Review Paper on Security Measures in Digital Watermarking

Lalita Verma
Assistant Professor, CSE, MIET
Gr. Noida, U.P.

Chandana Rathi
Assistant Professor, CSE, MIET
Gr. Noida, U.P.

Taranjeet Singh
Assistant Professor, CSE, MIET
Gr. Noida, U.P.

***Abstract*— Watermarking is the technique in which digital data is hidden in carrier signal. Steganography is the process in which digital data (file, message, video etc.) is embedded within another file, message and video. Steganography secures the information from intruders whereas watermarking algorithms are used for keeping the watermark robust to attack. When the intruder wants to penetrate the signal and tries to remove the watermark then quality of the signal is degraded and it becomes useless. There are many area in which information hiding is required. Two type of attacks are there. First one is active attack in which the attacker changes the whole content. Second one is passive attack in which the attacker tries to guess the secured information by eavesdropping. This paper presents different image data hiding attacks.**

***Keywords*— Attacks, Passive attacks, Steganography, Watermarking.**

I. INTRODUCTION

Watermarking is the process for the copyright protection of the digital images. There are various techniques for copyright protection in digital images. In digital image watermarking, the original image data is modified by embedding a watermark. This watermark contains key information such as authentication or copyright codes [1]. Digital watermarking technology is the process of embedding coded information called as watermark, tag or label into a multimedia object such as image, audio or video. This watermark can be detected or extracted later to authenticate and prove the ownership.

Watermarks vary greatly in their visibility; while some are obvious on casual inspection, others require some study to pick out. Various aids have been developed, such as *watermark fluid* that wets the paper without damaging it. A watermark is very useful in the examination of paper because it can be used for dating, identifying sizes, mill trademarks and locations, and determining the quality of a sheet of paper.

The word is also used for digital practices that share similarities with physical watermarks. In one case, overprint on computer-printed output may be used to identify output from an unlicensed trial version of a program. In another instance, identifying codes can be encoded as a digital watermark for a music, video, picture, or other file. [2]

In modern digital steganography, data is first encrypted or obfuscated in some other way and then inserted, using a special algorithm, into data that is part of a particular file format such as a JPEG image, audio or video file. The secret message can be embedded into ordinary data files in many different ways. One technique is to hide data in bits that represent the same color pixels repeated in a row in an image file. By applying the encrypted data to this redundant data in some inconspicuous way, the result will be an image file that appears identical to the original image but that has "noise" patterns of regular, unencrypted data.

The practice of adding a watermark -- a trademark or other identifying data hidden in multimedia or other content files -- is one common use of steganography. Watermarking is a technique often used by online publishers to identify the source of media files that have been found being shared without permission. The following table shows the comparison between Watermarking and Stagenography.

	Watermarking	Steganography
Robustness	Active attacks	Passive and Active attacks
Embedding Capacity	Low	High
Image Relationship	Exist	Does Not Exist
Imperceptibility	NotIimportant	Very Important
Message Encription	Not Important	Very Important

While there are many different uses of steganography, including embedding sensitive information into file types, one of the most common techniques is to embed a text file into an image file. When this is done, anyone viewing the image file should not be able to see a difference between the original image file and the encrypted file; this is accomplished by storing the message with less significant bites in the data file. This process can be completed manually or with the use of a steganography tool. [3]

II APPLICATIONS OF WATERMARKING

There are a range of application scenarios beyond that of content protection for which digital watermarks are also very suitable, particularly for situations where there exists no adversarial situation. Watermarking is not restricted to just retaining information of the author in the work, there are various other purposes for which watermarking may be incorporated into an object.

A. User Specific Requirement

Digital watermarks are particularly attractive for signals constituting a continuous stream such as audio or video signals. In case, such signals are transmitted in analog from, recovery must be possible from the analog form, presumably at a minimum after the signal has been attenuated, distorted and transformed in the process of transmission and reproduction. Particularly, in the case of analog video signals with their high bandwidth requirements, the recovery must then either be possible given only a very limited high fidelity recording of the original signal, or from a significantly lower bandwidth recording at a later stage. The former requirement can be further refined into real-time recovery requirements; in this case the watermark must be recovered given a signal passage with a duration delimited by a fixed upper time bound and given a fixed upper bound for the time permitted to recover the watermark after the signal excerpt has been available. For digitally transmitted signals, it must not be possible to detect (and therefore delete) the marking without an appropriately parameterized detector from either the encoded or the base band (decoded) signal and must be robust against digital-to-analog conversions. Since most multimedia signals transmitted digitally are encoded using a compression scheme and have only a fixed bandwidth available, an additional requirement levied on digital watermarks may be that the watermark does not increase the bandwidth required for the marked signal beyond the available bandwidth for a given signal. [4]

B. Copyright Protection

For the protection of intellectual property the data owner can embed a watermark (representing the copyright information) imperceptibly in his data. There has always been a problem in establishing the identity of the owner of an object. In case of a dispute, identity was established by extracting the watermark.[5]

C. Annotation Watermarking

Annotation watermarking is a technique that allows to associate content descriptions with digital images in a persistent and format independent manner. It is commonly used in medical applications and, hence, existing schemes have been designed to meet rigorous watermark transparency requirements. As a result, the effective capacity of such schemes is severely limited.

D. Fingerprinting

A fingerprinting is a technique by which a work can be assigned a unique identification by storing some digital information in it

in the form of watermark. Detecting the watermark from any illegal copy can lead to the identification of the person who has leaked the original content. [6]

E. Multimedia Authentication

Multimedia signal can be easily reproduced and manipulated. Although we cannot perceive the change, what we are seeing or listening to may have been changed maliciously for whatever reasons. Multimedia authentication is to confirm the genuineness or truth of the structure and/or content of multimedia. Multimedia authentication answers the following questions: (1) is the multimedia signal from its alleged source? (2) has it been changed in any way? (3) where and to what degree has it been changed if changed? There are mainly two approaches that can answer these questions. The first approach to multimedia authentication is cryptograph; while the second approach is the digital watermarking. In addition, cryptograph can be integrated into digital watermarking to provide more desirable authentication.

III TYPES OF ATTACKS

There are four types of attacks. In the first category the attacker knows nothing about the algorithms and does not possess a tool such as a watermark detector. Thus they may use different distortions such as compression, noise filters and geometrical and temporal distortions. In the second type, the attacker has more than one watermarked work. This enables the adversary to remove watermarks even without knowing about the algorithms. The third group of attackers is assumed to know the algorithms. This stems from Kerckhoffs' principle in cryptography that states the adversary knows everything about the algorithms except one or more secret keys. So, the attacker can exploit the vulnerabilities in detection process and launch attacks such as masking attacks. The last assumption about the attacker considers having a detector (the attacker may not have any knowledge about the algorithm). The detector makes it possible for the attacker to test different modified works and gain good knowledge about the operation of the detection algorithm. This may result in various types of attacks such as oracle attacks. Furthermore, some attacks may be specific to particular applications of digital watermarking as well as having different motivations. Thus the classification of attacks may vary regarding different perspectives and reasons. [10]

A. Message Removal Attack

The message is removed partially or completely from the carrier without the need of the security key. After the attack, any hiding algorithm will not be able to extract the watermark. There are many categories of attacks for removing the message. They can be broadly classified to denoising, quantization, collusion and remodulation attack. In denoising attack, the objective is to keep the quality of the message carrier while trying to remove the message. In the denoising processes, the carrier image is considered a signal and the watermark, or the message is considered a noise. The objective is to remove or reduce the noise. In quantization attack, for example the quantization step in JPEG compression, the attacker objective is to restore the original quantization table of JPEG compressed carrier image. JPEG compression starts with converting the color system of the image from any color system such as RGB to YUV [5].

B. Ambiguity Attack

This attack sometimes called IBM attack or Craver attack and it aims to puzzle the detector by generating fake watermark from a watermarked work. Thus, it leads to ambiguity in the ownership of the media content. The vulnerability that enables this kind of attack is related to the concept of being invertible in the watermarking system. In fact, being non-invertible (i.e. the inverse of embedding is computationally implausible) regarded as one of the preferred requirements that a watermarking scheme should possess. A possible countermeasure is to make watermarks signaldependent by using cryptographic hash functions.

C. De-synchronization attack

By misaligning the watermark and the detector, this attack is aimed at performing the detection of watermark tough. Several defence approaches have been proposed in the literature: Audio watermarking de-synchronization-resistant schemes: A robust audio watermarking scheme against time domain modification attacks introduced in [6]. This scheme applied an adaptive receiver providing exact estimation of the quantization step required defending against time scale modification attacks. Hong Peng et al. [7] offered an adaptive audio watermarking scheme based on kernel fuzzy c-means (KFCM) clustering algorithm. The original audio frame is segmented into audio frames, which further divided into subframes. Subsequently, a synchronization code is embedded into first sub-frame of each audio frame.

as well as concealing the watermark signal into DWT coefficients of second sub-frame of each audio frame employing an energy quantization method. Another novel algorithm incorporated wavelet moment and synchronization code to procure suitable auditory quality and resistance against de-synchronization attacks [11].

D. System Attack

Unlike unauthorized action-specific attacks, which exploit the vulnerabilities of watermarks, system attacks take advantage of the flaws in the ways that watermarks are employed (e.g. removal of a watermark detector chip in a device). These attacks should be taken into account when developing a system that utilizes watermarks. Scrambling attacks fall into this group of attacks. As the name implies, this attack involves scrambling of the samples of a watermarked digital media (e.g. pixel permutation in an image) in advance of presentation to a watermark detector. Then, subsequently the pieces will be descrambled. It should be noted that the scrambling must be invertible (or nearly invertible). A type of scrambling attacks called mosaic attack segments an image to sub-images to circumvent a web-crawling detector. The adversary can take advantage of the fact that most web browsers are able to correctly descramble the image. There are multiple types for mosaic attacks which have been classified based on the granularity level of the content segments. For instance, coarse mosaic attack [9] usually utilizes large portions of content such as movie or audio files. Through segregating multimedia files into the segments with specific length, this kind of attack is able to neutralize trusted source enforcement on discrete segments. To thwart coarse mosaic attack, it is necessary for multimedia equipment to save the history of content usage and refer to it for each new content service. The content usage some state of the art techniques to counteract these attacks were reviewed regarding the existing literature. Fortunately, for many known attacks, there are appropriate countermeasures; however, typical of the athistory keeps the track of any watermark extraction and its relevant information. By means of this technique, the estimation of enforcement condition can be accomplished with regard to the history and the extracted information for each item.

IV CONCLUSION

This paper presents a general view of attacks against the security of the digital watermarking schemes. Apart from this, tackers' behaviour, new attacks are expected to emerge. Moreover, the rapid growth of digital multimedia usage has resulted in serious concerns about the copy control and intellectual property protection. Thus, the goal is to make watermarking systems as secure as possible as well as maintaining the robustness of the watermarking schemes. Designing specific techniques and algorithms may help to accomplish this goal.

V REFERENCES

[1] Mr. Manjunatha Prasad. R, Dr.Shivaprakash Koliwad "A Comprehensive Survey of Contemporary Researches in Watermarking for Copyright Protection of Digital Images", International Journal of Computer Science and Network Security (IJCSNS), Vol.9 No.4, April 2009, pp.91-102.

[2] https://en.wikipedia.org/wiki/Online

[3] https://searchsecurity.techtarget.com/definition/Online

[4] M.S.Kankanhalli and K.F.Hau, "Watermarking of electronic text documents", Electronic Commerce Research, Vol.2, No.12, pp.169-187, 2002.

[5] Me Liehua and G.R.Arce, "A class of authentication digital watermarks for secure multimedia communication", Image Processing, IEEE Transactions, Vol.10, No.11, pp.1754-1764, 2001.

[6] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography, Second Edi., Burlington: Morgan Kaufmann, 2008, pp. 425-467.

[7] Hosam, O. (2013). Side-informed image watermarking scheme based on dither modulation in the frequency domain. The Open Signal Processing Journal, 5(1), 1-6.

[8] N. Cvejic and T. Seppanen, "Improved resistance against time desynchronization attacks in multibit audiowatermarking," Signal Processing and Its Applications, 2007. ISSPA 2007. 9th International Symposium on. pp. 1-4, 2007.

[9] W. J. Z. Z. Peng H., "Audio watermarking scheme robust against desynchronization attacks based on kernel clustering," Multimedia Tools and Applications, pp. 1-19, 2011.

[10] W. X.-Y. L. M.-Y. Niu P.-P., "A new digital audio watermaking scheme robust to desynchroniaztion attacks," in Proceedings - 5th International Conference on Frontier of Computer Science and Technology, FCST 2010, 2010, pp. 233-238.

[11] W. J. Z. J. Petrovic R., "Watermark screening in networked environment," in 2011 10th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services, TELSIKS 2011 - Proceedings of Papers, 2011, pp. 53-60.