Personal Rights Management - Taming camera-phones for individual privacy enforcement

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

[1] Katholieke Universiteit Leuven, ESAT/COSIC, Kasteelpark Arenberg 10,
B-3001 Leuven-Heverlee, Belgium
[2] Chair of M-Commerce and Multilateral Security, Johann Wolfgang
Goethe-University, 60054 Frankfurt am Main, Germany
{Mina Deng, Klaus.Kursawe}@esat.kuleuven.ac.be
Lothar.Fritsch@m-lehrstuhl.de

Abstract. With ubiquitous use of digital camera devices, especially in mobile phones, privacy is no longer threatened by governments and companies only. The new technology creates a new threat by ordinary people, who could take and distribute pictures of an individual with no risk and little cost in any situation in public or private spaces. Fast distribution via web based photo albums, online communities and web pages expose an individual's private life to the public. Social and legal measures are increasingly taken to deal with this problem, but they are hard to enforce in practice. In this paper, we proposed a model for privacy infrastructures aiming for the distribution channel such that as soon as the picture is publicly available, the exposed individual has a chance to find it and take proper action in the first place. The implementation issues of the proposed protocol are discussed. Digital rights management techniques are applied in our proposed infrastructure, and data identification techniques such as digital watermarking and robust perceptual hashing are proposed to enhance the distributed content identification.

Keywords: privacy protection, model for privacy infrastructures, mobile camera phones, data identification techniques

1 Introduction

Over the last years, privacy protection has become a major issue, and both the European Union and the US are investing significantly into research on this area. However, almost all of the current work assumes an asymmetric model; the privacy violator is a corporate or governmental institution (or at least an employee

[*] Mina Deng's work was partially supported by the Concerted Research Action (GOA) Ambiorics 2005/11 of the Flemish Government, the Research Foundation - Flanders (FWO-Vlaanderen), and the research institute IBBT of the Flemish Government.

[**] Lothar Fritsch's work was partially supported by the IST PRIME and IST FIDIS projects, he state of Hessen and T-Mobile, but expresses his opinion only.

thereof), while the victim is a normal citizen. Correspondingly, the main research areas cover issues such as identity management, policy enforcement, and anonymous communication. In the last years, however, a new privacy threat has emerged that cannot be addressed by such means. Due to improvements as well as the growing distribution of various handhold devices, an increasing number of people are equipped with miniature cameras (in their mobile phones) and voice recorders (in their music players).

1.1 Problem statement

Until the 1990s, public distribution of images could only happen in the press, either in print or in electronic broadcast media. To challenge the unauthorized distribution of an individual's image, a media company could be identified and contacted. Furthermore, the media company usually would know who the photographer was.

With the advent of the Internet as a public communication platform, fast and global distribution of images in public with Web pages became common means. Scanned photos then were available from an unknown number of private Web pages. The availability of digital cameras reduced the cost and shortened the time it took to put images online. However, due to the physical dimension pointing a digital camera at a person can still be noticed in many situations.

In recent years, camera-phones were introduced. The build-in camera lens on a mobile phone can hardly be recognized, which brings the possibility that anyone who holds a camera-phone in an individual's surroundings could be taking a photo of the individual without being noticed. The individual won't be able to see a camera while being photographed or filmed, and won't know whether his images are put on the Web or not.

With massive numbers of camera-phones out in the public, photos can be taken at any place. News stories about offenders being caught while shooting photos under women's dresses in public are available from the United States, Japan, Great Britain, Malaysia or even Saudi Arabia. Web sites like Voyeurweb.com have been around longer than digital camera phones exist to even commercially distribute the content. While this intrusive and offensive use of cameras is regarded illegal in many places in the world, other uses seem to create benefits for society - other news stories tell of offenders being identified thanks to camera-phone photos taken by bystanders of a crime. Considering the favorable uses of camera-phones in public, a solution that does detect, but not prevent from taking photos in public places may seem appropriate.

It has already shown to be a significant problem. At some beaches and in various companies, camera-phones are completely banned, and a number of countries have significantly increased the penalty for illegally taken pictures. Unfortunately, these countermeasures are by far not sufficient, as a growing number of Web sites boasting such pictures demonstrates. As it is impossible and unwanted to enforce a broad ban on camera-phones, and technical measures such as a simulated shutter noise when a picture is taken appear to be insufficient, we propose a novel way to complement such measures.

This paper deals with the challenge of protecting one's private data, such as image, and privacy issues attached to it. With respect to new mobile technologies and distribution channels, we sketch a privacy threat posed by millions of privately owned cameras in mobile phones.

Instead of preventing the picture from being taken, or call attention on the photographer when he takes the picture, we attack the distribution channel: if an inappropriate picture of an individual is taken and published, the victim has a fair chance of being the first one to actually find this picture, which enables her to request the pictures removal or invoke legal actions before significant privacy violation is done. The authors are aware that in extreme cases, it will be impossible to remove a picture from the Internet by legal means. However, we expect that most of the privacy violations we address are done in a context where the publisher could be convinced to remove the offending material without a legal escalation. To achieve this, we propose that each picture receives an identity, which is contained in the picture and broadcasted to the victim that is photographed. Although this approach may be insufficient against a highly dedicated attacker, it can help to prevent privacy violations from becoming a mass phenomenon, without inhibiting the use of camera-phones, motivating users to manipulate their devices, or significantly increasing the costs of the devices.

This paper is organized as follows. The legal situation is first reviewed and traditional law as well as recent efforts to tackle the issue with new laws or technological solutions is reviewed. Then the privacy threat is defined, where the attacker and attack scenarios are discussed. We introduce a basic protocol on an abstract level, and define the attack model. At a general architecture level, we propose an evolution approach from Digital Rights Management to Personal Rights Management. We propose the protocol based on content identification techniques such as digital watermarking or perceptual image hashing and broadcast channels to enable individuals to take notice when being photographed. Afterwards, we analyze the hardware infrastructure to implement our protocol, and investigate possible attacks on the hardware. Following this, we describe the software implementation of the protocol, both on the side of the camera device and on Internet search engines. Finally, we discuss various modifications of the basic scheme, and draw conclusions towards the feasibility of the technology on mobile phones with particular respect to already existing digital rights management (DRM) technologies.

1.2 Examples of legal context

Because of the fast growth of Internet new technologies as well as the incompatible policies between the different countries, in this context, privacy issues are complex. From a technical perspective, due to Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 [3], describes the protection of individuals regarding the processing and free movement of their personal data.

The right to privacy in the *EU* is defined as a human right under Article 8 of the 1950 European Convention of Human Rights and Fundamental Freedoms (ECHR). The implicit principles and constructs of The Directive define the enforcement and the representation of data protection. The terms privacy and data protection are often used interchangeably, though they are not necessarily equivalent. The Directive applies to all sectors of public life, with some exceptions. It specifies the data protection rights afforded to "data subjects", plus the requirements and responsibilities obligated for "data controllers" and by association "data processors" [10].

Several countries enacted laws against unauthorized taking of photos with individuals. More countries are debating legislation that is intended to ban camera-phones or their use. Some examples are given below.

In *Germany*, a copyright law ("Kunsturhebergesetz") protects one's own image against unauthorized publication since Bismarks's times. Photos can legally be taken without authorization, but their distribution without authorization, even to small audiences, is illegal. Exceptions are photos taken in public places at events where (press) photography usually happens. Also, individuals of "public interest" (e.g. politicians, actors, celebrities) can be photographed and published with limited restriction (see [11]).

In *Australia*, under the Commonwealth Crimes Act 1914 - Part VIIB, Section 85ZE it is an offence for "a person to knowingly or recklessly use a telecommunications service supplied by a carrier in such a way as would be regarded by reasonable persons being, in all the circumstances, offensive". In addition, following the widespread introduction of the internet, state laws were changed to address this issue. For example the Crimes Act in Victoria was amended in 1995 to include the offence of 'Stalking'. This includes telephoning and sending electronic messages with the intention of causing physical or mental harm.

While many countries do have legislation about camera based privacy invasions and the distribution of photos without consent of the photographed individuals, the question of the enforcement remains.

1.3 Current Solutions

The problem of secret photography has been recognized by most of the involved parties, including the manufacturers, politics and private citizens. Some actions have been taken, though with limited effect.

One solution is to fortify the privacy right on personal pictures and increased the punishment for the publication of such by *tougher laws*. However, this right may be hard to enforce. The photographed individual may never find out about the publication neither could do anything about it. Even though an offender was caught on the scene, the phone could already digitally transmit the photo away. Even with laws enacted, the only choice of an individual would be to arrest the offender instead of waiting for the police to show up. This is not a setting that helps all members of a society with their privacy rights.

The second approach is to *ban the use of camera-phones* in places, such as public swimming pools, gyms and Saunas, where illegal photographing is subjected. Though banning camera-phones could be the first choice in some places, this approach is only suitable for controlled areas with a high risk of secret photographing, such as companies or confidential institutes to counter espionage. The approach has also lead to the situation that even some mobile phone producers banned their own devices from their premises, e.g. Samsung and Motorola.

A more common sense solution is to add a sufficient loud *shutter-noise* such that whenever a picture is taken, it can be noticed by the environment. However, the feature is often poorly implemented. For example, if a mobile phone is switched into silent mode, the shutter noise is also turned off. Besides, given the noise pollution created by mobile phones anyhow, adding shutter noise can add to the annoyance of the technology. More, it violates the privacy of the photographer, as people around immediately learns about who being present with a camera. The approach is mostly ineffective, because the noise can be hard to heard due to general background noise or the environment, e.g. in a Discotheque, and it usually does not help the victim.

Given the difficulty to prevent pictures from being taken without dramatically infringing the rights of harmless photographers, our approach targets the distribution channel rather than the creation of the picture, i.e. pictures can be taken without restrictions. However, the individual is made aware that some picture has been taken. As soon as the picture appear on the Internet, she has a realistic chance to locate it at an early point in time, when it is still possible to inhibit the distribution by legal means. As an added value, outside of protecting the victim's privacy, this technology can also be used to distribute pictures to interested parties.

Another solution is to *enforce safe zones by broadcast.* Several businesses have developed a so-called safe haven technology which is intended to create zones where a broadcast unit tells cameraphones that photographing is forbidden there. [34] It enables digital cameras within a variety of electronic devices to be disabled including camera phones, camera PDA's, digital cameras and multipurpose MP3 players. HP is developing a privacy technology that can jam still and video cameras and blur faces of people who don't want to have their picture taken [32]. While this approach empowers property owners to define non-photographing zones, it also restricts a user's freedom of taking pictures with consent in the area. Another problem is that here is a need to implement the receiver technology into all manufacturers' handsets for an effect. Furthermore, to protect individual rights, one needs a portable unit. This only could guarantee personal rights independent from one's property protection policy.

1.4 The privacy tradeoff

In order to protect the privacy rights of the parties involved in our setting, it is necessary to make a tradeoff between the interests of the individual being photographed and the photographer. As the balance between the right to privacy and the right to photograph, we will now state the minimum rights of each party that should be preserved.

Ideally, the individual should have the right to give consent to every picture she plays a major role in; this is the actual right granted by law in the European Union. This right is hard to enforce technologically, however, as it includes judgment on when a picture is a picture of a person, or just a picture of a marketplace that happens to have people on it. As a minimum, the individual has the right to know she has been photographed, and to have a chance to get an early warning if the picture is being published, which allows her to take appropriate steps in needed.

As long as the photographer does not infringe any personal rights, he should have the right to take pictures without any major obstacles. In this, the protocol should preferably be passive, and not prevent him from taking pictures unless under well defined and measurable circumstances. Furthermore, the photographer has the right to stay anonymous, as long as he does not infringe anybody else's rights. Finally, the photographer has the right to modify his device; for example, the camera in a PDA should not stop working if the operating system is modified or replaced.

2 An infrastructure for personal rights management

2.1 Attack model

Possible attacks from both the technical and privacy aspects will be discussed. From a technical point of view, even with a technically perfect scheme, an attacker could easily circumvent the entire system by using a traditional camera with strong zoom optics or a traditional mini-camera. The problem is not only in the professional voyeurs, but also in the wide deployment of photographic devices and the ease of secret photographing. We assume the attacker can do simple modifications to the device and the picture, and that the corresponding instructions will eventually be published on the Internet. For instance, there are Internet sources to offer modified operating systems for mobile phones to turn off the noise generated while taking a picture. On the other hand, there are many possible attacks for content identification techniques proposed in the literature. However, there is always a balance between the risks for the service provider if the watermarking or hashing scheme is circumvent, and the benefit for the attacker to attempt to break the scheme compare to the amount of effort spent.

From the privacy and legal point of view, it is an unavoidable issue that we want to protect the rights of the harmless photographers: unless we treat every owner of a mobile phone like a criminal, there will possible for a sufficiently motivate attacker to escape from the scheme. Apart from making the technology stronger and therefore less attractive to the attackers, our protocol also has their merit if combined with legal measures. By attacking the scheme, it demonstrates a photographer has a "criminal intend". Therefore, it is easier to distinguish a normally harmless person that just couldn't resist taking a picture in a particular situation from a semiprofessional voyeur with manipulated equipment.

2.2 Basic protocol

Players. There are three major players in our setting: the photographer, the model, and the search engine. The *photographer (Bob)* is the person who takes the pictures. Bob uses a camera-phone, which is a mobile phone with a build in camera. From a privacy point of view, Bob has the rights not to be inhibited while taking the pictures and has his identity preserved as long as he does not infringe the rights of anybody. Bob also has the right to perform some "standard" changes to his camera-phone, such as updating the operating system.

The *individual (Alice)* is the person that is photographed by the photographer. The interest of Alice is that whether she has a control over the pictures taken of her or not. It means that in case she is the focus point of the picture, this picture should (ideally) not been taking without her consent. In our protocol, we grant her a lesser right: If a picture taken from her is published, she gets a fair chance to find out early. Alice uses a receiver, which registers the identities of pictures taken in her vicinity. The receiver could be her own mobile phone or a specialized piece of hardware. It can also be integrated in the infrastructure provided by external parties, for instance, the owner of a discotheque or even the GSM operators.

Finally, the *search engine* searches the Internet for picture identities and makes them publicly available. They are similar as any Internet search engines, with slightly modified rules.

The protocol. A possible scenario of our scheme will be discussed in this section. The goal is to let an individual "Alice" detect unauthorized publication of personal images taken by others "Bob". We name the complete setting a Personal Rights Management (PRM) system.

In the first step, Bob secretly takes private photos of unaware Alice with malicious intent, as shown in Fig. 1. Luckily, the camera on Bob's mobile phone applies PRM to the photo when it is taken. The photo can be identified and marked by using several data protection techniques, such as digital watermarking, robust perceptual hashing, or Digital Rights Management technology.

In case digital watermarking techniques are used, Bob's camera embeds the image content identification in the picture. In case robust perceptual hashing techniques are used, Bob's camera sends the picture together with the image hash values. All the possible techniques used for content identification will be discussed in the software implementation section.

On the other hand, the marked photo is broadcast with a short-range radio. Alice's receiver picks up the picture identification information and stores it for later use, as shown in Fig. 1.

In the next step, Bob publishes the unauthorized photo from Alice to an online community which is very unfavorable to Alice. Alice would take action on this if she knew the photo was published. Luckily, Alice can detect the unauthorized publishing of the photo using the PRM search engine (see Fig. 2). When Bob puts the picture from Alice on the Internet, the specialized search engines find it and index it by the extracted watermark or the perceptual image hash values. Alice uploads the collected photo marks or identification numbers to a specialized search engine. Then the search engine checks photos published on the web by photo identifications. Upon notification from the search engine, Alice

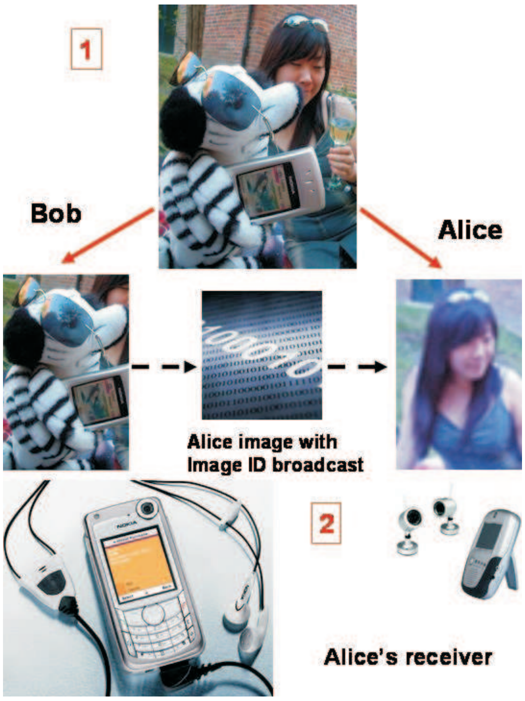
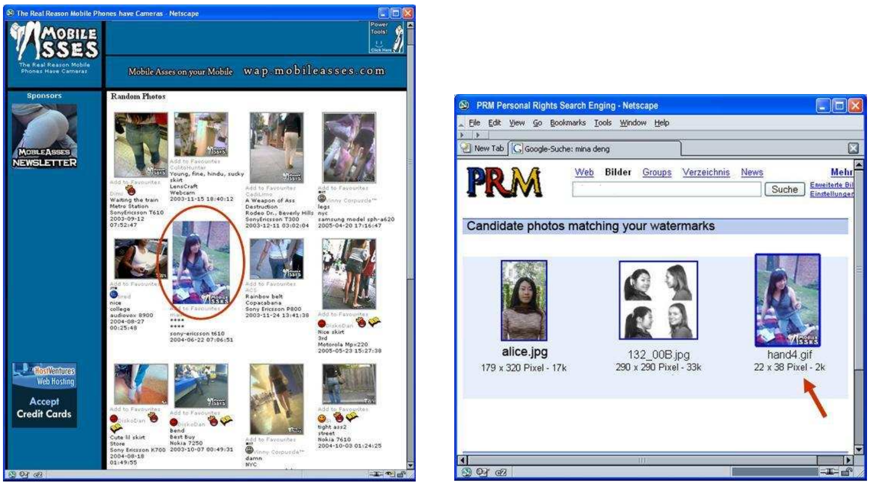


Fig. 1. The first two steps of the protocol, communication between Alice and Bob. Bob secretly takes private photos of unaware Alice with malicious intent. Alice's image together with identification information are sent to the receiver of Alice.



Candidate photos matching your watermarks

alice.jpg
179 x 320 Pixel - 17k

132_00B.jpg
290 x 290 Pixel - 33k

hand4.gif
22 x 38 Pixel - 2k

Fig. 2. The last two steps of the protocol, Bob publishes the unauthorized photo from Alice to an online community which is very unfavorable to Alice. Alice can detect the unauthorized publishing of the photo using the PRM search engine.

checks whether the photos found have her picture on them and takes appropriate actions to protect her privacy.

In summary, the photo taking is not prevented. From the beginning to the end, Alice and Bob both remain anonymous. Only upon publishing of an image, the image will be detected and reported to Alice.

2.3 Architecture evolution from DRM to PRM

At an system architecture level, there is a potential of adapting Digital Rights Management (DRM) systems for the purpose of Personal Rights Management (PRM) according to the legal requirements. DRM technology, developed for protecting intellectual property rights, appears to have features that would allow the development of a system-based approach to data protection compliance, i.e. Personal Rights Management.

DRM architectures support description, trading, protection, monitoring and tracking of the use of digital content. These technologies may be contained within operating systems, program software, or in the hardware of a device.

PRM manages personal data from the data subject, the originator and the owner of the personal data. The Directive [3] defines the authorities and boundaries of the relationships between each of the participants. The driving purpose behind DRM, thus the content distribution management, relates easily to data protection constructs constraining the exchange of personal data. [18]

For the purpose of expressing privacy in a PRM system, the Open Digital Rights Language (ODRL) [1] and extensible rights mark-up language (XrML) [2] can be applied, which are similar as the rights expression languages used in a DRM system.

Korba et al.[18] propose an adaptation of DRM functionality to provide PRM for individuals by assigning names to the functional parts in the DRM setting from the privacy enhancing techniques vocabulary. Thus it brings some form of taxonomy or meta-design for PRM.

3 Hardware implementation

3.1 Basic proposal

The hardware and software implementations of the proposed protocol will be discussed in the following sections. We assume that no mobile phone manufacturer will be willing to add a completely new communication technology into the devices to enable a protocol such as the one presented above. Therefore, we restrict ourselves to the current hardware available in the market. Three possible communication standards, Infrared, Bluetooth, and GSM network, can be used to establish the link between camera-phone from Bob and the receiver from Alice.

Infrared. One feature of infrared communication is that it is directed, i.e., the signal can be sent in a way that only the devices in the view of the camera can receive it. The penalty paid is that the bandwidth of infrared communication is fairly low, and the transmitting distance might be too small. It can cause a problem on the receiving side: if the receiver is not directed to the camera, it may not get any signal at all. It is fairly easy to block the communication by simply gluing an object onto the infrared port. This problem can be solved by building the receiver into the enabling function of camera lens. This way, blocking the communication would disable the ability to take pictures. The second problem could be to block the communication by jamming the signal with a strong infrared light. Though the problem is harder to deal with, it is possible to design a camera that can not take pictures if exposed to a strong infrared signal. However, another problem arises when the jamming signal may be directed and allow for a denial of service attack, i.e., preventing all camera phones to take pictures at all.

Bluetooth. Bluetooth communication is n a way the complement of Infrared. The communication is very difficult to jam, and the bandwidth is sufficient even for interactive protocols. The disadvantage is that a Bluetooth signal is undirected and all devices that are not in the visual scope of the camera get the signal as well. Another disadvantage is that currently enabling Bluetooth on a phone may pose a security risk. Recent studies[7] show that many Bluetooth phones are open to attacks that may reveal the entire phone memory, including the address book, the calendar etc. Thus, unless the security of this technique can be improved, to protect the privacy of Alice's pictures she may have to risk a privacy-invasion on her phone book.

GSM-Network. It is by the nature of mobile phones to communicate on the GSM network. However, the GSM protocol is ill-suited for device-to device communication. Adding this capacity would require major changes in the GSM standard, which is unlikely to happen for the purpose of protecting people form illegal pictures. It would be possible to use the base-station as an intermediate in a way that the photographer's device sends a signal to the base-station, which in turn sends a cell broadcast to all devices in the area. This creates new problems. One on hand, many devices that don't have anything to do with the picture will be noticed altogether. On the other hand, phones at the same location may be locked into another cell or use a different provider.

All of the above. A combination of those techniques can be proposed, for instance, an infrared flash could be used to command the device to listen to a Bluetooth signal or a GSM cellular broadcast. If implemented properly, this could combine the advantages of all technologies. As the infrared signal only has to carry a binary signal, the low bandwidth and limited range are not problematic anymore. And as receivers neither see the flash nor listen to the radio signals, they can be configured not to pick up the pictures out of their interests.

3.2 Attacks on the hardware

A few examples are given here on how an attacker can disable the proposed functionality by manipulating their devices. For some mobile phones, the shutter noise can be manipulated to be turned off when the entire phone is put in silent mode. For our protocol, it is possible to block the transmission by deactivating Bluetooth or by using it to communicate with another device while the picture is taken. Some users directly modify their mobile phone hardware to detach the infrared light or the Bluetooth antenna. For some mobile phones, there are some firmware to manipulate the corresponding functionality available on the Internet, and it is easy to perform by a normal audience. However, mobile phone manufacturers have recently started to think about other functionalities that a user may not manipulate, e.g., Superdistribution and Micropayment from Nokia. It is foreseeable that this problem will be solved in the near future, e.g. by using a core-operating system which cannot be changed by the owner and building the real operating system on top of this core, or by TCPA/TCG-like technologies.

4 Software implementation

4.1 Digital image watermarking

Digital watermarking is a technique for embedding information in digital content without perceptually altering its appearance[12]. In our system, one intuitive way could be to append a visible watermark on the host image. The visible watermark can be any information that identifies the photographer and/or the time stamping analogous to analog cameras. However, the obvious drawback is that an attacker can easily remove the watermark by an image editing software despite of destroying the watermarked region of the image.

Various imperceptible robust image watermarking applications are studied [17, 14]. In the system we proposed, the key point is to identify the secretly photographed image rather than to authenticate the image integrity. This is because Alice is more interested to identify whether the image is from her or not. The owners' and/or user's information can be embedded directly into the images to protect copyright. And a rather high level of robustness against malicious attacks is required.

For watermarking system, it should be computationally infeasible to extract the watermark information even if the algorithm of the watermarking principle is known. Therefore, secrete or public keys should be used to provide the security of watermarking. This is the same as the Kerkhoffs law[24] in cryptography.

The design of a watermarking algorithm always involved a tradeoff between robustness, imperceptibility and capacity [14, **?**,**?**]. In our proposed scheme, the optimal balance among these three attributes should be found if properly designed. The capacity of the watermark doesn't have to be large, thus extra robustness could be gained. In order to get optimal robustness, watermark should be embedded just below the perceptual level, and the knowledge of human vision systems (HVS) are applied to the imperceptible watermarking schemes[31].

A few benchmarking of watermarking to provide a fair evaluation of watermarking parameters are introduced, such as Stirmark[30], Optimark[36], and Checkmark[29], etc.

From a practical point of view, with an expected 70 million camera-phones sold by 2006, a 40-bit image identifier should be sufficient even for high usage of the cameras. Although there are no firm numbers, to embed a 40-bit watermark into a picture with 640*480 pixels is quite realistic. For example, the Stirmark[30] can perform the test with 100 bit watermarks on 512*512, 24-bit colored pictures.

Limitations of the watermarking scheme. One of the weaknesses of our watermarking scheme is that everybody has the ability to extract the watermark information from the picture. When facing a general audience, a secrete key sharing scheme is improper, thus it is better to use a public key watermarking scheme. The photographer embeds the watermark by his private key, and other interested party can extract the watermark by using the owner's public key. Thus it inherently works as a digital signature, and only provides authenticity of the photographer but little security of the algorithm. It also creates a privacy threat, although the watermark information itself can be a random string without any meaning, the private key used inhibits the privacy of the photographer. Moreover, it assists the photographer in attacking the watermark, as he can always verify whether his modifications destroyed the information or not. Possible modifications to solve the problem will be discussed in later section.

4.2 Search engines

The final player of our protocol is a search engine that allows the individual to locate the pictures on the Internet. The search engines could work just like any ordinary ones, except for the ability to extract the identification information from the pictures and use it as an index. It requires that the watermark extraction or other algorithms to be computationally feasible. Commercial web spiders are already available for copyright protection. As reported in [33], Digimarc, a company which holds most of the core patents on digital watermarking, introduced a tool called MarcSpider[22], purported to crawl the web to search images, test them for watermarks and report on infringers. Due to the fact that crawling the web quickly became an intractable task, as well as that only a small number of copyrighted images installed on the web, MarcSpider didn't work out as a huge success.

Some counter technologies have been developed to hide the pictures from the spider, for example by splitting it into many small pictures or by embedding it using JavaScript. This is another point where a sufficiently motivated attacker can circumvent the scheme, which is hard to deal with unless the privacy of the photographer is inhibited.

There could be a privacy problem if Eve will be unable to guess a valid watermark and query the search engine for a nice collection of Bob's photos from a particular event which is possibly including all of Alice' unfavorable photos. In order to void that, we propose that the particular broadcast code identifying a camera photo should be secure in the sense of "impossible to guess". Another privacy problem could be introduced by the search engine, such as profiling of all watermarks Alice submits in order to create an album of Alice's life. Besides, we define that the search engine is to be used with some anonymous connection to avoid linking of ID and image requests.

5 Modifications

5.1 Perceptual robust image hashing

The watermark-based approach is expected to be sensitive to malicious modifications of the media, thus brings the robustness issue dependent on applications. As the watermark is embedded into the host data, the data content is altered and image manipulations may be localized in most schemes[35].

Robust perceptual hashing, which can be used in multimedia applications both for data identification and robust data authentication, is meant to complement digital watermarking. The main advantage for perceptual hashing schemes is that the data is neither altered nor degraded. If a malicious attack on a watermarking scheme succeeded, the watermark would be destroyed. However, the perceptual hash value will remain the same as long as the perceptual features of the data are unchanged. This is also the reason why perceptual hashing is used instead of cryptographic hashing, which is very sensitive to a single input bit. Perceptual hash functions can be particularly useful to identify illegal copies, since the illegal content are usually lossy copies of the original.

The main requirement of our scheme is the image identification. An occasional collision between two picture-identities does not cause a significant trouble, although it merely poses a minor annoyance to a user. Therefore, the picture identity does not need to be excessively long. With a k-bit identifier, we need $1.2 * 2^k$ pictures for the to get 0.5 probability of a collision. Therefore, it is proper to apply perceptual hashing schemes to our application.

Four requirements for image hash functions are defined in [25]. A generic image hashing can be achieved into two steps: feature extraction and secure compression of the feature vector. It is shown that the robust feature vector detection is the key point for robust image hashing. Various feature extraction methods are developed based on different concepts, such as by using wavelet [25, 28, 27] , DCT [13], matrix invariance [19], different descriptors [26]. [23] propose a frame to achieve feature extraction in three steps: quantization, bit assignment, and error correcting code. Many algorithms are proposed for the second step that secure compress the feature vector, including those based on cryptographic hash functions procedure [35], error correcting codes [25, 28] , and secure compression for authentication applications [16]. Various image hashing methods are analyzed and the experiment results are compared in [35, 8].

Having generality and robustness as the two attributes, a feature detection algorithm can be considered robust if it identifies the same feature locations independent of different attacks, such as Stirmark attacks, compression, image processing or geometric distortions. Hamming distances between the hash values of perceptually similar images and between different images can be examined to evaluate the algorithm.

5.2 Broadcasting a sample picture

In addition to the image identifier, a strongly compressed sample version of the picture could be broadcasted as well. This would inform the individual whether there is a need to take immediate action or not, e.g . when a specially compromising picture has been taken or a credit card has been photographed. However, this costs a significant bandwidth, and significantly infringes the privacy of the photographer. Due to the content of the image taken by the photographer is broadcasted, the photographer could be easily identified, and therefore, the privacy of the photographer could be violated. Besides, the intellectual property of the photographer, i.e. his work of art in arranging and taking the photo, could be massively infringed by broadcasting it to the world.

5.3 Limited access to the identity verification

There exist security problems if any individual is able to verify the identity information. Therefore, a limited access control is required and it can be achieved by using shared secrete keys among authenticated parties for watermarking, perceptual hashing or encryption. The advantage is that it could increase the difficulty to attack the scheme, as it is not easy to verify if the watermark has been successfully removed. However, this would give the trusted parties an exclusive power to use the scheme. That might be unwanted, and it may also raise the question on who can select these trusted parties.

5.4 Hybrid DRM solutions

Several DRM techniques can be integrated into our scheme. In a generic DRM mechanism, digital watermarking and perceptual hashing are used for content protection and/or identification, while encryption and digital signature are used for content confidentiality and integrity[20]. New watermarking based techniques can be used to identify, trace and control the use of digital copy and enhance the content protection thus strongly improve DRM [21, 33]. In the application of mobile DRM, watermarking has been suggested as an key technology for *media identification*[37, 15], especially since user's identity is known in mobile networks. It is expected that the market will thrive by delivering multimedia content through Multimedia Messaging Service (MMS). The content should be wrapped in DRM packages prior to distribution. The proposed DRM technology for the Open Mobile Alliance (OMA) specifies three different methods that vary in complexity requirements, and that offer different levels of security for the distributed content [6]. *Privacy tracing* with the defense of intellectual property rights and *copy protection* where a copy-bit is un-removal from the host content[21] which require different level of requirement of watermarking robustness.

Encryption and watermarking are to be combined as two defensive lines to enhance DRM. For image content, selective encryption[5] is introduced to encrypt a portion of the compressed data. In our proposed scheme, to protect the photographer's privacy, the watermarking embedded information can be further encrypted by the user's ID as a secrete key, so that only the authenticated party can extract the information [4]. A watermark can be used to serve as a proof of ownership but is vulnerable to attacks such as average and collusion attacks [38]. In addition to ensuring that a watermark cannot be removed, the DRM system has to ensure that a fake watermark cannot be inserted. [21] analyze several DRM scenarios related to image distribution, and propose a fair and efficient benchmarking of open-source web based evaluation system. Benchmarking parameters and requirements are scenario dependent.

While we discuss the image content protection or identification from a technical perspective, it is important to note that any technique that allows a user to assert their ownership of any digital object must also be placed in the context of intellectual property right law [31].

6 Conclusions

Camera-phones have been used in much more malicious ways than just to invade privacy, and control over one's image is hard to enforce today. Several reports have been published of cases where credit card information has been obtained by secret photographing of the card. The problem is analyzed from both the privacy and technical aspects in this paper, and possible solutions are proposed. There is a tradeoff between the privacy rights of the individual to have control over images and the privacy rights of the photographer. It is of limited effort for initiatives to enact laws to ban the unauthorized photos when lacking of a technological support for the enforcement and prosecution. On the other hand, users and consumers reject technology that presses restrictions on them. While we are aware that our solution- due to the conflicting interests we need to satisfy- leaves a number of issues unresolved, we believe that a great advantage for individual privacy can be achieved by the proposed personal rights management.

We propose a detection system that combines cryptographic and data protection technologies together with legal regulations in order to control the distribution of private photos online. The scheme can empower individuals to detect and act upon violations without putting strong restrictions on cameras and photographers. Content identification mechanisms such as digital watermarking and robust perceptual hashing are integrated to enhance a PRM system. Techniques to apply in our scheme are discussed and possible attacks together with hard- and software solutions are analyzed.

To evaluate the usability of our proposed scheme, it is not difficult for one to imagine that it will require a significant amount of time and energy if Alice has to check hundreds of pictures per day from search engines. However, as a normal individual the chance that Alice gets a high amount of images taken is fairly low. This scheme can be interesting for celebrities though, who are able to afford hiring people to do the checking work in order to make sure that their personal rights are not violated.

Given the potential commercial value of the privacy market, an investment in Personal Rights Management appears to be worthwhile both in terms of what has to be done to achieve compliance with current legislative requirements and to meet privacy policies towards building a stronger trust relationship with clients.

7 Future work

The general concept of Personal Rights Management is designed to keep protection as well as to track the sharing process of personal data. Based on the PRM concept to control personal images as we proposed in this paper, further research can be focused on working out the protocol prototype implementations and security. TCPA/TCG- like trusted computing platforms or DRM systems could be integrated to the prototype to achieve an generic PRM architectures.

We discussed the time problem if Alice has to check hundreds of pictures per day. We propose to ease the problem by adding location data and biometric (facial etc.) recognition algorithms to search engines to reduce complexity for Alice. Future research could work out on how to implement this feature.

New applications of PRM could be expended into other aspects of peer to peer privacy violations. While private images taking are the most eminent area of privacy issues caused by peers, other threats are emerging. There is a vast increase of video camera-phones on the market, which brings a similar privacy threat as the privacy image scenario. There are many mp3 players equipped with recording functions. Though the tendency yet to put electronically recorded conversations or videos online on a large scale is not as high yet, the mere presence of such a high number of uncontrolled recording devices may pose a significant problem in the future. A recent story of a high school teacher Jay Bennish in the US shows an example for a problem caused by privately owned recording equipment. The teacher's speech was investigated, because of a student's recording in class and complained to the principal.[9] Another emerging problem is the ever increasing number of Weblogs, combined with search engines to efficiently find personal information therein. Furthermore, PRM scenarios could be applied to protect personal geographical location data as well.

Acknowledgements

The authors would like to thank Claudia Diaz for her constructive comments on our work and the valuable comments from the anonymous reviewers.

References

1. *Open Digital Rights Language (ODRL).* `http://www.odrl.net`.
2. *XrML is being contributed to the standards body OASIS Rights Language Technical Committee as its foundation technology.* `http://www.xrml.org`.

3. Directive 95/46/ec of the european parliament and the council of 24 october 1995. *Official Journal L 281, 23/11/1995*, page 0031 0050, 1995.
4. A. Adelsbach, S. Katzenbeisser, and H. Veith. Watermarking schemes provably secure against copy and ambiguity attacks. In *Digital Rights Management Workshop*, pages 111–119, 2003.
5. L. Agi and L. Cong. An empirical study of secure mpeg video transmissions. In *In Proc. of the Internet society symposium on network and distributed system security*, San Diego, CA, February 1996.
6. Open Mobile Alliance. *OMA digital rights management version 1.0.* OMA. `http://www.openmobilealliance.org/documents.html`.
7. John Blau. *Cracks appear in Bluetooth security.* NetworkWorld.com, Feb. 2004. `http://www.networkworld.com/news/2004/0211cracksappear.html`.
8. P. Cardin. *Robust signal representation for image identification and hashing.* Student Literature survey, 2005.
9. CNN. *Teacher's Bush remarks investigated - Some students protest teacher being put on leave*, March 2006. `http://www.cnn.com/2006/EDUCATION/03/03/teacher.bush.ap/?section=cnn_topstories`.
10. L. Deitz. Privacy and security ecs privacy directive: protecting personal data and ensuring its free movement. *Computers and Security Journal*, pages 25–46.
11. Alexander Dix. Das Recht am eigenen Bild – Anachronismus im Zeitalter des Internet ? In *Mediale (Selbst-)Darstellung und Datenschutz, Konferenz des LfD NRW*, 2000.
12. R. J. Anderson F.A.P. Petitcolas and M. G. Kuhn. Information hiding-a survey. volume 87, pages 1062–1078, 1999.
13. Jiri Fridrich and Miroslav Goljan. Robust hash functions for digital watermarkin, March. 2000.
14. F. Hartung and M. Kutter. Multimedia watermarking techniques. In *special issue on protecting of multimedia contents*, volume 87, pages 1079–1107. Proceedings of the IEEE, July 1999.
15. F. Hartung and F. Ramme. Digital rights management and watermarking for multimedia content for m-commerce. In *IEEE communications magazine*, volume 38, pages 78–84, Nov. 2000.
16. M. Johnson and K. Ramchandran. Dither-based secure image hashing using distributed coding. In *ICIP (2)*, pages 751–754, 2003.
17. S. Katzenbeisser and F.A.P. Petitcolas. *Information hiding techniques for steganography and digital watermarking.* Artech House, INC., 2000.
18. L. Korba and S. Kenny. Towards meeting the privacy challenge: Adapting drm. In *Security and Privacy in Digital Rights Management, ACM CCS-9 Workshop (DRM 2002)*, pages 118–136, November 2002.
19. S. Kozat, M. Kivanç Mihçak, and R. Venkatesan. robust perceptual hashing via matrix invariance. In *Proc. Of IEEE international conference on image processing ICIP*, Singapore, Sept. 2004. Springer-Verlag.
20. W. Ku and C. Chi. Survey on the technological aspects of digital rights management. In *ISC*, pages 391–403, 2004.
21. Benoit M. Macq, Jana Dittmann, and Edward J. Delp. Benchmarking of image watermarking algorithms for digital rights management. *Proceedings of the IEEE*, 92(6):971–984, 2004.
22. MarcSpider. *Digimarc image tracking service.* DigiMarc corporation, 2001. `http://www.digimarc.com/products/imagebridge/MarcSpider/default.asp`.

23. Elizabeth P. McCarthy, Felix Balado, Guenole C. M. Silverstre, and Neil J. Hurley. A framework for soft hashing and its application to robust image hashing. In IS&T/SPIE, editor, *In Proc. of SPIE, Security, Steganography, and Watermarking of Multimedia Contents VII*, volume 5681, pages 5681–06, San Jose, CA, USA, January 2005.
24. A. Menezes, P. van Oorschot, and S. Vanstone. *Handbook of Applied Cryptography.* CRC Press, 1997.
25. 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.
26. Krystian Mikolajczyk and Cordelia Schmid. A performance evaluation of local descriptors. Submitted to PAMI, 2004.
27. V. Monga and B. L. Evans. Robust perceptual image hashing using feature points. In *Proc. IEEE Int. Conf. on Image Processing*, Singapore, Oct. 2004. Singapore.
28. V. Monga, D. Vats, and B. L. Evans. Image authentication under geometric attacks via structure matching. In *Proc. IEEE Int. Conf. on Multimedia & Expo*, London, UK, July 2005. Amsterdam, The Netherlands.
29. S. Pereira, S. Voloshynovskiy, M. Madueno, S. Marchand-Maillet, and T. Pun. Second generation benchmarking and application oriented evaluation. In *IHW '01: Proceedings of the 4th International Workshop on Information Hiding*, pages 340–353. Springer-Verlag, 2001.
30. F.A. Petitcolas, M. Steinebach, F. Raynal, J. Dittmann, C. Fontaine, and N. Fates. Public automated web-based evaluation service for watermarking schemes: Stirmark benchmark. In *SPIE International Symposium on Electronic Imaging 2001*, volume 4314 of *Proceedings of the SPIE*, pages 575–584. SPIE, 2001. Security and Watermarking of Multimedia Contents III.
31. C. I. Podilchuk R. B. Wolfgang and E. J. Delp. Perceptual watermarks for digital images and video. In *special issues on identification and protection of multimedia information*, pages 40–51. IEEE, 1998.
32. Emily Raymond. *HP Developing Picture Jamming Technology to Block Unwanted Photographs.* `http://www.digitalcamerainfo.com/d/News.htm`.
33. B. Rosenblatt. Steganography revisited: watermarking comes in from the cold. 3(5), June 2003.
34. Sensaura. *UK companies team to solve worldwide camera phone privacy abuse. British Safe Haven technology enables digital cameras to be disabled in a localized environment.* Sensaura press release, Sept. 2003. `http://www.sensaura.com/news/pr.php?article=2003_09_11.inc`.
35. C. J. Skrepth and A. Uhl. Robust hash functions for visual data: An experimental comparison. In *Iberian Conference on Pattern Recognition and Image Analysis*, pages 986–993, 2003.
36. V. Solachidis, A. Tefas, N. Nikolaidis, S. Tsekeridou, A. Nikolaidis, and I.Pitas. A benchmarking protocol for watermarking methods. In *Int. Conf. on Image Processing (ICIP'01)*, volume 21, pages 1023–1026. IEEE, October 2001.
37. M. Trimeche and F. Chebil. Digital rights management for visual content in mobile applications. In *First International Symposium on Control, Communications and Signal Processing.* IEEE, March 2004.
38. M. Wu, W. Trappe, Z. Wang, and K. J. R. Liu. Collision resistant fingerprinting for multimedia. In *Signal Processing magazine*, volume 21, pages 15–27. IEEE, March 2004.