International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org, editorijaiem@gmail.com
Volume 2, Issue 2, February 2013 ISSN 2319 - 4847

Digital Watermarking and fingerprinting: A good idea for security

Miss. Nupoor M. Yawale[1], Prof. V. B. Gadicha[2]

[1]M.E. First year CSE
P R Patil COET, Amravati, India.

[2]HOD
P R Patil COET, Amravati, India.

ABSTRACT

In recent years, the distribution of works of art, including pictures, music, video and textual documents, has become easier. With the widespread and increasing use of the Internet, digital forms of these media are easily accessible. Digital documents are easy to copy and distribute. There are a number of methods for protecting ownership. One of these is known as digital watermarking. Digital watermarking is the enabling technology to prove ownership on copyrighted material, detect originators of illegally made copies, monitor the usage of the copyrighted multimedia data and analyze the spread spectrum of the data over networks and servers. Embedding of unique customer identification as a watermark into data is called fingerprinting to identify illegal copies of documents. Digital watermarking techniques are used to protect the data from either accidental or intentional attacks. Among the various biometrics, fingerprints are more famous in the authentication area, as they are unique to each person and are mainly used for the establishment of instant personal identity. Watermarking and fingerprinting technologies offer media producers and publishers a promising set of tools for fighting content crime, as well as for a variety of other purposes.

Keywords: copyright protection, customer copy identification, Data authentication, Digital Water marking, Fingerprinting.

1. INTRODUCTION

Information hiding can be mainly divided into three processes - cryptography, stenography and watermarks. Cryptography is the process of converting information to an unintelligible form so that only the authorized person with the key can decipher it. Stenography is the process of hiding information over a cover object such that the hidden information cannot be perceived by the user. Watermarking is closely related to stenography, but in watermarking the hidden information is usually related to the cover object.

Hence it is mainly used for copyright protection and owner authentication. Watermarking adds information, embedding it within a video and/or audio signal. Fingerprinting does not add any information, it analyses the media, identifying a unique set of inherent properties. Many identical versions of the same piece of video can be created, each with its own unique watermark.

The watermarking solution promises to protect your images by inserting text information and then tracking the images. Digital watermarking distinguishes digital copies and mark documents with owner's ID.

There are many reasons to embed information in digital content using digital watermarking. All information handled on internet is in digital form. Such digital content can be copy such that new file is indistinguishable from original one. Then content can be reproducing in large quantities. The Digital watermarking protects such illegal copying. A watermark discourages piracy and determines criminals of making illegal copies of digital media.

2. IMPORTANCE OF WATERMARKING AND FINGERPRINTING

In today's networked world, the need to maintain the security of information or physical property is becoming both increasingly important due to the increase in concern over copyright protection of content. Watermarks are useful for tracking individual assets, helping to identify who created a particular piece of content, determining whether content was obtained by legitimate means visible watermarks, such as network logos or station IDs. Anyone just viewing the videos would not be able to tell that they were different, but your watermarking system could identify each of them uniquely.

The purpose, value and execution of fingerprinting are quite different from those of watermarking. Watermarking relies on embedding information into the video and/or audio, and then uses that information to identify the piece of content.

Fingerprinting does not embed any information; it analyzes the video and/or audio to determine the unique characteristics of the content.

Figure 1: Use of Watermark

3. GENERIC FRAMEWORK

The framework has three key components: a watermark algorithm, a fingerprint protocol, and plugin architecture.
In this framework, the buyer and seller each have a private number for the session. The commonly known information between them is the hash of buyer's private number, and the hash of the seller's private number.[6] That way, neither side's private number can be guessed by the other. Although this sort of exchange is supposed to be done independently by both sides, it is unlikely that the buyer will insert their own private number into the media after it is downloaded.
The only way to ensure that the buyer's private number is inserted (without the use of a third party or custom software) would be to embed it on the seller's server. Since the server needs to know everything about the exchange anyway, it might as well do the exchange internally before sending out the fingerprinted media file. Although it may appear that all security is lost in this process, a chain of verifiable hashes keeps the webmaster from tampering with any of the code used to generate the media and the log files. Any change to either the code or the log entry would put the seller at a disadvantage, because then hashes would not match up.
During execution, the Framework calculates the hash of itself and each of the files, and creates a string from the data. The string includes the filenames, version information of the files, and the calculated MD5 hashes. This string is included in the log data, and can later be used to verify that the code running on the server is the same as the code in the official distributions.

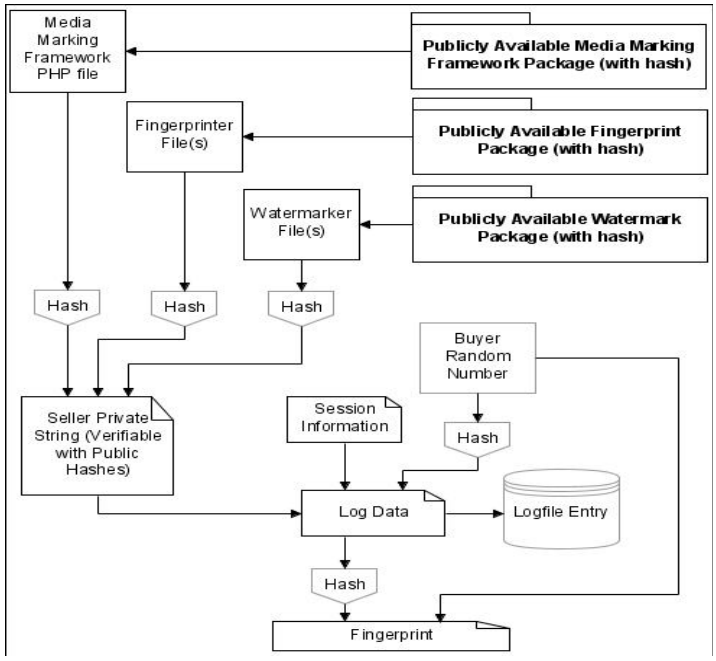

Figure 2: The flow of fingerprint generation by watermarking

Another item in the log data is the hash of the random 16-byte number that was generated for the buyer. The original number forms half of the final fingerprint, and acts as a reverse check and prevents the webmaster from regenerating the file. The rest of the log data consists of session information such as the date/time, username, file requested, and IP address. Finally, the log data gets stamped into the log file with a hash that is generated to complete the fingerprint. The total fingerprint size is 32 bytes. Tracing back the fingerprint from an In-the-wild media file is fairly simple. The

hash contained in the fingerprint is also in the log file, so a search of the log file will result in the entry. Additionally, the random number in the media file can be hashed, and a search for that hash will bring up the same entry.
If enough watermark information is lost so that a few bits are incorrect in the recovered fingerprint, it can still be matched with some degree of certainty to the log entry. However, the hash of the random number will fail to match with what is in the log. Just like the watermarking system, the fingerprinting system is plugin oriented. This allows new forms of fingerprints to be created that can keep up with current research. If a webmaster would like to use the secure and anonymizing services of a third party, a fingerprint plugin could be created and distributed by the third party. The framework allows quite a bit of flexibility for new fingerprinting plugins.

4. CONCLUSION

The large need of networked multimedia system has created the need of "COPYRIGHT PROTECTION". It is very important to protect intellectual properties of digital media. Internet playing an important role of digital data transfer. Digital watermarking is the great solution of the problem of how to protect copyright. Digital watermarking is the solution for the protection of legal rights of digital content owner and customer with the help of fingerprinting.

REFERENCES

[1] F,Y. Daun, I. King, "A SHORT SUMMARY OF DIGITAL WATERMARKING TECHNIQUES FOR MULTIMEDIA DATA", Department of computer science engineering, The Chinese University of Hong-Kong. Shatin, N. T. HongKong, China.
[2] Fernando P´ erez-Gonz´ alez and Juan R. Hern´ andez," A TUTORIAL ON DIGITAL WATERMARKING", Dept. Technology's de las Comunicaciones, ETSI Telecom., Universidad de Vigo, 36200 Vigo, Spain.
[3] Michael Gaylord,"COMPONENTS OF DIGITAL WATERMARKING AND PROTECTION OF OWNERSHIP", University of cape down ,department of computer science.
[4] Onur Mutlu," AN OVERVIEW OF IMAGE WATERMARKING ALGORITHMS", EE 371R Digital Image Processing.
[5] Elizabeth Ferrili, Matthew moyer ,"A SURVEY OF DIGITAL WATERMARKING".
[6] E. Rescorla, "RFC 2631 Diffie-Hellman Key Agreement Method", The Internet Engineering Task Force, 1999. [Online]. Available: http://tools.ietf.org/html/rfc2631.[Accessed: March 7, 2007].
[7] D. Boneh and J. Shaw, Collusion-Secure Fingerprinting for Digital Data. Proc. CRYPTO'95, Springer LNCS 963, pp. 452-465, 1995.
[8] I.J. Cox and M.L. Miller, A review of watermarking and the importance of perceptual modeling, Proc. of Electronic Imaging'97, February 1997.
[9] Ahmed, F. and Moskowitz, I.S. (2005) Composite Signature Based Watermarking for Fingerprint Authentication, ACM Multimedia and Security Workshop, New York, Pp. 1-8.
[10] Hui, K., Jing, L., Xiao-dong, Z. and Xiao-xu, Z. (2008) Study on Implementation of a Fingerprint Watermark, International Conference on Computer Science and Software Engineering (CSSE), Vol. 3, Pp.725-728.
[11] Schaathun, H.G. (2006) On watermarking/ fingerprinting for copyright protection, Proceedings of the First International Conference on Innovative Computing, Information and Control, IEEE Computer Society, Vol. 3, Pp. 50-53.
[12] Zebbiche, K. and Ghouti, L. et al. (2006) Protecting fingerprint data using watermarking. First NASA/ESA Conf. on Adaptive Hardware and Systems (AHS"06), Pp.451–456.
[13] http://en.wikipedia.org/wiki/Digital_watermarking.
[14] http://en.wikipedia.org/wiki/Digital_video_fingerpr-inting.
[15] E. Muharemagic and B. Furht, "Survey of Watermarking Techniques and Applications", Florida Atlantic University, 2005.

AUTHOR

Miss. Nupoor M. Yawale is a scholar of ME, (Computer Science Engineering), at P R Patil COET, Amravati, under SGBAU, India.

Prof. Vijay B. Gadicha, HOD, Computer science department of P R Patil COET, Amravati. He has done his M.E. from Ram Meghe Institute of Technology & Research, Badnera, India.