CERIAS Tech Report 2005-125

Multimedia security: the 22nd century approach

by Edward J. Delp

Center for Education and Research in
Information Assurance and Security,
Purdue University, West Lafayette, IN 47907-2086

Multimedia Systems (2005) 11(2): 95–97
DOI 10.1007/s00530-005-0193-4

REGULAR PAPER

Edward J. Delp

Multimedia security: the 22nd century approach

Published online: 14 October 2005

1 Introduction

In this paper I will describe where I think multimedia security will be headed in the next century. Will anything useful happen in the next 100 years? Will our content feel any safer?

This paper is based on the keynote address I gave at the ACM Multimedia and Security Workshop in Magdeburg, Germany on September 21, 2004. Why am I writing this paper? I am not clairvoyant! I cannot see the future! I will be long dead before we get to the 22nd century – hence I am not in trouble or wrong. I will give you my opinions and ideas.[1]

I will attempt to discuss various concepts in multimedia security and particularly data hiding and watermarking and predict how they will be affected in the next 100 years with respect to the impact of the technology on society, the legal aspects, and how research in this area will be driven. I will describe how data hiding and watermarking will be viewed at the dawn of the 22nd century.

With respect to impact of the technology in the next 100 years, the following issues will be important:

- What was the "killer application" for all this stuff?
- Did anyone make money on multimedia security systems?
- Did we ever find the better model for paying for content?
- Did consumers ever get anything from all of this?
- What did the "secure multimedia" system really evolve into in the late 21st century?
- What was the new paradigm that was developed in the late 21st century that worked?

E. J. Delp (✉)
Video and Image Processing Laboratory, School of Electrical and Computer Engineering, Purdue University, West Lafayette, IN, USA
E-mail: ace@ecn.purdue.edu

[1] I do not believe everything I say here but I hope I can stimulate the reader into thinking about the problems. Please remember: Working in this area has been a fascinating and personally rewarding experience for me – I have had fun and met some of the most intelligent people ever.

With respect to legal aspects, I believe the questions we must address in the next 100 years include:

- Will bits really be free in the 22nd century?
- Was there a legal fix for content protection in the 21st century?
- Did we need a technical solution or a legal fix?

Finally, what will the research questions and issues be with to watermarking and data hiding in the next 100 years?

- Is multimedia security still an important topic or was it just a "hyped" academic subject similar to AI in the 1980s, neural networks in the 1990s, and nanotechnology in the 2000s?
- Did the theoretical models proposed in the early 21st century really provide any insight?
- Will watermarking still be a "young" technology in the 22nd century?
- Is robust watermarking an oxymoron?

Before we see where we will be in the year 2101, first lets describe where we are now. Have there really been any successful uses of watermarking technology as we begin the 21st century? The simple answer is that there has been some success mainly in specific niche applications. The most successful application is content tracking or content fingerprinting whereby a watermark (e.g., serial number) is embedded in multimedia content and then used to track where the content or the origin of the content. For example, this has been used by the MPAA to track movies that are distributed to screeners for the Oscar Awards. It has also been reported that data hiding methods, particularly steganography, have been used by criminal and terrorist organizations for secret communication. Both applications are very specialized. Interestingly, we have not seen any real commercial success in using watermarking for content protection. Several watermarking companies have gone out of business, other companies have suspended their watermarking efforts, and some have had "business problems." This was suppose to be the "killer application" for watermarking. In general, multimedia security systems are tolerated by users. However, users

are frustrated by these systems and in some cases do not understand the rules imposed on them, for example, the rules with respect to copying and replacing lost content in the Apple iTunes system. It is difficult to convince consumers that multimedia security systems are good[2] for them and I am not aware of any company using its security system as a marketing feature to the consumer. Now lets talk about the future.

2 The future

What will be the major security problem at the dawn of the 22nd century? The simple answer is *trust*.

Who and what I do trust? One will need to trust people, data, and physical objects. This must be done in plain sight and will require methods that did not exist at the dawn of the 21st century and will not be based on cryptographic principles. I believe trust mechanisms (i.e., authentication) in the 22nd century will be a distant cousin to data hiding. Related to trust and authentication will be the area of forensics. For example, a user will want to know whether data delivered to them from a sensor (e.g., camera) can be trusted. Is the sensor valid? Is the data valid? Has the data been modified? This trust associated with the sensor and the data must be "bound" to the data and hence will require methods that are beyond current cryptographic-based methods. Biometrics will be used to trust people but the biometric data must be trusted.

We will also live in a surveillance society at the dawn of the 22nd century. There will be sensors everywhere monitoring anything we do and our environment. The expectations of privacy will be greatly diminished. If techniques for trust are not developed then it will be easy to alter reality or at least the way it is recorded. Our society will spiral down into possible chaos and complete upheaval.

3 Answers to the questions

What about answering the questions I posed in Sect. 1? How will they be addressed at the dawn of the 22nd century?

A. With respect to impact of multimedia security in the 22nd century:
   - *What was the "killer application" for all this stuff*?

   Authentication and the use of data hiding methods as auxiliary data channels will be the application that will be important and one that will make money for the industry. As I indicated earlier, I believe that trust will be most important security concepts in the next 100 years. Authentication is the mechanism for trustworthiness. Using data hiding methods to bind auxiliary data to content will be very important in fact I believe this will be the only financially viable application of data hiding and watermarking. It will not be content protection.
   - *Did anyone make money on multimedia security systems in the 22nd century*?

   No, particularly with respect to content protection. It was a lost cause. The money that was made was in data binding, such as content tracking and metadata.
   - *Did we ever find the better model for paying for content*?

   Yes, the "prepay model" (see later).
   - *Did consumers ever get anything from all of this*?

   Very little from content protection but great benefit from authentication and data binding.
   - *What did a "secure multimedia" system really evolve into in the 22nd century*?

   There are no secure multimedia systems in the 22nd century. Consumers never accepted the concept of not really owning the content that they purchased. New paradigms based on "pre-pay" models (e.g., the media pay model used in Europe) or auxiliary pay models (e.g., free movies on television that are paid for by commercials).[3]
   - *What was the new paradigm that was developed in the late 21st century that worked*?

   A new "prepay model" and auxiliary pay model was adopted (see earlier).

B. With respect to the legal aspects:
   - *Will bits really be free in the 22nd century*?

   Yes, but they will be worth nothing. The selling of bits will use the new pre-paid model. After they "released" into the user community, they will be free and worthless.
   - *Was there a legal fix for content protection in the 21st century*? *Did we need a technical solution or a legal fix*?

   There was never a technical fix for content protection but new legal approaches were developed—limits on human behavior always require fixes based on society and culture.

C. With respect to research in multimedia security in the 22nd century:
   - *Is multimedia security still an important topic or was it just a "hyped" academic subject similar to AI in the 1980s, neural networks in the 1990s, and nanotechnology in the 2000s*?

   Yes, but the research community is relatively small. However, the areas of trust, authentication and forensics will be the most important problems that will need to be addressed now and in the next 100 years!
   - *Did the theoretical models proposed in the early 21st century really provide any insight*?

   No, similar to the way theoretical source and channel coding methods did not provide new techniques in the

[2] Most multimedia security systems are usually known as "digital rights management systems" or DRMs. I will avoid this term in the paper to minimize the overall confusion. I am sure we will have a more encryptic name for these systems in the 22nd century!

[3] I do not know exactly what the pre-pay model will be but a system will have to be developed that collects payments up-front.

20th century. Theoretical methods will provide bounds and perhaps operational optimal approaches but the application domain is generally too complex.

- *Will data hiding and watermarking still be a "young" technology in the 22nd century*?

No, but it will still be interesting.

- *Is robust watermarking an oxymoron*?

Yes, this problem will never be solved. It will be an "arms race," every time a robust system is proposed new attacks will be developed. This is similar to the situation with the segmentation problem in computer vision in that it also will never be solved. Given that data binding methods will be the most important uses of data hiding, the robust system will not be as important as we thought it would in the 21st century, since we will not be using watermarking for content protection.

4 Conclusions

We are now in the early part of the 21st century and we must abandon the typical content protection model. It is a lost cause. It will probably take us 100 years to admit this. I do not believe in stealing content and I feel new laws will need to be developed to combat this but also protect the rights of consumers. New business models based on pre-pay will be developed.

Trust, authentication and forensics will be the most important problems that will need to be addressed in the future! We will have fun.

There is hope.

Acknowledgements This work was supported by the endowment associated with the Silicon Valley Professorship held by the author in the School of Electrical and Computer Engineering at Purdue University.