DOI: http://dx.doi.org/10.26483/ijarcs.v8i8.4840

ISSN No. 0976-5697

Volume 8, No. 8, September-October 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

CLASSIFICATION OF POSSIBLE ATTACKS AND PREVENTION METHODS IN DIGITAL WATERMARKING

G. Jansirani
Research Scholar, Dept. of Computer Science
Tamil University, Thanjavur, Tamilnadu, India

A, Senthilkumar
Asst. Professor, Dept. of Computer Science,
Tamil University, Thanjavur, Tamilnadu, India

Abstract: Digital Watermarking is aimed for providing ownership rights protection in an untrustworthy environment like internet especially on images and videos. It is effective technique. However, the rate of successful digital watermarking fully depends on the robustness that is attacks or destroying of host data, although it is one of the famous techniques for copyright protection and identification. In order to maintain the robustness of digital watermarking numerous prevention methods should be applied for those watermarking techniques. Researches' are going on to prevent attacks in watermarked content and numerous procedures have been developed so far. As the same thing number of prevention methods needed to prevent attacks of digital watermarking. However, this paper is not present all the possible attacks for all the techniques of digital water marking. This paper shows some few possible attacks in digital water marking for colour images and an attempt to classify them by its categories.

Keywords: Digital watermarking attack, classification of watermarking attacks, Watermarking attacks

1. INTRODUCTION

Internet is an open source for digital information but ownership and managing is very challenging one. Nowadays, digital content available anywhere with or without permission [1]. Freedom has been taken by the hackers to obtain the copyrighted multimedia content through the web. So, protecting those multimedia assets is essential. What is the optimal channel to do this? Absolutely, digital watermarking is the best and easiest way to tackle this issue. To defend illegal copying, re-modification and distributing multimedia information digital watermarking is the best way. It is the way to embed ownership or other legal information into the content. In other words digital watermarking is the process of hiding or imposing data stream in an image or video that is imperceptible [2]. A bits pattern embedded into a digital picture, video file and audio file that represent the ownership or copyright details. So, the robustness of watermarking is evaluated by some attacks. Attacks may occur or may not occur. Researchers should check the watermarked content by do some possible attacks. Algorithms for watermarking is far better also the attackers. Watermarked multimedia content not only damaged by the malicious users in the internet. It may be damaged from the noise of the network. Attacks and noise disturb is unavoidable in the digital watermarking domain. Make it harder for the intruders. Think about that if the intruding is hacking is a very toughest job in digital water marking, malicious users may suffer or malicious attacks may reduce, therefore, no surety that the host content received by the destination is not same as the original. In the destination, user should compare weather it is real or damaged. There are many applications existing in digital watermarking area. Copyright protection, Copy protection, Content authentication, Transaction tracking, broadcast monitoring etc [11]. Attack principles should be applied in various circumstances under digital watermarking is best way to overcome this issue. A well watermarking algorithm should be satisfied by means of digital watermarking properties like imperceptibility and robustness[10]. And this paper summarizes several possible attacks made by the intruders or hackers and distorting of data in some uncertainty network conditions. And the subsequent sections show the taxonomy of the attacks, significant prevention methods of attacks and briefly classifying the possible ways of distortions watermarked content.

2. TAXONOMY OF DIGITAL WATERMARKING ATTACKS

Digital watermarking is evaluated by two ways. One is its self resistance and processing of signals. Another one is visual appearance of the content. Here Fig1 shows the possible intrusion and distortion in digital watermarking.

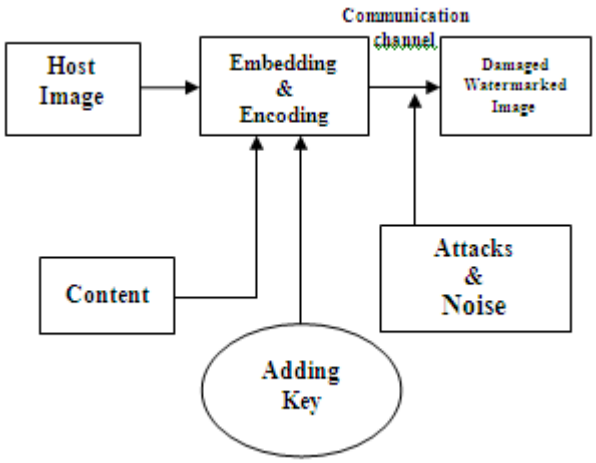

Figure 1

Noise is a type of attack and the attacks may occur in the of way receiver edge along the network path[12]. A study from BSA report that shows the value of commercial unlicensed software worth is $ 58,754 million in the year 2011, a study by the social science research council credits software piracy

as the key to Adobe's $ 3.10 billion earnings in the year 2011, mostly pirated Photoshop application are installed in all the PC's today and 16,990 downloads are made at any time that results potential revenue loss per day for that company is $18,670,310 in US alone [3]. How it can be stopped? The answer is it cannot be stopped never and ever but we can make it harder by the ways of using digital watermarking. So, the main motto of this journal is furnishing security issues of digital watermarking to researchers and scholars providing appropriate solution.

A. Classification of attacks

The designer of the digital watermarking application has not the knowledge in all way of attacks and it is very difficult the digital watermark will survey no longer by attacks [12]. Unauthorized attacks have some classifications. Unlike unauthorized attacks the system attacks has less sub classification. Earlier watermarking attacks classified mainly into four categories Removal attack, Geometric attack, Cryptographic attack and protocol attack[8]. And some other authors classified the watermarking as intentional and non-intentional [4]. Non -intentional refers the attack that was made when the transmission of the media and intentional attack refers the attacks happen when embedding, detection and removal like in the unauthorized category.

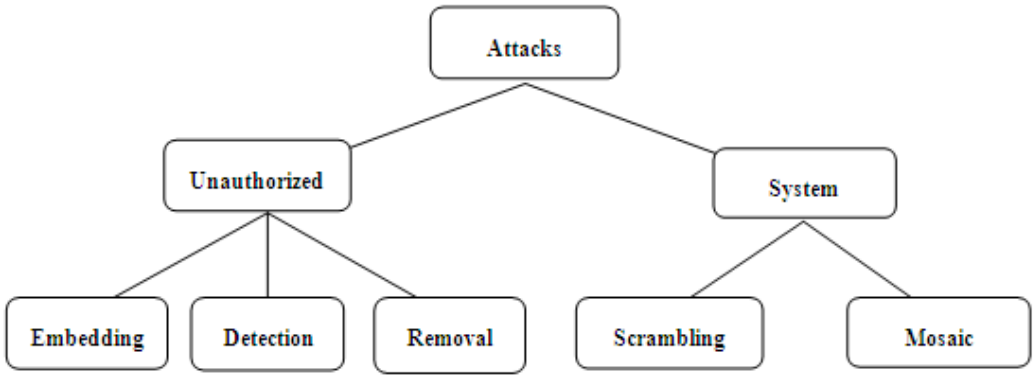

Figure 2

B. Unauthorized attacks

This type of attacking may happen on watermarking content hardly and this may call specific through the communication channels. Fig3 shows the typical classification of this category.

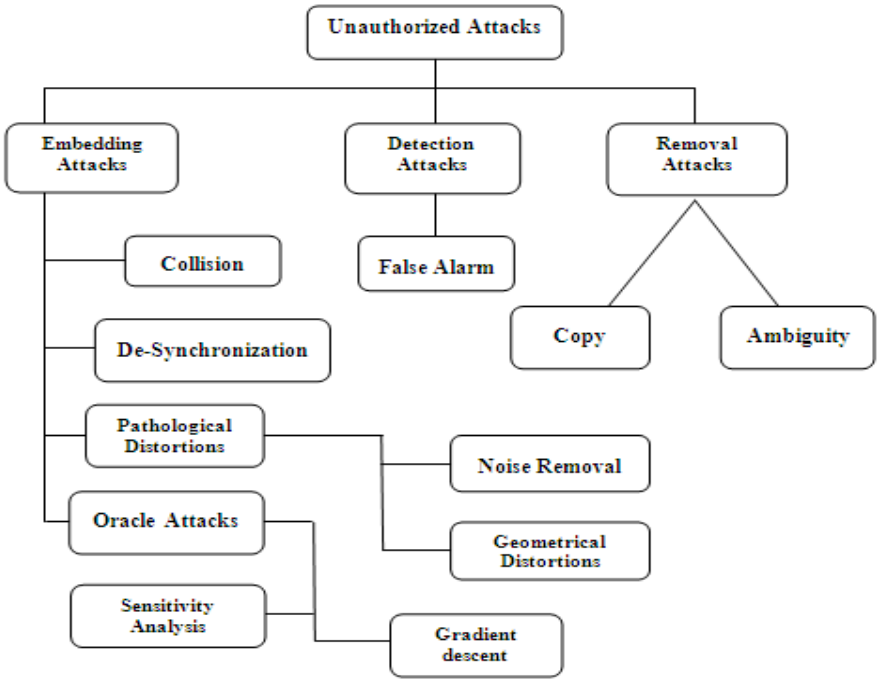

Figure 3

1. Embedding Attacks:

This type of attacks happen on embedding, that is content damaged in circumstances like collision, pathological distortions, Oracle attacks etc [3]. Collisions attacks are very harmful, in this manner hacker may try to remove or simply damage the watermark. Sometimes it may call active attack. This may cause serious trouble in finger print and other watermarking application. The de-synchronization is to

identify the synchronization patterns and deliberately remove them. The pathological distortions, which is noise removal and geometrical distortion. Geometrical distortions actually not remove the watermark but distort the watermarked content geometrically[4]. However, recent techniques help watermarks to protect from these types of attacks. Synchronization can be used for correcting this attack like skewing, rotation, scaling and translation[12]. However, this process quite expensive and time consuming. Noise may disturb the quality of watermarked content by communication channel. Image filtering techniques like Gaussian and median filtering may used to recover from such attacks[9]. And the oracle attack classified the sensitivity and gradient descent attacks. Sometimes it may call cryptographic attacks. This attack occur security of watermarked image. To protect from the gradient descent attack of a digital watermark, the countermeasure is to re-modify the authentication of algorithm used. And the resilient watermarking scheme for sensitivity analysis.

2. Detection Attacks

This type attack is aimed for reduce the possibility of watermark detection[3]. Sometimes it may go impossible. Sometime this may call re-modulation attacks. Like zooming and shifting and temporal direction attacks causes the detection of watermarking harder. False alarm is the better solution for this type of attack.

3. Removal Attacks

This is the last sub category in unauthorized attacks may called protocol attacks. Copy and ambiguity is the two classifications in this area. In this manner the attacker trying to copy the watermark from one content to another content. Attacker aim is simple the target data only without knowledge of the ownership security and this type of attack another type of protocol attacks and may not destroy the watermark[1],[8]. Best solution for this type signal dependent processing is the resistant, by occupying semantic deficits in the watermark implementation and taking advantage[7]. This may leads ambiguity attacks which confuses the detecting method to extract the watermarked content. Attackers may create duplicate watermark to confuse the security which was provided by the embedder. This leads ambiguity which one is authoritative watermark?

3. COUNTERMEASURES AND PREVENTION METHODS

Nowadays numerous ways found to reduce attacks in digital watermarking. But everyone depending on some particular watermarking attacks. There is no common countermeasure. Attacks are unique and that needs different approach to prevent. Researchers often trying to prevent such harmful attacks. Min Wu and Bede Liu [5], on their paper proposed some countermeasures to avoid such vulnerable in digital watermarking. They analysis watermark using DCT with some attacks and suggest double watermarking and large block size for locally. S. S. Sudha and K. K. Rahini [6], attacks in security of digital watermarking, they suggest applying effective cryptography method. In their paper they proposed AES algorithm for DCT watermarking security. Martin Kuttera and Sviatoslav Voloshynovskiya,b and Alexander Herrigel[7], describes the copy attack model and prediction methods for digital watermarking. Andreja Samcovic and Jan Turan [8], elaborates the attacks on digital wavelet watermarks for images. They conclude digital watermarking schemes are vulnerable and it needs more efficient and better watermarking techniques.

4. CONCLUSION

Thus the study ends and concludes attacks and countermeasures in digital watermarking arena. Nowadays, there are numerous attacks and numerous techniques are proposed by researchers. But the war is never ending between the attackers and researchers. No common solution existing or found yet for all the attacks in digital watermarking. Due to the heterogeneity of attacks, each of them needs different approach. This paper shows and elaborated various attacks in digital watermarking. In order to full fill the characteristics of digital watermarking, it is essential to find some new methods to avoid such attacks. Same time researchers should consider in all the possible angle of attacks. Although it is not as easy as we think and this process needs more time dedication due its complexity. Researchers must think in the vision of attacker's then only they found feasible counter measures. If the digital watermarking will survive longer it might adopts effective counter measures.

REFERENCE

[1] K. F. Tsang, O. C. Au, A Review on Attacks, Problems and Weaknesses of Digital Watermarking and the Pixel Reallocation Attack, Department of Electrical and Electronic Engineering, The Hong Kong University of Science and Technology, Clear Water Bay, Hong Kong

[2] Sviatolsav Voloshynovskiy, Shelby Pereira, and Thierry Pun, University of Geneva Joachim 1. Eggers and Jonathan K. Su, University of Erlangen-Nuremberg, Attacks on Digital Watermarks:Classification, Estimation-Based, Attacks, and Benchmarks, IEEE Communications Magazine August 2001.

[3] Maryam Tanha, S. Dawood Sajjadi, Mohd. TaufikAbdullah and Fazirulhisyam Hashim, an overview of attacks against digital watermarking and their respective countermeasures, The International Conference on Cyber Security, Cyber Warfare and Digital Forensics CyberSec 2012, Kuala Lumpur, Malaysia

[4] Abhishek Goswami, Graduate Student, Department of Electrical and Computer Engineering, Stony Brook, introduction to digital watermarks and classification of attacks, ESE558 DIGITAL IMAGE PROCESSING

[5] Min Wu and Bede Liu, ATTACKS ON DIGITAL WATERMARKS, Electrical Engineering Department, , Princeton University, Princeton, NJ 08544

[6] S. S. Sudha and K. K. Rahini, PREVENTION OF WATERMARKING ATTACKS USING CRYPTOGRAPHY METHOD, International Journal of Advanced Research in Computer and Communication Engineering ,Vol. 3, Issue 2, February 2014

[7] Martin Kuttera and Sviatoslav Voloshynovskiya,b and Alexander Herrigel, The Watermark Copy Attack, Proceedings of SPIE: Security and Watermarking of Multimedia Content II, Vol. 3971, January 2000

[8] Andreja Samcovic and Jan Turan, ATTACKS ON DIGITALWAVELET IMAGEWATERMARKS, Journal of ELECTRICAL ENGINEERING, VOL. 59, NO. 3, 2008, 131–138

[9] P.RAMANA REDDY, Munaga .V.N.K.PRASAD, D. SREENIVASA RAO, Robust Digital Watermarking of Color

Images under Noise attacks, International Journal of Recent Trends in Engineering, Vol 1, No. 1, May 2009

[10] Dr. Sanyam Agarwal, Priyanka, Usha Pal, Different Types of Attack in Image Watermarking including 2D, 3D Images, International Journal of Scientific & Engineering Research, Volume 6, Issue 1, January-2015.

[11] Prabhishek Singh, R S Chadha, A Survey of Digital Watermarking Techniques, Applications and Attacks, International Journal of Engineering and Innovative Technology (IJEIT), Volume 2, Issue 9, March 2013

[12] Prabhishek Singh, Aayush Agarwal and Jyoti Gupta, Image Watermark Attacks: Classification & Implementation, IJECT Vol. 4, Issue 2, April - June 2013.

[13] Mr.Mitesh Patel, Ms swati and Mr.Alpesh Chauhan, The study of various attacks on Digital watermarking technique, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3 Issue 5, May 2014