Watermark Attacks And Applications in Watermarking

Sunesh, Harish Kumar
Department of Computer Science & Applications, CDLU, Sirsa, Haryana

ABSTRACT

Digital watermarking of multimedia content has become a very active research area over the last several years. Digital watermarking is the process of embedding watermark into a digital signal. A digital watermark is a digital signal or pattern inserted into a digital document and carries information unique to the copyright owner, the creator of the document or the authorized consumer. This paper presents various watermark attack. Watermark attack is any processing (ability of unauthorized users) that may remove, detect and estimate, write or modify the raw watermarking bits (watermark).In this paper, we review watermarking applications areas such as ownership assertion, copy control, finger printing etc.

Keywords

Digital Watermarking, digital watermark, watermark attack

1. INTRODUCTION

With the ever-growing expansion of digital multimedia and the Internet the problem of ownership protection of digital information has become increasingly important. Watermarking or data hiding is designed to meet this demand. Digital Watermarking can be defined as a technology of embedding watermark with intellectual property rights into images, videos, audios and other multimedia data by a certain algorithm. This kind of watermark contains the author and the user's information, which could be the owner's logo, serial number or control information. If the signal is copied, then the embedded information is also in the copy. Digital Watermarking gets its name from watermarking, which is very old. Watermarking is very common in our everyday lives; you see watermarking in currency, government documents, stamps and many other common documents detection of the watermark or communication of the. The main use of watermarking is to provide a level of certainty about the authenticity and/or ownership of a document. In this paper , we will present a variety of applications areas of watermarking. Although significant progress has been made in watermarking of digital images, many challenging problems still remain in practical applications. Among these problems are water attacks. An "attack" is any processing that may impair information conveyed by the watermark some of *attacks are* easy to implement, but can make many of the existing watermarking algorithms ineffective. Examples of watermark attacks include Basic attacks, Removal Attack, legal attacks, Geometric attack, Protocol Attacks, Cryptographic Attacks.

The paper explains basic terms of watermarking system and reviews various watermark attacks and applications in watermarking.

2. GENERAL WATERMARKING SYSTEM

A digital watermarking scheme, in general, is a set of algorithms that allow us to embed some information (i.e., watermarks) into some host signal in such a way that these watermarks can later be extracted or detected, even if the cover objects are corrupted by a small amount of permissible noise. A watermarking scheme usually consists of three major components. A watermark generator generates desired watermarks for a particular application, which are optionally dependent on some keys. An embedder embeds the watermark into the cover object, sometimes based on an embedding key. A detector is responsible for detecting the existence of some predefined watermark in a cover object, and sometimes it is desirable to extract an message from the watermarked cover object.[4]

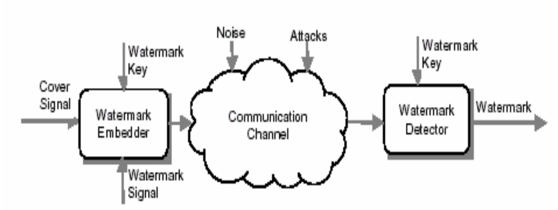

Fig1: Digital Watermarking Systems

2.1 Watermark

A digital watermark is a digital signal or pattern inserted into a digital document such as text, graphics or multimedia, and carries information unique to the copyright owner, the creator of the document or the authorized consumer. There are different types of watermarks such as:

Visible watermarks:
Visible watermarks are designed to be easily perceived by the viewer, and clearly identify the owner. The watermark must not detract from the image content itself, however.

Invisible watermarks:
Invisible watermarks are designed to be imperceptible. This type of watermark is not visible in the watermark image without degradation of image or data. Invisible watermark may be any logo or any signature**.** Most research currently focuses on invisible watermarks, which are imperceptible under normal viewing conditions.

2.2 Watermark Security

Watermark security refers to the inability by unauthorized users to have access to the raw watermarking channel. In other words, watermark security refers the inability of unauthorized users to remove, detect and estimate, write or modify the raw watermarking bits. In particular, watermark security is not concerned with the semantics of the watermarking bits, but solely with the physical presence of the watermarking bits which states that we must assume that the attacker knows the watermark embedding and detection algorithms. The security of watermarking should rely in the secrecy of the keys and only the knowledge of both the algorithm and the keys can break the algorithm. Therefore, we will also assume that the attacker does not have knowledge of the watermarking keys. The aim of an attacker is then to eliminate, remove or degrade the effectiveness of the watermark, to disable the detector or to attack the concept of the watermarking application. An attack is considered successful if the attacker disrupt any stage of the watermarked life cycle; thus, the content owner and the watermarking software have to ensure that each stage is secured against such manipulations.

3. WATERMARK ATTACKS

In watermarking terminology, an “attack” is any processing that may impair detection of the watermark or comunication of the information conveyed by the watermark. There are various types of attacks on watermarking schemes: Basic attacks, Removal Attack, legal attacks, Geometric attack, Protocol Attacks ,Cryptographic Attacks.

3.1 Basic Attack:

Basic attacks take advantage of limitations in the design of the embedding techniques. Simple spread spectrum techniques, for example, are able to survive amplitude distortion and noise addition but are vulnerable to timing errors. Synchronisation of the chip signal is required in order for the technique to work so adjusting the synchronisation can cause the embedded data to be lost. It is possible to alter the length of a piece of audio without changing the pitch and this can also be an effective attack on audio files.

3.2 Legal Attack

Legal attacks is the ability of an attacker to cast doubt on the watermarking scheme in the courts. These attacks rely on existing and future legislation on copyright laws and digital information ownership, the credibility of the owner and of the attacker, the financial strength of the owner versus that of the attacker, the expert witnesses, and the competence of the lawyers. A truly robust watermarking scheme has to minimize an attackers ability to cast doubt on technical evidences presented in court.

3.3 Removal Attacks

Removal attacks aim at the complete removal of the watermark information from the watermarked data without cracking the security of the watermarking algorithm (e.g., without the key used for watermark embedding). That is, no processing, even prohibitively complex, can recover the watermark information from the attacked data. This category includes denoising, quantization (e.g., for compression), remodulation, and collusion attacks. Not all of these methods always come close *to* their goal of complete watermark removal, but they may nevertheless damage the watermark information significantly.

3.4 Geometric Attacks

Geometric attacks do not actually remove the embedded watermark itself, but intend to distort the watermark detector synchronization with the embedded information. The detector could recover the embedded watermark information when perfect synchronization is regained. However, the complexity of the required synchronization process might be too great to be practical.

3.4 Cryptographic Attacks

Cryptographic attacks aim at cracking the security methods in watermarking schemes and thus finding a way to remove the embedded watermark information or to embed misleading watermarks.

3.5 Protocol Attacks

Protocol attack aim at attacking the entire concept of the watermarking application. One type of protocol attack is based on the concept of invertible watermarks. The idea behind inversion is that the attacker subtracts his own watermark from the watermarked data and claims to be the owner of the watermarked data. This can create ambiguity with respect to the true ownership of the data. Another protocol attack is the copy attack. In this case, the goal **is** not to destroy the watermark or impair its detection, but to estimate a watermark from watermarked data and copy it to some other data, called target data The copy attack is applicable when a valid watermark in the target data can be produced with neither algorithmic knowledge of the watermarking technology nor knowledge of the watermarking key. Again, signal-dependent watermarks might be resistant to the copy attack.

4. APPLICATIONS

Digital Watermarks are potentially useful in many applications including:

4.1 Ownership Assertion

Watermarks can be used for ownership assertion. In this context the creator of a work (e.g. a song, a picture, a movie or an object) wishes to prove that he is the only legitimate owner of the work. To do so, a watermark identifying him unambiguously is embedded in the work. for this kind of application, it is necessary to use a watermarking algorithm that assures inevitability or non-quasi inevitability of the watermark. A common way to confer a legal value to the verification procedure through watermark detection is to introduce the presence of a Trusted Third Party (TTP) that assigns a unique registration code to the owner of the work in order to proof the ownership of the registered asset without ambiguity.

4.2 Fingerprinting

In applications where multimedia content is electronically distributed over a network, the content owner would like to discourage unauthorized duplication and distribution by embedding a distinct watermark (or a fingerprint) in each copy of the data. If, at a later point in time, unauthorized copies of the data are found, then the origin of the copy can be determined by retrieving the fingerprint. In this application the watermark needs to be invisible and must also be invulnerable to deliberate attempts to forge, remove or invalidate. Furthermore, and unlike the ownership assertion application, the watermark should be resistant to collusion. That is, a group of k users with the same image but containing different finger prints, should not be able to collude and invalidate any fingerprint or create a copy without any fingerprint.

4.3 Copy Control

Watermarks can also be used for copy prevention and control. For example, in a closed system where the multimedia content needs special hardware for copying and/or viewing, a digital watermark can be inserted indicating the number of copies that are permitted. Every time a copy is made the watermark can be modified by the hardware and after a point the hardware would not create further copies of the data. An example of such a system is the Digital Versatile Disc (DVD). In fact, a copy protection mechanism that includes digital watermarking at its core is currently being considered for standardization and second generation DVD players may well include the ability to read watermarks and act based on their presence or absence.

4.4 Fraud and Tamper Detection

When multimedia content is used for legal purposes, medical applications, news reporting, and commercial transactions, it is important to ensure that the content was originated from a specific source and that it had not been changed, manipulated. This can be achieved by embedding a watermark in the data. Subsequently, when the photo is checked, the watermark is extracted using a unique key associated with the source, and the integrity of the data is verified through the integrity of the extracted watermark. The watermark can also include information from the original image that can aid in undoing any modification and recovering the original. Clearly a watermark used for authentication purposes should not affect the quality of an image and should be resistant to forgeries. Robustness is not critical as removal of the watermark renders the content inauthentic and hence of no value.

4.5 ID Card Security

Information in a passport or ID (e.g., passport number, person’s name, etc.) can also be included in the person’s photo that appears on the ID. By extracting the embedded information and comparing it to the written text, the ID card can be verified. The inclusion of the watermark provides an additional level of security in this application. For example, if the ID card is stolen and the picture is replaced by a forged copy, the failure in extracting the watermark will invalidate the ID card. The above represent a few example applications where digital watermarks could potentially be of use. In addition there are many other applications in rights management and protection like tracking use of content, binding content to specific players, automatic billing for viewing content, broadcast monitoring etc. From the variety of potential applications exemplified above it is clear that a digital watermarking technique needs to satisfy a number of requirements. Since the specific requirements vary with the application, watermarking techniques need to be designed within the context of the entire system in which they are to be employed. Each application imposes different requirements and would require different types of invisible or visible watermarking schemes or a combination there of.

4.6 Invisible Marking on Paper

Digital watermarks can also be adapted to mark white paper with the goal of authenticating the originator, verify the authenticity of the document content, or to date the document. Such applications are especially of interest for official documents, such as contracts. For example, the digital watermark can be used to embed the name of the lawyer or important information such as key monetary amounts. In the event of a dispute, the digital watermark is then read allowing authentication of key information in the contract. Alp Vision developed genuine process to invisibly mark white blank paper with normal and visible ink. This patented technology is now known as Cryptoglyph.

4.7 Intellectual Property Right (IPR) Protection

The protection of Intellectual Property Right or IPR protection is the very first targeted application of digital watermarking. This term includes the protection of the rights of the creator, the rights of the legitimate owner, copyright protection, moral rights protection (e.g. the integrity of the work in the respect of the moral beliefs of the creator). Three of the major tasks in IPR protection area are: demonstration of the ownership in legal disputes, fingerprinting, and copy control. It is very tough to protect the piracy of digital contents. 3D models creation is costly as well as effort taking so protections of these models are very important and responsibility of government.

5. CONCLUSION

In this paper we presented an overview of digital watermarking application areas and possible watermark attacks. First we looked into watermarking and presented general watermarking system with watermarks and watermark security also described. We then discussed various watermark attacks includes basic attacks , legal attack , removal attack etc.Then we looked at the range of applications that could benefit from applying digital watermarking technology. Protection of intellectual property right is very important nowadays because digital multimedia content can be copied and distributed quickly, easily, inexpensively, and with high quality. Other applications, such as fingerprinting, Ownership assertion, copy control and fraud and tamper detection have also been identified.

6. REFERENCES

[1] Ton kalker. Considerations on watermarking Security. http://wireless.per.nl/watermarks/research/papers/documents/WIA_Invited_Kalker_Philips_SPIE.pdf

[2] Dilip Kumar Sharma, Vinay Kumar Pathak and G.P. Sahu . Digital watermarking for secure E-Government framework. Computer Society Of India, 182-191.

[3] http://www.ee.sunysb.edu/~cvl/ese558/s2005/Reports/Abhishek%20Goswami/WatermarksByAbhishekGoswami.pdf

[4] http://isis.poly.edu/~qiming/publications/mcam07-springer.pdf

[5] http://www.infosyssec.com/infosyssec/Steganography/watermarkingAttack.htm

[6] Collberg C., and Thomborson C., 2002. Watermarking, Tamper-proofing and Obfuscation- Tools for Software Protection In IEEE Transactions on Software Engineering, Vol. 28, No. 8, 735-746.

[7] http://www.cs.uga.edu/~sadiq/pdf/Watermarking%20%20Basics,%20Types%20and%20Attack%20Resistance%20%20Report.pdf

[8] J.Du, C.H. L and H.-K.Lee Y. Suh .BSS: A new approach to watermark attack. In Proceedings of the IEEE Fourth International Symposium on Multimedia Software Engineering (MSE’02).