[DWA01] *Jana Dittmann, Petra Wohlmacher, Ralf Ackermann;* **Conditional and User Specific Access to Services and Resources using Annotation Watermarks;** Proceedings of the Conference on Communications and Multimedia Security (CMS 2001), May 2001, S. 137-148.

Conditional and User Specific Access to Services and Resources using Annotation Watermarks

Jana Dittmann[1], Petra Wohlmacher[2] , Ralf Ackermann[3]

[1]*GMD–IPSI, Darmstadt*
Jana.Dittmann@gmd.de

[2]*University of Klagenfurt*
petra.wohlmacher@uni-klu.ac.at

[3]*Darmstadt University of Technology, Industrial Process and System Communications (KOM)*
Ralf.Ackermann@KOM.tu-darmstadt.de

Keywords: digital watermarking, conditional access, e-commerce

Abstract: The tremendous recent efforts to develop and deploy ubiquitous mobile communication possibilities are changing the demands but also possibilities for establishing new business and commerce relationships. Within this paper we show our innovative approach for integrating watermark and cryptography based methods within a framework of new application scenarios spanning a wide range from dedicated and user specific services, "Try&Buy" mechanisms to general means for long-term customer relationships. Based on a description of the challenges of the application domain and the existing work we show, which methods must be used for establishing services in a fast convenient and secure way for conditional aceess services. The paper eloses with an overview of steps for practically establishing these concepts.

1. INTRODUCTION

Nowadays, multimedia systems are increasingly used. Capturing, storing, editing, retouching, printing, copying, and transmitting high quality colored images has become lucrative business, as well as one focus of national and international research institutions and organizations. With all this new and powerful imaging technology, unfortunately digital data can easily be manipulated and multiplied without information loss. To prevent the production of unauthorized copies, misuse, and theft of material, beside legal regulations mainly security solutions are required to provide control mechanisms.

Digital watermarking combined with other (cryptographic) mechanisms allows to offer several security services today. Robust digital watermarking can be used to claim copyright protection by embedding authors, producers or customer information (known as copyright watermarks and fingerprint watermark). Fragile watermarking techniques address the recognition of manipulations, known as integrity watermarks. Beside securing copyrights and authenticity of digital data, watermarks are used to annotate the data and provide additional information to the users. Therefore, these watermarks are called annotation watermarks [DSKS00].

Beside the security features of digital watermarks, the watermarking approaches facilitate additional value in electronic commerce. Printed documents annotated with watermarking information, allow to connect them with the digital world. For example, images of advertisements printed in newspapers may include annotation watermarks. Showing the image to a camera, the annotated image enables a direct and easy connection to the internet page of a dedicated company or vendor. This procedure is much easier and faster than typing in an URL which is moreover error-prone and difficult to handle. Technical solutions for this scenario are already available, e.g., MediaBridge [Dig01]. Furthermore, the embedded information can represent action descriptions to occur during retrieval of the watermark. This kind of annotation watermarks is also called active watermarks. For instance, with Digimarc MediaBridge, the watermark signal can be detected and read with a PC camera and the Digimarc MediaBridge reader (see [Dig01]).

Using these features, added watermarks conveys much more information to the consumer than text or audio alone. And with the advent of such active digital watermarking, yet another level of information can be invisibly added to an image. This additional information remains dormant until the reader software detects it. The information can then be displayed, used to control the software or hardware that is processing the image, and used to obtain more information from the internet. This dormant information gives the image intelligence; hence Digimarc have coined the term "smart image"

[Ala00]. Annotation watermarks can bridge gaps between various media representations.

Beside these new applications for watermarks, there is another ongoing process that supports the increasing mobility of people. Particularly, the setup of UMTS-technology based networks form a basis for the crowing of mobile business (M-Business) and especially mobile commerce (M-Commerce). Prognoses claim that in 2003 more than 1 billion people are going to use mobile phones. Additionally, further developments of personal digital assistant (PDA) together with appropriated security mechanisms are going to make them more suitable for mobile access to different networks. Both trends will lead to a high success for the M-Commerce sector.

Annotation watermarks are especially appropriated for M-Commerce, because they can easily support additional information which can be used for mobile access. Additionally, since annotation watermarks are available in a separate medium e.g. in a hard-copy version, they allow an easy way to get people paid for these additional information. But it is quite clear, that even unauthorized people owning a watermarked image, could try to get access to this information. Therefore, there is need for conditional access mechanisms. Those should combine annotation watermarks, strong cryptographic and online-communication mechanisms as provided by innovative equipment like WAP-Handies or networked PDAs.

In our paper we discuss new approaches to combine annotation watermark with additional security features to provide approaches for access control in M-Commerce applications. Our intention is to design a new conditional access mechanism combining annotation watermarks with cryptographical mechanisms. Initially, in the next section we describe important aspects of M-Commerce. In section 3 we give example scenarios that use annotation watermarks for access control strategies. In section 4 we discuss technical solutions together with cryptographic issues and possible attacks. Finally, we give conclusions and point out some future work.

2. ASPECTS OF M-COMMERCE

Traditional economy is under a rapid development and change at the moment in order to adapt to the needs of global markets and an evolving information and knowledge society. This results from a number of factors including the development of new communication devices and their general availability at relatively low prices, the ongoing deployment of new communication networks (such as GPRS or UMTS) that start to ensure a general network connectivity as well as from the evolving uses of the internet for both identifying products and offers as well as for purchasing those. That

leads to a new innovative kind of business and communication relationships that we describe as M(obile) Commerce.

The current mechanisms usually try to map existing procedures such as (search, order and buy a product) to the new (networked advertising and purchasing) channels and thus do not exploit all the potential benefits.

We give a definition of the area of and the characteristics that we have identified. In the conventional case (e.g. a customer buying a book) the product that he purchases is static. For both the customer (because he probably wants to receive updates, enhancements or just additional information to the item he has purchased) as well as for the producer or vendor of the item (who e.g. may want to sell more products or receive personalized information about the buyer), having a further interaction is very reasonable.

Though a number of possible ways for establishing such an ongoing relationship exist (think of a WWW page where new information is available for download or a kind of mailing or information list or a "push channel" that the customer is described to) which usually lack a fine granularity of identifying a particular partner and usually involve typing in a certain WWW address or filling out and sending a form. If the information how to do that is printed at the item itself without having an additional layer of indirection it may outdate and be incorrect very fast as well.

From those facts we can identify the following features that should be supported by a protocol framework appropriated for M-Commerce:

- placing individual information on an item should be possible at low cost, at a "late" (maybe just the selling) time within the production and selling process and regarding a fine granularity of distinguishing between customers, conditions and point of sale as well as price,
- the placement of the information should be as less obtrusive as possible though this requirement may be lowered under certain circumstances,
- retrieving and using the information should be easy and convenient for a user. Within the retrieval and usage process a flexibility (e.g. by means of an indirection step which gives) should be possible.
- since the mechanisms described above may influence a customers privacy (e.g. by having the means for tracking transactions and even user behavior) possible approaches have to regard this fact at an early design phase already. Legal regulations demand that a user should be aware of possible uses and must have a chance to actively influence or avoid them.

The application areas that we describe have a number of requirements that can not fully met using just conventional protocols. Especially they benefit from closing the existing gap between different media presentations and transport channels.

3. SCENARIOS USING ACCESS CONTROL

Access control mechanisms provide solutions for M-Commerce provider to limit access to additional value services for paying or preferred customers. In this section we discuss example applications for access control using annotation watermarks: E-Book, Errata, Prepaid Services, Try&Buy, and Long Term Customer Relationships.

1. **Buying Books:** Barcode and possible combination with other characteristics determine service. Buying books online or getting updates for them later on is a service that is very common meanwhile. A book holds a number of characteristics such as its ISBN that allow to identify it – but does that on a level that is not fine grain enough. By adding additional information via an annotation watermark to (e.g.) the printed barcode label there is a more flexible way to provide hidden information about the seller or the type of contract or price that was used or how to grant access to further information.
1. **Errata:** Update service with annotation watermarks. For a large number of products (either electronic but conventional ones as well) it is necessary to update information such as configuration data, firmware or just to provide corrections to the content. In these cases it is quite desirable to provide individual services to a user that has already paid for that service or is willing to do so. In this case an (individual) annotation watermark can be used to uniquely identify both the item as well as the selling channels. Thus, it is easier to ensure that the correct information is delivered and only persons that are also meant to receive it may use the service.
2. **Prepaid Services:** Code activates service. The prepaid service scenario offer the possibility to embed codes as annotation watermark into the data. Only after ordering an additional code, the additional service is activated and can be used.
3. **Try&Buy:** Partial access to annotations. Try&Buy mechanisms support authors, producers, resellers or content providers to allow evaluation of the data by potential customers. Interested parties receive data in inferior quality first to evaluate and to verify their intentions to buy the product. The data is not delivered in the original quality until the payment was done or until special conditions are fulfilled. Try&Buy transactions can be realized by a transparent encryption method.
   Another method is to restrict the access to the annotation watermark. For instance instead of reducing the quality of the images, the access to the annotation watermark is limited. If the customer has paid, he receives access codes to the full annotated data and the functionality.
4. **Long Term Customer Relationships:** Counting usage and getting additional service. Annotation watermarks can be used to support long term

customer relationships by using the watermarks like discount stamps. The issued annotation watermarks are counted and provide additional service depending on the amount of annotation watermarks the user can present.

4. TECHNICAL SOLUTIONS

All aforementioned scenarios together with their mechanisms do have in common, that they can (and usually must) rely on cryptographic support for a number of reasons. Annotation watermarks are particularly appropriated because they can not be forged since a specific (cryptographic) key is kept secret. Therefore, only the dedicated company owning the key is able to embed the watermark and also to remove the watermark information of an image. Additionally concerning images, the embedding of annotation watermarks can not be detected by human eyes and therefore, these watermarks do not effect the optical vision. Particularly, a costumer has an interest that the watermark is not damaged, lost or stolen, and thus, he will handle them carefully and take care of them.

Because images including watermarks can be copied without information loss and hard copies can be given away to any other person than the legitimated owner, e.g. the buyer of a book, further mechanisms are needed. These mechanisms should prevent the misuse of information by not legitimated persons or at least make it more difficult to misuse it. However, the level of security depends mainly on the amount of money that is investigated for security mechanisms -- but the cost of the mechanisms should not be higher than the cost of a damage that might be caused without seeurity mechanisms.

To provide conditional access for additional services or services for longer term customer relationships we use annotation watermarks and design four different strategies:

- Approach 1: Discount approach – annotation watermark is used as discount stamp.
- Approach 2: Secret sharing approach – annotation watermark is only accessible by combining several (shared) keys to get the information or additional service.
- Approach 3: Partial access approach – annotation watermark is partly accessible and contains further protected information which is only accessible by combining several (shared) keys to get the information or additional service.
- Approach 4: Key watermark approach – annotation watermark is used as a key to get access to another annotation watermark.

Approach 1 can be solved by an application, which counts the annotation watermarks registered by an user and provides the appropriate service depending on the accumulated discount stamps. Problems here are user identification and replay attacks. The annotation watermark needs to be designed like a fingerprint watermark to get unique identification of customers. To avoid replay attacks or limit the multiple usages the application has to register the usage.

Figure 1 illustrates an example of the discount protocol. A user has collected several watermarked data, he can register his data with the discount stamps via a discounting server, which can also be a part of the shop system itself. In the figure, the discounting server is shown as an separate part to collect discount stamps from different shops which are valued in all shops. The server creates a login for the user (here we can also use pseudonyms) and registers the watermarks. The shop systems have access to the discounting server and can request the accumulated watermarks and determine the discount stamps to grant discounts.

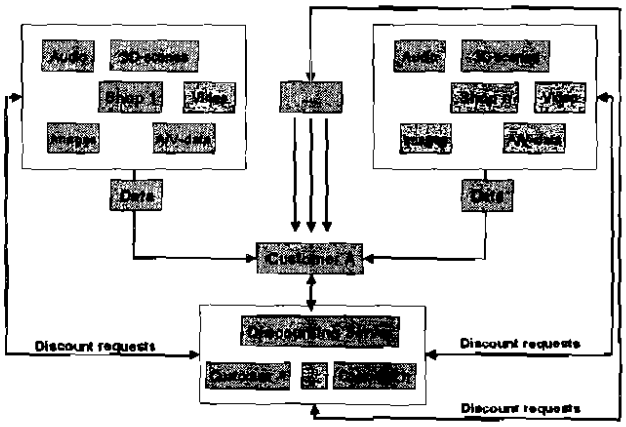

Figure 1: Discount approach

Approach 2 can be solved by cryptographic mechanisms, described in section 3.1. The annotation watermark is only accessible when the user has collected all necessary shared keys or even a specific number of them. Figure 2 illustrates the secret sharing approach. The user retrieves several keys from other or the same party, which allows to access the annotation watermark. In the figure, he stores the partial keys in a key database locally. Only the annotation watermarking algorithm knows how to use the shared keys within a dedicated secret sharing scheme.

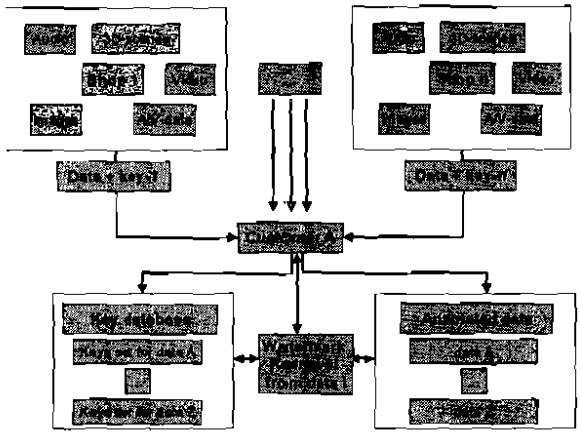

Figure 2: Secret sharing approach

In approach 3, the annotation watermark contains two parts: part 1 is fully accessible and part 2 is protected by one or more keys. Thus, approach 3 is a combination of a general accessible annotation watermark and approach 2. Figure 3 illustrates how the user can get access to the watermark.

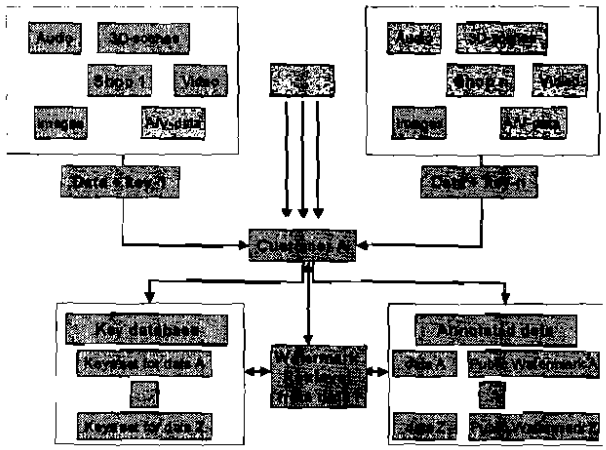

Figure 3: Partial access approach

In approach 4, the annotation watermark itself is used as a key for another annotation watermark, that contains e.g. the service for the costumer. The key can represent e.g. information for the annotation watermarking algorithm how to retrieve the watermarking from specific data. This kind of annotation watermark can be used in approach 2 or 3 to provide the neces-

sary keys. Here, the customer buys data with an annotation watermarking containing the key to access other annotation watermarks. The approach is shown in figure 4.

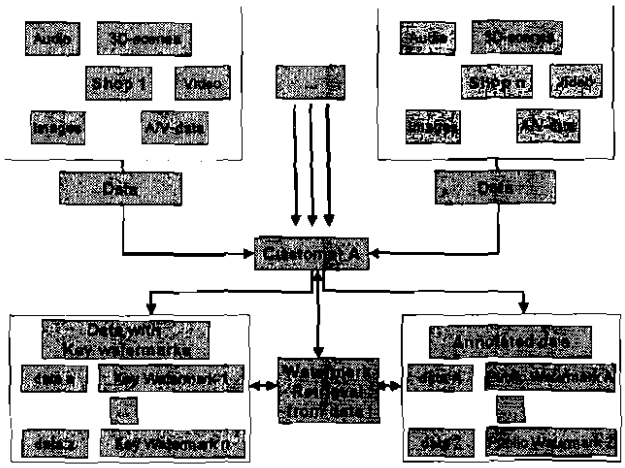

Figure 4: Key watermark approach

In the following, we describe mechanisms for approach 2, which can also be used in approach 3 and 4. Additionally, we describe some attacks and point out some counter-measures.

4.1 Cryptographic solutions

To realize approach 2 – the secret sharing approach – watermarking techniques can be combined with cryptographical mechanism and organizational aspects. The main idea is to use a well-known cryptographic mechanisms called secret sharing scheme where data are shared into several (secret) parts. Here, a secret splitted into n parts can be shared between n parties. The characteristic of these schemes is that the original data can only be reconstructed if and only if all n parts are known. There exist further secret sharing schemes like threshold sehemes [Sham79], where only at least t out of n parts (where $t <= n$) need to be known to reconstruct the whole data. In the following, we will focus on the n-out-of-n approach where we need all parts. In our context, these parts are called partial keys.

Due to that, we split our data e.g. representing information about the costumer-service into n partial keys. These keys should be stored on different places: firstly, we store one partial key as a annotation watermark in an image. All other n–1 partial keys are stored on other places – of course they can also be embedded in annotation watermark, and perhaps also different

storage media in such a way that this data is only available separately. This means, the mechanisms might also differ in the way how partial keys are made available. Depending on the application, it needs to be analyzed how many partial keys and how many different storage media are practicable. For the description of the basic idea, in the following we will only look at data splitted into two partial keys.

Because in M-Commerce a large number of costumers need to be addressed via a broadcast media (e.g. a newspaper), the annotation watermark represents one secret which is transported via the broadcast media. Therefore, a main requirement for annotation watermarks is that the embedded information is always identical. Otherwise, the application needs to provide different data for different users which can not be realized from the perspective of a broadcast application. The other part of the necessary information (e.g. second part of the secret) is distributed via another way and might be stored on distinctive media. For instance, this secret data can be sold as an additional card concerning codes for access called access-code card. Those access codes can be presented e.g. by numbers or even barcodes, where a barcode-scanner can be connected with personal computer or a personal digital assistant (PDA), or even by other images also including watermarks which can be recognized by the camera. If the card together with the annotation watermark is processed by the dedicated application, the original data can be reconstructed by using both partial keys. Then, the user grants access to specific information or services.

4.2 Example

The following example concerns approach 3, the partial access approach. We will point out the main proceeding and mechanisms by using two partial keys: A costumer buys a newspaper where the images of advertisements include annotation watermarks but also one partial key k_1. Using his personal computer, he start the dedicated application and shows the watermarked image to the camera used by the application. The camera scans the image and hands it over to the application that detects the annotation watermark as well as the partial key k_1. By using the information provided by the annotation watermarks, the costumer gets connected to the dedicated internet page. The key k_1 causes the application to show the costumer a message. This message concerns that he can get value-added serviees by buying specific access-code cards.

Now, the costumer visits a (even internet-) shop where he can buy access-code cards. Here, he has to choose from different cards for different value-added services. He chooses one and pays for it.

Next time, the costumer additionally shows his purchased access-code card providing another partial key k_2 for the specific service. This has to be done in an appropriate time window. Thus, the application reads the partial key k_2 and computes $I = f(k_1, k_2)$ by using the secret sharing scheme f. According to value I, the application grants access to the web-pages and the value-added services.

4.3 Possible Attacks

Initially, a value representing the access-right must be unique to a person who owns both the newspaper/image and the access code for additional data. This problem is easy to solve since the amount of possible values for secrets is large enough to prevent brute-force attacks.

Since access-code cards together with the watermarked image can easily be copied or handed out to other persons, there is need for additional mechanisms to prevent such a misuse. First of all we can think of an (in some circumstances anonymous) registration where each user gets a unique registration number or registration data. This data can represent a third secret of a secret splitting scheme and therefore, the data can be used as an additional secret value within a secret sharing scheme.

Another solution to prevent misuse is that an access code can only be used once. After getting access to dedicated data, the access code gets invalid and thus, useless. This method might not be accepted by the costumer because he paid for the additional value. To avoid this, an additional (external) database provided by the dedicated company or even a trustworthy party might be established for keeping track of transactions attacks (e.g. store already invalid access codes and check for misuse) and vulnerabilities resulting by open issues. Of course, this raises the question of how to ensure privacy protection of costumers – but this issue might be addressed with other methods.

A further solution to the problem mentioned above, is to change the access code by the company right after the costumer used the code. This means that an access code is only used once (like a session code) and the costumer gets another code for his next access. This is quite similar to the application of transaction numbers (TAN) well known from E-Banking. The code can also be generated after each session and then be transmitted to the costumer. This assumes, that the costumer must allow to receive specific data that must be stored on his computer.

Finally, it needs to be determined how the application is set up, especially how many secrets are needed to support the access mechanisms for value-added services.

5. CONCLUSION AND FUTURE WORK

In our paper we have introduced and discussed conditional access mechanisms for annotation watermarks. We have presented our approaches for conditional access solutions, that will form the theoretical basis of our ongoing work. Currently we are evaluating further approaches and develop and test a prototype system. This will also try to exploit the additional features provided by end systems with optical (e.g. camera) and biometric (e.g. fingerprint sensors) input equipment.

6. REFERENCES

[DSKS00] Jana Dittmann, Martin Steinebach, Thomas Kunkelmann, Ludwig Stoffels: H2O4M – Watermarking for Media: Classification, Quality Evaluation, Design Improvements. In: Proceedings ACM Multimedia 2000 Workshops, November 4, Los Angeles, California, pp. 107-110, ISBN 1-58113-311-1, 2000.

[Dig01] Digimarc, MediaBridge, www.digimarc.com

[Ala00] Adnan M. Alattar: Bridging Printed Media and the Internet via Digimarc's Watermarking Technology. In: Electronic Proceedings ACM Multimedia 2000 Workshops, November 4, Los Angeles, California, ISBN 1-58113-311-1, 2000.

[Sham79] Adi Shamir: How to share a secret. Communications of the ACM, 24(11), July 1979, pp. 612-613.