An Overview of Attacks against Digital Watermarking and their Respective Countermeasures

Maryam Tanha
Computer & Communication Systems Engineering Dept.,
Universiti Putra Malaysia,
Serdang, Malaysia.
maryam.tanha@ieee.org

Seyed Dawood Sajjadi Torshizi
Computer & Communication Systems Engineering Dept.,
Universiti Putra Malaysia,
Serdang, Malaysia.
dawood.sajjadi@ieee.org

Mohd Taufik Abdullah
Computer Science Dept.,
Faculty of Computer Science,
Universiti Putra Malaysia,
Serdang, Malaysia.
mtaufik@fsktm.upm.edu.my

Fazirulhisyam Hashim
Computer & Communication Systems Engineering Dept.,
Universiti Putra Malaysia,
Serdang, Malaysia.
fazirul@eng.upm.edu.my

***Abstract*— The increased and widespread usage of digital multimedia has aroused great concerns regarding issues such as copyright protection, copy control and proof of ownership. Digital watermarking serves as a solution to these kinds of problems; however, digital watermarking techniques have demonstrated to possess vulnerabilities. Thus opening avenues for malicious attackers to abuse these security breaches. Therefore, maintaining the security of digital watermarked media i.e. text, image, audio and video has received considerable attention. This paper has conducted a comprehensive research with special emphasis on the classification of malicious attacks against digital watermarking. Subsequently, it reviews the current countermeasures available to mitigate the intentional attacks. In addition, it procures a foundation for the evaluation of various watermarking algorithms.**

Keywords*— *watermarking; attacks; countermeasures; security; robustness; detector

I. Introduction

Thanks to the surge of using multimedia information in digital format, issues such as copyright protection, copy control and proving the ownership of digital content have gained public attention particularly among authors, content owners and distributers. Therefore, digital watermarking plays an important role to address these concerns. Digital watermarking involves the embedding of information, called a watermark, into a multimedia object (also called original content or host signal) in a way that the watermark can be detected or extracted later without damaging the host signal [1][2]. Digital watermarking system, in its simplest form, composed of an embedder and a detector. The inputs of the embedder are the watermark and the host signal. The output of the embedder is the watermarked work. The detector is responsible for determining the presence of a watermark in a digital content and decoding it [3]. A simplified watermarking scheme has been illustrated in Fig. 1.

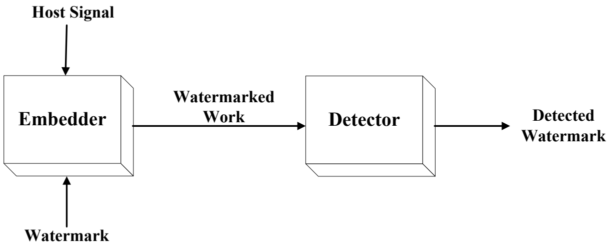

Figure 1. A simple digital watermarking scheme.

A. Digital Watermarking vs. Steganography and Cryptography

Although digital watermarking and steganography have overlap and share some technical aspects, it should be noted that the goals and definitions of the steganography and watermarking are relatively different. In fact, watermarking is considered as the practice of imperceptibly modifying media content i.e. text, image, audio and video to embed a message about that content whereas steganography involves the modification of media content in an undetectable way to embed a secret message [3][4]. So, with regard to the aforementioned definitions, in digital watermarking the embedded signal is not the key data to convey. In contrast, the concealed message is the most crucial part in the steganography [4]. Furthermore, unlike cryptography which provides the protection of the content during transmission without any additional examination of it after decryption, the watermark remains in the original content while not precluding a user from listening, inspecting, looking at or manipulating the content [2][3].

B. Security of Digital Watermarking System

As a common behavior, malicious attackers attempt to circumvent the watermarking techniques by taking advantage of their vulnerabilities. Therefore, maintaining the security of watermarking methods is of great significance. Authors in [3][4] differentiated between robust watermarks and secure watermarks. Robustness of a digital watermarking scheme is described as the survivability of the watermarking system during normal and legitimate processing while secure watermarks are devised to be resilient to deliberate tampering. In other words, robustness is a prerequisite but not thoroughly adequate for the security of a watermarking system i.e. if a watermark can be removed using normal processing such as lossy compression, format conversion and noise reduction, it is not regarded as secure. Adversaries aim at compromising either the robustness or security of watermarking techniques. In this research we have focused on the latter i.e. the security of watermarking techniques.

978-1-4673-1677-4

C. Contributions and Organization of the Paper

This paper is concerned with developing a detailed classification of intentional attacks against the security of watermarking systems and their respective countermeasures. The contributions of this research are considered as follows:

- Reviewing the literature and presenting a taxonomy of various types of malicious attacks that violate the security of digital watermarking techniques as well as their proposed countermeasures.
- Providing an appropriate base for assessing the robustness and security of watermarking algorithms.
- Furnishing scholars with information concerning the security issues of digital watermarking, thus encouraging them for conducting more research to enhance digital watermarking methods.

The rest of the paper is organized as follows. Section II reviews the related research work conducted on the classification of attacks against digital watermarking. Section III is concerned with providing a classification of attacks and their corresponding descriptions and countermeasures. Finally, Section IV concludes the paper.

II. BACKGROUND

There are several published work about classification of attacks against digital watermarking and their corresponding mitigation techniques. In [5], the technical problems and classes of attacks in IP (intellectual property) watermarking were described whereas in [6], some attacks which posed threat to IP watermarking schemes for VLSI (Very Large Scale Integrated circuits) design process were introduced. Research carried out in [4] encompassed a brief description of some related watermarking attacks without providing information about viable countermeasures. In [7], a more detailed classification of watermark attacks was presented with regard to the host signal including image, audio and video. In addition, the authors placed emphasis on the attacks which do not seriously affect the quality of watermarked content while not referring to the possible mitigation methods. Authors in [8], categorized the attacks considering various attack parameters such as mode of the attack (i.e. removal, estimation, writing and modification), the amount of information the attacker has at his/her disposal (e.g. partial, full etc.) and the degree of universality (i.e. whether the attack purpose is to eliminate a watermark from an individual object or to investigate the underlying secrets of the system under attack). A classification of attacks based on their impact on the watermark and how it is interpreted by the detector was presented in [9]. Both the former and the latter papers did not cover the defense mechanisms to thwart the attacks. A taxonomy of attacks against digital audio watermarks and their countermeasures with detailed description was proposed in [10]. Research in [11] focused attention on the knowledge available to an attacker about the watermarking algorithm to classify the attacks to fair (i.e. attacks which are just based on what is known) and unfair attacks (i.e. attacks which endeavor to find out the concealed parameters of the watermarking system). The authors offered a framework for watermarking security using the aforementioned concept of attacks. In [12], four categories of attacks namely, removal, geometric, cryptographic and protocol attacks were highlighted. These types of attacks intentionally made an attempt to damage the watermark without resulting in an inordinate distortion of attacked data; however the research lacks any mitigation mechanism for these sorts of attacks. Moreover, estimation-based attacks, which took advantage of estimating the original data or the watermark, were pointed out as well as some corresponding countermeasures. A classification of attacks on text watermarking as well as referring to the use of cryptographic tools as countermeasures against some types of attacks were presented in [13]. Finally, in a recent conducted research on watermarking attacks by S. Sherekar et al. [14], only the robustness is regarded as the major concern of security provisioning for different digital watermarking techniques.

In this paper, we attempted to provide a thorough taxonomy of deliberate and malicious attacks against watermarking systems and the existing and state-of-the-art countermeasures. In order to conduct this research, we developed the classification of attacks mostly based on the categorization offered in [3][4][7][10][12–15]. Then, regarding each type of attack, existing and published research work providing the defense solutions were investigated.

III. CLASSIFICATION OF ATTACKS AND COUNTERMEASURES

It should be noted that carrying out diverse types of attacks requires the adversaries to have various level of sophistication and knowledge about the watermarking systems. Based on assumptions about the knowledge of adversaries, four groups of attackers can be considered [3]. First, the attacker knows nothing about the algorithms and does not possess a tool such as a watermark detector. Thus he/she may use different distortions such as compression, noise filters and geometrical and temporal distortions. Second, the attacker has more than one watermarked work. This enables the adversary to remove watermarks (e.g. collusion attacks) 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. In this paper, we made an effort to present a comprehensive classification of the most prominent and prevalent attacks against digital watermarking. A main taxonomy of attacks against the security of digital watermarks may include unauthorized action-specific attacks and system attacks which has been presented in Fig. 2. Unauthorized actions further divided into unauthorized embedding, unauthorized detection and unauthorized removal. In the following sections we will go through these attacks and their corresponding countermeasures.

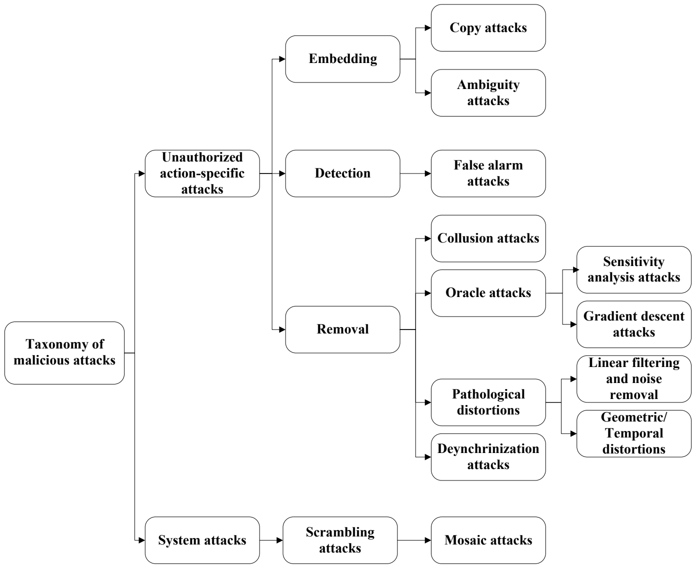

Figure 2. Taxonomy of watermarking attacks.

A. Unauthorized Embedding

In unauthorized embedding, the attacker whether makes original watermark or acquires a previous legitimate watermark and embeds it into the host data. Most well-known attacks in this group are copy attacks and ambiguity attacks. These attacks result in false detection of watermarks.

1) Copy attack: This attack is viable through obtaining a legitimate watermark from a watermarked content and copies or embeds it into another carrier signal (an unwatermarked work). As the definition implies, this attack requires performing a removal attack or carrying out some kind of estimation (using prior knowledge of signals' statistics, having the same host signal carrying different watermarks and etc.) to extract the watermark. To counter this attack, two approaches mentioned in the literature:

- Creating a link between the watermark and the carrier signal by means of cryptographic hash functions which has to be verified during the detection of the watermark [3][10].
- Making the watermark a function of the original carrier signal that leads to more difficult copying regarding the quality of the watermarked target carrier signal [10].

2) 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 signal-dependent by using cryptographic hash functions [3].

B. Unauthorized Detection

In unauthorized detection the purpose of the attacker may simply be realizing whether a watermark exists in the host data or not. In another form, the adversary attempts to decode the watermark especially in cases which maintaining the privacy of watermark is of great importance. In contrast, instead of decoding, an attacker can recognize the meaning of a watermark and draw conclusion about two or more watermarked digital content to have the same watermark or not. A well-known attack of this group named false alarm attack [10]. By accessing to the detector, the attackers are able to carry out false alarm attacks in which the attacker attempts to simulate the detection of watermark even though there is no such watermark in the host signal.

Although sometimes it is not possible to protect a watermarking system against unauthorized detection and message decoding, there are some solutions to alleviate the problem. Using a very large key space make the brute force search attacks against the watermarking scheme tougher. Moreover, employing cryptographic algorithms is effective for increasing the security of watermarks against this type of attacks.

C. Unauthorized Removal

Unauthorized removal aims to make the watermark undetectable. This process may result in the complete removal of the watermark and recovering the original host data, which is called elimination attack. It is also feasible to alter the watermarked media content in an intangible way and make it difficult for the detector to recognize the change (e.g. slightly rotating an image which has a watermark). These types of unauthorized removal attacks are referred to as masking attacks. Elimination attacks are more challenging to counter compared with masking attacks. Some of most prevalent attacks of this class are as follows.

1) Collusion attack: The term "collusion attacks" is applied to the attacks in which the attacker has more than one watermarked work with the same watermark in his/her possession. This enables the attacker to extract and identify the pattern of watermark. Another type of these attacks is possible when the adversary acquires several copies of a work, each having a different watermark. These copies can be combined to make the watermarks undetectable. To detect the presence of collusion or to confront this attack, several approaches have been proposed in the literature which we will go through some of them as follows.

- A collusion-secure code can be used which is secure against collusion attacks that take advantage of having several copies of the same work [3][16].
- In [17], two collusion attacks, which exploited the redundancy of host signal (e.g. analogous consecutive video frames in a movie clip, repetitive patterns in songs etc.) to remove the watermark, along with their corresponding countermeasures were presented.
- Authors in [18] offered a wavelet-based fingerprinting scheme and a statistical clustering method for collusion attack detection and colluder identification.
- Wu ge and Li guiying [19] proposed a video watermarking system resilient to collusion attack. They devised a novel algorithm, which employed a high-precision motion compensation based on H.264.
- Research conducted in [20], reviewed previous and recent research papers and works with focus on collusion-resistant fingerprinting systems and MC-CDMA-based fingerprinting scheme in particular.
- In [21], for defending against fading-like collusion attack, a spread spectrum image watermarking scheme using genetic algorithm was proposed.

2) Oracle attack: An attacker is able to launch an oracle attack without knowledge about the algorithm only by using a watermarked digital content, if he/she has a detector at his/her disposal. In this attack, the attacker has the opportunity to apply few modifications to the work and figure out whether it is inside the detection region or not. Repeating this process (i.e. altering the work and testing) provides the adversary with valuable knowledge regarding the operation of the detection algorithm. Two well-known attacks namely, sensitivity analysis attack and gradient descent attack are considered in this category. Sensitivity analysis attack utilizes a binary decision (i.e. yes or no) about the existence of the watermark, while gradient descent attack exploits the values of the detection statistic. Spread spectrum watermarking schemes are vulnerable to sensitivity analysis attacks. Some approaches to thwart these attacks are as follows.

- Three methods for countering oracle attacks were proposed in [15]. These three techniques involved modification of authentication watermarking algorithms into algorithms with a hash table memory and are based on randomization, delay or both.
- A sensitivity analysis-resilient watermarking scheme provided in [22] in which the addition or subtraction of watermark in sensitivity analysis did not have any impact on the detection process defined in the technique. Thus, the detector can be safely distributed.
- As a defense technique against gradient descent attacks, the detection statistic within the detection region should not reveal any useful information in identifying a short path out of the detection region [22].

3) Pathological distortions: Any process (a normal process or an improbable process happening during normal processing) that preserves the fidelity (i.e. the perceptual similarity between the original and watermarked versions of the host signal) of work could be exploited by an attacker to evade the detector through masking or removing the watermark. Two most commonplace group of attacks in this category include:

- Linear filtering and noise removal: Linear filtering arms an adversary with a tool to remove a watermark. For instance, a low-pass filter can be applied to degrade a watermark with considerable energy in the high frequencies. Moreover, watermarking systems with noise-like added pattern are susceptible to noise-removal techniques.
- Geometric/temporal distortion (synchronization attack): This attack involves synchronization (i.e. the process of aligning two signals in time or space) distortions such as delay and time scaling, rotation, zooming, shift direction, cropping or pixel permutation and so on.

4) De-synchronization attack: By misaligning the watermark and the detector, this attack is aimed at performing the detection of watermark tough. Several defense 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 [23]. This scheme applied an adaptive receiver providing exact estimation of the quantization step required defending against time scale modification attacks. Hong Peng et al. [24] 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 sub-frames. 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 [25]. Authors in [26], made use of dyadic wavelet transform (DYWT) to resynchronize the watermark. A new robust embedding technique using shape modulation presented as well as designing a new error correction coding (ECC) capable of bit-resynchronization to correct insertion, deletion and substitution errors in the watermark.

- Image watermarking de-synchronization-resistant schemes: Using robust and enhanced Harris corner detector, strong important feature points of an image (these points are more resilient to geometric attacks) are acquired and employed by Delaunay triangle matching and image restoration method to reduce synchronization errors [27]. In another defense technique, support vector regression (SVR) and particle swarm optimization were provided to shield gray images in discrete cosine transform domain from de-synchronization attacks [28]. In addition, in [29], the authors came up with a new image watermarking algorithm based on multi-scale SIFT (Scale Invariant Feature Transform) detector and local image histogram shape invariance with acceptable resilience to de-synchronization.
- General schemes: A message-passing approach investigated in [30] for countering de-synchronization attacks (e.g. scaling, amplitude modulation, fractional shift, arbitrary linear). They modeled the watermarking system using Forney-style factor graphs and solved the blind watermark decoding problem through message-passing.

D. System Attacks

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 [3]. 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 [31] 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 history 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. This method is able to mitigate the imposed attacks by using predetermined conditions efficiently without any demand to retrieve watermark at the time of using content. Another type of mosaic invasion is fine attack which performs content segregation through small granulation. Fine mosaic attack degrades the possibility of watermark extraction on single segments. For example, suppose a movie that is divided into one-second equal clips and stored as a collection of independent files. It is important to note that this type of attack involves large overhead for the sake of small files processing and it is not applicable for most of available devices in the market. The main point for the mitigation of this threat is the recognition of files less than a certain size e.g. multimedia files smaller than five seconds long can raise the alarm to prevent this invasion. Actually, general countermeasure against this group of attacks can be the reduction of the minimum needed size for robust watermark embedding.

IV. CONCLUSION

This paper provides a general view for the classification of attacks against the security of the digital watermarking schemes. In addition, 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 attackers' behavior, 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.

REFERENCES

[1] N. H. O. A. K. K. Adesina A.O., "Digital watermarking: A state-of-the-art review," in 2010 IST-Africa, 2010.

[2] C. I. Podilchuk and E. J. Delp, "Digital watermarking: algorithms and applications," Signal Processing Magazine, IEEE, vol. 18, no. 4. pp. 33-46, 2001.

[3] 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.

[4] X. H. Jian L., “A review study on digital watermarking,” in Proceedings of 1st International Conference on Information and Communication Technology, ICICT 2005, 2005, vol. 2005, pp. 337-341.

[5] A. T. Abdel-Hamid, S. Tahar, and E. M. Aboulhamid, “IP watermarking techniques: survey and comparison,” System-on-Chip for Real-Time Applications, 2003. Proceedings. The 3rd IEEE International Workshop on. pp. 60-65, 2003.

[6] L. J. M.-S. W. H. M. S. M. I. L. P. M. T. P. W. H. W. G. Kahng A.B., “Watermarking techniques for intellectual property protection,” in Proceedings - Design Automation Conference, 1998, pp. 776-781.

[7] N. K. H. L. H. B. Le T.H.N., “Literature survey on image watermarking tools, watermark attacks, and benchmarking tools,” in 2nd International Conference on Advances in Multimedia, MMEDIA 2010, 2010, pp. 67-73.

[8] T. Kalker, “Considerations on watermarking security,” in 2001 IEEE Fourth Workshop on Multimedia Signal Processing, 2001, pp. 201-206.

[9] T. S. T. A. S. V. Nikolaidis A., “A survey on watermarking application scenarios and related attacks,” in IEEE International Conference on Image Processing, 2001, vol. 3, pp. 991-994.

[10] M. Arnold, “Attacks on digital audio watermarks and countermeasures,” Web Delivering of Music, 2003. 2003 WEDELMUSIC. Proceedings. Third International Conference on. pp. 55-62, 2003.

[11] B. F. F. T. Barni M., “A general framework for robust watermarking security,” Signal Processing, vol. 83, no. 10, pp. 2069-2084, 2003.

[12] S. Voloshynovskiy, S. Pereira, T. Pun, J. J. Eggers, and J. K. Su, “Attacks on digital watermarks: classification, estimation based attacks, and benchmarks,” Communications Magazine, IEEE, vol. 39, no. 8. pp. 118-126, 2001.

[13] Z. W. W. Z. P. L. Zhou X., “Security theory and attack analysis for text watermarking,” in 2009 International Conference on E-Business and Information System Security, EBISS 2009, 2009.

[14] S. Sherekar, V. Thakare, S. Jain, and D. B. and T. Miss Ashwini, “Attacks and Countermeasures on Digital Watermarks: Classification, Implications, Benchmarks,” International Journal Of Computer Science And Applications, vol. 4, no. 2, 2011.

[15] I. Venturini, “Oracle attacks and covert channels,” Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 3710 LNCS, pp. 171-185, 2005.

[16] D. Boneh and J. Shaw, “Collusion-secure fingerprinting for digital data,” Information Theory, IEEE Transactions on, vol. 44, no. 5. pp. 1897-1905, 1998.

[17] D. J.-L. Doërr G., “Countermeasures for collusion attacks exploiting host signal redundancy,” Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 3710 LNCS, pp. 216-230, 2005.

[18] Y. G. Persaud A., “Collusion detection using multimedia fingerprints,” IFIP International Federation for Information Processing, vol. 222, pp. 105-118, 2006.

[19] L. G. Ge W., “Collusion-resistant blind video watermarking based on H264,” in ICCASM 2010 - 2010 International Conference on Computer Application and System Modeling, Proceedings, 2010, vol. 11, p. V119-V1113.

[20] K. C.-C. J. Cha B.-H., “Collusion-resistant fingerprinting systems: Review and recent results,” Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 6010 LNCS, pp. 34-50, 2010.

[21] S. J. M. S. P. D. C. Maity S., “Fuzzy-GA hybridization in M-band wavelets for collusion resilient optimized SS watermarking,” in 3rd European Workshop on Visual Information Processing, EUVIP 2011 - Final Program, 2011, pp. 205-210.

[22] W. S. Zhang X., “Watermarking scheme capable of resisting sensitivity attack,” IEEE Signal Processing Letters, vol. 14, no. 2, pp. 125-128, 2007.

[23] 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.

[24] 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.

[25] 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.

[26] W. Y. W. S. Huang J., “Audio watermarking scheme robust against desynchronization based on the dyadic wavelet transform,” Eurasip Journal on Advances in Signal Processing, vol. 2010, 2010.

[27] Q. J. Qi X., “A desynchronization resilient watermarking scheme,” Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 5510 LNCS, pp. 29-48, 2009.

[28] B. I. Ü. E. Findik O., “A digital robust image watermarking against desynchronization attacks,” Scientific Research and Essays, vol. 5, no. 16, pp. 2288-2294, 2010.

[29] N. P.-P. M. L. Y. H.-Y. Wang X.-Y., “A robust content based image watermarking using local invariant histogram,” Multimedia Tools and Applications, vol. 54, no. 2, pp. 341-363, 2011.

[30] S. Sadasivam, P. Moulin, and T. P. Coleman, “A Message-Passing Approach to Combating Desynchronization Attacks,” Information Forensics and Security, IEEE Transactions on, vol. 6, no. 3. pp. 894-905, 2011.

[31] 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.