

Piracy Prevention for Multimedia Data through Digital Watermarking

Robby S. Fussell
robby@nsu.nova.edu

Introduction

Multimedia provides instruments that enhance many different applications for life. For example, multimedia augments the delivery and retention of information for Websites and learning institutions. Multimedia also improves the way television programs are delivered and perceived. Multimedia consists of many elements, such as digital images and digital videos, to name a few. With the advent of high-speed networks, distribution of these elements to other end users places the digital media in a vulnerable situation. There is an issue that surrounds these elements in determining how to protect the owner's rights to the digital media. The current trend of protecting digital multimedia is through digital watermarking. Various digital watermarking techniques are currently being researched and developed. This article will examine those techniques, including advantages and disadvantages of digital watermarking. The objective is to provide an understanding of digital watermarking, some of the methods utilized, and their feasibility based on the effects of digital watermarking the media.

With the inventions of digital cameras and digital video recorders, a new technology has emerged to protect the digital images of creators. This new technology is termed digital watermarking and is being implemented for the protection of Intellectual Property Rights (IPR). There is a stronger need for this technology with the proliferation of high-speed networks and distributed systems. Digital watermarking has been researched and the technology has been shown to be an efficient solution for the protection of multimedia data.¹ Now with the invention of virtual art galleries, digital watermarking is being employed to protect the gallery and the artist of the digital images. Digital watermarking is the process of embedding certain data into the image without distorting the original image. Various algorithms are being developed to enhance this process.

Statement of the Problem/Topic

Developers of digital multimedia are losing substantial revenues yearly due to digital media piracy. This article will attempt to locate a solution that will prevent the loss of revenue from digital multimedia piracy. It was estimated in 2002 that before the release of two major motion pictures, roughly 1 million to 3 million individuals illegally downloaded the movies, which resulted in an average revenue loss of around 25.5 million dollars.² This is becoming a problem in all areas of digital multimedia. Due to digital media being pervasive and easily manipulated, illegal activities such as unauthorized distribution, duplication, and modification are becoming more prevalent.³ The scope of this problem is not only limited to movies but also to digital images. A solution would need to take into consideration all types of digital imagery and formats. This problem has evolved because people are less apt to pay for the digital multimedia products. The

advancement in network technology and computing power has assisted these individuals by making the digital multimedia easily accessible. More end users are connected at higher network speeds, and high-end computers have become extremely affordable. Digital data owners are becoming more reluctant in distributing their work due to the easy-to-copy ability of digital information.⁴

Goal to be Achieved

The goal of this article is to attempt to discover if a feasible solution exists that will prohibit digital multimedia piracy. The solution would need to have the ability to work with different multimedia types, including various file formats. The solution would also have to be accepted as an effective means of deterring and prohibiting digital multimedia piracy. Finally, the solution should have no visual impact on the digital multimedia image or images. Since the development of technology advances daily and since there are many developers throughout the world, solutions for digital multimedia copyright protection should be vast. The approach that is taken is to collect data on digital watermarking for digital multimedia copyright protection and analyze that data to determine if it is an effective solution. This article will address the question of whether or not there is an effective digital watermarking solution that can prevent the piracy of digital multimedia. Digital watermarking is a way of protecting (IPR) of distributed digital multimedia data.⁴ Listed are some research questions that will assist in identifying if the digital watermarking solution is effective:

- ▲ Does digital watermarking provide a mechanism for securing (IPR)?
- ▲ Will digital watermarking support various types of digital multimedia?
- ▲ Will digital watermarking prevent digital multimedia piracy?
- ▲ Can digital watermarking be used as a legal resource for determining (IPR)?
- ▲ Does the digital watermarking scheme provide confidentiality, integrity and accountability?

There are numerous instances in which digital watermarking has been effectively used for copyright protection. Digital watermarking has been determined to be an effective solution to providing copyright protection for digital multimedia designers.⁴ Digital watermarking has been used in many different situations, areas and implementations to provide copyright protection.^{3, 4, 11, 12, 13}

Relevance and Significance

A valid research topic is the protection of digital multimedia due to the ease of transmitting, duplicating and manipulating the digital information.⁵ The relevance and significance of this topic is due to its impact

on the global economy.² The problem of digital multimedia piracy is an international problem. Another problem with digital multimedia piracy is the loss of revenue.⁶ This problem prevents many digital multimedia developers from distributing their work.⁷ Digital watermarking resolves the problem of digital multimedia piracy by embedding data into the digital image through the use of cryptographic functions. These cryptographic functions are computationally infeasible to hack, thus providing a legal means of protecting (IPR) of digital multimedia data. By standardizing the cryptographic algorithms, the digital watermark solution would be a perfect means for the digital image creator to protect the digital multimedia. By developing a digital watermarking scheme that is an accepted standard, the professional practice of digital multimedia creation could improve by assuring the developers that the digital multimedia information would be protected.

Barriers and Issues

Currently, the goal of discovering a method of securing digital multimedia has not been realized. The difficulty with the digital watermarking solution is its lack of standardization and acceptability. Another problem with the goal or solution is that many cryptographic functions that are used for securing digital multimedia are weak.⁸ This was demonstrated when the DVD encryption scheme was deciphered. This fact makes them less apt for acceptance. Another barrier or issue is that the security of the digital multimedia must include confidentiality, integrity and accountability to be considered as an accepted legal means of (IPR) protection. It is typically known that there is not one overall solution that can provide confidentiality, integrity and accountability.⁹ When using cryptography to transmit multimedia across networks, another issue is the management of the encryption and decryption keys.⁹

Review Of Related Literature

Introduction

This literature review is to examine other peer-reviewed research that is applicable in providing solutions in the area of digital multimedia piracy. The proposed solution is the use of digital watermarking; however, does digital watermarking answer the questions stated earlier in the "Goal to be Achieved" section? Digital watermarking has been identified as a means of providing copyright protection; however, in order for it to be an acceptable solution, it must provide confidentiality, integrity and accountability.

Use of Digital Watermarking

Digital watermarking is the process of embedding digital information into a digital image or digital movie. The information that is embedded can consist of a visible or non-visible image, information that identifies the owner or creator of the digital multimedia information which is used to determine its authenticity, or tracking information for the distribution rights of the image.⁶ There are numerous methods for employing digital watermarking schemes and algorithms.^{1,4} Copyright protection is one scenario in which digital watermarking is being used. This process embeds a visible image onto the original image. This enables the ability for enforcement of IPR of legal commercial use of copyrighted digital images. In order for digital watermarking to be used effectively, the embedded code cannot be tampered with by any means. Another use of digital watermarking is for ownership identification. By embedding ownership information into an image that is not visible, the image can be used in its original form without visible disruption of the image. The image can still be checked for authenticity if suspected misuse has occurred. Another application of

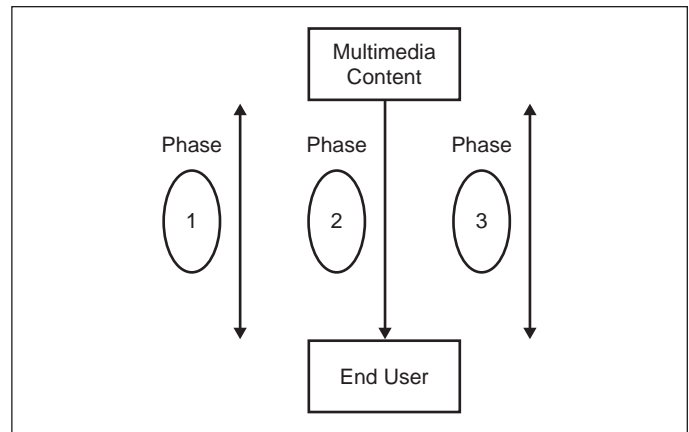


Figure 1: Content Distribution Model with Digital Watermark

digital watermarking is its use to track digital image distribution. Digital watermarking software has been created that would allow a certain distinguishing ID to be embedded into the image. A practical use of this would be where a photographer has sold digital images to another individual and the photographer embedded an ID in the images. If the photographer ever discovered one of his images being sold somewhere else that he/she did not sell to, he/she could check the image's ID and see which individual distributed the image and take corrective action.

Confidentiality

One step in providing a solution for digital multimedia is making the multimedia confidential. Confidentiality is the means of transferring the data to the intended recipient where only the receiver can view the data. A method used to accomplish this is encryption. By utilizing cryptography, the multimedia data can only be viewed by the possession of the decryption key. However, encryption alone cannot be the sole security feature to protect multimedia data. The decryption key must be protected also, and this is a problem in itself.⁹ Digital watermarking cannot be an effective method for confidentiality. Digital watermarking only embeds copyright, authentication and content tracking information which allows the multimedia data to still be viewable.⁹

Integrity

The next step in providing a means of digital multimedia security is the ability to prevent the change of the multimedia data. The current approach to this method uses visible digital watermarking. The problem with using digital watermarking as a means to provide multimedia data integrity is that the digital watermarking scheme is weak. Through the use of signal processing, which uses the process of file conversion or compression, digital watermarks can be rendered useless.¹⁰ Moreover, there are publicly available programs that can outright remove the digital watermark. Hence, the attacker can then insert their own digital watermark and claim the digital data as their own.¹⁰

Accountability

The last step in providing a secure means of digital multimedia security is the ability to substantiate the author of the media. Some digital watermarking schemes utilize digital signatures that are embedded into the digital media to provide proof of authorship; however, a problem arises with publicly available digital multimedia. What prevents a malicious individual from embedding his or her digital signature into a public image or video stream and claiming that it is their own work?¹⁰ This problem is referred as the deadlock problem.

Content Distribution Model

Since digital watermarking does not provide an adequate means for confidentiality, integrity and accountability, a model has been created that includes these traits along with digital watermarking in attempt to solve the stated problem of piracy (see Figure 1). The content distribution model contains three different phases that must be used to transfer digital multimedia data over public networks. This distribution model does provide digital multimedia security.

Phase 1

Phase 1 entails the process of key exchange. The multimedia content server contains various types of digital multimedia. An end-user could request a multimedia image from the multimedia content server via a Webpage. Once requested, the multimedia data would already contain a visible digital watermark with the multimedia content server's identification.

A public key exchange would take place between the end user and the multimedia content server where the public key of the end user would be sent to the multimedia content server and the digital image would be encrypted with the public key of the end user and then transmitted back to the end user for decryption (see Phase 2). This phase provides confidentiality and copyright protection.

Phase 2

Phase 2 is the transmission of the encrypted digital information to the end user. Once the end user receives all the data, he or she can decrypt the digital image with their private encryption key. Once decrypted, the image is viewable along with the visible digital watermark embedded by the multimedia content server. The encryption/decryption process will provide confidentiality and integrity. The integrity verification is provided by a hashing function such as SHA1 (Secure Hashing Algorithm) or MD5 (Message Digest). At this point, no monetary transaction has occurred. Also, since the digital watermark is embedded in the digital image, the image is still viewable but retains its ownership verifiability. At this stage, signal processing or other publicly available tools could be used to remove the digital watermark.¹⁰

Phase 3

The final phase consists of the obligation to purchase the digital media. The end user would provide payment for the digital image via the Website. Then, the multimedia content server would remove the visible digital watermark;^{6, 8} however, the tracking data or distinguishable ID would remain.¹

Summary

The problem for finding a solution for preventing digital multimedia piracy is that digital watermarking only provides copyright protection, authentication and content tracking.⁹ There have been models developed⁹ that, along with digital watermarking, also provide confidentiality, integrity and accountability through other mechanisms such as cryptography, hash functions, and digital signatures. However, these models do not provide a mechanism for preventing piracy once the digital information has been decrypted.

Methodology

A meta-analysis research methodology along with a methodological research methodology was utilized for this study. These research

methods involved the examination of existing peer-reviewed research and applications to determine a solution to the proposed problem statement of preventing digital multimedia piracy. These types of research methodologies will yield possible resolutions to the stated problem through the use of analyzing proposed solutions in related areas along with evaluating the proposed solutions' effectiveness. The research data collection process involved obtaining peer-reviewed research that dealt with copyright infringement and solutions that could possibly assist in resolving the problem of digital multimedia data piracy. Also, a potential solution was compared with the existing solutions to determine if the proposed solution was advantageous. Databases that were utilized for data collection:

- ▲ ACM Digital Library
- ▲ Applied Science and Technology (Wilson Web)
- ▲ IEEE Computer Society Digital Library
- ▲ Wiley Interscience


Results

Digital watermarking is used to embed digital information inside digital multimedia data. It provides copyright protection, authentication, and content tracking information.⁹ Digital watermarking schemes do provide a mechanism for securing multimedia information. Various digital watermarking schemes operate on different types of multimedia formats.^{1, 5, 6, 11} Digital watermarking exhibits inherent weaknesses of the algorithms used to embed digital watermark information.¹⁰ Therefore, digital watermarking does not provide confidentiality, integrity and accountability; however, the content distribution model proposed does provide these features but does not prevent digital multimedia piracy.

Conclusion

The conclusion of the research provides no current solution that can be used to prevent digital multimedia piracy. Based on the advantages and disadvantages of the several different digital watermarking technologies, digital watermarking methodologies still need to be explored. Even a digital multimedia security scheme that employed the following would not prevent digital piracy:

- ▲ Cryptography for confidentiality. This method would have to include a way of managing cryptographic keys.
- ▲ Hashing function for integrity. This hashing function would have to be tested by various groups to prove that it is indeed a one-way hash function.
- ▲ Digital signatures for accountability. This would involve an infrastructure that could issue and revoke digital signatures.

Digital watermarking does not provide a solution in preventing digital multimedia piracy even including confidentiality, integrity and accountability in a content distribution model. The problem that still eludes the research is how to protect the digital multimedia once it is decrypted and the digital watermark has been removed? Illegal acquisition of digital multimedia will continue even with litigation.² Digital watermarking does not prevent digital multimedia piracy; however, digital watermarking might be a deterrent in the illegal acquisition of digital multimedia. Research must continue in the area of preventing piracy of digital multimedia data in order to solve the problem of loss revenue due to piracy. 

Robby S. Fussell currently works for AT&T Labs Security Center of Excellence as a senior security engineer. He is international team lead for security vulnerability scanning. He develops security solutions for AT&T customers and for the corporation. He is also responsible for providing training on various security topics for AT&T.

¹ Cappellini, V., Bartolini, F., Caldelli, R., Rosa, A.D., Piva, A., Barni, M. and Wada, M., Copyright Protection of Cultural Heritage Multimedia Data through Digital Watermarking Techniques. in Proceedings of the 11th International Workshop on Database and Expert Systems Applications IEEE, (2000), IEEE, 1-5.

² Levack, K. Digital Darwinism: Piracy Pushes Progress EContent, 2002, 6-9.

³ Cheng, Q. and Huang, T.S., An image watermarking technique using pyramid transform. in Proceedings of the ninth ACM international conference on Multimedia, (2001), ACM Press New York, NY, USA, 319-328.

⁴ Bartolini, F., Piva, A. and Barni, M., Watermarking-Based Copyright Protection of Internet-delivered Multimedia. in Proceedings of the First International Conference on WEB Delivering of Music IEEE, (2001), IEEE, 1-7.

⁵ Tran, N., Hiding Functions and Computational Security of Image Watermarking Systems. in Proceedings of the 15th IEEE Computer Security Foundations Workshop, (2002), IEEE, 1-9.

⁶ Mintzer, F., Braudaway, G.W. and Yeung, M.M., Effective and Ineffective Digital Watermarks. in Proceedings of the 1997 International Conference on Image Processing (ICIP '97), (1997), IEEE, 1-4.

⁷ Adelsbach, A., Katzenbeisser, S. and Veith, H., Watermarking schemes provably secure against copy and ambiguity attacks. in Proceedings of the 2003 ACM workshop on Digital rights management, (Washington, DC, USA, 2003), ACM Press New York, NY, USA, 111-119.

⁸ Taylor, A., Foster, R. and Pelly, J. Visible Watermarking for Content Protection SMPTE Motion Imaging, 2003, 81-89.

⁹ Lin, E.T., Cook, G.W., Salama, P. and Delp, E.J., An Overview of Security Issues in Streaming Video. in Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC .01), (2001), IEEE, 1-4.

¹⁰ Kwok, S.H. Watermark-based copyright protection system security. Communications of the ACM, 46 (October 2003), 98-101.

¹¹ Dittmann, J., Stabenau, M. and Steinmetz, R., Robust MPEG video watermarking technologies. in Proceedings of the sixth ACM international conference on Multimedia, (Bristol, United Kingdom, 1998), ACM Press New York, NY, USA, 71-80.

¹² Lan, T.-H. and Tewfik, A.H., Fraud detection and self embedding. in Proceedings of the seventh ACM international conference on Multimedia, (1999), ACM Press New York, NY, USA, 33-36.

¹³ Zhang, J., Wang, N. and Xiong, F., Hiding a Logo Watermark into the Multiwavelet Domain Using Neural Networks. in Proceedings of the 14th IEEE International Conference on Tools with Artificial Intelligence, (2002), IEEE, 1-6.

