it is still impossible to control totally all the spheres, especially where it involves internet, P2P, M2M and other kinds of communications. Hackers can easily get into your computer through the internet and you may not even be able to notice it, somebody can upload a photo or video of yours to the social network which you actually would not like for other people to see at all. How to protect ourselves in this new cyber world which has crashed into our lives and keeps us strained for being always careful and checking time to times if there any visual information of us has been uploaded into a web. In this paper we introduce the suggestion of how the existing technologies could be combined together, so that at least one part of the privacy issues (in this paper we will talk about photographs) could be solved for our future internet communication. The main idea of our new propose is that a person no longer needs to control the people who hold the photos with him, but internet will control it. No watermarking technologies will be employed here. Everything is going to be processed online based only on the real time perceived data and processing it.

Keywords: Photo privacy, secure uploading, social networks.

Цомко Елена,
доктор філософських наук по
спеціальності безпека і управленіння
інформацією, асистент професора
факультету Мультимедіа,
Намсоул Університет (Республіка Корея)

ПОГЛЯД У МАЙБУТНЄ: «РОЗУМНИЙ» ОБМІН ІНФОРМАЦІЄЮ У КІБЕР ПРОСТОРІ, ПРОБЛЕМА ЗАХИСТУ ПРИВАТНИХ ФОТОГРАФІЙ

Анотація. З тих пір як технології стали розвиватися прискореними темпами, ми не встигаємо контролювати їх у всіх сферах, особливо якщо це стосується інтернету, P2P, M2M та інших за допомогою зв'язку. Хакери можуть легко проникнути у ваші комп'ютери через інтернет, і ви можете навіть не помітити цього. Хтось може завантажити в соціальну мережу ваше фото або відео, які ви вже точно не хотіли б робити доступними для сторонніх очей. Як нам захистити себе в цьому новому кібер просторі, який увірвався в наше життя і тримає нас у напрузі, змушуючи постійно бути обережними і перевіряти час від часу витік особистої візуальної інформації у всесвітню мережу. У даній статті ми пропонуємо ідею про те, як об'єднати існуючі технології для вирішення принаймні однієї частини проблеми захисту приватної інформації (в нашому випадку йдеться про фотографії) для майбутнього спілкування в інтернеті. Головна ідея нашої пропозиції полягає в тому, що користувачам більше не потрібно контролювати фотографії з їх зображенням, що знаходяться у сторонніх,

інтернет сам буде їх контролювати. Немає необхідності навіть задіяти технології «водяних знаків». Весь процес відбуватиметься в режимі реального часу, ґрунтуючись тільки на даних, отриманих в поточний момент.

Ключові слова: фото конфіденційність, безпечний обмін інформацією, соціальні мережі.

Цомко Елена,
доктор философских наук по
специальности безопасность и
управлениння информации, ассистент
профессора факультета Мультимедиа,
Намсоул Университет (Республика Корея)

ВЗГЛЯД В БУДУЩЕЕ: «УМНЫЙ» ОБМЕН ИНФОРМАЦИЕЙ В КИБЕР ПРОСТРАНСТВЕ, ПРОБЛЕМА ЗАЩИТЫ ЧАСТНЫХ ФОТОГРАФИЙ

Аннотация. С тех пор как технологии стали развиваться ускоренными темпами, мы не успеваем контролировать их во всех сферах, особенно если это касается интернета, P2P, M2M и других посредств связи. Хакеры могут легко проникнуть в ваши компьютеры через интернет, и вы можете даже не заметить этого. Кто-то может загрузить в социальную сеть ваше фото или видео, которые вы уж точно не хотели бы делать доступными для посторонних глаз. Как нам защитить себя в этом новом кибер пространстве, который ворвался в нашу жизнь и держит нас в напряжении, заставляя постоянно быть осторожными и проверять время от времени утечку личной визуальной информации во всемирную сеть. В данной статье мы предлагаем идею о том, как объединить существующие технологии для решения по крайней мере одной части проблемы защиты частной информации (в нашем случае речь идет о фотографиях) для будущего общения в интернете. Главная идея нашего предложения заключается в том, что пользователям больше не нужно контролировать фотографии с их изображением, находящиеся у посторонних, интернет сам будет их контролировать. Нет необходимости даже задействовать технологии «водяных знаков». Весь процесс будет происходить в режиме реального времени, основываясь только на данных, полученных в текущий момент.

Ключевые слова: фото конфиденциальность, безопасный обмен информацией, социальные сети.

Introduction. Nowadays, almost everyone deals with the technologies which just about 40-50 years ago were seemed to be impossible. For example, we can talk to a friend who is in another part of the continent seeing him perfectly by means of just the computer with the web-camera or even mobile phone which supports video call. We have world-wide famous social networks where anyone can post comments to anybody and can upload/download some photos/videos of himself or others. We can access the public cameras in other countries which are installed in some famous places and see what is going on there in real time. These all are just a few examples of what the couple of generations before ours could only think of as a fantasy.

But let us have a look at what we get along with all these new features of the human progress. **Table 1** shows briefly the difference in how some stranger could reach some person at the earlier days and how it is possible nowadays. Of

course, we all agree that nowadays it gets much easier to communicate with anybody you need or you would like to keep in touch with. But does this progress bring only comfort to our life? Yes, it is comfortable that you do not have to go to another city or even country to visit your friends, to see them and to talk live to them. You don't even need to spend much money for the intercity/international calls. All you need these days is just a computer, web-camera and internet (with moderate price which is much cheaper than international calls by land phone).

Table 1. Examples of reaching the person in earlier days and nowadays

period / action	before 90-s	from 90-s to nowadays
a random stranger can communicate with you	if seeing you personally or knowing your address (for mails) or phone number (to call)	
		through the e-mail, homepage, forums, etc.
a random stranger can see you	if seeing you personally or seeing the photos' hard copies or videos of you which are held by somebody else	
		the photos/videos in your/ somebody's homepage, some forums, websites or even at some spamming flash-banner
a random stranger can hear you	if being around you, or calling you or listening to the tape-recorded voice of yours	
		online through the messenger's calling or in the video clip at some website

By means of online communication, we can not only talk to friends but also share some visual information with them, for example send recent photos or videos. And here is the place where the issue comes. When we share the photos with somebody through the internet, sometimes other people are also depicted there, and who knows what these people think about those photos and would they want others to see them or not.

Recently, the internet privacy issue had become a hot topic all over the world. To be more precise, let us refer to its definition stated, for example, in wiki [1], "**Internet privacy** involves the right or mandate of personal privacy concerning the storing, repurposing, provision to third parties, and displaying of information pertaining to oneself via the Internet. Internet privacy is a subset of computer privacy. Privacy concerns have been articulated from the beginnings of large scale computer sharing." So, it is mentioned here about the control over the private information about somebody. But are we really able to control it as we want? No! Nothing can prevent a user to download somebody's photo from his homepage (even if access for saving the target is disabled, Print Screen option is still there) and upload it on another website. Even worse cases do

happen these days, where a user can take a photo, process it, for example, in Photoshop and upload the nude photo of somebody to the public website. What about our friends? We are sure that many people have the situations when during hanging out with friends, somebody takes pictures and then posts them into the social networking site, e.g. Facebook. And next day when you find the photos on your "friend's" page you are quite disappointed with how you look there or maybe do not want other people to see you at all. How many friendships had been broken because of such or similar situations, how many couples had separated thanks to the private information leaked into the cyberspace! Another example of privacy infringement can be a case where, let's say, some dating agency takes the photos of the married couples from some "couples forum" and put them into its own homepage saying that their firm had united those people, though the people on the photos have never had any relation to that agency!

Of course, somebody can say that if you don't want to get in such traps, don't post your photos, don't take pictures with friends, use modern technologies for your photos like watermarking, and so on. But if thinking so, then why do we develop the socializing culture in cyber world? Because people like to communicate, sometimes they want to share some moments of their life, and this is their right, along with the right to control which personal information and where should be open for public.

Most of the cases mentioned above can usually be solved post-factum, when the sufferer addresses to the uploader directly (if this is a friend or a person whom he may know) or by filing a sue against the infringer. However, the information had already been leaked and sometimes it can be that the reputation is discredited significantly. But how to prevent such cases in advance, so that a user can still upload his own photos on the preferred website but nobody else would be able to use this photo for other purposes. Or how to control a friend who takes the photos by his own camera and uploads them into a website and make him unable to upload the photos of other people depicted there?

In this paper we will introduce the idea on how to let users control which of their photos are going to be uploaded, where and by whom. In section 2 we will review some works that have been done in order to try resolving this hot issue. Section 3 will show detailed explanation of the method proposed here. In section 4 we will discuss about reliability and necessity of the Smart Secure Uploading technique, and section 5 will conclude this paper.

Related work. If we search for available techniques that already introduce some methods to strengthen our privacy issues we can find a few. For example, Burghardt et. al. [2] suggested PRIMO which is privacy aware image sharing system, including semantic annotations, automated face detection and recognition, automated conflict detection and interoperability. Once a user wishes to be aware of his photo uploaded into the web, he needs to open his account, make a contact list and training data. Contact list should include all

personal contacts of a user, whether or not they are friends, and training data should have at least 5 photos of a user for better recognition of his face in various images. However, does this system work if somebody from not a user's contact list wishes to upload a photo? Or what if a user's face has changed significantly? PRIMO also provides an option where a user can select in which cases to alarm him (for example if there is a photo of him with another person), but again, what if a single photo with him is processed and uploaded showing him as being nude?

Another technique, proposed by Newton et. al. [3] is about preserving privacy by de-identifying face images. Their method suggests that even if many facial details are preserved, the face still would be impossible to be recognized by existing facial recognition systems. This method helps those who do not want to be recognized from the public videos of surveillance systems, where one can identify a face comparing it with, for example, faces from the database with the driving license photos.

Yuksel et al. [4] suggested an API which provides grouping of friends through an automated system into different social groups by analyzing the user's social graph and depending on what common information they would like to share that should not be accessed by other friends. However, situation can change rapidly when a friend can be no more the one, but system would not know about it yet. And this system does not protect us from being exposed on the photos taken by other users and uploaded on their homepages or other online resources. Besmer A. and Lipford H.R. [5] also performed a research among the social networks users and concluded that majority of them would wish to have an ability to control the amount and quality of the visual information about them to be uploaded in the internet. Even such a new thing like tagging the photos doesn't help to control all the pictures. We can un-tag the photos we do not like, but the photos still remain there on a web-site and how many images of us are uploaded un-tagged that we do not know about? And how much time do we need to spend daily to check if any photo of us appeared there? Ahern et al. [6] discussed in their work about over-exposing and they also found that even now users are concerned about this issue. Though they classify photos and manage the groups who are able to see certain photos, cross-linking among other users and web-sites still holds the potential danger of leaking the information out.

So, we see that the problem of privacy in the internet is still there, especially when we talk about photographs in the world wide web. According to previous researches and articles in news sites, perfectly, many users would like to have such a system, which would control the processes of uploading the photos automatically. By now there are only a few options how to avoid/control appearing your photos in the internet:

- escape events where other people can take some photos of you (which is not comfortable since socializing is one of the forms to communicate with others and get acquainted with new friends or useful people for business);

- check popular social networking sites where your friends have accounts, and look at their photos on their albums (though it may be that access is closed for you but is open for others);
- watermark your own photos, before uploading to the internet (for example, to protect using it by others for commercial purposes without your consent);

Most of the methods which suggest solutions to control the photos uploaded into web, consider the situation where the photo is already uploaded and they only post process it, for example, finding watermarks or recognizing other objects there and deleting them, and so on. PRIMO [2] also suggests the scheme where the user will be alarmed only after his photo being uploaded, and not in all cases such event may happen. Therefore, we think that in future the websites should control uploaders what images they are going to share with the world. We also keep in mind that they should not be limited in their rights to share the information they want. And this can be possible if a new method will be developed and integrated widely, which will check the content of the photo, analyze it and process further (let upload) either without any changes or only after automatic retouching some part of it.

In this paper we propose the idea of how to make it possible for users to control an amount and content of the photos to be uploaded into websites. The algorithm is simple and in future it can be applied in real time for just a few minutes.

Smart Secure Photo Uploading. To start with, let us see the **Fig. 1** which briefly shows the algorithm of secure photo uploading process.

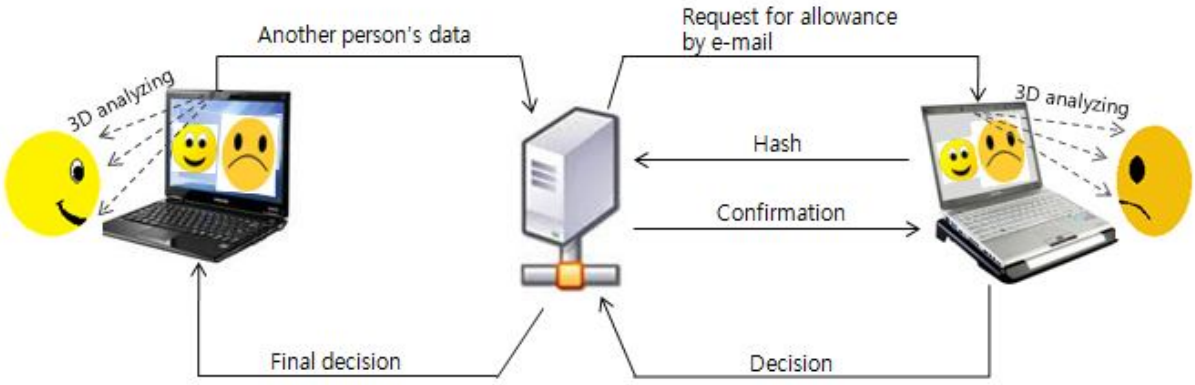

Fig. 1. Scheme of the algorithm for secure online photo uploading

This is an example algorithm for the case when a user wishes to upload (let's say to some forum) the photo with the two persons in it, himself and his friend. What we suggest is that, first, the forum's uploading page will require installing a Smart Secure Uploading (SSU) program. After the program is installed it automatically executes and starts to analyze the photo for detecting how many persons are pictured in its foreground. Once the figures are detected, the user is compared to confirm his identity with one of these. For the rest of the figures on the photo, uploader will be requested to enter their data (e.g., e-mail

address, or mobile number, or messenger ID, etc.), so that it will be sent to the server's database and the server, in turn, will send the e-mails to the mentioned parties with requests for allowing to upload the photo. Since in **Fig. 1** we have an example with two figures on the photo, where one is the uploader himself, for the second figure a request will be sent to a person pictured next to uploader. Before making a decision, allow or not uploading the photo, the second party will also need to go through 3D analyzing process in order to prove his identity with the one on the photo, otherwise if the identity is not confirmed, he cannot allow or forbid uploading the photo. After the server checks the result of 3D analyzing of another party and gets his decision it sends the command to allow or prohibit discovering the figures in the uploading photo. For better understanding of all the steps, let us describe them more precisely.

A) 3D analyzing. This is the most important step in our method. If nowadays the majority of the laptops are produced with the built-in web-cameras and many desktop users buy a separate web-camera, then we suppose that in future almost all PC users will have it, since it will be essential thing for communication.

This step is necessary for making sure that the person on the photo and the real one in front of the computer are the same. 3D analyzing is chosen because it will help not only to recognize the person better but also for proving that there is a real person in front of the PC by scanning him from different sides (See **Fig. 2**). Even though some years already passed since the photo had been taken, modern technologies already can identify people through the aging changes.

Fig. 2. SSU program performs 3D analyzing of a user by a web-camera

B) User's data. Since there are many people (but not everybody yet) who would like to control the photos with them to be uploaded to the internet sites, we suggest that this step will be voluntary. Whoever wishes to be asked before somebody is going to upload their photos, he needs to connect the server using SSU program just once and provide some unique information about him. The more fields he fills in the more chances that he will be contacted properly. Apart from the name, the person should also provide some unique data so that there would be no overlapping with the data of others. For example, e-mail address, messenger ID (Msn, Skype, etc.), phone number, and other, so that the person's friends would know at least one of them (**Fig. 3**). E-mail address is necessary for

the server to connect the user in future in case if somebody tries to upload a photo with him. Of course all the data should be properly secured in the server, and the user can update the data whenever something is changed.

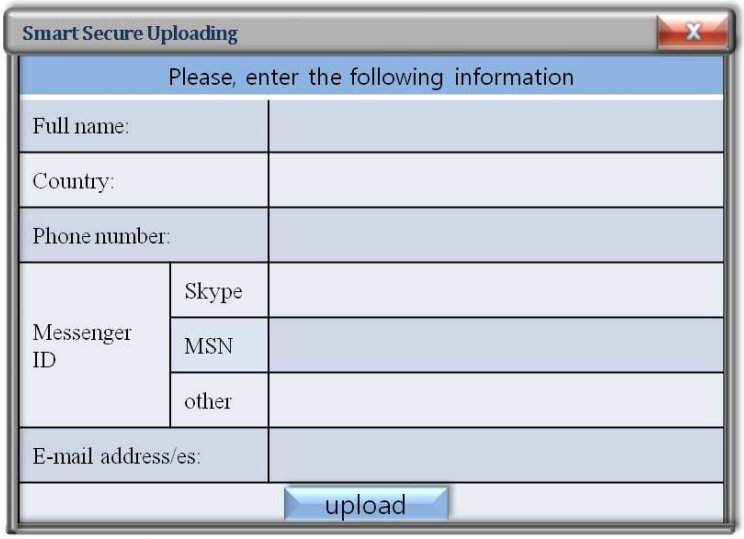

Fig. 3. SSU program requests a user's data to be uploaded into a server

C) Hash. Once a user has entered necessary data about him, next step will be to take a hash value of his 3D picture. Therefore, we suggest that SSU program will launch the user's web-camera, take pictures of him from different sides (**Fig. 2**), process them, get the hash value of it and transfer the value to the server. This hash value will be used in future to confirm that the appropriate user is going to give decision about allowing or forbidding uploading a photo with him, i.e., next time when he gets an e-mail from SSU server with request to allow or forbid uploading his photo, the user will need to process 3D analyzing, and this hash will further be compared with the original one stored in the server.

D) Final decision from the server. Once a person's identity is confirmed (by comparing the stored and real-time acquired hash values of the 3D images), the server needs to send a final decision to the one, who wishes to upload online the photo with another person pictured in it. Let us call the uploader as A and another person on the photo as B. If B's identity is confirmed and his decision is "to allow" uploading the photo, then the server will allow SSU program to proceed uploading the photo to the web-site. Otherwise, if B forbids uploading or if B's identity is not confirmed (or his data is not in the server's database), then the server will command to SSU program to deny uploading process. Another option can be developed where instead of denying uploading, the figures on the photo will be retouched and A can even choose the color in order to smooth the contrast of the retouched figure and the whole photograph tone. For example, in **Fig. 4** we have a grayscale photo with A and B pictured there. Therefore, if B forbids showing her on this photo online then A can choose to retouch B's figure with gray color.

Fig. 5 shows the block-diagram of the algorithm proposed in this paper.

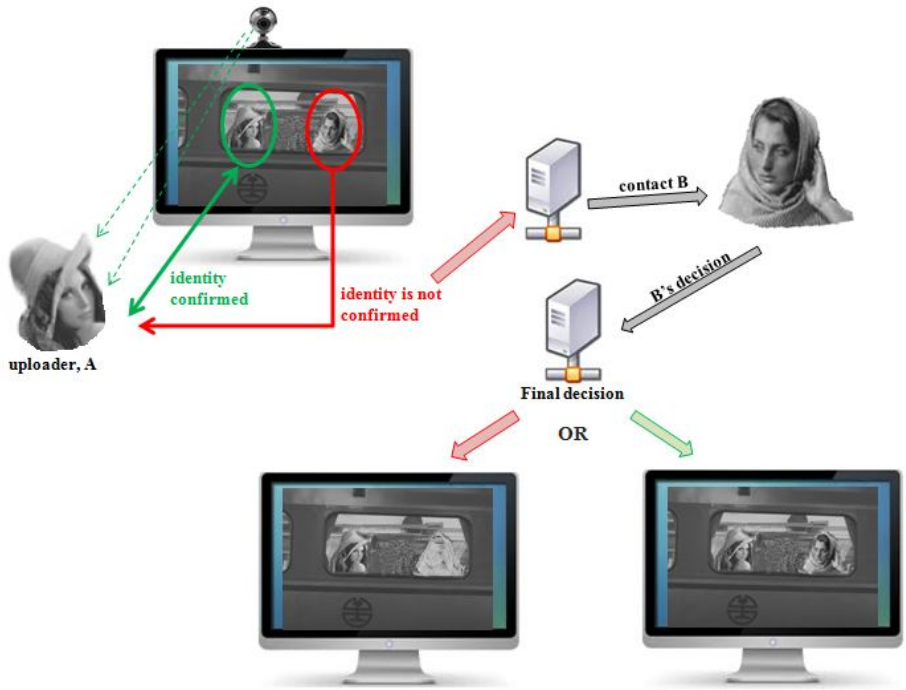

Fig. 4. Example on how the SSU scheme works

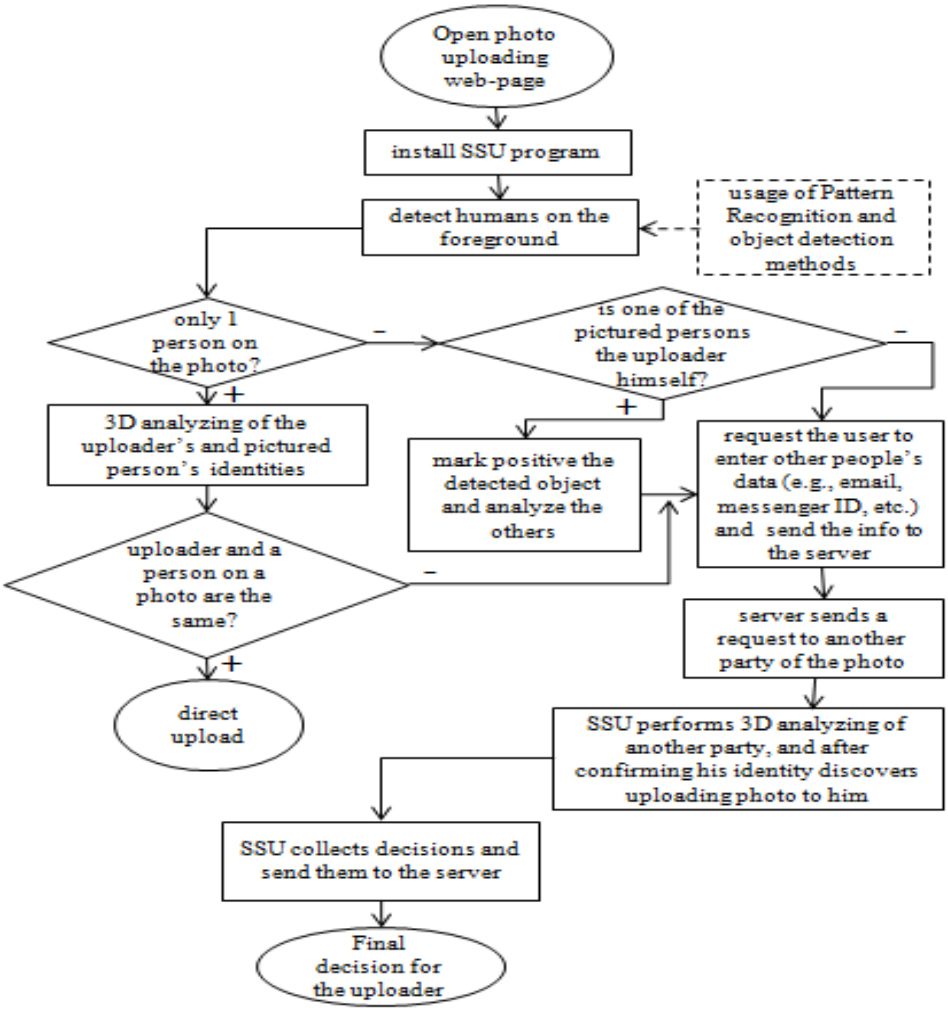

Fig. 5. Block-diagram of the algorithm for secure online photo uploading

Discussion about reliability and necessity of the SSU scheme. In descriptions mentioned above, we say that if A wants to upload a photo with B, then A should provide some data about B (e.g., name, messenger ID or e-mail) in order to contact him for asking allowance to upload the photo. Some readers may ask, "what if A knows nothing about B? Should system just prohibit uploading the photo or allow but with retouching B's figure from it? What if the person B is not alive anymore?" Therefore, we suggest that SSU program either deny uploading a photo or retouch another person's face.

The issues that may come for this scenario not to be able launched nowadays are:

a) unique hash values or other measures of 3D images of the people, which would be 100% robust against face aging or some other minor changes (for example, considering that more and more people are addressing to the plastic surgeries);

b) managing the server with the database, providing appropriate security to its data.

According to the first issue, state of the art technologies already can identify the people through the aging changes, however they are not 100% reliable yet and some more time is needed to make it work perfectly, especially for the case of 3D measuring. As for the second issue, we believe that with the modern temps of technologies' progress, creating and supporting such a server with a huge database, where millions of people could be registered, will be possible in future. And the whole process of analyzing the uploading photo, recognizing figures in it, identifying and contacting them, will be a matter of just a couple minutes.

Speaking of necessity of such technology that we propose in this paper, we would like to note that more and more online articles, news issues and forum discussions from the websites of different countries (for example, [7-16]) may be found about the situations with the photo privacy issue, surveys about the users wishing to control the photos with them exposed online and even some advices on how to protect yourself from being infringed by your own photos. Many people complain about either websites which settings have been broken and private online albums with allowed access only to selected members had been leaked, or other people who share their photos without their consent. There are plenty of cases when people not only lost their friends or their families had been broken because of the photos online, but many of them even lost their jobs because of it. From another side, if sharing the photos becomes so dangerous then why users still join those websites with options to upload and share personal photos and having such setting tool where the user can choose to "show images publicly" or "show only to selected groups"? It means that even though some users don't like to be exposed in some photos online, they still want to

share some visual information about them and they do want to control which information, when and where can be shared.

We also made a little survey among a group of 33 members with occupations ranging from housewives (mostly) to professional workers and engineers, and aging from 25 to 40. The question was: “Would you like it if in future there would be such technology that would always ask you for permission in case if somebody tried to upload a photo with you online?” The answers were as following:

a) Yes, I would like this technology to be available! – 26 (78.78%)

b) I think there is no necessity in this – 3 (9.09%)

c) Another answer – 4 (12.12%)

According to the answers above, even in a small survey within the people of different age and occupation the majority answered that they would like to control the photos of them to be uploaded into the cyber space. And again, remember the thousands of cases which you can easily find in the internet where other people also show their personal opinions and surveys of others’ ones about the relevance of strengthening privacy within online photo sharing issue.

We also assume that there can be a thing which may be arguable about. This is the legal issue on making the photo sharing websites to include the SSU program in their scripts mandatorily. We understand that the laws in each country are different, and what is allowed to be shown in one country may be considered as illegal or insulting somebody’s feelings in another country. Even there are some conventions between certain countries about enforcing common law in their cyber space, they still do not protect properly its citizens from suffering consequences of the photo privacy issues.

Conclusion. As one can see, along with developing technologies for making our life more comfortable we also need to think how to protect it from improper interruptions. Talking about photo privacy issue, we would like to point out that there are two options on how somebody’s photos can leak to other websites: a) from the person’s homepage on another site; b) from the uploader’s or somebody else’s camera. In first case, somebody can say that social websites provide the setting tabs for users where they can choose the options to show their information to everybody or to the selected people only (registered friends/users). However, it happens sometimes that after updating the website or some other works on it, the settings are reset to default ones, or hackers can break them. For the second case, we should remember that it is impossible to control all the people around us in our real life. For example, while one is having a coffee in a restaurant, somebody from another table can secretly take a picture of him and later upload it to the internet. There can be hundreds of examples where a person can be photographed with or without his consent and later his picture appears online. But what is even worse, the case when somebody’s photos are processed and impose to others quite an opposite image

of a person (e.g., nude photos, or photos showing him next to somebody else or being somewhere else, which have never had actually happened).

Therefore, in order to escape such cases in future and let people to control their photo privacy, we suggested in this paper the new idea how to make it possible. Considering that millions of people already registered on various websites and willing to control the photos with them to be shared online, we suppose that it would not be such a burden for them to register in a world-wide server for smart secure photo uploading service (for further connecting them if somebody wishes to upload their photo).

The only thing that may be disputed about is forcing all the websites (or at least the most famous ones) which hold the photographs (even in flash banners) to include the SSU program in their script (e.g. in ActiveX form) mandatorily. Let the cyber low specialists to think and discuss about this…

Literature:

1. http://en.wikipedia.org/wiki/Internet_privacy
2. T. Burghardt, A. Walter, E. Buchmann, K. Bohm, "PRIMO – Towards Privacy Aware Image Sharing," *Web Intelligence and Intelligent Agent Technology*, *2008. WI-IAT '08*, *IEEE/WIC/ACM International Conference on*, vol.3, pp. 21-24, Dec. 2008.
3. E.M. Newton, L. Sweeney, B. Malin, "Preserving Privacy by De-identifying Face Images," *Knowledge and Data Engineering, IEEE Transactions on*, issue 2, pp. 232-243, Feb. 2005.
4. A.S. Yuksel, M.E. Yuksel, A.H. Zaim, "An Approach for Protecting Privacy on Social Networks," *Systems and Networks Sommunications (ICSNC), 2010 Fifth International Conference on*, pp. 154-159, Aug. 2010.
5. Besmer, H.R. Lipford, "Moving Beyond Untagging: Photo Privacy in a Tagged World," *CHI 2010: Privacy*, pp. 1563-1572, Apr. 2010.
6. S. Ahern, D. Eckles, N. Good, S. King, M. Naaman, R. Nair, "Over-exposed?: Privacy Patterns and Considerations in Online and Mobile Photo Sharing," *CHI '07: Proc. of the SIGCHI Conf. on Human Factors in Computing Systems*, pp. 1-10, 2007.
7. http://www.cbsnews.com/stories/2011/02/06/sunday/main7323148.shtml (last accessed on Jan. 26th, 2015)
8. http://blog.internetcases.com/2011/03/12/facebook-privacy-photo-tagging-attorney-chicago-lawyer-social-media/ (last accessed on Jan. 26th, 2015)
9. http://internet-safety.yoursphere.com/2010/01/photo-privacy-on-social-networks-how-to-protect-your-kids/ (last accessed on Jan. 26th, 2015)
10. http://money.usnews.com/money/personal-finance/articles/2011/08/03/is-it-safe-to-post-photos-online (last accessed on Jan. 26th, 2015)
11. http://familyinternet.about.com/od/computingsafetyprivacy/a/Safe_to_post_photos_of_kids_online.htm (last accessed on Jan. 26th, 2015)
12. http://www.wantchinatimes.com/news-subclass-cnt.aspx?cid=1303&MainCatID=13&id=20110824000037 (last accessed on Jan. 26th, 2015)
13. http://abcnews.go.com/Technology/internet-destroying-privacy/story?id=13224589 (last accessed on Jan. 26th, 2015)
14. http://forums.techarena.in/technology-internet/1412908.htm (last accessed on Jan. 26th, 2015)
15. http://allthingsd.com/20090216/you-have-zero-privacy-anyway-get-over-it-that-goes-double-on-social-networks/ (last accessed on Jan. 26th, 2015)

16. http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10742619 (last accessed on Jan. 26th, 2015)

References:

1. http://en.wikipedia.org/wiki/Internet_privacy
2. T. Burghardt, A. Walter, E. Buchmann, K. Bohm, "PRIMO – Towards Privacy Aware Image Sharing," *Web Intelligence and Intelligent Agent Technology*, *2008. WI-IAT '08*, *IEEE/WIC/ACM International Conference on*, vol.3, pp. 21-24, Dec. 2008.
3. E.M. Newton, L. Sweeney, B. Malin, "Preserving Privacy by De-identifying Face Images," *Knowledge and Data Engineering, IEEE Transactions on*, issue 2, pp. 232-243, Feb. 2005.
4. A.S. Yuksel, M.E. Yuksel, A.H. Zaim, "An Approach for Protecting Privacy on Social Networks," *Systems and Networks Sommunications (ICSNC), 2010 Fifth International Conference on*, pp. 154-159, Aug. 2010.
5. Besmer, H.R. Lipford, "Moving Beyond Untagging: Photo Privacy in a Tagged World," *CHI 2010: Privacy*, pp. 1563-1572, Apr. 2010.
6. S. Ahern, D. Eckles, N. Good, S. King, M. Naaman, R. Nair, "Over-exposed?: Privacy Patterns and Considerations in Online and Mobile Photo Sharing," *CHI '07: Proc. of the SIGCHI Conf. on Human Factors in Computing Systems*, pp. 1-10, 2007.
7. http://www.cbsnews.com/stories/2011/02/06/sunday/main7323148.shtml (last accessed on Jan. 26th, 2015)
8. http://blog.internetcases.com/2011/03/12/facebook-privacy-photo-tagging-attorney-chicago-lawyer-social-media/ (last accessed on Jan. 26th, 2015)
9. http://internet-safety.yoursphere.com/2010/01/photo-privacy-on-social-networks-how-to-protect-your-kids/ (last accessed on Jan. 26th, 2015)
10. http://money.usnews.com/money/personal-finance/articles/2011/08/03/is-it-safe-to-post-photos-online (last accessed on Jan. 26th, 2015)
11. http://familyinternet.about.com/od/computingsafetyprivacy/a/Safe_to_post_photos_of_kids_online.htm (last accessed on Jan. 26th, 2015)
12. http://www.wantchinatimes.com/news-subclass-cnt.aspx?cid=1303&MainCatID=13&id=20110824000037 (last accessed on Jan. 26th, 2015)
13. http://abcnews.go.com/Technology/internet-destroying-privacy/story?id=13224589 (last accessed on Jan. 26th, 2015)
14. http://forums.techarena.in/technology-internet/1412908.htm (last accessed on Jan. 26th, 2015)
15. http://allthingsd.com/20090216/you-have-zero-privacy-anyway-get-over-it-that-goes-double-on-social-networks/ (last accessed on Jan. 26th, 2015)
16. http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10742619 (last accessed on Jan. 26th, 2015)

Рецензент: Дубко В.О.