PRACTICAL CHALLENGES FOR DIGITAL WATERMARKING APPLICATIONS

Ravi K. Sharma, and Steve Decker
Digimarc Corporation.
19801 SW 72nd Avenue, Suite 250
Tualatin, Oregon 97062, USA.

Abstract – The field of digital watermarking has recently seen numerous articles covering novel techniques, theoretical studies, attacks and analysis. In this paper, we focus on practical challenges for digital watermarking applications. Challenges include design considerations, requirements analysis, choice of watermarking techniques, speed, robustness and the tradeoffs involved. We describe common attributes of watermarking systems and discuss the challenges in developing real world applications. We present, as a case study, a hypothetical application that captures important aspects of watermarking systems and illustrates some of the issues faced.

INTRODUCTION

Digital watermarking provides a way to imperceptibly embed digital information into both digital (images, video, audio) and conventional (printed material) media content. Information contained within the watermark can be used to add value to a variety of applications [4] such as connected content, security, content protection, copy prevention, authentication, etc. A unique advantage of a digital watermark is that the information is imperceptibly bound to the original (cover or host) medium. The digital watermarking field is characterized by active research, with numerous articles covering new techniques, theory, various attacks on watermarking techniques, robustness and analysis. Given that the field is maturing rapidly, there needs to be at least an equal, if not greater, emphasis on the practical aspects of developing real-world watermarking applications. In this article, we focus on practical challenges for watermarking applications. Which watermarking technique to use? How to achieve a specific detection rate in limited time? How to balance watermark visibility with robustness? Our aim is to draw attention to these issues and the tradeoffs involved. To illustrate the challenges of practical applications and the tradeoffs, we use a case study based on a hypothetical application - one that uses digital watermarks to enhance the play value of children's toys.

Each watermarking application has its own needs that determine the required attributes of the watermarking system and drive the choice of techniques used for embedding and detecting the watermark. Commonly discussed attributes of real world systems include: the many forms of robustness against distortion and attack [3], visibility of the embedded mark [5], data capacity of the watermark, immunity of the detector to false alarms, and security. An attribute less commonly discussed, but very important for many real world applications is performance, i.e. the speed of embedding and of detection of the watermark.

0-7803-7025-2/01/$10.00 ©2001 IEEE.

There is an inherent tradeoff between many of these attributes that plays a critical role in a real-world application. At the detector, robustness, false positive rate and speed often compete with each other [1]. During detector design, these attributes must be balanced with the desire for speed to meet the application requirements. For example, robustness to geometric distortions can be achieved at the cost of reduced speed. Application requirements also influence the mode of data acquisition at the detector. The data acquisition device often determines the choice of watermarking technology and its capabilities. In our case study a PC camera provides an easy interface for image capture; the user holds a printed image up to the camera.

At the embedder, the main tradeoffs are between visibility, capacity, robustness and speed. The degree to which human intervention in the embedding process is permitted, impacts both speed of embedding and visibility. Capacity is always in tension with robustness. Watermark strength (energy of the embedded signal) also affects both visibility and robustness. The ability to automatically adapt visibility according to media characteristics without sacrificing robustness (or some other set of attributes) is the foremost goal in embedder design

The first task of application design is to determine the product requirements and use them to prioritize the various watermarking attributes As illustrated by the case study that follows, practical applications necessarily involve contradictory constraints and requirements that have to be traded against one another to achieve the intended goals and satisfy the customer's needs.

CASE STUDY OF A HYPOTHETICAL APPLICATION

The challenges and tradeoffs in developing watermarking applications are best understood by studying a real-world application. We describe a hypothetical application, Smart Toy, which touches upon several practical aspects of watermark application design and development.

A successful watermarking application requires that the customer perceive value in the product, not in the technology. In Smart Toy, the watermark adds play value to a child's toy. This application aims to provide an interactive link between children's toys and the computer. Some aspect of the child's toy will contain a digital watermark that can inform the computer as to the nature of the object and to a lesser degree its location and orientation.

Requirements of the Smart Toy watermarking application

For the purposes of this case study we will define the requirements for a toy:

1. Play action: The toy will consist of an expandable set of vehicles, houses, stores, and other familiar neighborhood locales. Each toy will be watermarked. On first showing the toy to the PC camera, the computer will retrieve a short video and sound clip from either the local database or the Internet. For example, the sounds of a fire engine and a short clip about firefighting could be played if a fire engine is shown to the camera. A different clip could be played the next time the same object is shown.

2. The toy includes a starter kit with software and 1 or 2 vehicles. An add-on kit contains more vehicles and buildings.
3. The Smart Toy system needs to distinguish around 100 toys each from about 50 manufacturers and needs to carry information about the minimum age (3 to 7 years) for which it is intended.
4. The detector must reject a frame in less than 0.1 sec when no watermarked object is presented to the camera. When a watermarked object is presented, the payload should be read in less than 2 sec.
5. When no watermarked object is presented to the camera, less than one false positive is permitted per hour of play. A false positive rate of 1 in 10^4 will satisfy this requirement at 10 fps.
6. The probability of mistaking one toy (false read) as another should be less than 1 in 10^3.
7. There is no security requirement for this application.
8. Camera and PC required are assumed to already exist in the home.

Design Considerations

Based on the requirements listed above, we can begin to describe how these requirements drive various design considerations.

Visibility of Watermark

In the Smart Toy application, the watermark should not affect the artistic value of the toy. The graphic elements of the toy are the cover medium and can be adapted to suit the watermark minimizing its impact on visibility.

Data Acquisition

The game will play by the child holding an object up to a PC camera. The detector has to deal with lens distortion, focus, image compression, image size, frame rate, sensor noise, and with geometric distortions introduced because location and attitude of the image is not controlled.

The toy software can control camera settings such as frame rate, compression, exposure and white balance as required. Given characteristics of the installed base of PC cameras, the capture rate will be 5-8 frames per second to capture uncompressed images. A typical PC camera has a 640 x 480 pixel image sensor. Typical imagers have pixels about 9um on a side. At a typical focal length of 5mm the pixels each subtend an angular distance of $\sim 2 \times 10^{-3}$ radians. This angular resolution sets the minimum meaningful size for a watermarking feature. At a working distance for the game of 20 cm, the minimum spatial extent of a resolvable feature is 4×10^{-2} cm. For robustness reasons, it may be advisable to oversample the watermarking information, leading to a larger watermarking feature

Robustness

The watermark should withstand distortions from camera capture, such as rotation, scaling, cropping, brightness adjustment, contrast enhancement, and lighting variations. Detection should be adaptive to camera-image distance. Detection should work on small watermarked areas on the toy (say of size 4 cm by 4 cm). The watermark must be detectable under conditions that include the soiling of the object

Synchronization

This application requires a synchronization signal that can recover the payload from an image acquired at any angle of rotation about the camera's optic axis, for any distance within the focal zone of the camera, and with small pitch and yaw deviations from normality to the optic axis.

Payload, error correction and spreading

The payload contains the following fields – toy ID (7 bits) that identifies the toy and the action, manufacturer ID (6 bits), intended minimum age (3 bits) and an open field (6 bits) for future use, giving a total of 22 bits. The payload size and importance of the individual fields determine the error correction scheme and the amount of spread employed. For fast detection, a simple repetition code (each bit repeated 14 times) is used for error correction. Each coded bit is further coded into 30 chips to give a total of 9240 bits. To these we append a 760-bit reference PN sequence derived from a key, to obtain a total of 10000 spread-spectrum bits. If the minimum camera resolvable feature has an extent of 4 x 10^{-2} cm, the watermarked area should be of order 4 cm on a side for maximum robustness.

Embedding the watermark signal

The watermarked image *I'* is obtained by embedding the watermark *W* in the original image *I*, $I' = f(I, g(I, W))$, where *f()* is a function denoting the embedding operation, and *g()* is a gain function that depends upon *W* and local and global image properties. These functions can either be linear or non-linear. Embedding can be done either in a transform domain (e.g., frequency domain) or the spatial domain. For the Smart Toy application, we choose *f()* to be an additive operation in the spatial domain. The watermark signal *W* consists of the spread spectrum bits combined with a synchronization signal, which can be a known pattern. Note that the spread spectrum signal itself can be designed to serve the dual purpose of a synchronization signal. The watermark signal is repeated in every M x N block of the image. A key determines the arrangement of the spread-spectrum and reference bits within the block.

Watermark detection

The detector has no knowledge of the original cover image. It obtains an estimate, $\hat{W}$, of the watermark signal from the watermarked image. The detector applies prediction techniques to estimate the original image from the watermarked one. $\hat{W}$ is then obtained by comparing the predicted image with the watermarked image. $\hat{W}$ contains an estimate of the synchronization signal, an estimate of the spread spectrum payload and remnants of the cover image. The detector then uses $\hat{W}$ and a knowledge of the synchronization signal to recover the geometry (rotation, scale, etc.) of the watermark. Before synchronization, the detector may apply pre-processing to suppress the unwanted components due to the image and the spread spectrum signal. Using the recovered synchronization, the detector proceeds to extract the reference bits and spread-spectrum payload. The extracted spread-spectrum data is first de-spread and then decoded to obtain the payload bits. Again, at the payload extraction stage, the detector may pre-process $\hat{W}$ to further suppress components due to the image and the synchronization signal. Comparison of the estimated reference bits with the reference sequence can also be used to aid in robust recovery of the payload.

False positives and false reads

The estimated reference bits are correlated with the reference PN sequence. The correlation threshold is chosen to give a false positive rate of less than 1 in 10^2. A false read occurs when a payload is falsely decoded as another. To reduce false reads, we partition the chips for the coded payload bits into two equal sets. These chips are de-spread and decoded independently. A read is declared valid only when the decoded bits from both sets match bit for bit. Assuming that the probability of chip error is 0.4 and that a 4 cm by 4 cm watermarked image is presented to the detector, this gives an approximate false read rate of less than 1 in 10^3. For unmarked images this gives an overall false positive rate of 1 in 10^5, which easily meets the requirement.

Detection speed

The detector gets a maximum of 100 ms to reject a frame that does not contain a watermark, implying a fast decision must be made about the presence or absence of the watermark. When a watermark is present, more time may be available for extracting the payload, since in this type of game the game takes a dramatically different action upon reading the watermark. The requirement that a marked object be detectable (at some high probability P_d) within T_{max} seconds of presentation to the camera illustrates a key speed tradeoff in the design. If the probability of detecting a watermark is P in any given frame and the average time to detect a frame is T then the tradeoff states that $P_d < 1 - (1 - P)^n$, where n is given by T_{max} / T. The average frame detect time can then be determined by the frame rate of the camera and the speed of the detector over a distribution of capture conditions.

Back end and Internet connectivity considerations

The toy is playable using the stored video clips provided with the toy software. Internet connectivity is not required. However, the game play can be enhanced by allowing connection to the Internet for the download of additional sound and video clips, for registration of the toy, and for update of the detection software.

Cost

Cost is a paramount consideration in the design of a toy or game. In this case the cost increase over the base toy is small for the watermarking and the CD-ROM for the detection software, this should give a cost increase for the watermarking enhancement of less than $1 US. By leveraging the existing PC and camera to implement the watermarking technology, the play value of the game is enhanced by far more than the cost.

Test Results

The design discussed above has been implemented and tested against a total of 4430 marked (two embedding strengths each) and 10,000 unmarked images in digital form. The unmarked images gave no false positives. The marked images gave the results summarized below: Captured images read as expected.

Image Set	Number of Images	Strength	Detection Rate	#False Reads	Average Correlation of PN seq.	Avg. chip error
JPEG	3428	1	78.24%	0	0.36	0.32
JPEG	3428	2	91.10%	1	0.48	0.26
TIF	1002	1	83.03%	0	0.38	0.31
TIF	1002	2	92.81%	0	0.50	0.25

CONCLUSIONS

Digital watermarking is a complex technology necessarily involving many conflicting requirements and tradeoffs. This paper has discussed the design process for real-world watermarking applications. The design process is dramatically simplified if the requirements of the intended product are carefully understood. A successful watermarking application only needs to satisfy the requirements of the product, not all possible requirements. Once realistic constraints on the system are established, the application may move ahead. As shown in the hypothetical case study, through careful design, product value can be enhanced by the judicious application of watermarking technology. In this case, a simple toy is dramatically enriched in play value through the use of watermarking technology to link the physical and virtual worlds.

ACKNOWLEDGMENTS

The authors would like to thank Burt Perry, Brian MacIntosh, Joel Meyer, Ammon Gustafson and Hugh Brunk of Digimarc Corporation for insightful suggestions.

REFERENCES

[1] S. Decker, "Engineering considerations in commercial watermarking", submitted for publication to IEEE Communications magazine, special issue on watermarking. August 2001.

[2] B. Perry, S. Carr, and P. Patterson, "Digital watermarks as a security feature for identity documents", in Proc. SPIE vol. 3973, *Optical Security and Counterfeit Deterrence Techniques III*, pp. 80-87, Apr. 2000.

[3] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Attacks on copyright marking systems", in Workshop on Information Hiding, Apr. 1998.

[4] I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital watermarking: principles and practices,* to be published October 2001.

[5] B. T. Hannigan, A. Reed, and B. A. Bradley, "Watermarking using improved human visual system model", to be published, Proc. SPIE, vol. 4314.