IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.7, Special Issue.1, Jan 2019 E-ISSN: 2347-2693

# Protection of Digital Media using Digital Watermarking

**S. Sarbavidya[1*]**

[1*]Department of Computer Science, The University of Burdwan, Burdwan, West Bengal, India

[*]*Corresponding Author: sirsendusarbavidya@gmail.com, Tel.: +91-96475-41312*

**Available online at: www.ijcseonline.org**

***Abstract*—** In the present era of Internet, all sorts of digital media (text, audio, video and multimedia) is freely and easily available to everyone over Internet. Anyone can easily access those digital media without taking any sorts of permissions from the owner of the digital media, distribute the digital media freely to others and claim the ownership of the digital media and sometimes make unnecessary changes to the digital media itself. So, the need of the time is to protect the digital media from unauthorized access, restrict free distribution of digital media to others and also to establish the ownership of the digital media in an easy, consistent and efficient manner. In this paper, several approaches using digital watermarking method are proposed, which embeds ownership information and copy protection mechanism within the digital media, to provide a powerful mechanism for protecting digital media in efficient and convenient manner.

***Keywords*—**Digital Media, Digital Watermarking, Security, Privacy, Ownership, Authentication, Protection.

## I. INTRODUCTION

This is an era of Internet. Almost everything is available online in digitized form. With the advancement of cheap distribution process and the increased speed of file transfer, illegal copies of digital media (text, audio, video, multimedia) is available at a very low cost. Anyone can freely make a duplicate copy of the digital media [1] and claims the ownership of the media. Apart from duplicating the digital media freely, a traitor can tamper the original media very easily and make unnecessary changes to the media to make it unusable. Digital media that are available online can need to be protected against all sorts of copyright infringement attacks [2], regeneration of digital media without permission [3] and tampering of documents [1], so that the original owner can claim the ownership of Intellectual Property (IP) and if needed take legal actions on the traitors based on ownership information. Digital watermarking [2] is helpful in establishing the ownership details of the digital media and also to control regeneration of illegal copies of the original digital media. In digital watermarking approach some invisible [4], integrated patterns (watermarks) are inserted within the digital media to establish ownership information and to restrict anyone from freely make illegal copies of the digital media and also to restrict them to tamper the original digital media. Most digital watermarking approaches are application specific and control only specific kind of attacks.

Section II of this paper gives a brief idea about the different kinds of security attacks on digital media. Section III describes history of watermarking techniques. In Section IV, the technology of digital watermarking is specified. Section V highlights different measurement approaches of digital watermarking to counter security threats on digital media. Section VI concludes research work with future directions.

## II. SECURITY ATTACKS ON DIGITAL MEDIA

In the modern days, advancement of digital multimedia processing tools helps to reproduce duplicate copies of digital media very easily [2] and at very low cost. There are several security aspects of digital media that needs to be addressed to protect it from unauthorized usage [5]. Following section identifies some of the major security issues of digital media.

- Attacks on copyright – anyone can claim himself as the owner of the digital media as the media is freely distributed over Internet without any authenticity [1] information available within the digital media.
- Attacks using signature – anyone can freely and easily add his identity (digital signature or fingerprint) within the digital media and claim the ownership [1] of the media by superseding [6] the original owner of the digital media.

 

- Attacks using regeneration of digital media – regeneration of digital media is very easy and cheap due to modern technological advancements. Anyone can make illegal copies [3] of the digital media and distribute them without taking permission from legitimate owner [7] of the media.

- Attacks via tampering – anyone can freely access the digital media and tamper the contents of the media to make it unusable [2] for future or change the very meaning of the document.

- Attacks of traitors – sometimes a traitor can access the copy the digital media which is actually not meant for him. There is no method to check the authenticity of the intended recipient [3] of digital media.

To overcome these kinds of attack on digital media, there are several approaches (cryptography, steganography, digital watermarking) [1, 4] available. But among all the approaches available, digital watermarking provides much better security on different kind of attacks. So in this paper, digital watermarking method is used to provide security on digital media.

## III. HISTORY OF WATERMARKING

Digital watermarking is a technique to insert some information into the content and hide them within the content, so that we can use the hidden information to identify the owner of the media and also used it to authenticate the available content within the media. The term watermark came from the German term *wassermarke* [7], which denotes the effect of water on paper.

In Italy, in the year 1282, a watermark was found in a paper [8], which is claimed as oldest watermark found till date. In earlier days, watermark is used to identify ownership within the papermaking industry [7]. In earlier days in France, watermark information available within a letter helps to solve a legal matter at court [3, 5]. William Congreve and William Henry Smith, two Englishmen, invented different techniques for paper watermarking [1, 4]. Paper watermarks are extensively used in bank notes and stamps nowadays.

Muzak Corporation designed first watermark for voice data in the year 1954 [2]. In 1979, a watermark method was developed for anti-counterfeiting. In the year 1986, watermarking for audio signal begins [8].

The term digital watermarking [8] was first used during late 80's and on that time it was similar to paper watermarking in every respect. In the year 1988, Komatsu and Tominga, first coined the term *digital watermark* [8] in their works. From 1995, digital watermarking has attracted a lot of attention from researchers as well as from digital media industries. The growth of digital watermarking is very fast due to its enormous application advantages. First global acceptance of digital watermarking happens on 1996, when Information Hiding Workshop (IHW) [7, 8] includes one of its sessions in the name of digital watermarking approach [6].

## IV. THE TECHNOLOGY OF DIGITAL WATERMARKING

In Digital watermarking approach, some digital information (watermark) is inserted into the content and hides them such a way within the content so that this hidden information is capable enough to identify the ownership of the document and authenticate the contents of the document. Digital watermarking is a way to protect ownership property from illegal usage. A watermark always resides permanently within the host information. No one can separately identify the existence of hidden watermark [9] within the original work and the work is still accessible. If the hidden watermark is tampered in adversely, then the original information will be inaccessible [8].

Using any specific method (watermark insertion algorithm), information (watermark) can be hidden within the original document (cover media) and after the hiding process is over, the document will be slightly modified (watermarked media) but still accessible for use. The watermarked media is then transmitted to the receiver via insecure communication medium and after transmission, the authenticity of the watermarked media is verified at the receiving end and ownership information is judged with the help of another process (watermark extraction algorithm). The watermark information is fully depends on the application type [7].

Watermark embedding and detection can sometimes be considered analogous to encryption and decryption in cryptography [2]. Using cryptography along with watermarking applications, two different approaches of watermarking - Secret-key approach and Public-key approach [3] will be produced.

Secret-key watermarking approach uses an embedding function and a message (original work) at the sending end and produces a watermarked work. On the other hand at the receiver end, a detection function is used which converts the watermarked work into original work. A watermark key is used to control the mapping between original work and watermarked work. The advantage of secret-key watermarking is that no one except the legitimate key holder can access and recover the work.

 

In this approach of secret-key watermarking, same secret key is used in both sides of the communication medium. Public-key watermarking algorithms have been proposed a system which consists of two types of keys: a public and a private one. Content can be watermarked using the private key, whereas the public key is used to verify the mark [1, 9].

In the sender end watermark embedding is done, which takes watermark information, a key (secret) and the original work. The key used here to help us to provide extra level of security and restricts unauthorized access of content. The outcome of the process is the watermarked document.

In the receiving end watermark detection takes place, which accepts watermarked document and a key (the same secret key which is used in the sender end for watermark embedding) and generates a signal [6] indicating the privacy and authenticity information of the original document and identifies the genuine owner.

## V. DIGITAL WATERMARKING APPLICATIONS FOR PROTECTION OF DIGITAL MEDIA

The watermarking approach that is used to comply any kind of security threats are always depends on the application specific area of the digital media. There is no global watermarking method available which suits all types of applications and attacks. A digital watermarking application is relatively effective if the watermark is robust enough against attacks and the ratio between the host signal and watermark is relatively low. In the following area, various applications of digital watermarking are mentioned that can be used to protect the digital media from different kinds of attacks mentioned in section II.

- Copyright Protection – one of the vital roles of digital watermarking is to establish ownership [1] of the digital media and identify Intellectual Property rights of the legitimate digital media owner. Here, the owner integrates a watermark containing his own identity information into the original digital media, hides the watermark within the content and distribute it to the receiver as usual. The receiver can never know the existence of the watermark within the digital media and can use them. The owner of the digital media can then proof his ownership, if needed, by extracting the hidden watermark from the distributed digital media.
- Data Authentication – using digital watermarking, anyone can prove the authenticity of a digital media. The owner of the digital media can inserts a watermark into the media and if anyone wants to destroy or change the content of the media, then the watermark will get changed [5]. So, if the watermark is extracted with erroneous information [2] then it can be proved that someone has changed the content of the digital media and it is not that one which actually distributed.
- Copy Protection – nowadays pay-per-view concept of digital media is highly available [3, 8] where the user is paying for the digital media and the owner of the media is supplying the media to that genuine user. But after getting the media from the owner, the user can easily reproduce multiple copies of the media and distribute them without taking consent from the legitimate owner. The digital media along with the inserted watermark and recording device can enables or disables the action of recording and protect the generation of illegal copies of the digital media.
- Fingerprinting – the digital media is sometimes individually marked with the fingerprint of the genuine buyer [2, 7]. The owner of the digital media can add two different watermarks into the media, one watermark of his own and another watermark of that buyer to whom the media is actually meant for. In this combination, it is very easy to identify those who make illegal copies of the digital media and distribute them.
- Broadcast Monitoring – to secure intellectual property rights of broadcasting agencies [1, 9] and restrict illegal usage of broadcasted information, digital watermark is added with the broadcasted material. This digital watermark is robust enough to different kinds of attacks and can automatically monitors streams of broadcast at satellite nodes all over the world to identify illegal usage of the broadcasting information. If any kind of malpractice is noticed, the system can terminate that node from receiving the feed of the broadcast and also delete the previously received content from that node and block the feed of the node forever.

Though digital watermarking provides various kinds of protection from attacks on digital media, it is still behave differently in different attacks.

## VI. CONCLUSION AND FUTURE SCOPE

Nowadays digital media is the need of the time. Everything is available in digital forms. With the growth of Internet and wide applications of it, digital media is easily available to everyone. Some sorts of protection on this digital media are needed and for that reason digital watermarking approach is used to protect the media from misuse. Though digital watermarking are used effectively to protect digital media from various attacks, most digital watermarking methods are

 

application specific [3, 4, 5] and lacks the main approach of intellectual property rights problems.

Protection of digital media using digital watermarking method is an attractive area of research [5, 8, 9] which needs innovative methods and approaches to counter the attacks. There is a possibility that in near future digital watermarking approach will not only get attention from big corporates but from common public also. There is a ray of hope that in future days, attacks on digital media will be possible to restrict using digital watermarking.

## REFERENCES


[1] Dhaked D., Yadav S., Mathuria M., Agrawal S., "User Identification over Digital Social Network using Fingerprint Authentication", Emerging Trends in Expert Applications and Security, pp 11-22, Advances in Intelligent Systems and Computing, Vol 841, Springer, **Singapore** (978-981-13-2284-6).

[2] F. Lynda-de-jason, Nitya M., "A Protocol for preventing insider attacks in untrusted infrastructure-as-a-service clouds", International Journal for Research in Science Engineering and Technology (2394 739x), pp 1-6.

[3] J. C. Ingemar, L. M. Matthew, A. B. Jeffrey, J. Fridrich, T. Kalker, "*Digital Watermarking and Steganography (2nd edition)*", Morgan Kaufmann Publishers, **USA**, 2008.

[4] Rathi V.O., Patil P.S., "Invertible message Hiding using Histogram Modification by LabView: A New Approach", International Journal of Applied Research, Vol 7, Issue 1, Jan 2017 (2249 555X).

[5] Indoviya A., Sharma O.P., "A chronological Review in Digital Watermarking", International Journal of Applied Engineering Research (0973 4562), Vol 13, No. 21 (2018), pp 15383-15385.

[6] B. Schneier, "*Applied Cryptography*", John Wiley & Sons, **New York, USA**, 2nd ed., 1996.

[7] Lin X., "Image Forgery Detection", Introductory Computer Forensics, Springer, **Cham** (978-3-030-00580-1), pp 507-555.

[8] J. Seitz, "*Digital Watermarking for Digital Media*", Information Science Publication, **Hershey**, 2005.

[9] Mondal S.N., "Control of Corruption in India: A Socio-Legal Challenge", International Journal of Advance Study and Research Work (2581 5997), Vol 1, Issue 5, August 2018.


## Authors Profile


**Sirsendu Sarbavidya** is a Research Scholar in Department of Computer Science, The University of Burdwan. He obtained his M.Sc. and M.Tech. degree from Calcutta University. Mr. Sarbavidya has several years of teaching experience in different reputed Govt. and Govt. Sponsored Institutions. The broad area of his research interest is in Information Security, Cryptography, Digital Watermarking and Image Processing. He has attended several National and International Conferences in recent years. He has published multiple research papers in reputed National and International Journals and proceedings in the area of his research interest.


 