Personal Rights Management– Enabling Privacy Rights in Digital Online Content

Mina Deng[1,⋆], Lothar Fritsch[2], and Klaus Kursawe[1]

[1] Katholieke Universiteit Leuven,
[2] Univeristy of Frankfurt
{MDeng, KKursawe}@esat.kuleuven.be
Lothar.Fritsch@m-lehrstuhl.de

Abstract. With ubiquitous use of digital cameras, e.g. in mobile phones, privacy is no longer threatened by governments and companies only. A new threat exists by people, who take photos of unaware people with no risk and little cost anywhere in public and private spaces. Fast distribution via online communities and web pages expose an individual's private life to the public. Social and legal measures are taken to deal with this, but they are hardly enforcable. We propose a supportive infrastructure aiming for the distribution channel such that if the picture gets publicly available, the exposed individual has a chance to detect it and take action.

Protection of personal privacy has become a major issue. Most of the current work assumes an asymmetric model; the violator is an institution, while the victim is a person. Recently, a new privacy thread has emerged. An increasing number of people are equiped with miniature cameras, taking photos anywhere and anytime, thus endangering privacy when they publish the photos. Countermeasures, like penalties or a ban on cameraphones have proven insufficient, as a growing number of websites promoting such photos (e.g. the Mobile Asses website [1]) shows. As it is infeasible to enforce a broad ban on cameraphones or artificially inhibit their usage by technical measures (e.g., simulated shutter noise), we propose a novel way to complement such measures: we attack the distribution channel. If a picture of a person is taken and published, the victim has a good chance of being the first to find this picture, enabling her to request the pictures removal or invoke legal action in time.

Three major players are in our setting: the photographer (Bob), the individual (Alice), and the search engine. Bob is the photographer using a cameraphone. We assume that Bob should not to be prevented from taking the pictures and have his identity protected as long as he does not infringe the rights of anybody. Alice is being photographed by Bob. The interest of Alice is that she has some control over pictures taken of her, so we assume this picture should not be distributed without her consent. We grant her this option: If a picture of her is

⋆ Mina Deng is funded by research grants of the Katholieke Universiteit Leuven, Belgium.

J. Dittmann, S. Katzenbeisser, and A. Uhl (Eds.): CMS 2005, LNCS 3677, pp. 266–268, 2005.

taken and published, she can find out early. Alice uses a receiver, which registers the identities of pictures taken in her vicinity. The receiver is her own mobile phone or a piece of hardware. It can also be integrated in the infrastructure provided by external parties, for instance, the owner of a discotheque or the GSM operators. Finally, the search engine searches the Internet for picture identities and makes them publicly available with a matching scheme.

The scenario: In the first step, Bob chooses to take a picture of unaware Alice. The camera generates and broadcasts a unique picture identifyer embedded into the picture (either by watermarking or perceptual hashing). On the other side, Alice's receiver picks up the picture identification information and stores it for later use. When Bob publishes Alice' picture, the search engines can find it and index it by the embedded ID. Alice sends requests to the search engine with all picture identities that her receiver picked up, and thus locates the picture taken by Bob. Hardware implementation: Our protocol must not require any significant changes to the devices' hardware. Three communication standards can be used to establish the link between camera phone and the receiver: Infrared, Bluetooth, and the GSM network. Infrared has a low bandwith and is easy to block, but can be directed; bluetooth is reasonably realiable and fast, but can be received by devices not in the camera range and poses a potential security risk. GSM is the most natural channel for a cellphone to communicate on, but requires support of the provider and will cover a high number of receivers. We recommend to use a combination: an infrared flash could trigger the receiver to listen to a bluetooth signal We are not protecting against a higly sophisticated attacker, but against users with both limited criminal energy and technical skills to prevent privacy violation from becoming a mass phenomena. In this, the contemporary DRM technologies for mobile devices can be applied to protect a user's personal privacy.

Software implementation: Embedding the information is done with digital watermarking [2,3]. In the our system, we identify the secretly photographed image rather than authenticating its integrity. A high level of robustness against malicious attacks is required, though the amount of data we need to embedd is relatively small (40 bits). We expect low resolution photos to allow for sufficient robustness in this setting. Perceptual hash functions can be used to identify the picture [4]. Their advantage is that the data is neither altered nor degraded. Occasional collisions do not pose a problem, as they make the user find irrelevant pictures; as long as this does not cause too much effort, is is acceptable. The final part of our protocol is a search engine that locates the pictures on the Internet. The special feature is the extraction of the identification information from the pictures to use it as an index. Similar technlogies are already in place, for example Digimarc's MarcSpider. Though technologies exist to fool such engines, one can expect a reasonable success rate in a practical setting.

References

1. ... *Mobile Asses.com - The real reason mobile phones have cameras!* . 2005.
2. R. J. Anderson F.A.P. Petitcolas and M. G. Kuhn. Information hiding-a survey. volume 87, pages 1062–1078, 1999.

3. S. Katzenbeisser and F.A.P. Petitcolas. *Information hiding techniques for steganography and digital watermarking*. Artech House, INC., 2000.
4. M. Kivanç Mihçak and R. Venkatesan. New iterative geometric methods for robust perceptual image hashing. In *ACM CCS-8 Workshop on Security and Privacy in Digital Rights Management*, pages 13–21, London, UK, 2002. Springer-Verlag.