17

A Study on Implementation and Service of Digital Watermark Technology Architecture for Distribution Management

Manabu Hirakawa
Department of Industrial Engineering and Management, Tokyo Institute of Technology
Japan

1. Introduction

Recently, fake brand-name products and other problems concerning the manufacture of counterfeit goods, as well as the abundance of pirated music and movies, and the misuse of personal information, have been the subject of extensive news coverage. Numerous problems related to security have also been reported, in addition to the falsification of expiration dates and production location information labels on food products. As can be seen from these examples, consumers' trust, especially in regard to food safety, is at risk of being damaged. Information technology has advanced, and traceability has become technologically possible. However, I believe that a societal system for preventing such problems is lacking, and a fundamental reason for this may be a gap in perspective at the business management level with respect to the low-cost requirements of the market place. In society, individuals managing information are assumed to have good intentions. I believe that this system itself is beginning to fail. These problems are seen in the lower reliability of distribution systems, for example, the falsification of information about freshness dates and product origin. At present, the social system for preventing these problems is mostly defective, despite the technologically availability of traceability by means of information technology. Accordingly, new measures for dealing with these problems are urgently needed. It is important to note that ensuring safe distribution, improving security, and managing cost are not independent of each other, but are actually interconnected.
In this research, I analyze these problems in the context of the societal system and propose a solution that uses digital watermarking technology. My focus is on different types of information carriers including multimedia content such as movies and music, distributed manufactured products. At present, the security rules for information carriers are complex and are not uniformly applied to specific objectives and applications. Applying digital watermarking technology to information carriers will allow uniform information to be given to various media regardless of the application and environment; further, mobile services can be provided that do not depend on specific hardware and software. These mobile services be affected neither by structural disparities in applicable systems and codecs, nor by differences of copyright management policy.

2. Background of this research

Distribution is what connects the producer with the consumer. Physical products that we can see with our eyes, and those that we cannot, such as data, are both distributed. Images, videos, and audio that can be used on a computer are all forms of digital media. Therefore, recently pressing DVDs and CDs and creating packaging and other types of physical processing have become unnecessary. There are now cases where the data alone can be sent and received thus providing the service. Traditional distribution systems run the risk of increasing production costs due to media creation and packaging, and due to the need to hold unnecessary inventory. On the other hand, digital content services use the infrastructure of the Internet to transmit the digital data directly; therefore, these services have the following advantages: 1) no need to hold unnecessary inventory, 2) reduced distribution time, 3) reduced overhead costs, and 4) the ability to have customers around the world, without borders. Such distribution systems resolve the problems with existing systems, and are still expanding today. Digital content businesses that handle the distribution of images, videos, and audio are able to use the Internet to disclose, transmit, and distribute copyrighted work directly to the consumer. Many Web sites already use this service. On the other hand, there are many illegal Web sites that infringe on copyrights and negatively impact legitimate digital content businesses.

Relevant actors in the upstream process where content is created include the producer, the copyright holder, the secondary copyright creator, and the license manager. At this stage copyright comes into play, so we know that it is necessary to add copyright information to the content. Next, looking at the downstream processes of distribution and disclosure, the irrelevant actors include the distributor, the network company, the broadcasting company, e-commerce site managers, and administrators. Other content is distributed for offline use via Internet downloads, magazines, or DVDs and CDs. In these cases it is necessary to add information on the use of the content. There is an urgent need for a framework to be constructed that can take this copyright information and detect the illegal use of content as copyright infringement, and that can legally enforce copyright.

To ensure the solid growth of the promising digital content industry, content protection technology is necessary, which will be the used as the mechanism to protect copyright holders and their content. Content protection technology is an all-inclusive concept that involves the prevention and deterrence of unauthorized copying of content, as well as copyright protection technologies. Digital watermarking is an example of an effective content protection technology. Digital watermarking technology development began around 1995, and its full-fledged application began around 1998. Digital watermarking places an imperceptible mark that identifies the copyright holder into the digital content itself. In the event that the content is copied, the watermark can be used as evidence for tracking. Digital watermarking does not prevent unauthorized copying. However, it can be applied broadly, and it is effective in enforcing copyright.

3. Problems

Digital content businesses that deliver images or music make it possible to release, transmit, and sell copyrighted data directly to users via the Internet. Numerous Web sites already provide this service. On the other hand, there are many illegal Web sites that infringe on copyrights and negatively affect digital content businesses [1]. Music, images, and video that can be used on a computer are digital data, so the full service can be provided by simply sending and receiving the data. This eliminates the need for pressing CDs and DVDs, packaging, and other physical processing. This is the concept behind the digital

content business. Conventional distribution systems have problems of increased production costs due to CD or DVD manufacturing and packaging, and the risk of carrying unnecessary inventory. With these conventional general distribution systems, there is a fear that it is difficult to commercialize content that has a low sales outlook.
On the other hand, because digital content services use the Internet as the infrastructure to send digital data, it has developed into a distribution system that resolves the problems of conventional systems as follows.

- No need to carry unnecessary inventory
- People around the world can be customers in a "borderless" manner
- Short distribution time
- Reduced costs

Moreover, with the development of infrastructure, the range of customer categories has expanded from the conventional range. Reaching target customer audiences and diversifying categories has become a recent remarkable trend.
As previously noted, the handling of digital content is highly anticipated in the future business scene, but the news is not all good. Because digital data can easily be copied, the user can sell it to a third party without permission, and there is also the possibility that the content will be illegally copied while en route over the Internet. Because there are no markings on the content itself that shows who holds the copyright, who sold it, or who purchased it, it is difficult to determine the route if the content is redistributed. If there is no evidence, then it is impossible for the copyright holder to prove a copyright claim when the content is illegal copied. Because of this, if illegal copies of content are made on a regular basis then the distributor cannot collect income appropriate for the content provided, and the business model will collapse. From the perspective of digital content businesses that use the Internet and construct their business models based on the ability to protect their digital content, the anticipation for success is high [2]. On the other hand, they also bear the risk of loss due to illicit copying of their content [3].
In recent years there have been major changes in the environment surrounding digital music [4]. There have been many reports of illegal MP3 Web sites [5]. These Web sites illegally copy music data from commercially available CDs, or from regular broadcasts, and then convert the data into MP3 files. They then publish the MP3 files on Web sites that they run and answer the requests of their users by making the files freely available for download. Commercially available CDs and other distribution media have a legally recognized specific copyright that makes it illegal for users without rights to copy and distribute the content without permission. Because this type of use ignores the legally recognized rights of copyright holders, the Web sites are considered to be illegal MP3 Web sites. The number of Web sites similar to illegal MP3 sites has increased. When digital content is distributed for free, it negatively affects the state of CD distribution, harming its commercial viability. One technology that will form a pillar of the solution is digital watermarking.

4. Comparison with existing technology

In recent years, there have been many cases where RFID[1](Fig. 1) and QR codes[2](Fig. 2) technology have been introduced as new technologies for distribution management. In this

[1] Radio-Frequency IDentification. RFID is an automatic identification method.
[2] Quick Response Code. A matrix code (or two-dimensional bar code).

research, as shown in Fig. 3, I apply digital watermarking to a variety of information media, I examine objectives and applications such as copyright protection

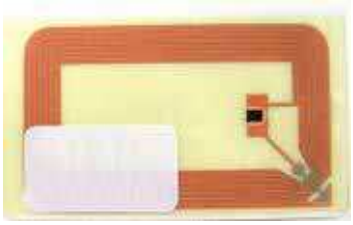


Fig. 1. Example of RFID Card

Fig. 2. Example of QR code

Fig. 3. Example of digital watermark to various information carriers

I compared RFID and QR codes and digital watermarking technology.
The following items were compared.

- Raw material processing and age degradation: heat resistance, waterproofing properties
- Degrees of freedom of the markings: Minimum required area, degrees of freedom for shape
- Security: Confidentiality, protection against duplication, protection against alteration
- Reading: Ease of reading, reading rate, compatibility with reading devices
- Cost

The results of the technical comparisons of the above items are shown in Table 1.
In terms of the raw materials during the processing stage and in the environment of practical use, RFID has inferior heat resistance. RFID uses RF tags to perform wireless communication. RFID can be constructed from multiple elements on a circuit board, or can be implemented on a single chip, both of which are prone to destruction by heat.
Although the impact of heat is reduced in QR codes as compared to RFID, preserving the print condition of the markings becomes a challenge.

In digital watermarking, a laser directly burns the markings into the raw materials, and therefore it has heat resistance and waterproof properties that are superior to those of the conventional technologies.

	RFID	Watermark	QR Code
Heat resistance	△	○	△
Waterproof	△	○	△
Minimun required area	○	○	×
Degrees of freedom	○	○	×
Confidentiality	△	○	×
Protection against duplication	○	○	×
Protection against alteration	○	○	×
Ease of reading	○	△	△
Cost	△	○	○
Reading device	○	×	○

Table 1. Comparison of copyright protection technologies
(○ : Applicable △ : Partially applicable × : Not applicable)

Next, in regard to the degrees of freedom of the markings and the reading environment, QE codes have more restrictions. QR codes have between 21 × 21 cells in version 1 and 177 × 177 cells in version 40. The required minimum area is determined by the amount of embedded data and the resolution of the reader. If the area of the managed materials is greater than the minimum area of the QR code, there is no problem. However, if the available area is less that this minimum, it is not possible to mount the marking. Also, reading might not be possible if the managed material is curved, such as a sphere or cylinder (error correction can improve the reading rate). RFID is strong in regard to this point: if it is possible to mount the RF tag, then recognition is certain. Marking for digital watermarking is performed in accordance with the shape; thus, the markings have a high degree of freedom, and reading can be performed easily regardless of the shape.

There are many security concerns with QR codes. QR codes are compatible with reading devices such as specialized readers and mobile phone terminals, and are the most common of these three technologies. However, they are weak in terms of confidentiality and protection against alteration.

The benefit of RFID is that it can ensure non-contact recognition by using wireless communication. However, there is the problem that RFID reader eavesdropping can be performed from an unintended location. In terms of cost, RFID requires that RF tags be installed in all of the target objects. Although the cost is currently lower than 10 yen per RF tag, when the number of target objects is great, this amounts to a cost that cannot be ignored. In QR codes and digital watermarking, the cost can be controlled relatively well since the markings are constructed by printing or burning.

One challenge for digital watermarking is its compatibility with reading devices. Although specialized terminals are used as readers in the current stage of development, the range of usability should be increased in the future by using readers for conventional PCs and mobile terminals.

5. Media types and their objectives

Numerous types of information media surround us. In this section, I will discuss the types of media in which digital watermarking technology can be used, and the objectives and applications of its use. Copyright in this digital and networked environment has been debated from a variety of perspectives [6-7]. However, in regard to technology, the advance of digital technology has led to proposals of new copyright protection technologies. In recent years, digital watermarking has been gathering attention as one technology for copyright protection [8-9]. Digital watermarking is technology that directly embeds additional information into content at a level that cannot be detected by the human sense of hearing or sight. Including copyright protection information into these digital watermarks makes it becomes possible to protect the copyright of the author. A variety of engineering methods have been researched regarding digital watermarking technology that can be embedded into a variety of data formats, such as static images, videos, and audio [10-12].

Generally speaking, "multimedia" data comes in three forms: static images, videos, and audio. Here, I have included documents such as public documents and research papers as a type of image medium. From the background to this research, the following five points regarding the objectives and applications for digital watermark use can be noted: 1) copyright protection, 2) distribution traceability, 3) proof of authenticity, 4) security advantages, and 5) sales promotion. Table 2 summarize the objectives and applications of digital watermarking for physical media and static images, and for video and audio, respectively.

Digital information has the characteristic that even if it is processed or edited, the quality will hardly deteriorate at all. Therefore, copyright protection, an item listed in the table 2, is a critical issue. In the past, the © mark has been displayed to indicate the copyright holder, but a common problem is that this mark can be removed through illegal processing or editing [13]. In response to cases like this, digital watermarking can be used on video, image, and voice media to implement a mechanism to prevent the alteration of the copyright owner information, thus protecting the copyright.

In relation to this, the distribution traceability of information media is discussed. Recently, with the spread of digitization and the Internet, the situation is such that content distribution is done over networks, sharing the information with the world [14]. Such an environment makes thorough compliance extremely important. The improvement of people's morals in regard to information must be maintained in tandem with defense mechanisms built into the system; however, the reality is that weak security can cause people's moral sense to decline. By using digital watermarks to embed distribution route information into image, video, and music media, in the case that the information is leaked, it will be possible to clearly determine what route the information followed. Similar to copyright information protection, information traceability can also be achieved, which should already exist, and can prevent a malicious user from intentionally altering the information during the distribution process.

It is not easy for the user to determine whether public documents, research papers, or other purchased products are actually legitimate, which is referred to as proof of authenticity in Table 2. From the fact that counterfeit goods of famous brands are being sold extremely cheaply, it can be inferred that a large quantity of these counterfeit goods are detected [15]. Digital watermarks can be used as one method to differentiate between authentic and counterfeit products. Until now, digital watermarks have almost exclusively been used in digital data such as images, videos, and audio. However, current research has shown that it is possible to use digital watermarks to embed information into physical media such as metals, printed-circuit boards, acrylic boards, and cloth [16].

During the manufacturing process, invisible digital watermark information is embedded into the patterns or logos of legitimate products. In the distribution process and at the purchase stage, if the digital watermark is detected, the product can be determined to be legitimate. If the digital watermark is not detected, then the product can be determined to be a counterfeit. There is also a method to determine authenticity from another perspective. If the strength of the digital watermarks is purposely reduced, the digital watermarking information in the areas that are altered or processed will be lost. This makes it possible to determine what areas have been tampered with. In this way, depending on the application, two different models can be selected. In one, the strength of the digital watermarks can be increased to improve its evidential capacity, and in the other, the strength can be reduced to enable identification of areas that have been altered.

In regard to the previously mentioned copyright protection, traceability, and proof of authenticity, I believe that adding information that cannot be seen by the human eye to the medium can be effective. On the other hand, displaying a visible mark on the medium could have the effect of deterring illegal use; I refer to this as the deterrent effect. Explicitly displaying visible logos or names on products has the potential to have a deterrent effect, thus providing defense against illegal copying. Credits are often displayed on the edge of images or videos. However, the major difference between credits and visible digital watermarks is that by purposely using a release key afterwards, the visible portion can be removed, allowing the original content to be extracted without leaving any excess. In other words, a service model can be created in which content is first released having the deterrent effect, and users can then be provided the original content upon completing official procedures.

Until now, I have focused on means of protecting media. Next, I will discuss the application of digital watermarking for sales promotion. Digital watermarking is a technology that was originally designed considering strong security elements. However, the use of digital watermarking for advertising purposes can be easily considered [17-19]. By embedding URL information into image, video, or audio content using digital watermarking, a mobile phone camera can be used to read the watermarks and guide the user to Web pages that contain information related to the media content. In the case of video and audio media, unlike images and physical media, the content changes with the passage of time. Therefore, this method has a significant advantage in that users can acquire and view information related to the content of interest, unconstrained by time. As an example of practical use for music content, a model can be devised in which the user can easily be guided to an artist's Web site while listening to music content of interest.

		Digital watermarking for physical media	Digital watermarking for static images	Digital watermarking for video	Digital watermarking for audio
Medium characteristics	Visible/ Invisible	Visible	Visible	Visible	Invisible
	Physical/ Electronic	Physical media	Electronic data	Electronic data	Electronic data
	Changes over time	Does not change over time	Does not change over time	Changes over time	Changes over time
Copyright protection		Embedding copyright information	Embedding copyright owner information	Embedding copyright owner information	Embedding copyright owner information
		Copyright protection for physical media (metals, cloths, plastics, etc.)	Copyright protection for images and pictures	Copyright protection for DVDs, broadcasts, and movies	Copyright protection for CDs, broadcasts, and music

		Copyright protection for public documents and research papers		
Distribution traceability	Add the producer's information, and the tracking information for the distribution route to the products and goods	Add the tracking information to the contents for first-time use (use by the copyright holder), and second-time use (reselling)	Add the tracking information to the contents for first-time use (use by the copyright holder), and second-time use (reselling)	Add tracking information to contents for first-time use (use by the copyright holder), and second-time use (reselling)
	Detect a product's unique information from the physical medium (Apply to products that cannot support QR codes and RFID) Adding traceability to products and goods in high-temperature or high-humidity environments	Understand the distribution process by adding copyright holder and buyer information to movie and photo download sales	Tracking illegal movie recording	Understand the distribution process by adding copyright holder and buyer information to music download sales
Proof of authenticity	Detect unique information about products from physical media Detection of counterfeit brand name goods, or discovery of the illegal export using the vehicle identification number	Detection of illegal copying and alteration of public documents and research papers	Detection of pirated DVDs and illegal video distribution websites Tracking illegal movie recording	Detection of pirated CDs and illegal music distribution websites
Can be used on printed materials		Detection of illegal copying for magazines, gravure, and CD jacket images Detection of illegal copying of public documents and research papers	- -	- -
Deterrent effect (Deterrent effect from using visible digital watermarks)	Intimidation against illegal copying of products and goods	Protection for copyright and portrait rights for images and pictures Removed depending on the situation (e.g., legitimate sales) Intimidation against illegal copying	Protection for copyright and portrait rights for images Removed depending on the situation Intimidation against illegal copying	- - -
Sales promotion	Guidance to related websites and websites with product details Detect unique information about the product from the physical media (Services available to the purchaser only, introduction campaigns for new products, etc.)	Guidance to related websites and websites with product details Online provision of the latest magazines and books (Services available to the purchaser only, introduction campaigns for new products, etc.)	Guidance to related websites and websites with product details Acquire detailed information from TV broadcasts and videos	Guidance to related websites and websites with product details Download ring tones or entire song for karaoke Provide visual information from the audio for individuals with hearing disabilities

Table 2. Types of digital watermarking and their objectives and applications

6. Solution by integrated framework

Digital watermarking technology embeds information that cannot be detected by the human eye into the content. By using the redundancy in digital contents to slightly change the values of the pixels across the image, data that the user cannot normally see can be stored in the image in addition to the usual image data. Fig. 4 shows the use case chart of the digital watermark.

As shown in Fig. 4, this data is directly embedded into the image, and therefore it has the characteristic feature that it cannot be removed even if the image is compressed, formatted, modified, cropped, or printed. This enables the automatic discovery of unauthorized copies of an image file among the enormous number of images on the Internet by embedding the image ID, the copyright holder's name, or other conditions into the image. In addition, by proactively communicating to users that this feature is in use, it will deter unauthorized use.

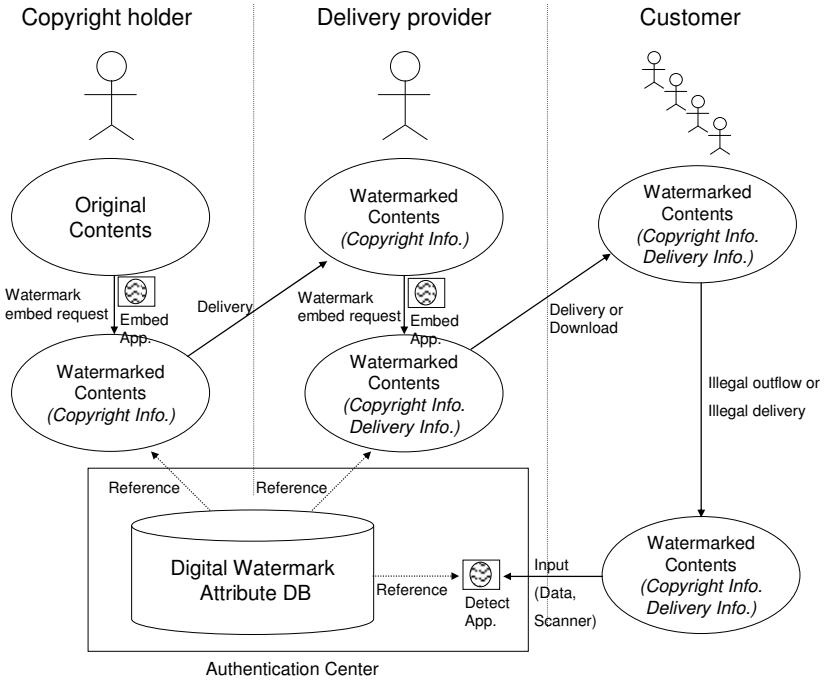


Fig. 4. Use case chart of the digital watermark

I have discussed a variety of ways in which digital watermarking technology can be used to secure information media, and also how it can be used for sales marketing. The framework that integrates these is shown in Fig 5.

The platform's general utility is a critical element in implementing this technology on mobile devices such as mobile phones [20]. There are two methods for detecting watermarking on mobile devices. The first is a client-server method where the file itself is sent to a server and the server detects the watermark. The second is a method where the mobile device itself

detects the digital watermark. Performance is rarely an issue with the client-server method as detection is performed on servers with high processing power. However, the disadvantage of this method is that the file must be sent to the server, a process that is time consuming and entails communication costs. In cases where a digital watermark cannot be detected, this result can only be known after sending the file to the server. By performing the entire process of detecting digital watermarks on the mobile device, users can be guided to a variety of network services such as Web services and e-mail to obtain information without incurring communication costs. For this reason, digital watermarking processes in a mobile environment are preferably based on a method where the detection of digital watermarks is performed on the mobile device, preferably using a digital watermark detection application that supports mobile OS middleware such as Java and BREW.

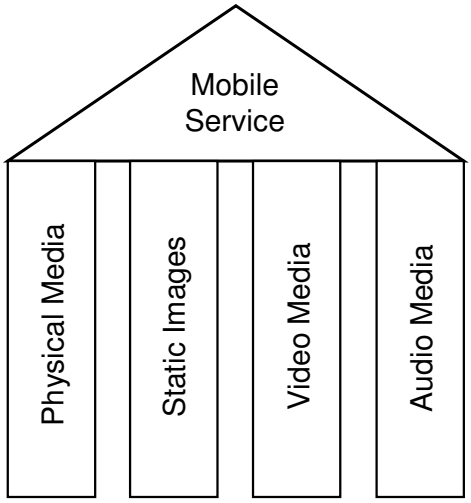


Fig. 5. Integrated framework

As shown in Fig. 6, since middleware neutralize the various differences in the bottom-most hardware layer, generic utility of the platform and good development efficiency are achieved. Device manufacturers can outsource the development of embedded software and concentrate on hardware development. Software developers can develop applications without worrying about differences between platforms. Also, developers do not have to develop different applications for different device vendors. This will eventually lead to applications for not only mobile phones but also smart phones and PDAs.
Next, I explain a mobile solution of the digital watermark to each media.

6.1 Physical media

Data management is performed by using a laser to burn a digital watermark into raw materials such as iron, aluminium, stainless steel, and plastic, and then reading the marking with a reader. The read data is linked to a database, after which management, acceptance examinations, sorting, and distribution can be monitored. An encryption algorithm protects the marking itself, and user authentication and alteration prevention are considered.

As shown in Fig. 7, DPM[3] is a method where markings are made directly onto a product itself. As part of this research project, digital watermarking is implemented using DPM. One characteristic of DPM is that because the markings are made directly onto the material, there is no need to worry that the markings might peel off like an adhesive label. Markings made using DPM can be used in harsh environments and deterioration of the markings is slow, so they can be used over a long period of time [21].

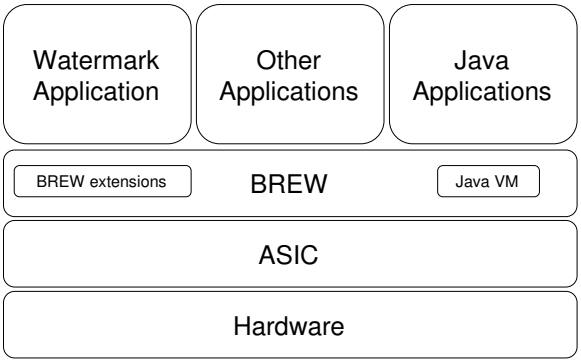


Fig. 6. Software stack for mobile equipment

Fig. 8 is an example of the mobile application for physical media. In one example, the application of DRM technology to the design of brand name products allows for legitimate product authentication and makes it possible to identify the distribution route. Also, directions to the Web site of the relevant brands can also be added. An example applies DRM technology to the coating and parts of an automobile. By recording the automobile data, which cannot be altered by the user, DRM can be used as a theft detection and crime-prevention measure. In addition, services can be provided, such as promotions with information about new car models from the car manufacturer, or the current market price for used cars. These markings can be used in the manufacturing industry to embed a unique ID or lot number into metallic parts for the purpose of automobile detection and accident prevention.

Fig. 7. Example of information detection from physical media

New data management and business schemes can be constructed by using the previously mentioned digital watermarking. Digital watermarking technology was originally used to enforce copyright and for certifying authorship. However, new business models have been established on the basis of this technology.

[3] Direct Parts Marking. Direct Parts Marking is a process to permanently mark parts.

Fig. 8. Example of mobile application for physical media

Additionally, a system that confirms distribution routes with absolute certainty can be designed and applied in other fields, for example, by embedding digital watermarks into medical equipment (e.g., scalpels or scissors) and managing the equipment with a database. In this way, equipment that needs a lease renewal or quantity check can be managed.

6.2 Static images

Presently many posters, pamphlets, magazines, and company brochures have Internet URLs printed on them. Details that cannot be printed on paper such as the latest information or information about related services are published on the Internet. However, there are various problems. Inputting a URL while looking at the printed material is troublesome, input mistakes can occur, and even if there are multiple information items introduced on the printed material, usually only the URL to the top page of the Web site is noted, making it difficult to locate the desired information. Also, the use of many recognition technologies has been hampered by problems with the layout and design of existing media.

A characteristic of using digital watermarking technology in a mobile environment is that mobile content is accessed directly from printed material, providing cross-media marketing. Digital watermarking facilitates the normally difficult task of measuring the effectiveness of promotions using printed medium. When the specialized application software is downloaded, the customer's data is collected, and a unique digital watermarking ID is embedded based on the type of printed medium, the distribution time, and region. Because the connection destination URL information is managed on the server, the user sends the ID information to the content management server and then receives the URL information. In this way, a detailed access log with information on when and where it was accessed, who accessed it, and what print medium was used can be collected, allowing the effectiveness of the printed material to be measured and analyzed.

6.3 Video media

In the introduction, I explained that the distribution of pirated media created from the illegal recording of motion pictures has become a major societal problem [22]. In recent years, motions pictures have been distributed not only on film, but also, in many cases, in digital formats as video data. Information about the time and location that the movie is shown can be embedded into the movie as digital watermarking information and then the movie is shown. The viewers will watch the movie without noticing that this information has been embedded. If the movie is pirated and shown illegally via DVD or over the Internet, when the movie was copied and from what movie theater can be determined by detecting the digital watermarking information. Fig. 9 is an example of detecting information from movie media.

Fig. 9. Example of information detection from movie media

Next, let us consider a service that links the movie database with mobile devices. In recent years, increasing numbers of TV stations and other companies that possess movie content have been managing their digital data as a media archive stored in a database. They can reuse the content by redistributing them on television or over the Internet, or create added value and use them as services for the mobile market. Information about related sites can be embedded as digital watermarks into the movie content that is managed using the database.

If digital watermarking is used to embed a URL into movie content, the URL can be extracted from the video by inputting it via the mobile phone's camera by simply holding the phone up to the display. On TV programs information is sometimes displayed temporary on the screen, such as sports scores, or recipes in the case of cooking shows. However the amount of time that this information is provided is extremely short and the necessary information is often missed. With paper media such as magazines it is possible to use a QR code or a URL to link to a mobile Web site, but it is difficult to acquire information from movie content because the screen is constantly changing. It is also undesirable to constantly display a QR code or URL on a screen. However, if digital watermarking for movies is used, the required information can be extracted from the movie itself and linked to the mobile phone. This eliminates the need to display information on the screen for long periods of time. The mobile phone only needs to be held up to the screen to access the information, so there is no need for the viewer to hurry to write down the information. The extremely convenient interface places little burden on the user. For example, the following information could be provided: shop information during a gourmet TV program, recipes during a cooking program, or lodging information during a travel program. It would also be possible to search for and acquire the necessary information from mobile phone sites after the TV program has ended. Also, by holding up a mobile phone to the screen when a favorite musician is playing during a music program, the user can easily access the music data and the artist's Web site. Finally, similar to the measures to prevent the illegal recording of movies, copyright information could be embedded into the watermark to use in measures to prevent illegal usage.

6.4 Audio media

Next, let us turn our attention to services that utilize digital watermarking on audio media. By embedding digital watermark information onto music or audio files, and reading these files on mobile phones and mobile devices equipped with microphones, such as PDAs, information and content can be displayed that is relevant to the music or audio the user is listening to, and users can also be guided to predefined sources of information such as Web sites. Depending on the specification of the digital watermark detection program and the content of embedded information, users, in addition to being guided to a particular Web site, will also be able to access phone numbers and e-mail information, as well as view relevant video.

In Fig. 10, this schematic shows an example where the mobile device reads digital watermark information embedded in broadcasts or karaoke tunes, and the user is guided to an advertisement site or presented with information such as coupon information or information on the site of a particular manufacturer. For example, the user can select a favorite karaoke tune, visit the artist's site, the URL for which is extracted from the audio being played back, and then download the original song.

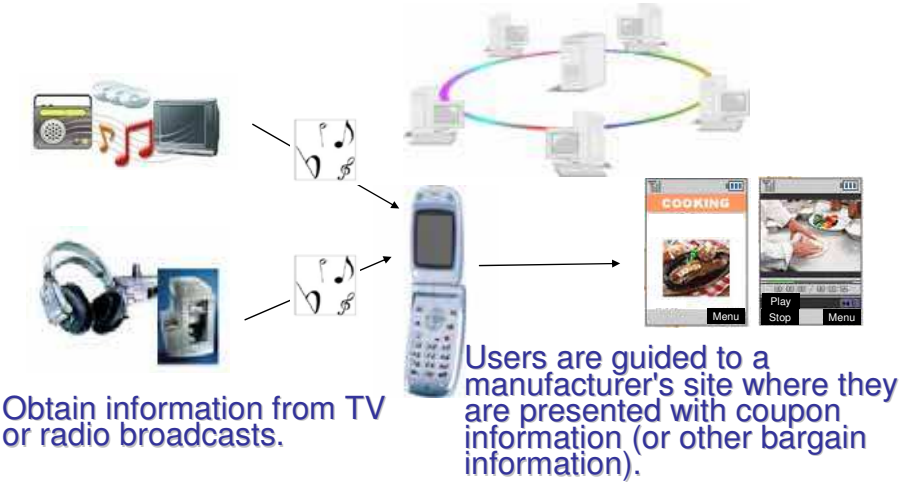


Fig. 10. Guiding users to mobile services from audio media

Digital watermarking can also be used as an information feature at public facilities such as zoos and museums. Since the input source is in audio format, information can be obtained easily over a broad area as opposed to QR codes, which require users to take close-up shots of a specific point. This will be an effective way to provide guidance information in large venues where visitors can often get lost.

Audio files do not require special equipment and can be played back on any consumer market speaker. This technology enables operators to provide interactive services in situations where only a mobile phone or PDA is used. More information can be provided if the mobile device is equipped with Internet connectivity. Compared to similar services based on RFID, digital watermarking, which extracts information from audio files without the use of IC tags, delivers the same effect at a lower cost. Since generic mobile phones can be used instead of special devices, development costs, and device purchase costs can be reduced, expanding the technology's range of applications.

7. Conclusion

In this way, watermarking technology can identify certain copyrighted content and the related rights during the distribution process or after distribution. If revolutionary and new content distribution and usage models can be realized, the confirmation of the copyright owner and rights management will become possible. However, there has been little research done on the implementation method. Especially in the case of embedded software, which is widely used in mobile devices, implementation is seen to be difficult due to the limited implementation resources. Also, in regard to the assimilation of different implementations and platforms of the wide variety of digital watermarking algorithms, the amount of development work is becoming huge and existing resources are only rarely being reused. Moreover, the increasing complexity of errors and memory management that has accompanied this increase in development scale has become a problem that can no longer be ignored. Uncertainty can be actively managed and exploited. The unexpected developments in an environment can be actively managed through flexible designs that can adjust to changed conditions. Moreover, these new states can provide opportunities. Thus, it is important to broaden one's perspective to consider not only risk but also opportunities. Architecture is important. It is useful and productive to consider explicitly how the parts of an engineering system interact with each other. It may often be essential to do so, to enable us to deal effectively with the need to reconfigure systems in response to new possibilities and new requirements.

Digital multimedia content requires a copyright protection system to be constructed due to the ease by which they can be copied and edited, and due to the ease of high-volume distribution through digital distribution channels. By embedding copy control information into digital watermarks, which are robust against digital disturbances, it is possible to construct a copyright protection system that can prevent illegal copying. The control information that is embedded into digital watermarks can be securely transmitted to the system through both the packaging for physical distribution, and through the network for digital distribution, thus strongly protecting the author's copyright. Many security rules for information media are complex, and they are not unified across regions and for every application. By using digital watermarking technology on information media, information can be embedded into different media without regard to the application or environment. Moreover, the service can be provided regardless of what hardware or software is used. In sum, digital watermarking is a technology that is not affected by various conditions such as business models or the structure of the system that is used, software differences, coding differences, or copyright management policies. I anticipate that using an economical copyright protection system that uses digital watermarking will promote the digitization of multimedia content, and protect the author's copyright. This will also foster more open and global multimedia content distribution.

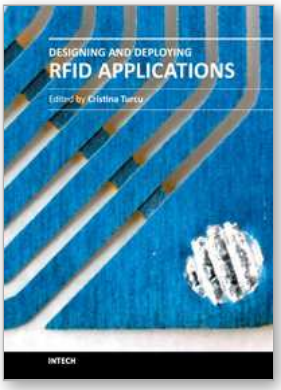
8. References

[1] Kineo Matsui. (1998). *Base of Digital Watermark* (In Japanese), Morikita Publishing Co., Ltd.,

[2] Liquid Audio, Music on the Net, A Topographic Tour of the Online Music World, http:/ / www.minidisc.org/ music_internet.html (Accessed: Oct. 8, 2010)

[3] Kazuhiro Okamura. (2008). The one that electronic watermark brings -First part-(In Japanese), *Monthly Automatic Operation Recognition*, Feb. 2008 Vol.21 No.2, Japan Industrial Publishing Co. Ltd., pp.36–38

[4] Business Software Alliance, Web site, (In Japanese), http:/ / www.bsa.or.jp/ press/ related/ 2010_Global_Piracy_Studyj.html (Accessed: Oct. 8, 2010)
[5] Manabu Hirakawa, Junichi Iijima. (2009). "Validating the effectiveness of using digital watermarking technology for e-commerce website protection," *Proceedings of the 9th Asian eBusiness Workshop*, No.21, pp.127-132
[6] Kotaro Nawa. (1996). *Copyright of Cyberspace* (In Japanese), Chuokoron-sha, p.194
[7] Kenji Naemura. (1997). *Copyright of Multimedia Society* (In Japanese), Keio University Press Inc., p.285
[8] Fumitada Takahashi. (1997). "The digital watermark keeps to the multimedia era (In Japanese)," *Nikkei Electronics*, Nikkei BP Marketing Inc., Vol.683, No.2-24, pp.99-124
[9] Satoshi Nanamatsu, Toshihiro Masumoto, Kazuyoshi Tanaka. (2000). "Multimedia digital contents and copyright protection (In Japanese)," *Information Management*, Vol.42 No.12 pp.1013-1021
[10] Kineo Matsui. (1998). *Base of Digital Watermark - New Protection Technologies for Multimedia* – (In Japanese), Morikita Publishing Co., Ltd.,
[11] Kineo Matsui. (1998). "Electronic watermark and the evaluation item," *Institute of Image Electronics Engineers of Japan Magazine*, Vol.27, No.5, pp.483-491
[12] Kiyoshi Yamanaka. (1998). "Problem in application to electronic watermark and copyright protection," *Information Management*, Vol.40, No.10, pp.933-940
[13] Naohisa Komatsu, Kenichi Tanaka. (2004). *Digital watermarking technology – Digital content security* (In Japanese)," Institute of Image Electronics Engineers of Japan Magazine
[14] Tsukasa Ono. (2001). *Digital Watermark and Contents Protection* (In Japanese), Ohm-sha Co., Ltd.,
[15] Manabu Hirakawa. (2008). "A digital watermark service model's effectiveness of verification in copyright protection (In Japanese)," *Proceedings of National Spring Research Conference 2008*, The Japan Society for Management Information, pp.G4-2
[16] Manabu Hirakawa, Junichi Iijima. (2008). "A study on usage of digital watermark in distribution management (In Japanese)," *Proceedings of National Autumn Research Conference 2008*, The Japan Society for Management Information, pp.B1-3
[17] Key Pousttchi, Dietmar G. Wiedemann. (2006). "A Contribution to theory building for mobile marketing: Categorizing mobile marketing campaigns through case study research," *Proceedings of ICMB '06. International Conference*, pp.1-1
[18] Andreas Albers, Christian Kahl. (2008). "Design and implementation of context-sensitive mobile marketing platforms," *Proceedings of E-Commerce Technology and the Fifth IEEE Conference on Enterprise Computing*, 10th IEEE Conference, pp.273-278
[19] Phyoung Jung Kim, Young Ju Noh. (2003). "Mobile agent system architecture for supporting mobile market application service in mobile computing environment," *Proceedings of Geometric Modeling and Graphics International Conference*, pp.149-153
[20] Hidemi Mizoguchi, Yukinori Miyakita, Yuta Tokoro. (2007). *EZ Applications Explained (BREW) Programming*, RIC Telecom Co., Ltd.,
[21] Kazuhiro Okamura. (2008). "The one that electronic watermark brings -Latter part-(In Japanese)," *Monthly Automatic Operation Recognition*, Mar. 2008 Vol.21 No.3, Japan Industrial Publishing Co. Ltd., pp.33–36
[22] Japan and International Motion Picture Copyright Association, Inc. Homepage, http:/ / www.jimca.co.jp/ index.html (Accessed: Oct. 8, 2010)



Designing and Deploying RFID Applications

Edited by Dr. Cristina Turcu

ISBN 978-953-307-265-4
Hard cover, 384 pages
Publisher InTech
Published online 15, June, 2011
Published in print edition June, 2011

Radio Frequency Identification (RFID), a method of remotely storing and receiving data using devices called RFID tags, brings many real business benefits to today world's organizations. Over the years, RFID research has resulted in many concrete achievements and also contributed to the creation of communities that bring scientists and engineers together with users. This book includes valuable research studies of the experienced scientists in the field of RFID, including most recent developments. The book offers new insights, solutions and ideas for the design of efficient RFID architectures and applications. While not pretending to be comprehensive, its wide coverage may be appropriate not only for RFID novices, but also for engineers, researchers, industry personnel, and all possible candidates to produce new and valuable results in RFID domain.

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821