

We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,900

Open access books available

186,000

International authors and editors

200M

Downloads

Our authors are among the

154

Countries delivered to

TOP 1%

most cited scientists

12.2%

Contributors from top 500 universities



WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com



A Survey on Piracy Protection Techniques in Digital Cinema Watermarking Schemes

Behrouz Zolfaghari and Pinaki Mitra

Abstract

Watermarking is used in several areas such as CDNs (Content Delivery Networks), as part of the rights management system for counterfeit prevention. Watermarking schemes need some additional features in order to be used in digital cinema. In fact, extra watermarks are added to movies by cinema projectors in projection time, which help identify the cinema hall in which the illegal copy has been recorded. But distortions caused by hand vibrations and the point of view angle make it difficult to recover the watermark. This makes it necessary to be distortion-resistant for the watermarking schemes used in digital cinema. On the other hand, theatre owners would like to locate the camcorder that has recorded the pirate copy. This requires watermarking schemes to be able to estimate the distance and angle using the distributed pirate copy. In this chapter, we present a review on watermarking techniques specifically designed to attack the aforementioned problems.

Keywords: watermarking, piracy, digital cinema, copyright, survey, digital distribution

1. Introduction

Digital distribution has been considered by researchers since four decades ago [1–3]. With the growth of available bandwidth in the telecommunications infrastructures, it gradually appeared as one of the main purposes of communication during two decades. This encouraged a lot of research on different aspects of digital distribution over internet [4–6]. Digital distribution brings about several challenges among which one can refer to performance, but in this chapter, we are more interested in security. Security of digital distribution has been investigated from different aspects [7–9]. One of the most challenging aspects in digital distribution security is digital rights management, which has been the topic for several research works [10, 11]. With the emergence of internet, online digital distribution found its applications in a variety of environments [12–14]. Meanwhile, the public access to internet made security more and more challenging [15].

Content delivery is a branch of digital distribution, which is growing very fast in different aspects [16, 17]. The more content delivery systems grow, the more complex security their security management becomes [18]. Among advances in content delivery, one may mention CDNs [19–21]. These networks serve to high-performance delivery of digital contents as well as streaming of audio and video in collaboration with other technologies such as cloud computing [22, 23].

Different aspects of security in CDNs such as privacy [24], digital property management [25], intrusion detection [26], trust [27], and eavesdropping protection [28] have been studied by researchers.

Digital cinema is a service that can be provided using CDNs. It is an online video streaming and projection service gaining a research focus in recent years [29–31]. Security is a serious challenge in digital cinema [32–34] like other services provided over CDNs. One of the most important aspects of digital cinema security is digital rights management [35, 36], which is about preserving the publication rights for the generator of contents. Counterfeit protection is one of the most challenging problems in the area of digital cinema rights management.

Digital property management and especially counterfeit protection mostly depend on watermarking in a variety of environments [37–39]. Digital watermarking has been finding its applications in digital cinema in recent years [40, 41]. But, there is a delicate challenge faced by watermarking systems used in digital cinema. In the absence of proper protective measures, counterfeit copies of movies can be recorded by handheld cameras in the cinema hall. Movie theater holders are obliged to take preventive measures in this regard. This creates two problems, which need to be taken into consideration while designing watermarking schemes for digital cinema. These problems are explained in the following.

The first problem is faced by movie providers. When a pirate copy is distributed, providers would like to identify the theatre where the copy has been recorded. Then they can sue the identified theatres as they have not fulfilled their legal obligations. One way to approach this problem is to add watermarks to the movie by the projector in projection time. This watermark carries some identification information about the cinema hall as well as the projection time. This makes it possible to identify the hall in which a counterfeit copy has been recorded. But, the distortions made by hand vibrations and point of view angle, makes it difficult to recover the watermark from the movie. Thus, watermarking schemes designed for digital cinema should be specifically resistant against these distortions.

The second problem is to locate the seat on which the camcorder has been recording. This problem is to be solved by cinema holders as they are legally responsible for illegally recorded copies. Solving this problem requires digital cinema watermarking schemes to be able to calculate distance and angle.

There are some surveys on techniques used to solve the two problems mentioned above. But, they are outdated for such a fast-growing area [42, 43]. This motivates our work in this chapter, which is a comparative review on watermarking schemes used in digital cinema and the methods used by these schemes in order to achieve the mentioned goals.

The rest of this chapter is organized as follows. Section 2 presents an introduction to digital cinema. Section 3 discusses watermarking and related concepts. Section 4 presents a survey on watermarking in digital cinema. Section 5 concludes the chapter and suggests further research.

2. Digital cinema

Digital cinema refers to the set of processes, tools, and components which aim at the preparation, transmission, and projection of digital movies in cinema. This system is taking the place of traditional cinema which depends on reels of film being projected by film projectors.

In digital cinema, 2K (2048×1080 or 2.2 megapixels) or 4K (4096×2160 or 8.8 megapixels) resolutions are commonly used.

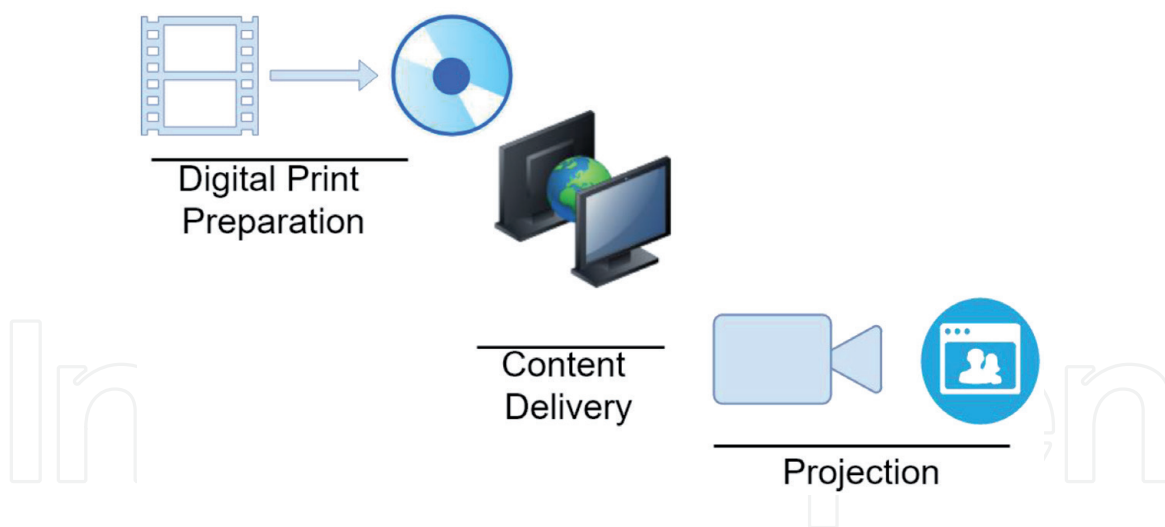


Figure 1.
A typical digital cinema system.

Among the advantages of digital cinema, we can point out reduction in time to market, reduction in cost per print, greater reach, and piracy control.

A digital cinema system consists of three main processes. In the first process, the film is converted to a digital print called DCP (Digital Cinema Package). The DCP is then delivered to the theatres and ingested (stored) by the related servers. This can be done through physical transportation of hard disks or through a digital distribution system. A content delivery network can serve to this purpose [44]. The DCP is often encrypted, and the keys required to decrypt the file are ingested in the screening tools to prevent theater owners from illegal screen extensions. In the third process, the movie is played back using a digital video projector. The aforementioned three processes are shown in **Figure 1**.

The first system specification for digital cinema was published in 2005 by a consortium of six major studios. This specification is referred to as DCI (Digital Cinema Initiatives) and uses JPG 2000 video encoding with XML playback standard.

3. Digital watermarking

Watermarking is a copyright ownership identification method used for noise-tolerant media such as video, image, and audio. In this technique, an intentional noise is added to the signal in the form of covertly embedded information. In most cases, the hidden information is normally not perceptible. Rather it requires some revealing process to be extracted from the carrying content file. However, in some cases, it can be perceptible. For example, it can be visibly added to a film or image in order to encourage the user to buy the original version without the mark.

The hidden information should be robust (resistant) against simple modifications normally used to the media type. For example, a marker hidden in an image should not be removed when the image is converted from Bitmap to JPG.

Steganographic techniques such as watermarking and steganography are evaluated using measures like robustness, imperceptibility, and capacity. In watermarking, the main objective is robustness. It should not be confused with steganography where imperceptibility is the main goal [45].

Figure 2 shows how the character “a” can be watermarked in a video using a simple watermarking scheme.

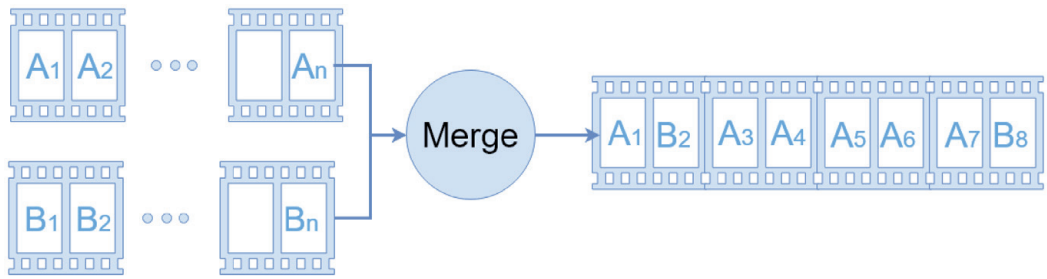


Figure 2.
Watermarking the character “a” in a movie.

In the example shown in **Figure 2**, the video is first decomposed into n segments. Then two different variants of the video represented by A and B are prepared which are imperceptibly different in each segment. Each segment can be chosen from the variant A or B . The choice of A for a segment watermarks the bit value “0,” and choosing B means watermarking “1.” In this example, the ASCII code “01000001” assigned to the character “a” has been watermarked to the video by choosing segments 2 and 8 from the variant B and the others from A .

4. Survey on watermarking in digital cinema

Illegal recording from the cinema screen using handheld cameras is a serious problem encountered by film makers. Watermarking, as a fingerprinting method aiming at piracy protection is a promising method for attacking this problem in the context of digital cinema. The watermarking process can be performed in show time and embed information regarding the projector and the playback time into the video. Since theatre owners are obliged to prevent handheld cameras in their premises, they are responsible for the pirate copies, and the watermark extracted from the pirate copies can specify the theatre where the copy has been recorded.

One of the most serious problems in the application of watermarking in digital cinema is that perspective, zoom, and some other parameters can be changed by the handheld camera, which leads to geometrical distortions. These distortions make it difficult to recover the watermark. This problem is faced by movie providers as they need to identify the theatre from which the pirate copy has been recorded. A watermarking system should guarantee distortion resistance in order to be capable of being used in digital cinema. In fact, old correlation-based watermark schemes are unable to prevent piracy because they are not robust to geometric distortions created by the handheld camera [46, 47].

The second challenge, which is faced by theatre owners, is locating the pirate in the theatre. Since theatre owners are sued when a pirate copy is distributed, they need mechanisms to identify the person who has recorded the illegal copy. To do this, they need to locate the camcorder. This way, they can identify the criminal using their ticket databases. This raises the need for watermarking methods capable of locating the camcorder.

The two aforementioned challenges have been part of the topic in several research works since early 2000s [48, 49], and they are still considered as research concerns in this area [42, 50]. In the following, we separately review the methods used by different watermarking schemes in order to attack each of the problems.

4.1 Identifying the theatre

In this section, we study the methods used in order to identify the theatres wherein hand camera copies are recorded. These methods mainly depend on geometric process while storing or detecting the watermark.

4.1.1 Temporal watermarking

One solution to the aforementioned problem is to design methods which use only the temporal access to embed the watermark. A watermarking scheme of this kind was proposed in [51, 52], which modifies the mean luminance value in each frame of the video according to the samples of the watermark. In this research report, it has been taken into consideration that the human visual system is sensitive to flickers in low spatial frequencies. Thus, the proposed scheme attempts at avoiding this kind of flickers. To do this, the same watermark is applied to a certain number of consequent frames.

In the aforementioned scheme, the watermark is considered as a pseudo-random sequence of length n consisting of 1 and -1 values. Embedding the watermark causes the luminance of each pixel to increase or decrease. But the change depends on a local scaling factor which has higher values for moving textual areas and lower values for non-moving flat areas. This scaling factor is defined as the minimum of a spatial scaling factor and a motion scaling factor. Moreover, there is a maximum allowable change that cannot be violated.

The motion scaling factor for each pixel is calculated as the difference from the corresponding pixel in the previous frame. On the other hand, the spatial scaling factor is calculated using a Laplacian filter. **Figure 3** shows this watermarking scheme.

In **Figure 3**, $T_{Texture}$ and $T_{Texture}$ are predefined thresholds and $|ABS|$ represents the absolute operator. Moreover, $0 \leq q < 1$, k is the number of the frame among the selected set of consecutive frames for embedding the watermark, and K is the number of consecutive frames.

The authors of this report successfully tested the robustness of their watermark under several conditions such as changing the zoom and angle of the camera in addition to handheld camera recording and people walking between the camera and the screen.

4.1.2 Compensation

Compensation is another solution to the geometrical distortion problem. In this method, a pre-process is used to restore the geometrical distortions before watermark extraction. A method based on compensation was proposed in [53]. The authors of this report made a simplifying assumption in order to make it easier to model the nonlinear distortions. They assumed that the handheld camera is located far from the screen at the back of the movie theatre but not so far from the center line of theatre.

The authors of [53] present a parameterized mathematical model that compares the pirate copy with its original in a general case. For each specific pair of pirate-original pair, the compensation method tries to find the values for the parameters such that the model best matches the case. They modeled the distortions with four mathematical transformations as follows.

- Affine transformations: there is assumed to be six degrees of parameters for this kind of transformations, which model rescaling (zooming), translation

(shifting caused by shakes of the camera), rotation (caused by the angle of the camera), and shearing (caused by cropping).

- Bilinear transform: this kind of transform can convert a square to an ordinary quadrilateral with eight degrees of freedom.
- Curved transform: it is a simple mathematical transform that models the impacts of the lens properties such as short focal length.
- Curved-bilinear transform: it has been designed to compensate the bilinear transform as well as the curved transform.

They tested their method via simulating a handheld camera. The simulation process applies a curved-bilinear transformation along with converting from 1920×1980 resolution to 1024×576 and then cropping to 720×576 . **Figure 4** shows this transformation. Their method successfully recovered a 64-bit watermark from the transformed video.

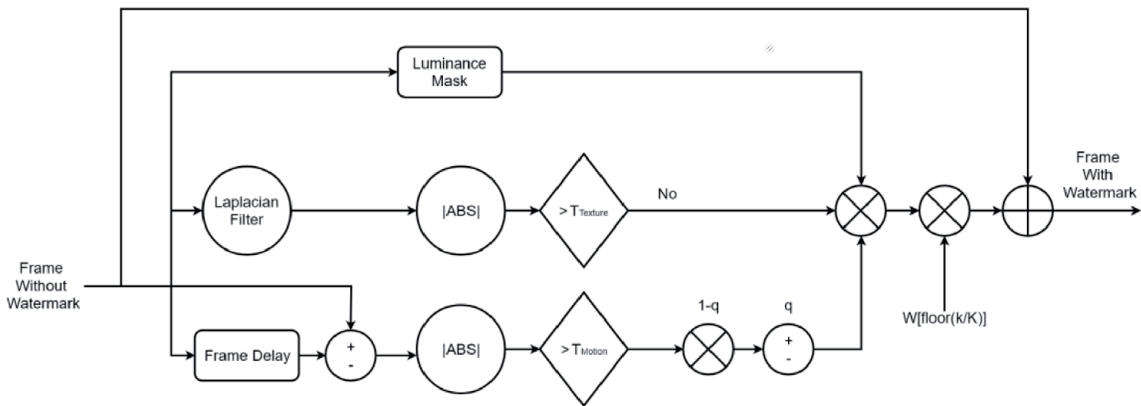


Figure 3.
The watermarking scheme presented in [51, 52].

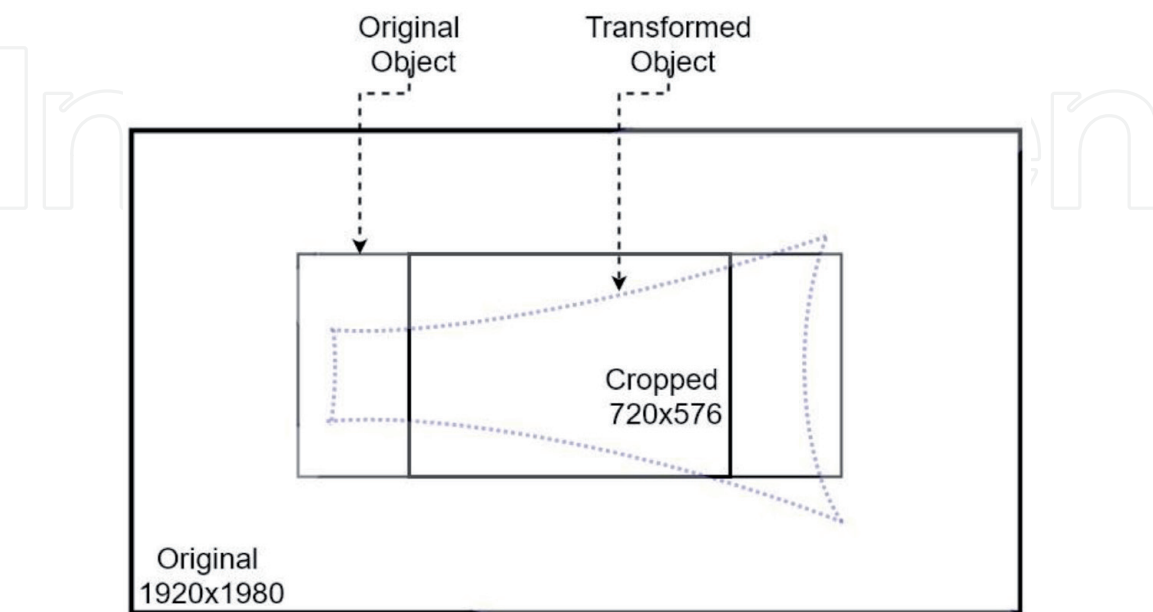


Figure 4.
The curved-bilinear transformation in [48].

4.1.3 Hardware-based additional watermarking

A hardware-based watermarking scheme named “Additional Watermarking” was presented in [54–56], which does not require the original movie for the recovery of the watermark. This method uses DWT (Discrete Wavelet Transform) instead of the Laplacian transforms. In this scheme, watermarks are added to the video in both the encoding and the decoding processes. This method uses CRC32 as a hash function for selecting random places in the video to embed the watermark. This method places the mark in the lowest frequency components of the video. It was shown in the research that the proposed method does not make any perceptible change in the original video and it is robust to a variety of signal processing transforms.

4.1.4 Spread transform dither modulation

The problem of tradeoff between fidelity and robustness was posed in [57]. A watermarking scheme based on STDM (Spread Transform Dither Modulation) was proposed in this research which uses the HVS (Human Visual System) properties of wavelet in order to resolve the tradeoff. These properties include the following facts.

- Noise in high resolution bands is not clearly perceptible to human eyes.
- HVS is less sensitive to changes to very high or very low brightness portions of the video.
- HVS is not very sensitive to changes in highly textured portions unless they are close to the borders.

In this scheme, the watermark is embedded during the JPEG2000 decoding phase. **Figure 5** shows a screen shot from Big Buck Bunny film before and after watermarking with this method.

4.1.5 Spread spectrum watermarking

In [53] another application for watermarking in digital cinema was proposed. This report proposes a watermarking method based on spread spectrum. This method is not only robust to geometric distortions, but also able to estimate the position of the handheld camera that has recorded the pirate copy. This may help identifying the ticket number and the credit card number of the person.



Figure 5.
A screenshot from Big Buck Bunny before and after watermarking (Courtesy to [57]).

The method proposed in [58] embeds the watermark in the payload in a way that the geometric transformation applied by the handheld camera can be identified in addition to the position of the camera. This method requires the watermark payload to follow a periodic pattern. A basic pattern is generated using a secret key in a way that it follows a periodic Gaussian distribution with the mean equal to zero and the variance equal to one. Then the payload, which contains the serial number of the projector as well as a time stamp is embedded into the video after the modulation process using an additive spread-spectrum method.

The authors of [58] tested the accuracy of their method in a small seminar room as well as a large auditorium. The mean absolute error was at maximum 6.87 cm for the small-scale test and 50.38 cm for the large-scale test.

Another watermarking scheme based on spread spectrum techniques was introduced in [59]. This method stores the watermark in the YCbCr color space using translation, rotation, scaling or composite operations.

Table 1 compares the methods used to identify the theatre. The parameters used in this comparison are as follows.

- Resistance against hand vibrations
- Resistance against perspective drifts
- Resistance against obstacles such as people’s heads or people walking between the handheld camera and the screen
- Resistance against zoom changes

One point to note here is that the distortion factors studied in **Table 1** are not the only factors that make it complex to recover the projection time watermark from pirate copies. For example, it was shown in [60] that the lamination flickers, induced by the interplay between an LCD and a camcorder can cause some difficulties in the recovery of the watermark. In addition to temporal luminance variations studied in [60], spatial luminance variations induced by camcorder recording have been studied in [61].

4.2 Locating the camcorder

In this section, we study the methods that can be used by cinema owners in order to locate the pirate camera.

		Method				
		Temporal	Compensation	Additional	Spread transform	Spread spectrum
Presented in		[51, 52]	[53]	[54–56]	[57]	[58, 59]
Robust Against	Vibration	NO	NO	YES	YES	NO
	Angle	YES	YES	YES	YES	YES
	Obstacles	YES	YES	YES	YES	YES
	Zoom	YES	YES	YES	YES	YES

Table 1.
A comparison among watermarking schemes used in digital cinema.

4.2.1 Audio watermarking

An approach to estimating the camcorder location has been proposed in [62]. In this method, unlike previous methods, audio is watermarked in the movie soundtrack instead of images, numbers or text messages being watermarked in the video itself. Most of the methods introduced in the literature avoid audio watermarking because of its complexity. In fact, it is difficult to hide any audio in soundtracks as they contain different types of audio such as voices, sound effects, and music.

The method proposed in [62] depends on a stochastic analysis in the watermark detection process. This method uses the audio watermarking technique introduced in [63]. The idea behind this method is that the attenuation of an audio signal depends on the distance. Thus, a few watermarked audio signals played from different locations can provide adequate information for locating the pirate. The advantage of this method is that audio is not prone to geometric distortion.

4.2.2 Hybrid audio-video watermarking

Some recent research works such as the one reported in [50] have combined video watermarking and audio watermarking in order to achieve the advantages of both methods. Audio watermarking is not affected by geometric distortions resulting from perspective, zoom, and vibrations. On the other hand, video watermarking is not affected by distance. Thus, it looks pertinent to combine them to achieve better results.

In the method proposed in [50], audio is watermarked in the video itself instead of the soundtrack. This way, there is no need for the watermarked audio to be played from different sources.

Another hybrid audio-video watermarking scheme was introduced in [64]. In this method unlike the one presented in [50], audio and video are separately watermarked in the soundtrack and in the movie itself.

5. Conclusion

In this chapter, we introduced the challenges faced by watermarking schemes in digital cinema. Then, we presented a review on watermarking methods specifically designed to confront these challenges. We focused on two main problems, first of which is the geometric distortion problem which and the second is camcorder location estimation. Our work in this chapter can be continued by studying other security and performance aspects of digital cinema.

IntechOpen

Author details

Behrouz Zolfaghari[†] and Pinaki Mitra^{*}

Department of Computer Science and Engineering, Indian Institute of Technology
Guwahati, India

^{*}Address all correspondence to: pinaki@iitg.ac.in

[†] Equally contributed.

IntechOpen

© 2020 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/3.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

References

- [1] Hata M, Fukazawa A, Bessho M, Makino S, Higuchi M. A new 40 GHz digital distribution radio with single local oscillator. In: Proceedings of IEEE-MTT-S International Microwave Symposium Digest; 1978
- [2] Hata M, Fukasawa A, Bessho M, Makino S, Higuchi M. A 40-GHz digital distribution radio with a single oscillator. *IEEE Transactions on Microwave Theory and Techniques*. 1980;9:951-962
- [3] Stranathan BL. Issues to be considered—The implementation of a digital distribution system by the commercial broadcast networks. *SMPTE Journal*. 1997;106(11):795-798
- [4] Rupp P, Estier T. A model for a better understanding of the digital distribution of music in a peer-to-peer environment. In: Proceedings of Annual Hawaii International Conference on System Sciences; 2003
- [5] Zhao J, Liu H, Guangxian LV, Wang L, Ji Y. Research and development on digital distribution network. In: Proceedings of International Conference on Sustainable Power Generation and Supply; 2009
- [6] Wang B, Huang T, Dong X, Jiang B, Bo ZQ. Dynamic emergency control in digital distribution substation with MW PV power. In: Proceedings of International Conference on Critical Infrastructure (CRIS); 2010
- [7] Cilaro A, Barbareschi M, Mazzeo A. Secure distribution infrastructure for hardware digital contents. *IET Computers and Digital Techniques*. 2014;8(6):300-310
- [8] Lee N-Y, Hwang T. On the security of Park et al.'s key distribution protocol for digital mobile communications. In: Proceedings of International Symposium on Personal, Indoor, and Mobile Communications (PIMRC); 1996
- [9] Higuero M, Unzilla J, Saiz P, Jacob E, Aguado M, Goirizelaia I. A practical tool for analysis of security in systems for distribution of digital contents based on 'attack trees'. In: Proceedings of IEEE International Symposium on Broadband Multimedia Systems and Broadcasting; 2009
- [10] Ghatak P, Tripathi RC, Chakravarti AK. Digital rights management: An integrated secure digital content distribution technology. *Journal of Intellectual Property Rights*. 2004;9:331-331
- [11] Liu Q, Safavi-Naini R, Sheppard NP. Digital rights management for content distribution. In: Proceedings of the Australasian information security workshop conference on ACSW frontiers; 2003
- [12] Gauche E, Coelho J, Treive RCG. An online distribution feeder optimal reconfiguration algorithm for resistive loss reduction using a multi-layer perceptron. In: Proceedings of International Conference on Neural Networks (ICNN); 1997
- [13] Clemons EK, Aron R. Online distribution: A taxonomy of channel structures, determinants of outcome, and determinants of strategy. In: Proceedings of the 35th Annual Hawaii International Conference on System Sciences; 2002
- [14] Azevedo DNR, De Oliveira JMP. Application of data mining techniques to the storage management and online distribution of satellite images. In: Proceedings of Seventh International Conference on Intelligent Systems Design and Applications (ISDA); 2007

- [15] Lo SW. Towards secure online distribution of multimedia codestreams [thesis]. Singapore: Management University; 2016
- [16] Kuang J, Yu S-Z. Broadcast-based content delivery in information-centric hybrid multihop wireless networks. *IEEE Communications Letters*. 2017;21(4):889-9892
- [17] Xiao X, Ahmed M, Chen X, Zhao Y, Li Y, Han Z. Accelerating content delivery via efficient resource allocation for network coding aided D2D communications. *IEEE Access*. 2019;7:115783-115796
- [18] Azogu IK, Ferreira MT, Liu H. A security metric for VANET content delivery. In: *Proceedings of IEEE Global Communications Conference (GLOBECOM)*; 2012
- [19] Chen M, Wang L, Chen J, Wei X, Lei L. A computing and content delivery network in the smart city: Scenario, framework, and analysis. *IEEE Network*. 2019;33(2):89-95
- [20] Bilen T, Canberk B. Handover-aware content replication for mobile-CDN. *IEEE Networking Letters*. 2019;1(1):10-13
- [21] Al-Abbasi A, Aggarwal V, Lan T, Xiang Y, Ra M-R, Chen Y-F. Fasttrack: Minimizing stalls for cdn-based over-the-top video streaming systems. *IEEE Transactions on Cloud Computing*. 2019;27(2):835-847
- [22] Tang G, Wang H, Wu K, Guo D. Tapping the knowledge of dynamic traffic demands for optimal CDN design. *IEEE/ACM Transactions on Networking*. 2019;27(1):98-111
- [23] Taleb T, Frangoudis PA, Benkacem I, Ksentini A. CDN slicing over a multi-domain edge cloud. *IEEE Transactions on Mobile Computing (Early Access)*. 2019:1-1
- [24] Cui S, Asghar MR, Russello G. Multi-CDN: Towards privacy in content delivery networks. *IEEE Transactions on Dependable and Secure Computing (Early Access)*. 2018:1-1
- [25] Chattopadhyay T, Sinha A, Hardikar A. H.264 compressed domain watermarking in content delivery network (CDN) environment. In: *Proceedings of 2nd International Conference on Computational Intelligence, Communication Systems and Networks*; 2010
- [26] Fiadino P, D'Alconzo A, Bär A, Finamore A, Casas P. On the detection of network traffic anomalies in content delivery network services. In: *Proceedings of 6th International Teletraffic Congress (ITC)*; 2014
- [27] Li S, Doh I, Chae K. Non-redundant indirect trust search algorithm based on a cross-domain trust model in content delivery network. In: *Proceedings of 19th International Conference on Advanced Communication Technology (ICACT)*; 2017
- [28] Huang T-C, Shieh C-K, Miao Y-B. Java Application's Packet Eavesdropper for content delivery network. In: *Proceedings of International Conference on Advanced Information Networking and Applications (AINA)*; 2005
- [29] Boitard R, Jacquemin J-P, Damberg G, Stojmenovic G, Ballestad A. Evaluation of color pixel representations for high dynamic range digital cinema. *SMPTE Motion Imaging Journal*. 2018;127(2):46-56
- [30] Gong B, Qin H, Chen D, Wang F. A study of stereoscopic digital cinema in china including new standards and recommendations. *SMPTE Motion Imaging Journal*. 2016;125(3):1-7
- [31] Schuck M, Ludé P. An analysis of system contrast in digital cinema

auditoriums. SMPTE Motion Imaging Journal. 2016;**125**(4):40-49

[32] Stone JJ. A new integrated system for digital cinema projection and security. In: Proceedings of The IEE 2-Day Seminar on IT to HD; 2004

[33] Bloom JA. Digital Cinema Content Security and the DCI. In: Proceedings of Annual Conference on Information Sciences and Systems; 2006

[34] Stone JJ, David MWA. An integrated system for digital cinema projection and security. SMPTE Motion Imaging Journal. 2005;**114**:10-11

[35] Bloom JA. Security and rights management in digital cinema. In: Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP); 2003

[36] Bloom JA. Security and rights management in digital cinema. In: Proceedings of International Conference on Multimedia and Expo. (ICME); 2003

[37] Ma H, Jia C, Li S, Zheng W, Xmark W. Dynamic software watermarking using Collatz conjecture. IEEE Transactions on Information Forensics and Security. 2019;**14**(11):2859-2874

[38] Kricha Z, Kricha A, Sakly A. Accommodative extractor for QIM-based watermarking schemes. IET Image Processing. 2019;**13**(1):89-97

[39] Shayan M, Bhattacharjee S, Tang J, Chakrabarty K, Karri R. Bio-protocol watermarking on digital microfluidic biochips. IEEE Transactions on Information Forensics and Security. 2019;**14**(1):625-639

[40] Shukla D, Sharma M. A novel scene-based video watermarking scheme for copyright protection. Journal of Intelligent Systems. 2017;**27**(1):47-66

[41] Kelkoul H, Zaz Y. Digital cinema watermarking state of art and

comparison. International Journal of Computer, Electrical, Automation, Control and Information Engineering. 2017;**11**(2):256-261

[42] Dubey NK, Modi H. Comparatives study of various techniques against camcorder piracy in theater. In: 6th International Conference on Multimedia Computing and Systems (ICMCS); 2018

[43] Dubey NK, Kumar S. A review of watermarking application in digital cinema for piracy deterrence. In: ourth International Conference on Communication Systems and Network Technologies; 2014

[44] Bertrand N, Durou J-D, Charvillat V. The DCP bay: Toward an art-house content delivery network for digital cinema. In: Proceedings of 7th International Conference on Advances in Multimedia (MMEDIA); 2015

[45] Sharifzadeh M, Aloraini M, Schonfeld D. Adaptive batch size image merging steganography and quantized gaussian image steganography. IEEE Transactions on Information Forensics and Security. 2020;**15**:867-879

[46] Kalker T, Depovere D, Haitsma J, Maes M. A video watermarking system for broadcast monitoring. In: Proceedings of IS&T/SPIE/EI25; 1999

[47] Bender W, Gruhl D, Morimoto N. Techniques for data hiding. In: Proceedings of the SPIE; 1995

[48] Lubin J, Bloom JA, Cheng H. Robust content-dependent high-fidelity watermark for tracking in digital cinema. Proceedings of SPIE. 2003;**5020**(1):536-545

[49] Nguyen P, Balter R, Montfort N, Baudry S. Registration methods for nonblind watermark detection in digital cinema applications. Proceedings of SPIE. 2003;**5020**(1):553-562

- [50] Kelkoul H, Zaz Y, Tribak H, Schaefer G. A robust combined audio and video watermark algorithm against cinema piracy. In: 6th International Conference on Multimedia Computing and Systems (ICMCS); 2018
- [51] Kalker T, Haitsma J. A watermarking scheme for digital cinema. In: Proceedings of International Conference on Image Processing; 2001
- [52] Van Leest A, Haitsma J, Kalker T. On digital cinema and watermarking. In: Proceedings of SPIE 5020; 2003
- [53] Delannay D, Delaigle J-F, Barlaud M. Compensation of geometrical deformations for watermark extraction in the digital cinema application. In: Proceedings of SPIE Security and Watermarking of Multimedia Contents; 2003
- [54] Vural S, Tomii H, Yamauchi H. Traceable robust watermarking for digital cinema system. In: Proceedings of International Symposium on Signal Processing and Its Applications; 2005
- [55] Vural S, Tomii H, Yamauchi H. Video watermarking for digital cinema contents. In: Proceedings of European Signal Processing Conference; 2005
- [56] Vural S, Tomii H, Yamauchi H. Robust digital cinema watermarking. International Journal of Computer and Information Engineering. 2008;2(10):3606-3611
- [57] Darazi R, Callau P, Macq B. Secure and HVS-adaptive exhibition spread transform dither modulation watermarking for digital cinema. In: Proceedings of First IEEE International Workshop on Information Forensics and Security (WIFS); 2009:1-12
- [58] Callau P, Darazi R, Macq B. Exhibition QIM-based watermarking for digital cinema. Proceedings of SPIE. 2009;7254(1):1-12
- [59] Dubey NK, Kumar S. An effective approach of distortion-resistant video watermarking for piracy deterrence. International Journal of Security and Its Applications. 2015;9(1):283-294
- [60] Hajj-Ahmad A, Baudry S, Chupeau B, Doerr G, Wu M. Flicker forensics for camcorder piracy. IEEE Transactions on Information Forensics and Security. 2017;12(1)
- [61] Kelkoul H, Zaz Y. Registration methods for nonblind watermark detection in digital cinema applications. International Journal of Computer, Electrical, Automation, Control and Information Engineering. 2003;11(2):2107
- [62] Nakashima Y, Tachibana R, Babaguchi N. Watermarked movie soundtrack finds the position of the camcorder in a theater. IEEE Transactions on Multimedia. 2009;11(3)
- [63] Tachibana R, Shimizu S, Kobayashi S, Nakamura T. An audio watermarking method using a two-dimensional psuedo-random array. Signal Processing. 2002;82(1):1455-1469
- [64] Gosavi CS, Mali SN. Secure, robust video watermarking to prevent camcorder piracy. Indian Journal of Science and Technology. 2017;10(18):1-10