Computer Networks 75 (2014) 531–543

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Distributing privacy policies over multimedia content across multiple online social networks

Constantinos Patsakis [b,*], Athanasios Zigomitros [b,c], Achilleas Papageorgiou [b], Edgar Galván-López [a]

[a] Distributed Systems Group, School of Computer Science & Statistics, Trinity College, College Green, Dublin 2, Ireland
[b] Department of Informatics, University of Piraeus, Greece
[c] Institute for the Management of Information Systems, "Athena" Research Center, Greece

ARTICLE INFO

Article history:
Received 15 November 2013
Received in revised form 18 July 2014
Accepted 11 August 2014
Available online 5 October 2014

Keywords:
Social networks
Digital watermarks
Identity theft
Privacy

ABSTRACT

Online Social Networks (OSNs) are currently playing a crucial role in our everyday social life. Their great growth has sparked the interest of hackers and individual users that try to disclose as much information as possible, which in many cases unfortunately is possible. In such events, the users' privacy settings are bypassed by the leakage of their shared media content. To address this challenging but important research problem, we introduce a new distributed scheme for media content sharing on online social networks that may minimize users' privacy exposure, through automated procedures. The novelty of the proposed scheme is the ability to enforce a user's privacy policies across multiple online social networks, even if she is not subscribed to all of them, without using a trusted third party. Moreover, the proposed framework is a step towards enabling OSNs to interact, exchange information with equal rights, independently of their size, focus and underlying infrastructure.

1. Introduction

In the web based interconnected world, the processing, storage and distribution of users' data consist of very sensitive area. Web communities, companies or even governments try to provide more secure and privacy oriented services and regulate such services. Millions of users worldwide share, everyday, huge amounts of private information through blogs, wikis, Online Social Networks (OSNs) and more social media applications. The technological advantages in big data storage, cloud computing, semantic web, mobile services and other fields, facilitate the design and development of new social web services.

Social media platforms like Facebook, Google+, Twitter and LinkedIn have completely changed people's behavior on the web. Simultaneously, new social media like Pinterest and Instagram highlight that multimedia sharing, more precisely images, either personal or computer generated, are a modern niche market with huge revenues for the service providers. Without any doubt, the biggest part of the shared information within social media is multimedia content, uploaded and shared by their users. Nevertheless, the provided security and privacy is often questioned [14,24,27,29].

Many of the privacy risks that a user's privacy is exposed to stem from the authentication and management mechanisms of published information. Malicious users have reportedly managed to bypass users' privacy settings of these services in many cases. As a result, new offenses ranging from identity theft up to personal information

* Corresponding author.
E-mail addresses: kpatsak@unipi.gr (C. Patsakis), azigomit@unipi.gr (A. Zigomitros), axilpapa@gmail.com (A. Papageorgiou), edgar.galvan@scss.tcd.ie (E. Galván-López).

http://dx.doi.org/10.1016/j.comnet.2014.08.023
1389-1286/

exposure are disclosed on a daily basis. The ease of re-uploading and re-publishing a user's images, without any form of notification, often harm the original owner both social and economically.

It should be noted that the term of ownership, throughout this work, should not be considered in terms of property or copyright, but it rather refers to the fundamental right to privacy. Users expect that by submitting their personal photos on OSNs, they are free to set their own privacy policies, allowing access only to the users that they decide. The uploaded content is part of their private lives and therefore belongs to them. Therefore, users should be able to selectively reveal themselves to the world [15].

Modern users normally do not have a single account for an OSN. In fact, users have accounts in many OSN and/or even multiple accounts in some of them. Let us assume that Alice and Bob belong to the same online social network OSN_1. Bob can easily download a photo from Alice's profile, obviously without Alice's consent or any kind of notification. Bob can make several alterations on Alice's photo offline, and then share it in another online social network OSN_2. It is clear that Alice will not be notified of the incident and no matter what privacy policies she has set on the photo, they will be bypassed.[1]

The core of this problem is that currently OSNs do not check what multimedia are being uploaded, *e.g.* whether a photo has already been published, by whom, what are the privacy policies etc. Additionally, modern OSNs treat themselves as a separate entity, which have nothing to do with any other OSN. Of course, even if many of the existing OSNs have a different orientation like socializing, health issues, professional or academic profiles, OSNs do not tend to interact, in order to gather more users. Due to the competition, this attitude seems fairly logical, nevertheless, redefining the problem in the context of other services, such as telecommunications or emails, reveals the importance of the problem. In this case, the subscribers of one provider would only be able to communicate with others of the same provider. However, the growth of both these services was achieved because the users were allowed to exchange information independently of the provider. Therefore, to further advance OSNs it is crucial to allow and develop mechanisms, in which all OSNs can exchange information.

This change is very probable to become a need quite in the near future. According to several researchers, fragmentation of current social networks is due to come. For instance, Boyd argues that fragmentation is closer to the human state of being since it allows them to focus on specific groups of interests, rather than generic and monolithic ones [6]. Additionally, while major OSNs allow some flexibility in creating smaller "groups" which are user created and more coherent, their actual capabilities are rather restricted, compared to smaller yet "specialized" OSNs. The latter fulfill the actual needs of their target groups as they are specially crafted for them, thus they are far more efficient than trying to provide patches to allow some additional functionality.

Independently of whether fragmentation of OSNs will happen, or how users log into their accounts, it is definite that through cooperation, OSNs may protect their users or even offer them additional services. In this work we focus on former.

This work is motivated by the following research question: "*Can we have more privacy-aware solutions for current Online Social Networks?*". We argue that such solutions do exist, even by applying well-known techniques. Thus, we focus on how they can be achieved and their feasibility within current structures, in terms of implementation effort, processing needs and economic constraints. The main contribution of this work is a new scheme that enables collaboration between OSNs to enhance users' privacy. The novelty of the scheme resides in the fact that it is completely decentralised and does not depend on a trusted third party (TTP). The proposed scheme counters many problems that stem from sharing multimedia content on OSNs such as identity theft, unauthorized content sharing and distortion of malleable content. Additionally, the scheme allows a new feature, the shared ownership of multimedia content.

One may argue that the current business model does not allow for such changes as the big "players" do not have the proper incentive to push such solutions forward. They are well established and want to increase their market shares. Therefore, one could claim that cooperation does not seem probable. The recent example of Schema.org[2] exemplifies that this is far from true. The search engine giants decided to cooperate and create a common framework that helps them to carry out their business easier and more efficiently. One should also take into consideration the role of regulatory authorities. The recent deal between EU anti-monopoly authorities and Google[3] signifies that big players can be forced to play with more "open" rules. Thus, developing a common privacy-aware framework for OSNs under the pressure of regulatory authorities[4] is not a far-fetched plan.

It is worthwhile to notice that while OSNs disregard each other, there is another link between many of them. Major OSNs may not interact with each other, nevertheless, they allow smaller OSNs to exploit their authentication mechanisms. Therefore, the majority of smaller OSNs are not registering their users directly, but rather obtain user authorization, through *e.g.* OAuth,[5] to use some of the information from bigger OSNs. This fact indicates that OSNs can further cooperate.

The main concept of this work is based on [37], updating and extending the findings of the conducted experimental results and discussing them in depth. However, the main contribution of this work is the introduction of a novel distributed scheme, without TTPs, which allows multiple OSNs to apply the privacy policies of their users among them, even if one user is registered to a single

[1] The case where Bob re-uploads the photo on the same OSN is addressed in [37].

[2] www.schema.org.

[3] http://europa.eu/rapid/press-release_IP-14-116_en.htm.

[4] https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-07-14_PH_for_EV_online_EN.pdf.

[5] http://www.oauth.net.

one. The proposed scheme tries to automatically resolve issues related to identity theft, unauthorized content sharing, distortion of malleable content and shared ownership.

The rest of this article is organized as follows. Section 2 presents some related work such as privacy issues within OSNs and some tools that have been proposed as solutions. Then it provides an overview of digital watermarks and illustrates the scheme of Zigomitros et al. [37]. Section 3 focuses on experimental results regarding image watermarking adoption from three major OSNs. Then, Section 4 illustrates how to extend the Zigomitros et al. scheme to more OSNs, allowing users to enforce their privacy policies on multimedia content, even to OSNs where they are not registered. Section 5 discusses the economical impact of the proposal given the additional operative and maintenance costs from OSNs. Finally, we conclude with some remarks and ideas for future research.

2. Related work

2.1. Privacy issues in OSNs

Privacy in OSNs can be approached by different points of view. Many researchers are focusing their efforts on the publication of anonymized graphs that represent the connections between users of OSNs. The majority of attacks are based on neighborhood attacks, a special type of attacks which is based on the fact that even if anonymization techniques have been applied on the provided data, an adversary may exploit some background knowledge about the "neighborhood" of a target victim. To this extent, known relationships among its neighbors can be exploited, leading to the re-identification of the victim. Therefore, special anonymization techniques, belonging to what is called privacy-preserving data publishing [11], are being applied to protect users [36,12].

Even if the aforementioned attacks are very important, we are interested in attacks "within the neighborhood". This means that the attacker belongs to the victim's neighborhood, tries to enter the neighborhood or tries to create a neighborhood that can be attributed to the victim. The ideal scenario would demand users to allow access to people that they truly trust, so that their shared information is not leaked. Nevertheless, as everyday living shows, this is not the case. People within social networks tend to have hundreds or even thousands of "friends", allowing them to access information that they would not do in real life. Apart from the obvious problem of how people regard their privacy on the Internet, we argue that OSNs should provide more mechanisms to increase the privacy of their users and protect them, as their privacy policies can be trivially bypassed as shown in [27,37].

The main privacy issues in OSNs, as discussed in [35,26], are the following:

In an **Identity Theft** attack, the attacker tries to masquerade as another person to hurt his social profile, or to exploit the trust that other people have in his authority and to obtain money, usually in form of credit. The victim's shared multimedia, which are usually of high quality, can be used to launch attacks in real-life as well, *e.g.* print fake ID cards or company passes. Fraudsters can also extract useful information from the shared multimedia content on OSNs. In cyberspace the replication of victim's account, multimedia content and information, can be achieved easily while this process can even be automated [5]. Closely related to the identity theft are the following two attacks, which are often regarded as specific cases. If we have replication of the victim's profile in the same OSN, then we have the so called **Profile Cloning** attack. Otherwise, if the attacker exports the victim's information and multimedia content and creates a profile to another OSN then we have the **Profile Porting** attack. This attack may be more effective for victim impersonation since a search query at an OSN will only return a single profile, the fake one.

In the **Sybil Attack** scenario, a user creates multiple accounts to manipulate and affect a result as desired by him and his purpose [10]. It is essentially an escalation of Profile Porting attack. The goal of the adversary can vary from a simple voting scenario to a de-anonymization attack.

If a user uploads a multimedia file, setting her desired privacy policy for example to be shared only with her friends, implies that she trusts her group of friends in that they will not share or re-upload her file. Nevertheless, as already discussed in the introduction, in current OSNs her shared multimedia content is usually one click away from bypassing her privacy preferences, leading to the **unauthorized content sharing** attack.

Another privacy exposure stems from the use of **static links**, which are used by the majority of OSNs. OSNs use static links to bind the shared content, which can easily be copied and arbitrarily shared on any other medium.

Finally, most OSNs do not allow **shared ownership** of content. Anyone who possesses it is considered its sole owner and can define privacy policies for it. Thus, if she re-uploads it, she automatically can set different privacy policies.

2.2. Tools for privacy in OSNs

In principle, it should be noted that very closely related to our research is the work on Social Identity Management (SIdM). This can be understood as the set of methods that OSNs use to allow users to disclose information to specific groups of their contacts. This allows them to manage the attributes and information that they disclose regarding their social identities/roles, attributed by others or themselves. As it becomes apparent, SIdM is not only focused on multimedia content, but any attribute that an OSN user can have.[6] The interested reader is referred to [23,28].

Currently, several solutions concerning users' privacy on existing centralized or decentralized OSNs, have been proposed. The bulk of these solutions come as external applications and are not native solutions, having several drawbacks that do not allow their wide adoption. For instance, many of them are *experimental* solutions or proofs of concept. Therefore, the interface and support is

[6] The shared multimedia content, can be considered an abstract attribute of a user's profile.

quite limited. The nature of these tools might even bypass the terms of service of each OSN *e.g.* as they use cryptographic or steganographic methods, which hide the main source of income of OSNs, information. Therefore, the solutions which are discussed in the following paragraphs are not widely used and many times users are unaware of their existence. For instance, completely decentralized OSN architectures like Diaspora,[7] Safebook [8] and OneSocialWeb[8] never managed to attract massive amounts of users to change the rules of the game.

In NOYB [13], groups of users share a key and break their personal information into "atoms" which are then permuted with the "atoms" of other users, using the key to generate the permutation. Thus, the real information is hidden from the OSN and the users who do not have the key.

Persona [3], allows users to encrypt their data and exchange a public key with selected users. This way, Persona provides an attribute based encryption to users' data, which allows them to apply their desired privacy policies regarding data access. EASiER [17] extends Persona, by creating decryption keys that are associated with each user, allowing data access, only when a user contacts the proxy with the appropriate key. Another encryption based tool, is FlyByNight [21]. It mainly uses public key encryption algorithms to exchange users' messages in Facebook. Scramble [4] is a Firefox extension which allows OSNs users to encrypt their uploaded content storing it either at a TinyLink server or the OSN.

PrivacyJudge [19] allows users to manage who can access their posted content, hosted in their own or a trusted third party privacy server. Data treatment is specified by labels to reduce the risk of accidental exposure of personal information. In this area, we also have Lockr [31] an access control system and Facecloak's [22] which obfuscates users' profiles by providing fake information to the OSN and storing personal information on an application server in encrypted form. Another cryptographic solution was proposed by Patsakis and Solanas [25] who propose a novel methodology for sharing data within social networks. When users encrypt all their data, they create small encrypted keyword dictionaries on the data that they are willing to share. By sharing the dictionaries' decryption keys with advertising companies, users allow them to mine their data. If they find a promising profile, they can place a bid to access the full data.

Some privacy-aware solutions towards connecting users have been proposed. For instance in [9], De Christofaro et al. propose the use of private set intersection (PSI) protocols to disclose only the common connections that two users have. On the other hand, based on PSI protocols, Li et al. introduce a recommender system for social networks, which matches users with similar interests, without disclosing their preferences [20].

Following radically different approaches we find X-pire! [2] and unFriendly [30]. In the case of X-pi.e!, users set expiration dates for their shared multimedia content, to make them unavailable after that date. On the other hand, unFriendly proposes a solution for enforcing multiparty privacy in published photos so that they are co-managed by the people who are depicted in them.

Finally, it should be highlighted that both Facebook [1] and Google+[9] have recently started using face recognition services. The focus of these services is mainly to tag the shared content and allow better search capabilities. However, one could claim that these services could also be used to counter ID theft attacks. The main drawback of these solutions is that the images have to be checked against huge amounts of photos, so that even if the identification error is quite small, the total of amount of false positives creates an enormous amount of manual processing. On top of that, one should consider the fact that many users tend to use and share many common pictures, which would issue many false alarms.

2.3. Watermarking

Digital watermarking is the process of embedding information into media, usually in order to prove the origin of the content and also its integrity. A watermarking algorithm has to balance between the least possible distortion and robustness while allowing the desirable capacity. Nowadays, watermarking has been proposed as a solution for a variety of applications with the most often being copyright protection, authentication and tamper detection, copy and device control, fingerprinting and metadata/feature tagging [38,7].

The most basic property of image watermarks is their *invisibility*, that is they must be imperceptible by the human visual system, allowing them not to be traced and removed from unskilled attackers or to alter the quality of the image. Depending on the application needs, watermarks have different robustness. *Fragile* watermarks are used to check the integrity of multimedia files, as the slightest modification can break them, triggering an alert to the watermarking system. *Semi-Fragile* watermark systems detect malicious modifications on the host image, *e.g.* object insertion or cropping, while common image processing as random noise and/or lossy compression do not trigger any alarm. Finally, *robust* watermarks are made to withstand a wide range of possible attacks as they are mostly used for proofs of ownership. An attack from a malicious user would be the removal of watermark or making it undetectable. However, this should not be possible without a great degradation of the host image.

The *capacity* of the watermark refers to the maximum number of information bits that can be embedded to a multimedia file of a given size. Depending on the application, the minimum capacity that is required can range from 1 bit, in copy control application, to a whole photograph.

Finally, there are two categories of algorithms based on the requirement to access the original multimedia file during extraction. *Non-blind* algorithms compare the original with the watermarked image to extract the information. On the other hand, *blind* algorithms do not need access to the original image.

[7] https://joindiaspora.com.
[8] http://onesocialweb.org/about.html.
[9] https://support.google.com/plus/answer/2370300?hl=en.

Table 1
Summary of needed properties for application. *Note:* ∗: varies.

Application/properties	Invisibility	Robustness	Capacity	Blind/non-blind
Copyright	Both	Robust	∗	Both∗
Auth. – tamper detection	Invisible	(semi-) Fragile	∗	Both∗
Copy control	Invisible	Robust	Low	Blind
Device control	Invisible	Any∗	Low	Blind
Fingerprinting	Invisible	Robust	∗	Both∗
Metadata – feature tagging	Invisible	Any∗	High	Blind

Table 1, summarizes the needed properties for the aforementioned applications. For more on watermarking and possible attacks the interested reader is referred to [33,32].

2.4. Enforcing privacy policies within a single OSN

Users trust their multimedia files in OSNs and the majority of users do not seem to bother whether OSNs alter their content due to resizing or compression, as long as the content does not have visible distortions. When a conflict of multimedia content ownership or misuse occurs, OSNs are heavily dependent on user reports. This approach has major drawbacks. The most obvious one is the manual nature of the system. Secondly, this policy enables a malicious user to report everyone, adding an additional cost because there is not an automated system to handle these requests. Finally, and perhaps the most important, a user can report a misuse only when he becomes aware of it, which is usually through another user's feedback or by sheer luck. For the latter case the OSNs do not take any precaution measures, neither do they offer any kind of notification mechanisms to their users.

Addressing these problems, as a first line of defense, a dual watermarking scheme was introduced in [37]. The solution might not solve the problem completely, as there are successful watermark attacks, but in order to exploit probable watermark vulnerabilities, the users must be skilled and the result of such attacks usually leads to great degradation of the multimedia quality. The scheme that was proposed can prevent many privacy leaks and drastically decrease the manual intervention from OSN's side. Definitely, user reporting will still have an important role inside OSNs for cases that demand serious decision making, context awareness and additional user feedback, as not all issues can be automated. For instance a user shares on an OSN an image depicting someone without his consent (the image is not uploaded from the prosecutor), or the uploaded image is offensive and misuses the terms of service of the OSN. The proposed solution apart from deterring privacy leaks, provides a notification mechanism so that users become aware of how their shared information is treated by others.

The watermarking scheme proposed by Zigomitros et al. [37] is mainly focused on images, but can be applied to other multimedia content such as audio and video. The scheme uses two watermarks, a robust and a semi-fragile, both explained previously, for storing user's multimedia content. A use-case scenario can clarify the need for the dual watermark scheme. We assume that user *A* provides to OSN an original multimedia. Then the OSN starts the embedding process and embeds a robust watermark, which identifies the multimedia content uniquely and associates it with the user. A semi-fragile watermark can be embedded in the host media at the same time or afterwards [18], since the robust watermark can tolerate this kind of process. The dual watermarked media is stored in OSN servers and becomes available to users of the OSN according to privacy settings defined by its owner.

The robust watermark is used to identify the media and the owner of it uniquely, and can be recovered even if the watermarked media has been processed. Meanwhile, the semi-fragile watermark enables the detection of alterations, malicious or not. The scheme is illustrated in Fig. 1.

3. Experiments

3.1. The process

The lack of detailed reference manuals on how the shared information is managed, processed and stored from most OSNs, due to their closed source code notion, has led us to conduct several experiments in order to test the possible existence of image watermarking schemes. The experiments that where conducted in [37] were repeated to test if there is any change in the policies. The original tests were made on the two most widely used OSNs, namely Facebook and Google+. However, we decided to include in our experiments a fast growing OSN, VK (vk.com), which claims to currently host more than 100 million active users.

For our experiments we used two groups of images, which are going to be referred as Test Set 1 and Test Set 2, using two user accounts, user *A* and *B* respectively. The concept was to upload both sets of images on the two accounts and then download again the images from each users' profile and perform some comparisons. Firstly, we downloaded the images from the profile of user *A* and compared them against their originals. Then, the same procedure was executed for user *B*. Then, we compared the downloaded images of the two users, trying to trace possible differences. The same procedure was repeated for each OSN, from different PCs and at different time frames. These steps allowed us to avoid computer fingerprinting and exclude the time factor from our experiments.

Two groups of images were created. **Test Set 1** includes 40 computer generated and grayscale images from TESTIMAGES.[10] The resolution of 20 of these images

[10] http://sourceforge.net/projects/test./files/.

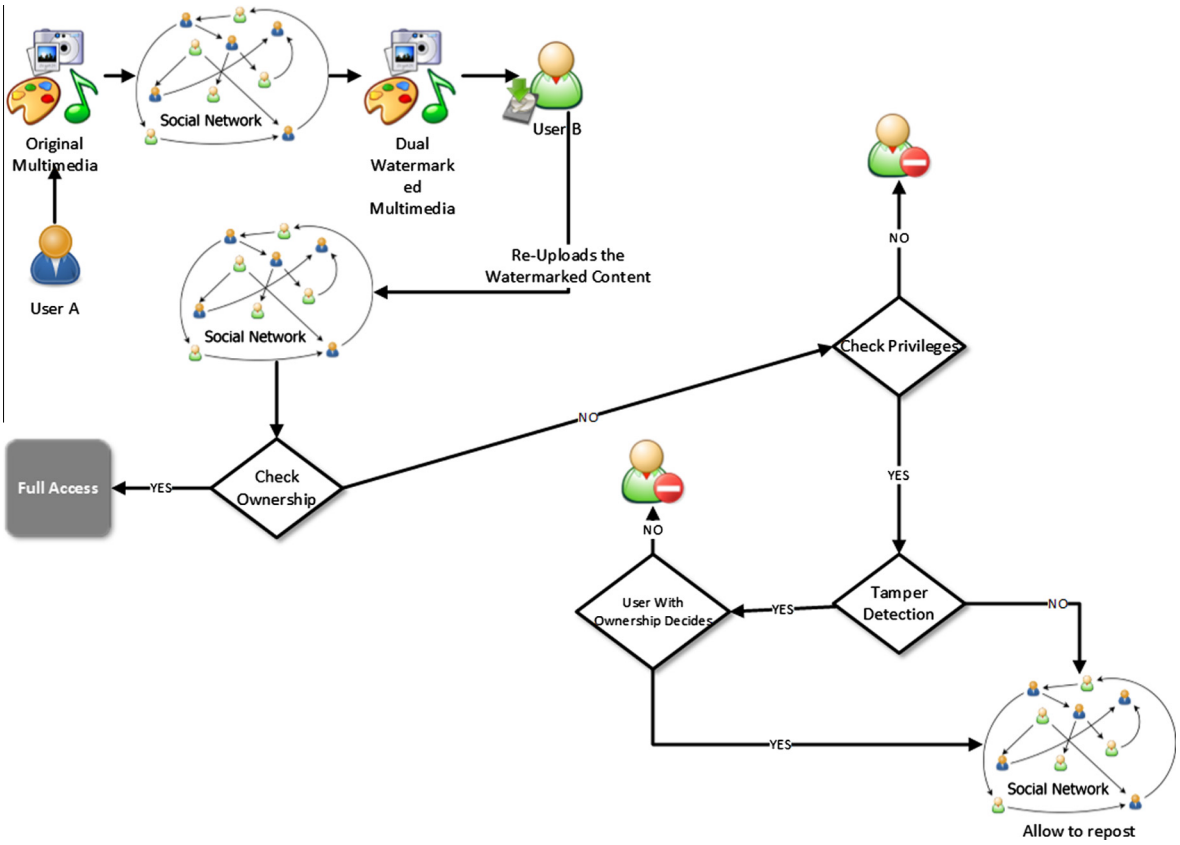


Fig. 1. The Zigomitros et al. scheme.

is 1200 × 1200 pixels, while the rest of them have resolution 600 × 600 pixels. **Test Set 2:** has also 40 images but are closer to what could be characterized as typical user images. This set consists of 20 images with resolution greater than 1200 × 1200 pixels, which range from 2048 × 1536 pixels to 3648 × 2736 pixels. These images were taken from 4 different devices, 7 were taken from the camera of an Apple iPhone 3GS, 6 from a Casio EX-Z1050 camera, 4 from a LG KU 990i mobile and 3 with a Cannon IXUS 130 camera. The rest of the images, were taken again from TESTIMAGES, 10 images of 1200 × 1200 pixels and 10 of 600 × 600 pixels.

The basic image characteristics that are reported in the experimental results were conducted with Matlab.

3.2. Results

Since the results vary on the three OSNs, we group their results accordingly. Therefore, firstly we present some general remarks and then we discuss our findings for Facebook, Google+, and finally, for VK.

For the Test Set 1, the comparison between the downloaded users' images showed that there was no difference in their size or resolution for Google+. The next test was regarding the differences in filesizes of the downloaded images compared to the original ones. In Fig. 2 we present the histogram regarding the differences in filesizes for Test Set 1. It is obvious that the test set images had no difference compared to the original ones in their filesize when they were uploaded on Google+. However, in almost all of them we notice a reduction on their filesize, when they were uploaded on Facebook.

Significant differences were traced in the case of Test Set 2, which consists of high resolution images. The OSNs have thresholds on the image resolution that can be shared. This is a rectangle of 2048x1536, in portrait or landscape orientation. Beyond this bound, images are resized by both OSNs to fit the optimal resolution within the aforementioned rectangle. In Fig. 3, we observe again that Google+ does not make any change in the image size, if the image is within these bounds. In the Facebook case however, a big reduction in the filesize is observed, even if the image was of the appropriate resolution. The distortion on several image characteristics is summarized in Table 2.

The results for VK presented more differences. The main difference is that VK has three resolution thresholds for uploaded images, beyond these thresholds, images are resized to fit these boundaries. Therefore, only 30 cases (20 for Test Set 1 and 10 for Test Set 2) fit these boundaries and could be compared against the original ones, all of them being identical. Testing the downloaded images from the profile of user *A* to the respective from user B, showed again that they are identical, even in the case of size reduction.

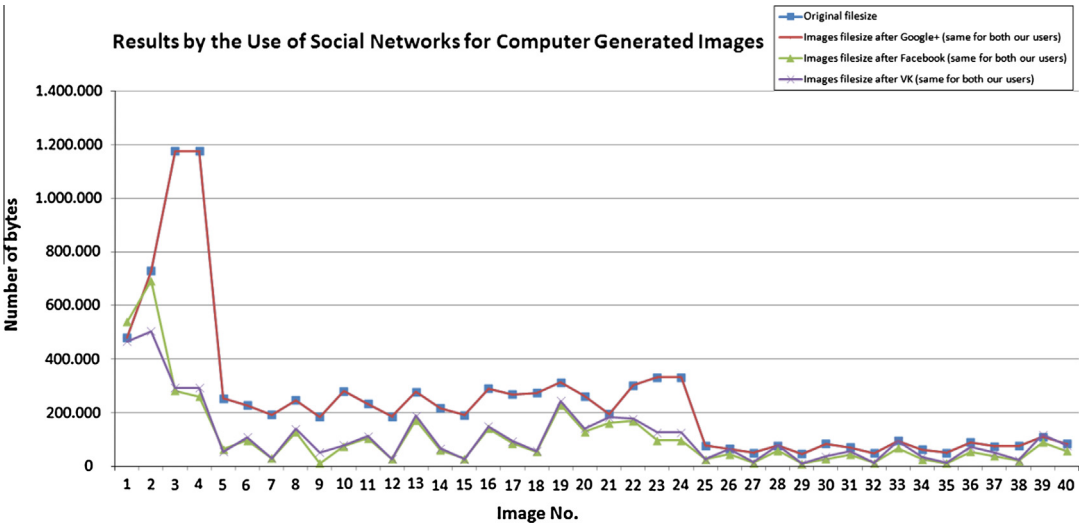


Fig. 2. Test set 1, image file sizes.

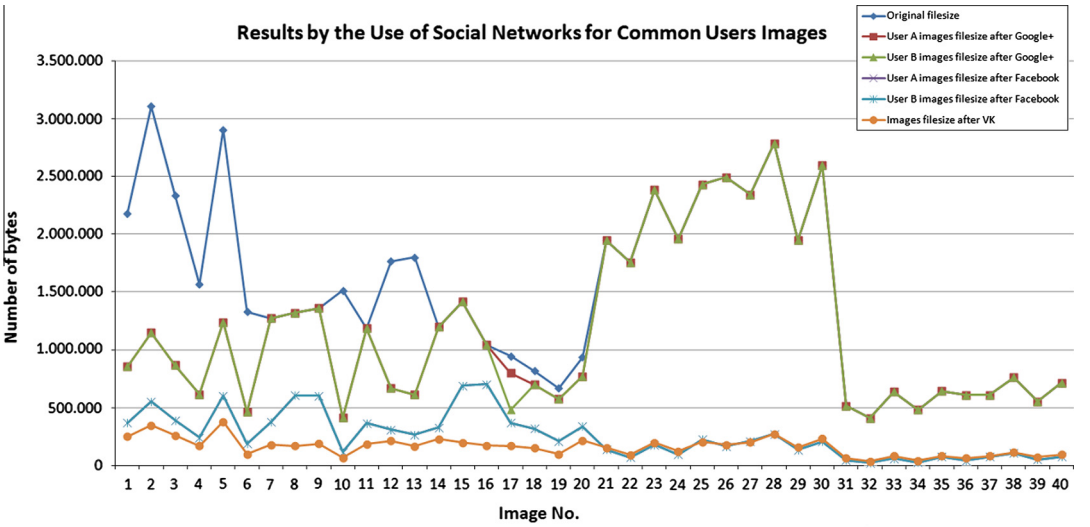


Fig. 3. Test set 2, image file sizes.

Table 2
Mean values of basic image characteristics. The table refers to the images that had no change in their resolution.

	Test Set 1 Original vs. FB	Test Set 2 Original vs. FB	Test Set 1 Original vs. G+	Test Set 2 Original vs. G+	Test Set 1 Original vs. Vk	Test Set 2 Original vs. Vk
Mean square error	18.081	14.6884	0	0	4.6918	14.0569
Peak signal to noise ratio	42.2241	41.4557	∞	∞	49.3408	41.8773
Normalized cross-correlation	1.0013	0.9993	1	1	0.9986	0.9993
Structural content	0.9975	1.0005	1	1	1.0027	1.0004
Average difference	−0.5513	−0.0441	0	0	0.0265	−0.0313
Maximum difference	34.525	55.3333	0	0	18.55	55.6
Normalized absolute error	0.0139	0.0259	0	0	0.008	0.0225

3.3. Discussion

Since there are variations on the results for each OSN, we have kept the discussion of the results for each one of them separate. However, as will become apparent, with very high probability we can deduce that, no watermarking scheme is used by any of them.

3.3.1. VK

VK was detected to have three different thresholds depending on the vertical and horizontal ratio. In case of square images that threshold is 1024×1024, for portrait is 768×1024 and for landscape 1280×960.

The results from VK clearly illustrate the complete lack of any watermarking mechanism. The images that are not resized are identical to the original ones. Even when images are resized, both users end up having the exact same images. Therefore, it can be safely deduced that no watermarking has been applied, as this would result to differences in the images of the two users.

3.3.2. Google+

The results for Google+, are more or less the same with the first results in [37], with minor differences. In Google+, when the image resolution does not exceed the aforementioned size threshold, the uploaded image is exactly the same with the original one. Compared to the first experiments, an interesting change was observed in the new images. Whenever Google+ had to resize an image, it inserted an image ID tag in the file's metadata, which was the same for both users. Interestingly, in the new experiments this only happened for one of the photos and for one of the users. The embedded tag cannot in any case be considered as watermark, as it can be removed very easily. Therefore, we can safely deduce in this case that no watermarking is being applied. Moreover, if the image resolution exceeds the threshold, the image is resized, yet, the image is exactly the same for both users. Hence, we may assume that no watermarking is being applied by Google+ on the uploaded images in either case.

3.3.3. Facebook

In the case of Facebook, again the results in [37] are more or less still valid. Before discussing the findings, we have to highlight at this point that Facebook's policy is to convert all uploaded images to the lossy JPEG format. This is blocking users from sharing animated GIFs and distorts lossless formats like PNG. If the images are not resized, then the two downloaded images of the two users are identical. An interesting behavior was noticed when the images are above the allowed threshold and have to be resized. Specifically, all the images from Test Set 1 do not have any distortions between the users, as their resolution is below the Facebook thresholds. The images that were different between the two users were separated, and were afterwards checked for steganographic content with stegdetect[11] and stegsecret.[12] The results from both tools were negative, so no steganografic method was traced.

The image differences, could hint the existence of an undetected watermarking scheme. Nevertheless, this approach would be quite peculiar. The distortion is traced only on large photos. Watermarking only high resolution photos does not sound a good or solid privacy policy, as the allowed thresholds enable attackers to launch attacks on all lower resolution photos. Perhaps, this behavior could be justified by the existence of a resizing algorithm that uses randomization.

A major difference compared to the previous experiments in Facebook, is the image URLs and file names. In the previous experiments, the URL contained the user ID and still does, however, the user ID was embedded in the filename of the downloaded files as well. This enabled third parties to trace the source of an image against others, only from its filename, whenever someone re-posted them or just sent them.

We should note that in all three OSNs, the links to media files are static. Users can copy and paste these URLs share them within the same OSN or even worse, share them with people who are not subscribed to the OSN. Moreover, even in the case of re-uploading an image from another user's profile, there is no notification. This check in particular is very easy and lightweight to implement, as it could be checked with the already implemented hashes that are calculated to check the integrity of the uploaded files.

Fig. 3 clearly illustrates that for the images that exceed the resolution threshold, both Google+ and Facebook apply a similar algorithm in terms of compression when images are resized, as the filesizes are almost identical, with the Facebook being a bit more efficient (see Fig. 4).

4. Proposed solution

4.1. Overview of the solution

As previously discussed, OSNs regard themselves as completely separate worlds that do not interact. Nevertheless, this is not the case, as there is a direct link between all of them and this is none but their users. More precisely, the users which have accounts to other OSNs. The idea of "one OSN to rule them all" does seem probable, as more or less each OSN has its own target group, providing different functionality and services to its users. Given that a unification of OSN's is not probable, the only solution to enforcing privacy measurements across multiple OSNs is their cooperation. The scheme of Zigomitros et al. can be applied to a single OSN, however extending it would result in several problems. The most obvious one is who is applying the watermark. Creating a Trusted Third Party (TTP) which watermarks every medium that is supplied from the OSNs might sound a good idea. However, this would demand the generation of new data centers and additional communication costs. Nevertheless, the major drawback is the fact that OSNs would have to go under the umbrella of a unique authority. The latter could be accepted from small OSNs, however, major OSNs are unlikely to accept such an approach, given their market position.

We argue that a solution without a TTP and with minimal interaction between OSNs is feasible. This can be achieved by altering the watermark that each OSN applies to the uploaded media. We assume that we have n OSNs that cooperate on enforcing cross-OSN privacy policies on multimedia content, that share a common watermarking key K.[13] Without loss of generality, we assume that a user

[11] www.outguess.org/detection.php.
[12] http://stegsecret.sourceforge.net/.
[13] K is used to watermark each image with a dual watermark, a robust and a semi-fragile as in the original Zigomitros et al. scheme.

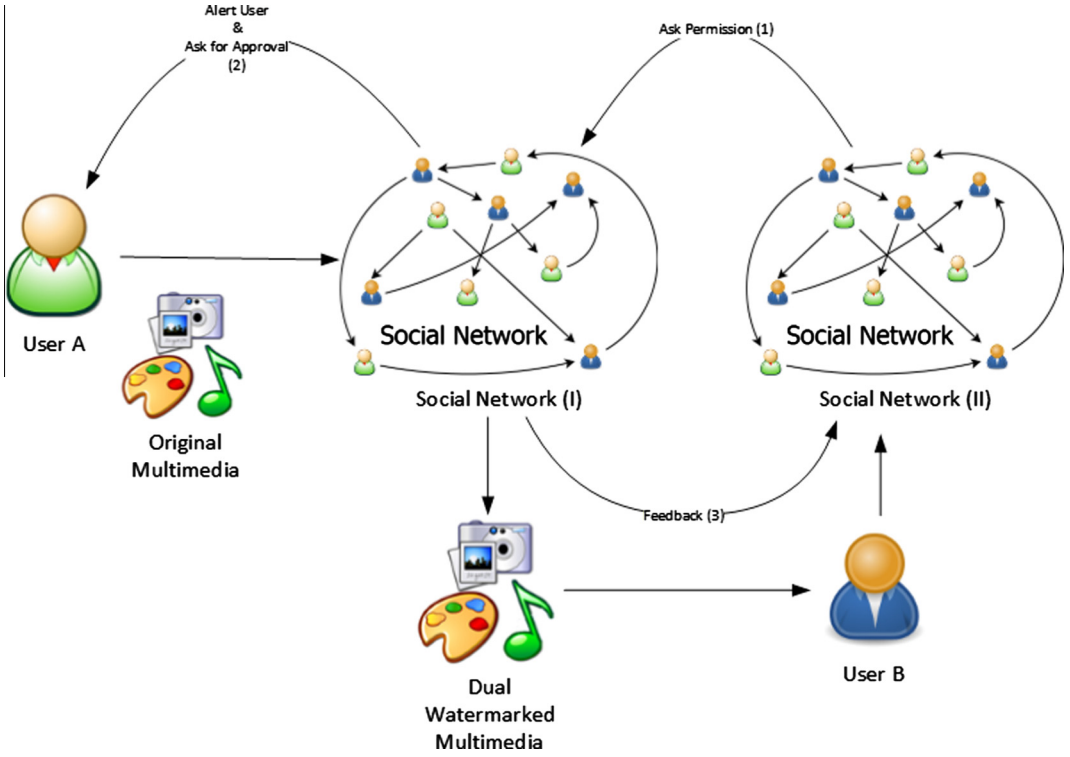


Fig. 4. Managing media files in two social networks.

uploads an image file, however, the procedure is the same for any multimedia file. We estimate that the least information that should be embedded in each watermark is the following: The userID which allows each OSN to determine the owner of the media. A mediaID field which notifies the OSN where the image was originally hosted. There is also a need for a timestamp field to indicate when the media was watermarked. Finally, we believe that a publication license ID is also needed. This information might seem unnecessary, as an OSN will have to check for the user's policy. Nevertheless, this may solve other problems that are going to be discussed in the following paragraphs.

Moreover, we assume that each OSN has its own private and public key pair $(Priv_{OSN_i}, Pub_{OSN_i}), i \in \{1, \ldots, n\}$ and a symmetric key Sym_{OSN_i}.

Let us assume that Alice uploads an image to OSN_1, then OSN_1 creates a vector v as follows:

$v = (E_{Sym_{OSN_1}}(UserID||rnd), MediaID, Timestamp, PublicationLicense, E_{Pub_{OSN_i}}(OSN_{m_1}Data), \ldots, E_{Pub_{OSN_i}}(OSN_{m_k}Data))$where:$\{m_1, \ldots m_k\} \subseteq \{1 \ldots n\}$ and rnd a random value.

The first field is encrypted with Sym_{OSN_1} so that OSN_1 can recover the UserID quickly. UserIDs are salted with a random value in order to obfuscate the UserID. Leaving the userID just encrypted allows other OSNs to profile users by storing the encrypted form of their IDs. If they are salted, then only the original OSN can find the owner of the media and all other OSNs are hidden not only from the owner, but from any other media of the same user. The next three fields are not encrypted, so that everyone can retrieve the mediaID, the timestamp and the publication license of the user. Finally, the rest of the fields contain information that is specific for each OSN and can be retrieved only by them. The vector is signed by OSN_1 so the information that is embedded in the watermark w is $w = v, E_{Priv_{OSN_1}}(H(v))$, where H is a secure hash function. Using K, OSN_1 embeds the dual watermark in the photo and publishes it.

If a user wants to upload the same photo to OSN_2, then OSN_2 will use K to extract the watermark. From that, OSN_2 will get the vector w and verify that it is correctly received from the digital signature. Based on the publication license and the message that OSN_1 has encrypted for OSN_2, OSN_2 will decide whether or not it will publish the photo and with what privacy settings, notifying OSN_1 about these actions.

4.2. Discussion

The proposed scheme enables users to apply their privacy policies on their multimedia content across multiple OSNs. It is important to highlight that the users do not need to be registered to all OSNs to allow this functionality. Moreover, users can be notified of any attempts to violate their privacy. The scheme does not need any trusted third party, therefore, there is no further trust dependency.

The use of timestamp in watermarks is considered essential as they can be used to define fine-grained policies in our scheme. Since each photo is watermarked on upload, users can use this information to define time-based policies. For instance, a user may allow a photo to be public after 2 years, or stop sharing one after 5 years. On top of

that, timestamps can be used in case of conflict to determine which user has uploaded the content first and deduce its origin. The latter can be understood only in the case when a new OSN joins and checks its content against its peers.[14]

The introduced publication license field is very important, as users may use standard licenses such as Creative Commons[15] or define custom ones, excluding specific users or OSNs from distributing the content. It is clear that personal photos will have custom policies, while others will have more generic ones. To illustrate this concept, we assume that Alice publishes a photo with a "Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License". This means that Alice does not allow modifications of her work or commercial use. Bob finds this photo and can publish it in his profile. If Alice decides to withdraw the photo, then this will not have any impact on Bob's profile and Bob will not have any problem with publishing the photo even after Alice removes the photo. Nevertheless, if Bob has downloaded the image, processed it and tries to upload it to OSN_2 where Alice is not registered, OSN_2 will detect the alterations from the dual watermark and since the license does not allow modifications, block Bob from uploading the photo.

In another scenario, Bob might try to upload a photo from Alice's profile in OSN_1, where her characteristics are quite clear to the professional OSN_2 where Alice is not registered. Since Alice's photo is personal, she has watermarked it with a non distribute license. Therefore, if Bob wants to perform an identity theft attack to Alice, OSN_2 will block his actions by reading the embedded watermark.

The scheme allows OSNs to have different policies among themselves, without publicly disclosing them. Hence, several OSNs, depending on their interests, conflicts and policies, may choose to cooperate under different schemes, without exposing critical information to the rest of the participants. This way, Alice who is registered in OSN_1 can allow only users from OSN_2 to re-upload some of her photos. Given that Alice might have two accounts on different accounts, she can notify OSN_1 so that photos are co-owned from another user from OSN_2, specifying her ID in OSN_2 and vice versa.

The proposed scheme reestablishes the roles of OSNs, as not only do they host content, but they become Content Certification Authorities (CCAs). CCAs can certify the origin of a submitted multimedia file, hence detect if it belongs to one of its users or not, to the users of another affiliated OSN and even detect alterations.

Obviously, this scheme enables not only privacy aware sharing of media content, but furthermore the unification of user accounts among different OSNs. This unification, might seem on first sight scary for most of the OSNs, especially the ones with fewer users. Nevertheless, depending on the differentiation of the services that each of them provides, this unification can only enhance their status. This can be achieved due to the fact that the unification can enable developers and OSNs to deliver more solid, useful and fine grained solutions to the users. The decentralized nature of the scheme enables the equal treatment of all the participants, which is very crucial for its continuity, creating a web of trust not only among the OSNs, but among their subscribers as well.

One of main advantages of this scheme is that user's privacy is greatly enhanced, as the user has total control of his media. He can keep track of where his media files are being used, who has access to them and revoke or grant access to them on real time, independently of the OSN that he is registered. The obvious drawback of this solution is what happens with the already shared content and how to tackle with cases were different users share the same content and one of them declares ownership. Of course, human intervention cannot be avoided, yet the best approach would be to watermark all this content by current OSNs and mark it as non further distributable, unless all the parties agree on the ownership.

Finally, the proposed scheme allows OSNs to automatically respond to changes in the legal system. In the upcoming years, many changes are expected to be made in the privacy laws in national and international level. This may have serious implications to OSNs as they will have to change the way they distribute content according to the new laws. A framework, as the one we propose allows OSNs to automatically conform, as the changes in one of them will lead to cascading changes to the rest of the OSNs, significantly reducing the cost of law compliance.

Additionally, the proposed solution could enable common ownership schemes. Let us assume that two users agree to share the ownership of a photo. Then, they declare this to the OSN they are registered to, which generates a user ID that maps to both of them. This way, each user can set his own privacy preferences independently, and the OSN will enforce the intersection of their policies, whenever it has to be accessed. If a violation of the policies is detected or someone tries to share it, or its modification, to another OSN, this action will be reported, the OSN will apply the necessary policies and send the according notifications to the users.

Finally, OSNs instead of using the proposed dual watermarking scheme, they could use a public watermarking scheme, such as [34]. The adoption of such scheme provides another layer of security. The use of such scheme removed the risk of leakage of the common watermarking key k.

Some OSNs might decide not to play fairly, trying to create an advantage for their users. In the proposed scheme, the key is common for all OSNs, therefore, malicious OSNs can track where the watermark is stored and alter it, so that it appears as the medium belongs to their users. While this attack is possible, if OSNs use a public watermarking scheme, then this action cannot be performed, as the embedding key is different from the extraction key. Additionally, this act can easily be traced and the misbehaving OSN prosecuted not only by the users, but from the other OSNs who have economic advantages to close down one of their competitors. It becomes apparent that enforcing the scheme by some OSNs may force the others to act

[14] It should be highlighted that while the proposal is straightforward regarding new content, managing already published content or how a new OSN joins is more complicated and is going to be discussed extensively in future work.

[15] http://creativecommons.org/.

accordingly. Finally, as already highlighted, according to the European Data Protection Supervisor P. Hustinx, "controllers will therefore also require them to think better about the legitimacy of what they intend to do...the new framework will also provide for strong sanctions – administrative fines of millions of euros – for the most serious cases where these rules have not been respected." Therefore, regulatory authorities are expected to enforce such policies in the near future. In this context, misbehaving OSNs are expected to face serious legal consequences.

5. Economical impact

Most of the OSNs are operating under the so-called "freemium" model, meaning that they offer the service free to the users, in exchange of accessing, mining their data and offering targeted advertisement to their customers. Watermarking their massive amounts of photos is certainly a serious cost, as all this procedure demands many additional processing hours. Therefore a very important question that has to be addressed to is the economical impact of the proposal in the current established business model.

To fully understand the economical impact of the proposal it is important to understand how much computational effort is needed to apply this scheme. To estimate it, we used a Java implementation of a typical DCT watermarking scheme. On a desktop computer running on Intel Core i7-3770 CPU clocked at 3.40 GHz and without a fully optimized implementation, a photograph with resolution of 2048×1536 needs on average approximately 1.5 s to be watermarked per core. Given that this processor has 8 cores, such a computer can watermark around 460,800 photos per day. According to [16], each day, 350 million photos are uploaded to Facebook. Therefore, Facebook would need approximately 760 such computers to balance the computational effort for its daily traffic. On the other hand, it takes around 1 s to extract the watermark. It should be highlighted that these figures could be further reduced with a more optimized implementation or with exploiting GPUs.

The cost of maintaining this additional infrastructure cannot be considered neither negligible nor prohibitive, nevertheless we believe that it is something manageable. Currently, even if millions of people are using OSNs, sharing huge amounts of information, they are aware that this way is not the most privacy-aware method. If some OSNs decide to build or reformat their structure, offering more privacy to their users via their collaboration, on the one hand they will increase their maintenance expenses, on the other hand it is expected that they will attract many additional revenues. Firstly, providing a feature such as cross-OSN privacy policies is expected to attract more users, especially at this point of time where people are becoming more aware of privacy. The latter was sparked by recent relations about background actions from secret government agencies. Many start-up companies are rushing to exploit this new niche market of privacy. Therefore, since the proposed scheme minimizes the leakage of users' information, many new users will be attracted. Moreover, people will be able to share more information, or even more sensitive, as the privacy-aware shift from these OSNs will renew their trust to the service. All the above, make the collaborating OSNs more attractive to advertising companies, as they will host more people, more information to mine and perhaps more valuable for the advertising companies.

A privacy-aware service for subscribers, is an additional feature that can attract artists of all genres to publish and share more of their work on OSNs. With this target group, but without watermarks, Pheed[16] is gradually getting more and more users promoting itself as a free social multimedia platform that allows multimedia sharing and streaming. Given that many artists do not share their work due to leakages, the proposed scheme would make such OSNs even more attractive.

In other applications or extensions of OSNs, watermarking techniques are considered essential, as they provide the necessary trust to the users that access them. Typical examples are professional, medical and dating OSNs or their extensions. In such cases, it is crucial to guarantee that the users are real and that their profiles contain the right information. Identity theft or even extortion attacks on such cases can harm the public and professional image of the victim severally and immediately. To address such challenges, applications such as Badoo[17] have resulted to visible watermarks, degrading the actual medium. However, the necessary functionality is not provided, as these watermarks could be easily cropped in many cases.

Consequently, it is clear that subscriptions of premium accounts or the attraction of more users and better quality of content sharing can mitigate the costs of applying watermarking schemes in OSNs and maintaining the needed infrastructure.

6. Conclusions

The privacy of the multimedia content which is a significant ingredient for the success of OSNs, has not drawn the proper attention yet. The OSNs so far only deal with metadata of multimedia content by erasing them or by letting users set privacy settings for the geolocation of the content if available. As OSNs affect more and more our daily lives, the development of new security and privacy policies for multimedia content becomes essential. Towards this end, this work introduces a scheme that allows users to enforce their privacy policies not only on multimedia shared in the OSN that they belong to, but among others to which they are not registered. This is achieved by the use of watermarks on the multimedia with either public encryption algorithms or public watermarking techniques. The major contribution of this work is the unification of privacy policies across multiple OSNs in a distributed way without the use of trusted third parties.

The proposed solution can be implemented without having to redesign current OSNs from scratch, therefore it can be easily adopted, in terms of deployment. One may argue that the proposed methodology hints towards

[16] www.pheed.com.
[17] www.badoo.com.

DRM practices, however, the watermarks are only used to protect the users' content and users could opt in or out of this service for all or some of their multimedia content. Additionally, we have quantified the cost of adopting the proposed solution in terms of computational effort and proposed solutions to counter the economic cost.

As discussed, the main issue towards adopting this solution is the already uploaded content. It is a fact that the implementation of this solution will give ownership to users for all their uploaded content even if they do not have the right to own it. If an image, for example, belongs to user *A*, yet user *B* also uploaded it, it would seem that it belongs to user *B*, so user *A* should report it in order to settle the dispute. The holder of the original multimedia content can upload it again at any time on the OSN even if a previous watermarked version of this content has been uploaded by another user before the implementation. Definitely, such a scenario is realistic, yet we can see that the balance of what can be automated from the proposed solution and what is left on the human level is drastically decreased, leaving far less problems to be manually solved. Nevertheless, the complexity of this issue should be examined thoroughly in future work. Finally, it has to be noted that the more that such solutions are not applied, the more the cost is increased, as users are uploading new and more content every day.

Acknowledgement

Edgar Galván-López gratefully acknowledges funding from the Irish Research Council, co-funded by Marie Curie Actions.

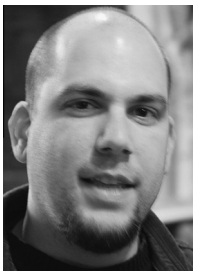
References

[1] DeepFace: closing the gap to human-level performance in face verification, in: Conference on Computer Vision and Pattern Recognition (CVPR), 2014.
[2] Julian Backes, Michael Backes, Markus Dürmuth, Sebastian Gerling, Stefan Lorenz, X-pire!-a digital expiration date for images in social networks, arXiv preprint arXiv:1112.2649, 2011.
[3] Randy Baden, Adam Bender, Neil Spring, Bobby Bhattacharjee, Daniel Starin, Persona: an online social network with user-defined privacy, ACM SIGCOMM Comput. Commun. Rev., vol. 39, ACM, 2009, pp. 135–146.
[4] Filipe Beato, Markulf Kohlweiss, Karel Wouters, Scramble! your social network data, in: Simone Fischer-Hbner, Nicholas Hopper (Eds.), Privacy Enhancing Technologies, Lecture Notes in Computer Science, vol. 6794, Springer, Berlin, Heidelberg, 2011, pp. 211–225.
[5] Leyla Bilge, Thorsten Strufe, Davide Balzarotti, Engin Kirda, All your contacts are belong to us: automated identity theft attacks on social networks, in: Proceedings of the 18th International Conference on World Wide Web, WWW '09, ACM, 2009, pp. 551–560.
[6] Danah Boyd, It's Complicated: The Social Lives of Networked Teens, Yale University Press, 2014.
[7] I.J. Cox, M.L. Miller, J.A. Bloom, Watermarking applications and their properties, in: Proceedings of the International Conference on Information Technology: Coding and Computing, IEEE, 2000, pp. 6–10.
[8] Leucio Antonio Cutillo, Refik Molva, Thorsten Strufe, Safebook: a privacy-preserving online social network leveraging on real-life trust, Commun. Mag. 47 (12) (2009) 94–101.
[9] Emiliano De Cristofaro, Mark Manulis, Bertram Poettering, Private discovery of common social contacts, in: Javier Lopez, Gene Tsudik (Eds.), Applied Cryptography and Network Security, Lecture Notes in Computer Science, vol. 6715, Springer, 2011, pp. 147–165.
[10] JohnR. Douceur, The sybil attack, in: Peter Druschel, Frans Kaashoek, Antony Rowstron (Eds.), Peer-to-Peer Systems, Lecture Notes in Computer Science, vol. 2429, Springer, Berlin, Heidelberg, 2002, pp. 251–260.
[11] Benjamin Fung, Ke Wang, Rui Chen, Philip S Yu, Privacy-preserving data publishing: a survey of recent developments, ACM Comput. Surv. (CSUR) 42 (4) (2010) 14:1–14:53.
[12] Ralph Gross, Alessandro Acquisti, Information revelation and privacy in online social networks, in: Proceedings of the 2005 ACM workshop on Privacy in the Electronic Society, ACM, 2005, pp. 71–80.
[13] Saikat Guha, Kevin Tang, Paul Francis, Noyb: privacy in online social networks, Proceedings of the 1st Workshop on Online Social Networks, vol. 1, ACM, 2008, pp. 49–54.
[14] G. Hogben, Security issues and recommendations for online social networks, ENISA Position Paper 1, 2007.
[15] Eric Hughes, The electronic privacy papers, Chapter A Cypherpunk's Manifesto, 1997, pp. 285–287.
[16] internet.org, A Focus on Efficiency white paper from Facebook, Ericsson and Qualcomm. September 2014.
[17] Sonia Jahid, Prateek Mittal, Nikita Borisov, Easier: encryption-based access control in social networks with efficient revocation, in: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ACM, 2011, pp. 411–415.
[18] Darko Kirovski, Henrique Malvar, Yacov Yacobi, A dual watermark-fingerprint system, Multimedia 11 (3) (2004) 59–73.
[19] B. Könings, David Piendl, Florian Schaub, Michael Weber, Privacyjudge: effective privacy controls for online published information, in: 3rd International Conference on Privacy, Security, Risk and Trust (PASSAT), and 3rd International Conference on Social Computing (SocialCom), IEEE, 2011, pp. 935–941.
[20] Ming Li, Ning Cao, Shucheng Yu, Wenjing Lou, Findu: privacy-preserving personal profile matching in mobile social networks, in: Proceedings of INFOCOM, Springer, 2011, pp. 2435–2443.
[21] Matthew M Lucas, Nikita Borisov, Flybynight: mitigating the privacy risks of social networking, in: Proceedings of the 7th ACM workshop on Privacy in the Electronic Society, Springer, 2008, pp. 1–8.
[22] Wanying Luo, Qi Xie, Urs Hengartner, Facecloak: an architecture for user privacy on social networking sites, International Conference on Computational Science and Engineering (CSE'09), vol. 3, IEEE, 2009, pp. 26–33.
[23] Michel Netter, Moritz Riesner, Michael Weber, Gunther Pernul, Privacy settings in online social networks – preferences, perception, and reality, in: 46th International Conference on System Sciences (HICSS), IEEE, 2013, pp. 3219–3228.
[24] Constantinos Patsakis, Alexandros Asthenidis, Abraham Chatzidimitriou, Social networks as an attack platform: Facebook case study, in: 8th International Conference on Networks, IEEE, 2009, pp. 245–247.
[25] Constantinos Patsakis, Agusti Solanas, Privacy as a product: a case study in the m-health sector, in: 4th International Conference on Information, Intelligence, Systems and Applications (IISA), IEEE, 2013, pp. 1–6. July.
[26] Constantinos Patsakis, Athanasios. Zigomitros, Achilleas Papageorgiou, Agusti Solanas, Privacy and security for multimedia content shared on osns: issues and countermeasures, Comput. J. (2014). in press, http://comjnl.oxfordjournals.org/gca?gca=comjnl%3Bbxu066v1&submit=Go&allch=&action=Get%20All%20Checked%20Abstracts.
[27] Guojun Qin, Constantinos Patsakis, Mlanie Bouroche, Playing hide and seek with mobile dating applications, in: Nora Cuppens-Boulahia, Frric Cuppens, Sushil Jajodia, Anas Abou El Kalam, Thierry Sans (Eds.), ICT Systems Security and Privacy Protection, IFIP Advances in Information and Communication Technology, vol. 428, Springer, Berlin, Heidelberg, 2014, pp. 185–196.
[28] Moritz Riesner, Michael Netter, Günther Pernul, Analyzing settings for social identity management on social networking sites: classification, current state, and proposed developments, Information Security Technical Report, 17(4) (2013) 185–198.
[29] Katherine Strater, Heather Richter, Examining privacy and disclosure in a social networking community.
[30] Kurt Thomas, Chris Grier, DavidM. Nicol, unfriendly: multi-party privacy risks in social networks, in: MikhailJ. Atallah, NicholasJ. Hopper (Eds.), Privacy Enhancing Technologies, Lecture Notes in Computer Science, vol. 6205, Springer, Berlin, Heidelberg, 2010, pp. 236–252.
[31] Amin Tootoonchian, Stefan Saroiu, Yashar Ganjali, Alec Wolman, Lockr: better privacy for social networks, in: Proceedings of the 5th International Conference on Emerging networking Experiments and Technologies, ACM, 2009, pp. 169–180.

[32] Sviatolsav Voloshynovskiy, Shelby Pereira, Thierry Pun, Joachim J Eggers, Jonathan K Su, Attacks on digital watermarks: classification, estimation based attacks, and benchmarks, Commun. Mag. 39 (8) (2001) 118–126.
[33] Peter Wayner, Disappearing Cryptography: Information Hiding: Steganography & Watermarking, Morgan Kaufman, 2009.
[34] Ping Wah Wong, Nasir Memon, Secret and public key image watermarking schemes for image authentication and ownership verification, Trans. Image Process. 10 (10) (2001) 1593–1601. October.
[35] Chi Zhang, Jinyuan Sun, Xiaoyan Zhu, Yuguang Fang, Privacy and security for online social networks: challenges and opportunities, Network 24 (4) (2010) 13–18.
[36] Bin Zhou, Jian Pei, Preserving privacy in social networks against neighborhood attacks, in: 24th International Conference on Data Engineering (ICDE 2008), IEEE, 2008, pp. 506–515.
[37] Athanasios Zigomitros, Achilleas Papageorgiou, Constantinos Patsakis, Social network content management through watermarking, in: 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE, 2012, pp. 1381–1386.
[38] Athanasios Zigomitros, Constantinos Patsakis, Cross format embedding of metadata in images using qr codes, Intelligent Interactive Multimedia Systems and Services, Smart Innovation, Systems and Technologies, vol. 11, Springer, 2011, pp. 113–121.

Constantinos Patsakis (Marousi, Attiki, Greece, 1979) is a research fellow at the Distributed Systems Group, Department of Computer Science, Trinity College, Dublin, Ireland. He received his BSc in Mathematics from University of Athens, Greece and his MSc in Information Security from Royal Holloway, University of London. He holds a PhD from Department of Informatics of University of Piraeus. His main areas of research include cryptography, security, privacy and number theory. He has participated in several Europeanfunded projects. In 2009 he was elected lecturer at the Department of Informatics of University of Piraeus. He has been teaching several computer science courses in Greek and Catalan universities, and worked as researcher at the CRISES Research Group and the UNESCO Chair in Data Privacy in the Department of Computer Science and Mathematics at the Rovira i Virgili University (URV) of Tarragona, Catalonia, Spain.

Athanasios Zigomitros was born in Chromio Kozani, Greece, in 1980. He received the BSc degree in Business Planning and Information Systems from TEI of Patras, Greece in 2004 and the MSc in Advanced Computer Systems from the University of Piraeus, Greece in 2008. Currently he is a PhD candidate at University of Piraeus, focused in contentbased Information Retrieval in Multimedia Streams. He is a member of Decision Support System Laboratory, Department of Informatics, University of Piraeus. Additionally holds a scholarship from the Institute for the Management of Information Systems, Research Center ''Athena'' in the research area of ''Privacy protection''. His current research interests include Multimedia Retrieval and Metadata, Privacy Preserving Data Publishing, Anonymity, Watermarking and Digital Currencies.



Achilleas Papageorgiou was born in Marousi, Attiki, Greece, in 1983. In 2008 he receives a BSc in Communications, Informatics and Management from TEI of Epirus, Greece and in 2011 a MSc in Digital Communications and Networks from University of Piraeus, Greece. Currently, he is a Web developer and SEO Specialist at Intelligent Media LTD, which is a private company in Greece. His expertise lies in the fields of design, development and optimization of web-based applications, internet marketing and digital projects management. In 2008 he was honored with a Best Research Paper Award and a Best Young Scientist Paper Award in Pan-Hellenic conferences. His research interests include privacy and security in social networks, e-health and e-learning activities. He is a IEEE Member.

Edgar Galván-López is an ELEVATE Postdoctoral Fellow in the School of Computer Science and Statistics at Trinity College Dublin. His research has focused on the use and study of Evolutionary Algorithms (EAs) and Monte Carlo Tree Search in dynamic environments. In 2009, he completed his PhD thesis, from University of Essex, UK, on the study of EAs, with particular emphasis in the use of Genetic Programming (GP). He has independently been ranked as one of the top 2% researchers in GP.