Recent Advances in Multimedia Information System Security

Shiguo Lian
France Telecom R&D (Orange Labs) Beijing
2 Science Institute South Rd., Haidian District, Beijing 100080, China
E-mail: shiguo.lian@orange-ftgroup.com; sglian@gmail.com

Dimitris Kanellopoulos
Educational Software Development Laboratory (ESDLab)
Department of Mathematics,
University of Patras, Greece
E-mail: d_kan2006@yahoo.gr

Giancarlo Ruffo
Department of Computer Science
University of Turin, Italy
E-Mail: ruffo@di.unito.it

Keywords: multimedia system, security, encryption, authentication, digital rights management, forensic, watermark, biometric, copy detection, data mining

Received: September 1, 2008

A multimedia communication system enables multimedia data's generation, storage, management, distribution, receiving, consuming, editing, sharing, and so on. In such systems, there are various security issues, which must be considered such as eavesdropping, intrusion, forgery, piracy and privacy, etc. Until now, various security solutions for multimedia communication systems have been reported, while few works have surveyed the latest research advances. This paper gives a thorough review to multimedia information system security. It introduces a general architecture of multimedia information system, and investigates some security issues in multimedia information systems. It reviews the latest security solutions such as Digital Rights Management (DRM), confidentiality protection, ownership protection, traitor tracing, secure multimedia distribution based on watermarking, forgery detection, copy detection, privacy-preserving data mining, secure user interface, intrusion detection and prevention. Moreover, the paper presents some hot research topics such as Trusted Computing, steganography, security in network or service convergence, security of content sharing in social networks, privacy-preserving data processing, multimedia forensics and intelligent surveillance in multimedia information system security. It is expected to benefit readers by providing the latest research progress, advising some research directions and giving a list of references about multimedia system security.

Povzetek: Prispevek podaja pregled novejših pristopov pri zagotavljanju varnosti multimedijskih informacijskih sistemov.

1 Introduction

Nowadays, multimedia information applications such as mobile TV, on-line chatting, digital library, videoconference etc. [1][2] become more and more popular in human being's life. Generally, a multimedia communication system enables the generation, management, communication and consuming of multimedia data such as texts, images, audios, videos, animations, etc. Multimedia communication systems can be classified into various types. For example, according to the content, they can be classified into web systems, audio systems, audio-visual systems, etc. According to the communication infrastructure, they can be classified into broadcasting systems, multicasting systems, peer-to-peer (P2P) systems, etc. According to the service mode, they can be classified into living systems, content-on-demand systems, file downloading systems, etc.

Security protection is an important issue for multimedia information systems [2], which aims to protect the multimedia content, service interaction and user privacy, etc. For example, the content related to commercial secret needs to be protected against unauthorized users, the payment interactions between the user and the seller are sensitive to the third party, and the user profiles are private and should not be published. Until now, various techniques and tools have been proposed for multimedia information system security. Most of them focus on multimedia content security, secure interaction, and on privacy protection.

It is really difficult to give a thorough review on multimedia information system security because of two reasons. First, multimedia information system's diversity leads to the complexity and diversity of security issues and the corresponding protection means. Secondly, various new multimedia systems arise timely, which bring new security issues and solutions. Thus, few works have been done to review the state-of-art of multimedia information system security, and the existing works focused only on a certain kind of multimedia system. For example, in [3][4], Thuraisingham described security and privacy issues for multimedia database management systems including access control for multimedia database management systems, security policies and security architectures for such systems, and privacy problems resulted from multimedia data mining. However, only the secure database management system is focused, while some other systems, the key techniques and their advances are not introduced.

This paper aims to give a thorough review to multimedia information system security. It introduces a general architecture of multimedia information system, investigates some security issues in multimedia information systems, reviews the latest security solutions (their research advances and open issues), and presents some hot topics in multimedia information system security. It is expected to provide the latest research progress, advise some research directions, and give a list of references about multimedia system security to researchers.

The rest of the paper is organized as follows. In Section 2, the general architecture of multimedia information system is introduced, and the security issues are presented in Section 3. In Section 4, the latest technical solutions are reviewed in detail, including Digital Rights Management (DRM), confidentiality protection, ownership protection, traitor tracing, secure multimedia distribution based on watermarking, forgery detection, copy detection, privacy-preserving data mining, secure user interface, and intrusion detection and prevention. Then, in Section 5 some hot topics are proposed including trusted computing, steganography, the security in network or service convergence, security of content sharing in social networks, privacy-preserving data processing, multimedia forensics and intelligent surveillance. Finally, in Section 6, some conclusions are drawn.

2 General architecture of multimedia information system

Now, there are various multimedia information systems [2][3]. A general architecture of multimedia information system (Figure 1) is composed of several parts, i.e., multimedia content generation, content storage, content distribution, content receiving, and content consuming, editing and sharing. The architecture includes most of the steps from content generation, communication to consuming.

Multimedia content generation: It denotes the process to generate multimedia content produces (TV program, film, music, flash, web, etc.). Generally, various devices are used in this process, such as digital camera, Digital Video, audio recorder, etc. For some payable services, the multimedia content is usually generated by professional producers, while, for user generated content sharing there is no limitation to producers.

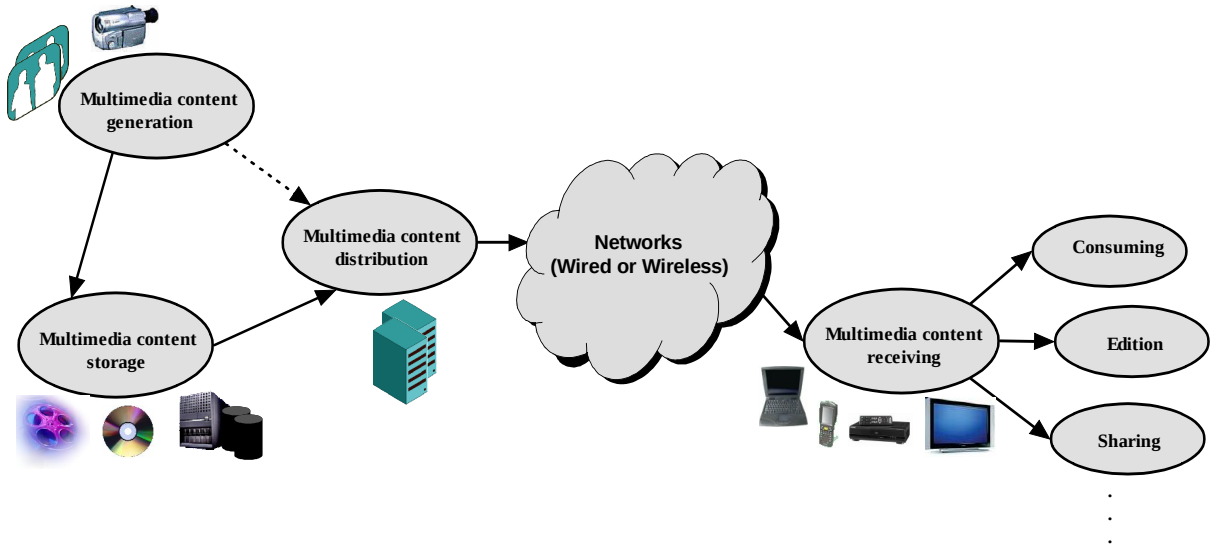


Figure 1: General architecture of multimedia information system

Multimedia storage and management: Multimedia content is often stored or backed up before being transmitted. For example, the film is recorded in the cinefilm, the music is burned into the Compact Disc, and the videos or web data are buffered in the computer servers. Generally, to make the data access or management more convenient, multimedia contents and their index information are ordered and stored in

the database, while some search or data mining techniques can be used. Additionally, to save the storage cost, multimedia content is often compressed and then stored.

Multimedia distribution: Multimedia services such as mobile TV, Internet TV, Online Music, and Content Sharing in Social Networks become more and more popular in human being's life. Among them, multimedia distribution acts as the key technique, which transmits the content from one user to others. There are two kinds of multimedia content to be transmitted, i.e., real-time content and stored content. The former one denotes the generated content without delayed storage, such as live TV or telephone call. The latter one denotes the content stored in the database, such as the video clips for video-on-demand, music segments, web data, etc.

Distribution networks: In multimedia distribution, the network is the core component. Now, various networks have been developed and popularly used. According to the physical communication channel used, they can be classified into wired networks and wireless networks. According to the communication modes, they can be classified into unicasting, broadcasting, and multicasting networks. According to the logical structure, they can be classified into client-server based networks and distributed networks (peer-to-peer networks, sensor networks, etc.). According to the application environments, they can be classified into Internet, GSM/GPRS, Satellite broadcasting, etc.

Multimedia receiving: The client receives multimedia content with terminals such as PC, TV set, mobile phone, telephone, etc. Depending on the service, certain terminal may be used. For example, PC is used for Internet access, mobile phone for short message sending, TV set for TV program watching, and telephone for calling and chatting. However, the functional difference between the terminals becomes more and more fuzzy. For example, PC is also used for chatting, and mobile phone for TV consuming and Internet access.

Multimedia consuming, editing and sharing: After receiving multimedia content, the user consumes it by decoding and playing it with terminals. He can request and browse the Web over the PC, watch TV programs over the TV set, and listening music through his mobile phone. According to the rights assigned to the user, the multimedia content may be downloaded, edited or even shared with others. For example, the user uses a PC to download a video clip from Internet, shorten it by cutting some frames and send it to his friends by peer-to-peer sharing networks. In another example, the user uses his cell phone to download a song, consume it, and then send it to his friends through Multimedia Message Sending. These operations depend on the terminal's functionalities and the content's properties

3 Security issues

In multimedia communication, security issues [3], which are generated from the transmitted information's sensitivities, should be considered. For example, the information may be related to military forbiddance, commercial secret or personal privacy. Only some authorized users can access this kind of information, and any action aiming to make the information released is regarded as the attack. With respect to the complexity of the information system, there are various threats. Some of them are described below.

3.1 Eavesdropping

Eavesdropping is the act of surreptitiously listening to a private conversation. This is commonly thought to be unethical. Eavesdropping can be done over telephone lines (wiretapping), email, instant messaging, and other methods of communication considered private. Wiretapping, also named telephone tapping, is the monitoring of telephone and Internet conversations by a third party, often by covert means. The wire tap received its name because, historically, the monitoring connection was applied to the wires of the telephone line being monitored and drew off or tapped a small amount of the electrical signal carrying the conversation. Now, eavesdropping is extended to the attack that steals the information from any network or device. Generally, it can be classified into two types: passive eavesdropping and active eavesdropping. The former one attempts only to observe the flow and gain knowledge of the information it contains, while the latter one attempts to alter the data or otherwise affect the flow of data.

3.2 Intrusion

Intrusion [5] denotes unwanted attempts at accessing, manipulating, and/or disabling of computer systems, mainly through a network such as the Internet. These attempts may take the form of attacks, as examples, by crackers, malware and/or disgruntled employees. Generally, the intrusion behavior can be classified into several types, i.e., network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and malware (viruses, trojan horses, and worms). Among them, the first one makes use of the apparent weakness of multimedia service systems to make them out of work, the second one adopts the iterated data requests and interactions to paralyze the applications, the third one uses the host role (with more rights than the authorized role) to steal information, and the fourth one denotes the executable program that can access, steal or tamper the software or hardware data.

3.3 Forgery

Forgery is the process of making, adapting, or imitating objects, with the intent to deceive. A forgery

is essentially concerned with a produced or altered object (multimedia content, user information, etc.). For example, in the 18th century, Europeans were curious about what North America looked like and were ready to pay to see illustrations depicting this faraway place. Some of these artists produced prints depicting North America, despite many having never left Europe. Recently, in some photo competitions, some presented photos were found non-initial produces and having been tampered with editions. Today, more and more famous drawings are imitated in order to be sold with a high price. Additionally, some attackers attempt to personate the authorized users to enjoy multimedia services.

3.4 Piracy

Copyright infringement (or piracy) is the unauthorized use of material that is covered by copyright law, in a manner that violates one of the copyright owner's exclusive rights, such as the right to reproduce or perform the copyrighted work, or to make derivative works. Especially for electronic and audio-visual media, unauthorized reproduction and distribution is occasionally referred to as piracy. Generally piracy behavior can be classified into two types, i.e., unauthorized access and unauthorized distribution. The former one denotes the unauthorized users access the multimedia content, while the latter one means that the users redistribute the accessed multimedia content to other unauthorized users. For example, the unlawful downloading of copyrighted material and sharing of recorded music over the Internet in the form of MP3 and other audio files is more prominent now than since before the advent of the Internet or the invention of MP3, even after the demise of Napster and a series of infringement suits brought by the American recording industry. Additionally, promotional screener DVDs distributed by movie studios (often for consideration for awards) are a common source of unauthorized copying when movies are still in theatrical release. Movies are also still copied by someone sneaking a camcorder into a movie theater and secretly taping the projection, although such copies are often of lesser quality than copied versions of the officially released film.

3.5 Privacy

Privacy is sometimes related to anonymity, the wish to remain unnoticed or unidentified in the public realm. When something is private to a person, it usually means there is something within them that is considered inherently special or personally sensitive. The degree to which private information is exposed therefore depends on how the public will receive this information, which differs between places and over time. Privacy can be seen as an aspect of security - one in which trade-offs between the interests of one group and another can become particularly clear. Almost all countries have laws which in some way limit privacy. An example of this would be law concerning taxation, which normally requires the sharing of information about personal income or earnings. In multimedia information systems, some personal information is private, such as user login information, subscribe information, user profile, and interaction records. Additionally, in some social networks, such as User Generated Content sharing networks, users can produce or post some multimedia content that is shared with other users. The user generated contents may be also private.

4 Technical solutions

To solve the security issues in multimedia information systems, some proposed technical solutions can realize confidentiality protection, ownership protection, traitor tracing, forgery detection, media source identification and copy detection, etc. The typical techniques include Digital Rights Management (DRM), multimedia encryption, digital watermarking, digital fingerprinting, multimedia forensics, privacy-preserving data mining, secure user interface, intrusion detection, etc. Hereafter, we describe these techniques.

4.1 Digital Rights Management (DRM)

The role of DRM [6] in distribution of content is to enable business models whereby the consumption and use of content is controlled. As such, DRM extends beyond the physical delivery of content into managing the content lifecycle. When a user buys content, he may agree to certain constraints, e.g., by choosing between a free preview version or a full version at cost, or he may agree to pay a monthly fee. DRM allows this choice to be translated into permissions and constraints, which are then enforced when the user accesses the content.

4.1.1 Scopes of DRM

Generally, a DRM system takes into consideration the following aspects: data to be protected, communication scenarios to be protected, access rights to be protected, the supported business model, and core techniques.

- **Data to be protected:** Image, video, audio, game, software, text, etc.
- **Communication scenarios to be protected:** Fixed-line services (telephone, visual telephone, etc.), Mobile/wireless services (broadcasting, Short Message Sending, Mobile TV, etc.), and Internet - based services (video-on-demand, P2P, music downloading, etc.).
- **Access rights to be protected:** access control (access to the content), usage restriction (play, playback, preview, copy, etc.), Inter-terminal copy (transfer to another terminal) and physical copy (copy the physical support), etc.
- **The supported business model:** Free, Subscription, pay per view, pay per time, etc.

- **Core techniques:** Right Expression Language, Identification and Authentication, Encryption/Decryption, Copy Protection, Access Control, etc.

4.1.2 General architecture

The general architecture of a DRM system is shown in Figure 2. It is composed of 4 main components: *Content Encoder, Content Server, Rights Issuer* and *User*. Content Encoder secures the content, Content Server distributes the content, Rights Issuer handles the license generation and assignment, and User reads the content. The typical DRM system works this way:
(1) The Content Encoder encrypts the multimedia content with the key and packages the content and key in certain format;
(2) The User requests the service from Rights Issuer and Content Server;
(3) The Content Server sends the encrypted content to the User through the manners, e.g., Internet, DVD/CDROM, email, Instant Message, Peer-to-Peer, etc.
(4) The Rights Issuer charges the service fees and distributes the rights (containing the key) to the User.
(5) The User decrypts and decodes the content with the key and consumes the content with the corresponding rights.

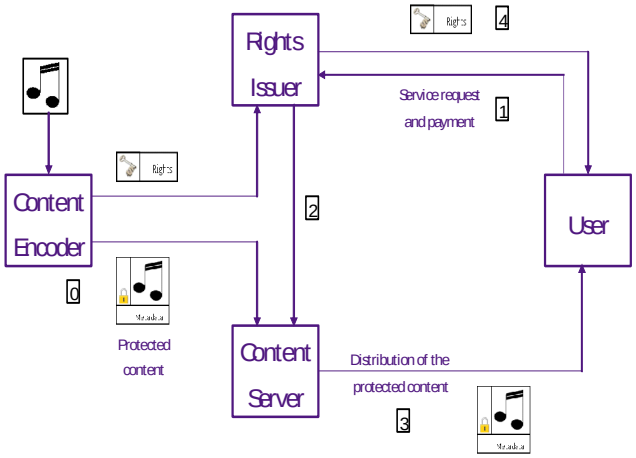


Figure 2: General architecture of a DRM system

4.1.3 Typical DRM systems

Previously, there have been various DRM systems for the corresponding services and networks. For example, the ISMACryp (Internet Stream Media Alliance Cryp) [7] is used for Internet streaming, Open Mobile Alliance DRM (OMA DRM) [8] for GSM/GPRS network, DVB-H Content Protection and Copy Management (DVB-CPCM) [9] for DVB-H network, and, High-bandwidth Digital Content Protection System (HDCP) [10], Certified Output Protection Protocol (COPP) [11] and Digital Transmission Content Protection (DTCP) [12] is used for home networks or devices. Henceforth, these DRM systems are briefly described.

ISMACryp ISMACryp [7] provides the digital rights management means for Internet Streaming Media. It defines the encryption and authentication for MPEG-4 [13] data streams. The ISMACryp specification does not mandate a cipher but AES in Counter Mode, the default encryption and authentication transform in the specification, is the de facto cipher [7] used by ISMACryp implementations. ISMACryp is different from traditional secure protocols (SRTP and IPsec). Whereas ISMACryp encrypts MPEG-4 access units (that are in the RTP payload), SRTP encrypts the whole RTP payload, and IPsec encrypts packets at network level. Thus, ISMACryp implements full end-to-end protection. Till now, there are two versions for ISMACryp, i.e., ISMA Encryption and Authentication Version 1.1 (ISMACryp 1.1) and ISMA Encryption and Authentication Version 2.0 (ISMACryp 2.0). ISMACryp 1.1 only addresses MPEG-4 codecs, such as H.264/AVC and AAC. Differently, ISMACryp 2.0 is compatible with any codec that can be stored in files of the MP4 family. This includes H.263 video and AMR audio, as widely used in mobile networks. It is compatible with any IP-network and can operate on any device, including mobile handsets.

OMA DRM The scope of OMA DRM [8] is to enable the controlled consumption of digital media objects by allowing content providers have some abilities, for example, to manage previews of DRM Content, to enable super distribution of DRM Content, and to enable transfer of content between DRM agents. The OMA DRM specifications provide mechanisms for secure authentication of trusted DRM agents, and for secure packaging and transfer of usage rights and DRM Content to trusted DRM agents. Before content is delivered, it is packaged to protect it from unauthorized access. A content issuer delivers DRM Content, and a rights issuer generates a Rights Object. The content issuer and rights issuer embody roles in the system. OMA DRM makes a logical separation of DRM Content from Rights Objects. DRM Content and Rights Objects may be requested separately or together, and they may be delivered separately or at the same time. For example, a user can select a piece of content, pay for it, and receive DRM Content and a Rights Object in the same transaction. Later, if the Rights Object expires, the user can go back and acquire a new Rights Object, without having to download the DRM Content again. The OMA DRM defines the format and the protection mechanism for DRM Content, the format (expression language) and the protection mechanism for the Rights Object, and the security model for management of encryption keys. The OMA DRM also defines how DRM Content and Rights Objects may be transported to devices using a range of transport mechanisms, including pull (HTTP Pull, OMA Download), push (WAP Push, MMS) and streaming. Any interaction between network entities, e.g. between rights issuer and content issuer, is out of scope.

DVB-H CPCM CPCM [9] is a system for Content Protection and Copy Management of commercial digital

content delivered to consumer products and networks. CPCM manages content usage from acquisition into the CPCM system until final consumption, or export from the CPCM system, in accordance with the particular usage rules of that content. Possible sources for commercial digital content include broadcast (e.g., cable, satellite, and terrestrial), Internet-based services, packaged media, and mobile services, among others. CPCM is intended for use in protecting all types of content, i.e., audio, video and associated applications and data. CPCM provides specifications to facilitate interoperability of such content after acquisition into CPCM by networked consumer devices. CPCM is only concerned with content after it has been acquired. The fundamental boundaries of control within CPCM are the local environment, and the Authorized Domain (AD). The AD is defined as a distinguishable set of DVB CPCM compliant devices, which are owned, rented or otherwise controlled by members of a single household. Content is bound to its Usage State Information (USI) which describes how it can be consumed, copied or exported relative to this Authorized Domain. This concept is fundamentally different from today's CA and DRM techniques, which normally operate on a single device basis.

HDCP High-bandwidth Digital Content Protection (HDCP) [10] is a form of Digital Rights Management (DRM) developed by Intel Corporation to control digital audio and video content as it travels across Digital Visual Interface (DVI) or High-Definition Multimedia Interface (HDMI) connections. HDCP's main target is to prevent transmission of non-encrypted high definition content. Generally, three methods are adopted to meet the goal. Firstly, the authentication process disallows non-licensed devices to receive HD content. Secondly, the encryption of the actual data sent over DVI or HDMI interface prevents eavesdropping of information. It also prevents "man in the middle" attacks. Thirdly, key revocation procedures ensure that devices manufactured by any vendors who violate the license agreement could be relatively easily blocked from receiving HD data. HD DVD, Blu-ray Disc and DVD players (with HDMI or DVI connector) use HDCP to establish an encrypted digital connection. If the display device or in the case of using a PC to decrypt and play back HD-DVD or Blu-ray media, the graphics card (hardware, drivers and playback software) does not support HDCP, then a connection cannot be established. As a result, a black picture and/or error message will likely be displayed instead of the video content.

COPP COPP [11] is a device driver technology used to enable High-bandwidth Digital Content Protection (HDCP) during the transmission of digital video between applications and high-definition displays. COPP is a Microsoft security technology for video systems that require a logo certification. For security drivers are authenticated and protected from tampering to prevent unauthorized high-quality recording from the video outputs. COPP control signals are also encrypted. Certified Output Protection Protocol (COPP) enables an application to protect a video stream as it travels from the graphics adapter to the display device. An application can use COPP to discover what kind of physical connector is attached to the display device, and what types of output protection are available. Protection mechanisms include HDCP, Copy Generation Management System - Analog (CGMS-A) and Analog Copy Protection (ACP). COPP defines a protocol that is used to establish a secure communications channel with the graphics driver. It uses Message Authentication Codes (MACs) to verify the integrity of the COPP commands that are passed between the application and the display driver. COPP does not define anything about the digital rights policies that might apply to digital media content. Also, COPP itself does not implement any output protection systems. The COPP protocol simply provides a way to set and query protection levels on the graphics adapter, using the protection systems provided by the adapter.

DTCP DTCP [12] is a DRM technology that aims to restrict "digital home" technologies including DVD players and televisions by encrypting inter-connections between devices. In theory this allows the content to be distributed through other devices such as personal computers or portable media players, if they also implement the DTCP standards. DTCP is one link in an end-to-end solution using licensing terms and conditions to enforce copy protection. It is based on well-known cryptographic algorithms and techniques and suitable for implementation on PCs and Consumer Electronics devices. The content is encrypted by DTCP source devices prior to output, and the device outputs are limited to "compliant" devices. The renewability capabilities enhance long-term integrity of system through device revocation. This system's implementation needs the supports from IT industry, CE industry, content distributors, content industries and conditional access providers.

4.1.4 Hot topics and open issues in DRM

Although various DRM systems have been proposed recently, there are still some open issues that constitute hot research topics.

DRM for P2P system P2P networks differ from traditional server-client networks. In P2P networks, the content is transmitted directly from one peer to another without going through a server, and the content is used by an indeterminate number of users. Thus, for the P2P DRM system, the distribution of user rights is a challenge. Some works [14] attempts to get the tradeoff between security and content sharing efficiency by introducing the super peer that is responsible of rights issuing and user management. However, some other issues are still pending: deployment of rights management functions, preventing the distribution of copyright infringing content, preventing the registration of illegal content, and taking into account secondary distribution in managing.

Domain-based DRM. The concept of domain is firstly introduced in DVB-H CPCM, which denotes the set of DVB CPCM compliant devices. In fact, it is suitable for many scenarios with local content sharing, such as home

networks [15], campus networks, family networks, and social networks. Thus, the content or rights can be shared with the users during the domain, and even inter-domains. To realize these functionalities, some works need to be done, including the domain's modeling, interaction protocols, and business models.

Interoperable DRM. Most of the existing DRM systems focus on certain services or networks, and there are some conflictions between different DRM systems. From another perspective, popular ubiquitous multimedia services often request users or devices access different services or networks. Therefore, it is imperative to implement the interoperability between different DRM systems. The Digital Media Project (DMP) [16] proposes the interoperable DRM and defines the architecture and components that are compatible with existing DRM systems. However, the diversity of services, networks and DRM functionalities makes it a challenge.

4.2 Confidentiality protection

Multimedia encryption is the key technique to protect the content confidentiality, which transforms multimedia content into an unintelligible form. Generally, the content is encrypted with a cipher controlled by the key that aims to resist the eavesdropping attack.

4.2.1 Performance requirements of multimedia encryption

Due to multimedia content's properties (high redundancy, large volumes, real time interactions, and packaged into certain format) multimedia encryption algorithms often have some specific requirements, i.e., security, efficiency, compression ratio, format compliance and supporting direct operations.

- Security is the basic requirement of multimedia content encryption. Different from text/binary encryption, multimedia encryption requires both cryptographic security and perception security. The former one refers to the security against cryptographic attacks [17], and the latter one means that the encrypted multimedia content is unintelligible to human perception [18].
- Since real-time transmission or access is often required by multimedia applications, multimedia encryption algorithms should be efficient so that they don't delay the transmission or access operations.
- Multimedia encryption algorithms should not change compression ratio or at least keep the changes in a small range. This is especially important in wireless or mobile applications, in which the channel bandwidth is limited.
- Multimedia data are often encoded or compressed before transmission, which produces the data streams with some format information, such as file header, time tamp, file tail, etc. Encrypting the data except the format information will keep the encrypted data stream format-compliant.
- In some applications, it will save some cost to operate directly on the encrypted multimedia data. For example, the encrypted multimedia data can be recompressed, the bit-rate of the encrypted multimedia data can be controlled, the image block or frame can be cut, copied or inserted, etc.

4.2.2 Typical multimedia encryption algorithms

According to these requirements, partial encryption is often focused, which encrypts only parts of multimedia content, while leaving the other parts unchanged. According to the type of multimedia data, the existing partial encryption algorithms can be classified into audio encryption, image encryption and video encryption.

Audio encryption. Audio data are often encoded before being transmitted in order to save transmission bandwidth. Thus, audio encryption is often applied to the encoded data. For example, encrypting only the parameters of Fast Fourier Transformation (FFT) during speech encoding process [19] encrypts the speech data. In decryption, the right parameters are used to recover the encrypted data. For MP3 music, only the sensitive parameters of MP3 stream are encrypted, such as the bit allocation information [20]. For encrypting only few data, this kind of encryption algorithm is often of high efficiency.

Image encryption. A straightforward partial encryption algorithm for images is bit-plane encryption [21]. That is, in an image, only several significant bit-planes are encrypted, while the other bit-planes are left unchanged. By reducing the encrypted bit-planes, the encryption efficiency can be improved. However, the security cannot be confirmed, especially against replacement attacks. In replacement attacks, the encrypted data part is replaced by other data, which may make the encrypted image intelligible. For compressed images, the algorithms based on DCT and wavelet codecs attract more researchers, such as JPEG or JPEG2000. The algorithm proposed in [22] encrypts only some significant bit-planes of DCT coefficients, which obtains high perception security and encryption efficiency. The algorithm proposed in [23] encrypts only the significant streams in the encoded data stream, which is selected according to the progressiveness in space or frequency. Generally, no more than 20% of the data stream is encrypted, which obtains high efficiency. Another algorithm [24] encrypts different number of significant bit-planes of wavelet coefficients in different frequency bands, which obtains high security in human perception and keeps secure against replacement attacks.

Video encryption. Since video data are of larger volumes compared with image or audio data, video data are often compressed in order to reduce the bandwidth. Generally, the compressed video data stream is composed of such parts as format information, texture information and motion

information. Thus, according to the data parts, video partial encryption algorithms are classified into several types: format information encryption, frame encryption, texture encryption, and both motion vector and texture encryption.

Format information encryption. Since format information helps the decoder to recover the multimedia data, encrypting the format information will make the decoder out of work [25]. However, it is not secure in cryptographic viewpoint to encrypt only format information. This is because the format information is often in certain grammar, which can be broken by statistical attacks. These algorithms change the format information, and thus the encrypted multimedia data cannot be displayed or browsed by a normal browser.

Frame encryption. In such video codec as MPEG1/2/4, the frame is often classified into three types: I-frame, P-frame and B-frame. I-frame is often encoded directly with DCT transformation, while P/B-frame is often encoded by referencing to adjacent I/P-frame. Thus, I-frame is the referenced frame of P/B-frame. Intuitively, encrypting only I-frame will make P/B-frame unintelligible. However, experiments [25] show that this is not secure enough. The reason is that some macroblocks encoded with DCT transformation in P/B-frame are left unencrypted. For some videos with smart motion, the number of such macroblock is high enough to make the encrypted video intelligible. As an improved method, SECMPEG algorithm [26] encrypts all the macroblocks encoded with DCT transformation in I/P/B-frame. In these algorithms, the motion information is left unencrypted, which makes the motion track still intelligible.

Texture encryption. The coefficients in DCT or wavelet transformation determine the intelligibility of the multimedia data. Encrypting the coefficients can protect the confidentiality of the texture information. For example, the algorithm proposed in [27] encrypts the signs of DCT coefficients. In AVC codec, the intra-prediction mode of each block is permuted with the control of the key [28], which makes the video data degraded greatly. These algorithms are efficient in computing, but not secure enough. Firstly, the motion information is left unencrypted, which makes the motion track still intelligible. Secondly, the video can be recovered in some extent by replacement attacks [18].

Both motion vector and texture encryption. To keep secure, it is necessary to encrypt both DCT/wavelet coefficient and motion vector. Considering that these two kinds of information occupy many percents in the whole video stream, they should be encrypted partially or selectively. Generally, two kinds of partial encryption method are often used, e.g., coefficient permutation and sign encryption. For example, the algorithm [29] permutes coefficients or encrypts the signs of coefficients and motion vectors in DCT or wavelet transformation, and the algorithm [30] encrypts the DCT coefficients and motion vectors in AVC codec with sign encryption. These algorithms encrypt both the texture information and motion information, and thus, obtain high security in human perception. Additionally, the partial encryption operation, such as coefficient permutation or sign encryption, is often of low cost, which makes the encryption schemes of high efficiency. Furthermore, these partial encryption algorithms keep the file format unchanged.

4.2.3 Open issues in multimedia encryption

During the past decades, many algorithms have been reported for multimedia content encryption and they satisfy various applications. However, there are still some open issues.

Security analysis Due to the difference between multimedia encryption and traditional encryption, the security analysis methods may also be different. Taking partial encryption for example, not only such cryptographic attacks but also some ciphertext-only attacks (aims to recover the content intelligibility) should be considered, such as replacement attacks [31] and other unknown attacks. To the best of our knowledge, it is still difficult to get a suitable metric on the intelligibility of multimedia content, which increases the difficulty to analyze a partial encryption algorithm.

Communication-compliant encryption In practice, it is difficult to avoid transmission error or delay in multimedia communication. Thus, making the encrypted data robust to transmission error is necessary. Till now, few solutions have been reported. The segment encryption [30] is a potential solution. In this algorithm, the data stream is partitioned into segments, and then encrypted segment by segment, with each segment independently encrypted. However, it is still difficult to determine the size of the segment because segment size often contradicts the security.

Format independence or format compliance In order to keep format compliance, the encryption algorithm often varies with the compression codec. In some cases, format independence is more attractive. Taking Digital Rights Management (DRM) for example, it is required that all the content encoded with various codecs should be protected equally. Thus, there is a contradiction between format compliance and format independence.

4.3 Ownership protection

Watermarking technique [32] is used to protect multimedia content's ownership, which embeds the ownership information (e.g., the producer's name or ID) into multimedia content by modifying the content slightly. Later, the ownership information can be extracted and used for authentication. Generally, invisible watermarking that embeds the ownership information imperceptibly is often used for ownership protection, and it is also investigated here.

4.3.1 Performance metrics of watermarking

A good watermarking algorithm satisfies some performance metrics such as imperceptibility, robustness, capacity, security, oblivious detection, etc.

- *Imperceptibility* means that the watermarked content has no perceptual difference with the original one. It is also named 'transparency' or 'fidelity' and makes sure that the watermarked copy is still of high quality and commercial value.
- *Robustness* refers to the ability for the watermark to survive such operations including general signal processing operations (filtering, noising, A/D, D/A, re-sampling, recompression, etc.) and intentional attacks (rotation, scaling, shifting, transformation, tampering, etc.).
- *Capacity* denotes the maximal data volumes that can be embedded in multimedia content. Considering of transparency, the capacity of each approach is not infinite, which is in relation with the carrier content.
- The *security* against various attacks should be considered when constructing a watermarking algorithm. Generally, some encryption operations are introduced to watermarking algorithms in order to keep secure.
- *Oblivious detection* means that the detection process needs not the original copy. It is also named blind detection. On the contrary, non-blind detection means that the original copy is required by the detection process.

4.3.2 Existing watermarking algorithms

During the past decades, many watermarking algorithms have been reported, which can be classified by different methods. According to the carrier media type, they can be classified into image watermarking, video watermarking, audio watermarking, text watermarking and software watermarking. Among them, image watermarking embeds information in images based on images' redundancy and the perceptual property of human's eyes. For example, the algorithm proposed in [33] embeds information in perceptual imperceptible bits. Video watermarking makes use of temporal information besides spatial information compared with image watermarking. For example, the algorithm [34] embeds information in I-frames, which is similar to image watermarking, while the one [35] embeds information in motion vectors. Audio watermarking adopts audio redundancy and human psychoacoustic model to hide information. For example, the algorithm [36] uses the echo property to hide information. Text watermarking [37] hides information by slightly adjusting such textures as vertical distance, horizontal distance or font. This kind of watermarking is only suitable for texts but not for other data. Software watermarking [38] is used to protect software copyright and it is often classified into two categories: static watermarking and dynamic watermarking. Static watermarking embeds certain sentences in the source code, but does not change the software's functionality. Dynamic watermarking designs some dynamic information in the software, such as dynamic data structure or dynamic implementation tracking.

According to the embedding method, watermarking algorithms can be classified into three categories: replacement-based watermarking, modulation-based watermarking and encoding-based watermarking. Replacement-based watermarking replaces some parts of the cover work with watermarking. For example, the LSB method [39] replaces the least significant bits with the transmitted message directly. This kind of embedding method obtains high capacity, but it is seldom robust to attacks. Modulation-based watermarking [32] modulates the cover work with the message, and can realize either blind detection or non-blind detection. It is often robust to some attacks. Compared with the above two methods, encoding-based watermarking hides information by encoding some parts of the cover work. For example, Patchwork method [40] encodes watermarking into the relation between block pairs, the authentication watermarking [41] encodes watermarking into the relation between pixels. There are also some other algorithms such as histogram-based algorithm [42] and salient-point algorithm [43]. Although they are robust to some attacks, these encoding-based watermarking methods should be carefully designed based on the cover work's properties, and the capacity is often limited.

According to the embedding domain, watermarking can be embedded in either temporal domain, spatial domain or frequency domain. Taking video watermarking for example, the watermark can be embedded in the frame-pixels, the motion vectors or the DCT coefficients, which obtains different performances. Spatial domain watermarking embeds information in pixels directly, such as the LSB method [39] and the perceptual model based methods [44][45]. Generally, these methods are often not robust to signal processing or attack, although they are efficient in computing. Frequency domain Watermarking is embedded in transformation domain, such as DCT transformation [41], wavelet transformation [46], etc. Compared with the watermarking in spatial domain, the one in frequency domain obtains some extra properties in robustness and imperceptibility. Additionally, the embedding can be done during compression, which is compatible with international data compression standard. Temporal domain Watermarking is embedded in temporal information. For example, in audios, echo property is used to hide information, which is named echo hiding [36]. In videos, the temporal sequence is partitioned into static component and motive component, with information embedded into motive component [47]. Considering that human's eyes are more sensitive to static component than to motive one, embedding in motive component can often obtain higher robustness. However, error accumulation or floating makes the watermarked videos blurred in some extent, which should be improved by error compensation.

4.3.3 Open issues and hot topics in watermarking research

Watermarking is still not widely used in practical services because of some unsolved issues. Additionally, there are some interested topics need to be investigated.

Security of watermarking algorithms. It is still not confirmed whether watermarking algorithm should be kept secret against attackers. If so, it is different from cryptography system, and needs special security evaluation metrics. Otherwise, most of the existing watermarking algorithms are vulnerable to attacks.

Robustness to mixed operations. Some algorithms may be robust to certain operations, while they are still difficult to resist mixed operations, such as camera capture that consists of noise, rotation, transformation, scaling, etc.

Watermarking special carriers. For different carriers, the performance requirement is also different. For example, high-definition data permit little degradation, which needs the watermarking algorithm with high fidelity or transparency. Similarly, for such carrier as digital map or database, the watermarking should exit in everywhere of the carrier (each region in the map or each recorder in the database). These special requirements encourage the research of novel watermarking algorithms.

Web-based applications. Based on its potential applications in identification and authentication, watermarking may be applied in web-based applications such as access control, web monitoring, web-based identification or web based data linking, etc. Compared with traditional methods, watermarking does not make up extra storage, and is sometime imperceptible.

4.4 Traitor tracing

Multimedia content distribution often faces such a problem, i.e., a customer may redistribute the received content to other unauthorized customers. The customer who redistributes the content is called the traitor. This typical problem often causes great profit-losses of content provider or service provider. As a potential solution, digital fingerprinting [48] is recently reported and studied. It embeds different information, such as Customer ID, into multimedia content, produces a unique copy, and sends the copy to the corresponding customer. If a copy is spread to unauthorized customers, the unique information in the copy can be detected and used to trace the illegal redistributor.

4.4.1 Collusion attacks

The most serious threat to watermarking-based fingerprinting is collusion attack. That is to say, several attackers fabricate a new copy through combining their unique copies in order to avoid the tracing. Attackers intend to remove the embedded fingerprinting by making use of the slight difference between different copies. This kind of attack is often classified into two categories: linear collusion and nonlinear collusion. Among them, linear collusion means to average, filter or cut-and-paste the copies, while nonlinear collusion means to take the minimal, maximal or median pixels in the copies. Generally, five kinds of collusion attacks are considered, i.e., averaging attack, linear combinatorial collusion attack (LCCA) [49], min-max attack, negative-correlation attack and zero-correlation attack.

4.4.2 Existing digital fingerprinting algorithms

Since the past decade, finding new solutions resisting collusion attacks has been attracting more and more researchers. The existing fingerprinting algorithms can be classified into three categories, i.e., orthogonal fingerprint, coded fingerprint and warping-based fingerprint.

In orthogonal fingerprinting [50], the unique information (also named fingerprint) to be embedded is the vector independent from each other. For example, the fingerprint can be a pseudorandom sequence, and different fingerprint corresponds to different pseudorandom sequence. The orthogonal fingerprint can resist most of the proposed collusion attacks, which benefits from the orthogonal property of the fingerprints. According to the property of orthogonal sequence, such detection method as correlation detection is still practical although there is some degradation caused by collusion attacks. For example, the algorithm [50] produces orthogonal fingerprinting for each customer, the fingerprinting is then modulated by the cover video, and correlation detection is used to determine the ownership or colluders from the copies. For each copy, correlation detection obtains a big correlation value that determines the customer who receives the copy. For the colluded copy (e.g., averaging between N copies) the correlation value becomes R/N, which is smaller than the original correlation value R. Thus, if the correlation value R/N is still no smaller than the threshold T, the fingerprint can still be detected, otherwise, it cannot. In fact, the correlation value decreases with the rise of colluders. That is because the fingerprint is cross-affected by each other. In order to improve the detection efficiency, some detection methods are proposed, such as recursive detection (tree-based or correlation based) [51].

Fingerprinting can be carefully designed in codeword form, named coded fingerprinting [52][53], which can detect the colluders partially or completely. Till now, two kinds of encoding methods are often referenced: the Boneh-Shaw scheme [52] and the combinatorial design based code [53]. Boneh-Shaw scheme is based on the Marking Assumption, i.e., only the different bits are changed by colluders, while the same bits can not be changed. By designing the primitive binary code, at least one colluder can be captured out of up to c colluders. And it can support more customers if it is extended to outer code. Differently, in combinatorial design based anti-collusion scheme, the fingerprint acts as a combinatorial codeword. The combinatorial codes have the following property: each group of colluders' fingerprint produces unique codeword that determines

all the colluders in the group. The codeword is constructed based on combinatorial theory, such as AND-ACC (anti-collusion codes) or BIBD [53]. Compared with orthogonal fingerprinting, the coded fingerprinting has some advantages. Firstly, the embedding method is not only limited to additive embedding, some other existing embedding methods are also usable. Secondly, the correct detection rate does not depend on the number of colluders. However, with respect to LCCA attacks, the coded fingerprinting is not so robust. That is because the linear operation may remove the fingerprint information and make the fingerprint bit undetectable. In desynchronized fingerprinting [54], the multimedia content (e.g., image or video) is desynchronized imperceptibly with some geometric operations in order to make each copy different from others. This kind of fingerprinting aims to make collusion impractical under the condition of imperceptibility. That is, to de-synchronize the carrier. Thus, the colluded copy is perceptible (generates perceptual artifacts). These de-synchronization operations include random temporal sampling (video frame interpolation, temporal re-sampling, etc.), random spatial sampling (RST operations, random bending, luminance filtering or parameter smoothing) or random warping. In the warping-based fingerprinting, the original video copy is warped under the control of customer ID, which produces different copies with slight degradation. In collusion attacks, the colluded copy is degraded so greatly that it can not be used in high definitional applications. Additionally, the more the colluders, the more the degradation. According to this case, warping-based fingerprinting makes collusion attacks unpractical, and thus is secure against collusion attacks. However, in this scheme, the compression ratio is often changed because of the pre-warping operations. Additionally, it is a challenge to support large number of customers by warping the content imperceptibly.

4.4.3 Open issues and hot topics in digital fingerprinting

It is worth mentioning that the digital fingerprinting based traitor tracing is still a new topic, and there are some open issues.

Collusion-resistance and the supported users. The existing digital fingerprinting algorithms can not get the good tradeoff between collusion-resistance and the supported users. Some new fingerprinting algorithms with high robustness to collusion attacks and good performance in efficiency can be expected. Foexample, some fingerprinting codes based on random sequences [55][56] are reported having good performances although they are still not used in multimedia content.

Efficient fingerprinting embedding In secure multimedia content distribution based on digital fingerprinting, where (at sender side, in the mediate or at receiver side) to do the embedding operation is related to the system's efficiency [57]. Additionally, for different networks, e.g., unicasting, broadcasting, multicasting and P2P, different fingerprint embedding scheme will be considered.

Fingerprinting and DRM The fingerprinting based traitor tracing scheme can be combined with existing Digital Rights Management (DRM) systems in order improve the traceability. Where and how to introduce fingerprinting operations are still open issues.

4.5 Secure multimedia distribution based on watermarking

Considering that fingerprinting technology produces different media copy to different customer, it is easily implemented in unicast network. In contrast, it is difficultly implemented in broadcast or multicast network. The key points to be confirmed are the security and the efficiency. Till now, some distribution schemes based on digital fingerprinting have been proposed. These schemes can be classified into three types as shown in Figure 3.

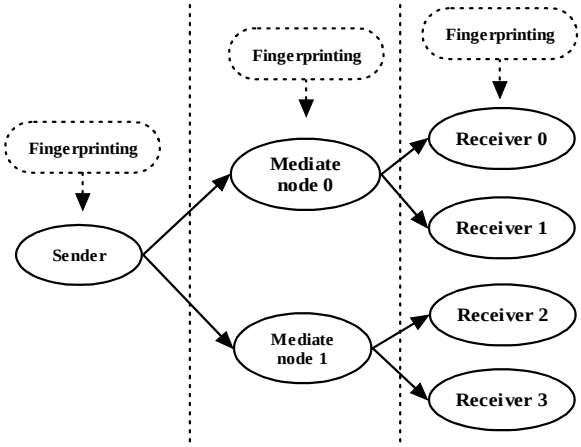


Figure 3: Watermarking - based multimedia distribution schemes

The first one [58] embeds the fingerprint and encrypts the fingerprinted media at the server side, and decrypts the media content at the customer side. In this scheme, for different customer, the media data should be fingerprinted differently, which increases the server's loading, and is not suitable for the applications with large number of customers. The second one [59] embeds the fingerprint and encrypts the fingerprinted media by the relay node, and decrypts the media at the customer side. This scheme reduces the server's loading greatly. However, the fingerprinting or encryption operation in relay node makes the network protocol not compliant with the original one. The third one [60] encrypts the media data at the server side, and decrypts the media and embeds the fingerprint at the customer side. This scheme reduces the server's loading greatly. However, for the decryption and fingerprinting operations are implemented at the customer side, the means to confirm the security is the key problem. To decrypt the media and embed the fingerprint independently is not secure, because the decrypted media data may be leaked out from the gap between the decryption operation and fingerprinting operation, as shown in Figure 4.

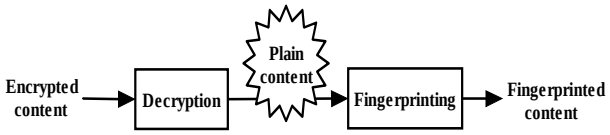


Figure 4: Leakage of multimedia content

4.5.1 Embedding Fingerprint at Sender Side

Straightforwardly, multimedia content is firstly fingerprinted, then encrypted, and finally distributed by the sender. These schemes [58] obtain high security since they forbid customers fingerprinting multimedia content. However, they need to transmit different copy to different customer, which cost much time or transmission bandwidth. To solve this problem, some improved schemes have been reported, such as broadcasting encryption and partial fingerprinting.

Broadcasting Encryption. In the broadcasting encryption based method [61], media data are partitioned into segments, each segment is watermarked into two copies, and all the segments are encrypted and distributed. At the receiver side, a key is used to select one segment from the couple segments, and different key selects different segments that produce different media copy. In this scheme, traditional ciphers can be used, which keeps the system's security. However, the key disadvantage is that double volumes need to be transmitted.

Partial Fingerprinting. In the partial fingerprinting method [62], media data are partitioned into two parts, e.g., encryption part and fingerprinting part. Among them, the former one is encrypted and broadcasted to different customers, while the latter one is fingerprinted and unicasted to each customer. Since only a small part of multimedia content is unicasted, the time cost or bandwidth cost can be reduced greatly. The difficulty is to make the two kinds of communication modes work together simultaneously.

4.5.2 Joint Fingerprint Embedding and Decryption (JFD)

To obtain a tradeoff between security and efficiency, some schemes [63][64][65][66] are proposed to joint fingerprint embedding and decryption (JFD). In these schemes, the fingerprint is embedded into media content during decryption process, which produces the fingerprinted media copy directly, thus avoids the leakage of plain media content and improves the security of embedding fingerprint at the customer side.

Chamleon Method. The Chamleon method [63] firstly encrypts the media data at the server side, then distributes the media data, and finally, decrypts the data by modifying the least significant bits under the control of different decryption key. Here, the encryption and decryption processes use different key tables, respectively. It was reported that the scheme is time efficient and secure against cryptographic attacks. However, for different customers, different key tables should be transmitted, which cost bandwidth. Additionally, the least significant bits are not robust to signal processing, such as recompression, additive noise, filtering, etc.

Kundur's Method. The JFD scheme proposed in [64] firstly encrypts the media data partially at the server side, then distributes the data, and finally, decrypts the data by recovering the encrypted parts selectively. The position of the unexplored parts determines the uniqueness of a media copy. Here, the DCT coefficients' signs are encrypted. The scheme is robust to some operations including slight noise, recompression and filtering, while the imperceptibility can not be confirmed, the encrypted media content is not secure in perception and the security against collusion attacks cannot be confirmed.

Lian's Method. The scheme proposed in [65] encrypts media data at the server side by encrypting the variable-length code's index, and decrypts media data at the customer side by recovering code's index with both decryption and fingerprinting. The scheme is secure against cryptographic attacks, while the robustness against some operations including recompression, filtering and adding noise, cannot be confirmed.

Lemma's Method. The scheme proposed in [66] encrypts media data at the server side by partial encryption, and decrypts media data at the customer side with a new key stream. The scheme is robust against signal processing, which benefits from the adopted watermarking algorithms, while the security against cryptographic attacks cannot be confirmed. Additionally, the transmission of key stream costs much time and space.

4.5.3 Open issues in this topic

Clearly, the watermarking-based multimedia distribution is still a new topic, and there are some open issues, which must be considered.

Security of partial fingerprinting. For the schemes embedding fingerprinting at sender side, the multiple content copies need to be transmitted from the sender to the receiver. Partial fingerprinting can reduce the repeated transmission costs. However, the security of partial fingerprinting scheme needs to be investigated.

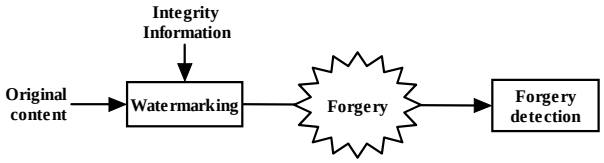
Interference between fingerprinting and encryption. In JFD schemes, the suitable fingerprinting operation and encryption operation should be considered in order to reduce the interference between them. For example, the homomorphic encryption and fingerprinting operations are potential.

Key distribution. In these schemes, different customers use different keys to decrypt the content. Some means are required to realize secure and efficient key distribution or exchange. This depends on the application environment, such as unicasting network, multicasting network, broadcasting network or P2P network, etc. Additionally, some other research directions are also attractive such as efficient broadcasting encryption, partial encryption based content distribution, combined encryption and watermarking, and so on.

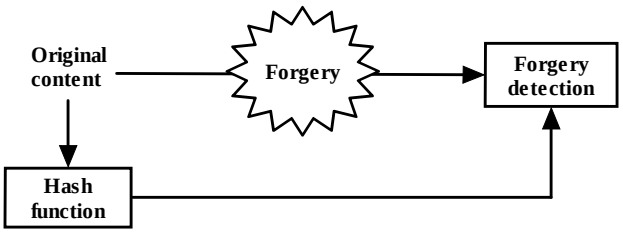
4.6 Forgery detection

4.6.1 General forgery detection schemes

Forgery detection aims to tell whether the multimedia content is authentic without forgery operations. Till now, several means have been proposed to detect forgeries, i.e., watermarking based scheme [32], perceptual hash based scheme [67], and multimedia forensic based scheme [68]. In the first one, as shown in Figure 5(a), the watermark information (e.g., integrity flag or ownership) is embedded into multimedia content imperceptibly. This embedding operation is realized during multimedia content generation (e.g., in the camera). In forgery detection, the embedded information is extracted from the operated multimedia content and compared with the original information. The comparison result tells whether the image is forged or not and even localizes the tampered regions. There are two apparent disadvantages for this scheme. Firstly, the embedding operation is needed during media generation, which is often unavailable in practical applications. Secondly, the information embedding operation degrades multimedia content's quality, which is not permitted in some applications.



(5a) Watermarking-based forgery detection scheme



(5b) Hash-based forgery detection scheme

(5c) Multimedia forensic-based forgery detection scheme

Figure 5: Various forgery detection schemes

In the second one, as shown in Figure 5(b), the perceptual hash function is applied to multimedia content, which generates the hash value composed of a certain-length string. The hash value is stored by the authenticator. In forgery detection, a new hash value is computed from the operated multimedia content, and compared with the stored one. The comparison result tells whether the content is forged or not. Similar with the watermarking based scheme, the hash based scheme realizes the hash computing operation during multimedia content generation, e.g., in the camera. The difference is that the hash value does not change the multimedia content. Similarly, the disadvantage is that the hash computing operation implemented during media generation is not always available in practical applications.

In the third one, as shown in Figure 5(c), the intrinsic features are extracted from the operated multimedia content, then, the features' properties are analyzed and compared with a common threshold, and the comparison result tells whether the content is forged or not. The extracted intrinsic features have apparent difference between the natural one and the forged one, and the difference can be distinguished by the threshold. The core technique in this scheme is to extract the distinguishable features. Generally, it depends on the model of the forgery operation, and different features will be extracted for different forgery operations. Different from the former two schemes, the forensic based scheme does not need the original media content, and neither changes the quality of media content.

4.6.2 Existing forgery detection methods based on multimedia forensics

Under the condition without pre-processing, only forensic methods can be used to detect the forgery. These forensic methods extract the features that can distinguish the original media and operated one. Generally, there are some forgery detection methods based on special features, i.e., correlation feature, double compression feature, light feature, and media statistical feature, and some methods with special functionalities, e.g., duplication detection.

Correlation based detection. Some correlations between adjacent temporal or spatial sample pixels are often introduced during multimedia content generation or content operations. From the multimedia content, these correlations can be detected and used to identify forgeries, e.g., resample [69] and color filter array interpolation [70]. These forgery detection methods can detect either the image's authentic or the image regions' authentic. However, they work with the assumption that the images are firstly interpolated during image generation and then modified during image forgery. Thus, they are not robust again re-interpolation attacks.

Double compression detection. In multimedia content forgery, the edition software often stores the content in compression formats, e.g. JPEG or MPEG2. Thus, the forged multimedia content may be recompressed. Intuitively, recompression introduces different distortions compared with once compression, which can be used to detect whether the multimedia content is recompressed [71]. Thus, if an image is recompressed, the probability of forgery is increased. The method's disadvantage is the vulnerability to attacks. For example, if the modified JPEG image is cropped before being saved in JPEG format, the periodicity of distortion is difficult to be detected.

Light property based detection In practice, the captured picture conforms to certain light direction. Suppose there is only a point light corresponding to the picture's scene, then the estimated light directions for all the objects in the picture should intersect to a point. Differently, if one object in the picture is tampered, the estimated light direction of the object will be inconsistent with other objects' light directions. Thus, by detecting the light directions, the image forgery can be detected [72]. This method can detect either the image's authentic or the image objects' authentic. Its computational complexity and robustness depend on the adopted light direction estimation methods.

Feature-based detection. With respect to the different generation processes of a natural image and the forged image, there are some specific image features, which can exhibit the difference such as the high-order statistical feature, the sharpness/blurriness, and feature fusion and classifier fusion. These features can be used to detect forgeries [73]. This method can detect whether a media region is forged or not. The challenge is how to design the optimal strategy for selecting the features or classifiers.

Duplication detection In multimedia forgery, duplication is one of the often used tampering operations. Till now, there are various duplication detection methods, i.e., direct detection and segmentation based detection. Direct detection means to detect the duplicated regions directly without any information about the regions, e.g., DCT domain sorting [74]. Segmentation based detection means to detect the duplicated objects after segmentation [75]. These methods can detect an image object's authentic, including the object deletion, healing or duplication.

4.6.3 Open issues in forensic based forgery detection

According to the above investigation, multimedia forensic-based forgery detection is still at the beginning, and there are some open issues.

Detection accuracy For the existing forgery detection methods, the correct detection accuracy is still not good enough for practical applications. One important reason is the natural media's diversity. There are so many media sources and media contents that make it difficult to design a fixed classifier or decision threshold.

Counter attacks Sometimes, it is easy to detect a single forgery operation. However, in practice, there are often more than one forgery operations on the same media content, which may reduce the detection accuracy because of the interference between different operations. Additionally, some high-level attackers may make the forgery by considering of the means to counter the forgery detection methods. In the existing detection methods, the attacks are seldom considered.

Video Forgery With the advancement of video edition software, video forgery becomes more and more popular. But video forgery detection is seldom considered. Compared with image forgery, video forgery has an additional dimension, i.e., the temporal space. Thus, some new detection methods focusing on video forgery are expected.

Test bed. Up till now, no public tests are done for forgery detection, which delays the steps to practical applications. It is caused by the shortage of a general test bed. The test bed will contain a multimedia content database and be capable of evaluating various performances, including detection accuracy, robustness and security.

4.7 Copy detection

Recently, the concept of content-based copy detection (CBCD) [76] has been proposed as an alternative means of identifying illegal media copies. Given an image registered by the owner, the system can determine whether near-replicas of the image are available on the Internet or through an unauthorized third party. If it is found that an image is registered (i.e., it belongs to a content owner), but the user does not have the right to use it, the image will be deemed an illegal copy. The suspect image is then sent to the content owner for further identification and a decision about taking legal action against the user. Image copy detector searches for all copies of a query image, and is different from content-based image retrieval (CBIR) [77] that searches for similar images. Thus, it is not usually feasible to apply existing CBIR techniques to CBCD because they may cause a considerable number of false alarms. For CBCD, the key challenge is to extract the suitable features that can obtain a good tradeoff between discriminability and robustness. The discriminability denotes the ability to distinguish different media contents. The robustness refers to the ability to survive such operations as cropping, noising, contrast changing, zoom, insertion, etc. Generally, the extracted features are compared with the registered ones, whose distance tells the repetition.

4.7.1 Existing copy detection algorithms

According to the methods that extract features, the CBCD algorithms can be classified into two types: global feature-based algorithms, and local feature -based algorithms. For example, the algorithm in [78] extracts the global features from wavelet transformed coefficients and colour space, the one in [79] extracts the ordinal measure of DCT coefficients from the whole image, the one in [80] uses elliptical track division strategy to extract features from all the elliptical track blocks, and the one in [81] uses a sliding window to extract the block's relationship with its neighbouring blocks. These global feature-based algorithms often obtain good discriminability, while bad robustness. For example, they are not robust to such operations as block cropping. Differently, local feature-based algorithms have better robustness. For example, the algorithm in [82] computes many descriptors for each image, in which, each descriptor corresponds to one image block, and the algorithm in [83] extracts the key points from

each image part. They can still identify the content even when it is tampered (e.g., cropped or modified) greatly. Their disadvantage is the high computational complexity, and the research challenge is how to determine the block size.

4.7.2 Open issues

The CBCD research is at the beginning, and there are some open issues. Firstly, the operations to be resisted need to be defined, and thus, the various CBCD algorithms can be evaluated. Secondly, the tradeoff between discriminability and robustness needs to be investigated. No existing algorithms can obtain good level in both the performances. For example, the algorithms with local features have more computational costs but present interesting results in term of robustness, while the ones with global features are very efficient for small transformations. Thirdly, for practical applications (e.g., over Web), some means should be taken into consideration to enable the algorithm running in real-time. For example, the feature extraction and comparison operations need to be fastened, and a larger set of queries should be built to support large number of users.

4.8 Privacy-preserving data mining

Privacy preserving data mining [84] is a novel research direction in data mining and statistical databases. The main consideration in privacy preserving data mining is two fold. First, sensitive raw data, e.g., identifiers, names and addresses, should be modified or trimmed out from the original database, in order for the recipient of the data not to be able to compromise another person's privacy. Second, sensitive knowledge, which can be mined from a database by using data mining algorithms should also be excluded. In privacy preserving data mining, the main objective is to develop algorithms for modifying the original data in some way, so that the private data and private knowledge remain private even after the mining process.

4.8.1 Existing privacy-preserving data mining techniques

In general, data modification is used in order to modify the original values of a database that needs to be released to the public and in this way to ensure high privacy protection. Needless to say that a data modification technique should be in concert with the privacy policy adopted by an organization. Methods of modification include perturbation, blocking, aggregation or merging, and sampling. In the privacy preservation technique, selective modification that leaves some information unchanged is required in order to achieve higher utility for the modified data given that the privacy is not jeopardized. Until now, various techniques have been reported, which can be classified into three types: heuristic-based techniques, cryptography-based techniques and reconstruction-based techniques.

Heuristic-based techniques (e.g., adaptive modification) modify only selected values that minimize the utility loss rather than all available values. The values in data mining include association rule, classification rule, etc. For example, the association rule is confused by the centralized data perturbation [85] or by the centralized data blocking [86], and the classification rule is confused by the centralized data blocking [87]. These techniques are often efficient in implementation, while their security depends on the adopted modification methods.

Cryptography-based techniques use secure multiparty computation to realize private data mining. In secure multiparty computation, two or more parties want to conduct a computation based on their private inputs, but neither party is willing to disclose its own output to anybody else. The key-point here is how to conduct such a computation while preserving the privacy of the inputs. Thus, a computation is secure if at the end of the computation, no party knows anything except its own input and the results. For example, the method is proposed to mine private association rules from vertically partitioned data [88], the method to mine private association rules from horizontally partitioned data [89], and the method to induct private decision tree from horizontally partitioned data [90]. These techniques can obtain enough security benefiting from secure computation. But, actually, because of the nature of this solution methodology, the data in all of the cases that this solution is adopted, is distributed among two or more sites.

Reconstruction-based techniques firstly perturb the data, and then reconstruct the data's distributions at an aggregate level in order to perform data mining. Thus, the original distribution of the data is reconstructed from the randomized data. For example, the numerical data (e.g., individual records) can be perturbed and then reconstructed by estimation [91], and the binary or categorical data (e.g., association rules) are randomized and reconstructed in [92]. For these techniques, the successful reconstruction operations determine the performance of data mining.

4.8.2 Open issues

Obviously the privacy-preserving data modification results in degradation of the database performances, such as the confidential data protection, the loss of mining functionality and the communication cost. Till now, no existing techniques outperform all the others on all the performances. For example, cryptography-based techniques have better confidential data protection, while they limit some mining functionalities and needs high cost for information exchange between different sites. As a result, better techniques are expected to obtain the good tradeoff between different performances.

4.9 Secure user interface

In multimedia information systems, various secure user interface methods [93] have been widely used, which prevent or authorize the users to access services. According to the information carriers, they can be classified into three types, i.e., possession-based method, knowledge-based method and biometrical method. Possession-based method uses the specific "token", such as a security tag or a card, to realize authorization. Knowledge-based method uses a code or password to authenticate the users. Biometrical method uses the biometrics to identify specific people by certain characteristics. Biometrics can overcome the weakness in traditional authentication systems that use tokens, passwords or both. Weakness, such as sharing passwords, losing tokens, guessable passwords, forgetting passwords and a lot more, were successfully targeted by biometric systems. Biometric characteristics can be divided in two main classes: physiological characteristics and behavioural characteristics. Among them, the former ones are related to the shape of the body, such as fingerprint, face, hand, iris and DNA, while the latter ones are related to the behavior of a person such as signature, keystroke dynamics and voice. The typical biometrical methods being widely used include fingerprint recognition, face recognition, hand geometry, iris recognition, speaker recognition, etc.

4.9.1 Biometric system

A biometric system is often composed of the following components [93]: template storage, sensor, pre-processing, feature extractor, template generator, matcher and application device. Generally, it works as following steps. First, the templates corresponding to persons are stored in a database. Then, the sensor is used to acquire all the necessary data, i.e., face photo, fingerprint photo, speech samples, etc. The acquired data are then pre-processed to remove sensor artifacts, e.g., removing background noise. Then, some features are extracted from the sensor data, and used to create a template. The obtained template is then passed to a matcher that compares it with other existing templates, and the comparison result will be output for driving the application device. Generally, a biometric system can provide two functions [94], i.e., verification and identification. The former one authenticates its users in conjunction with a smart card, username or ID number. The biometric template captured is compared with that stored against the registered user either on a smart card or database for verification. The latter one authenticates its users from the biometric characteristic alone without the use of smart cards, usernames or ID numbers. The biometric template is compared to all records within the database and a closest match score is returned.

4.9.2 Existing biometric systems

For biometric systems, their performances are often measured by two errors, i.e., False Rejection Rate (FRR) and False Acceptance Rate (FAR) [95]. FRR denotes the probability to reject the match mistakenly, while FAR denotes the one to accept the match mistakenly. Now, some biometric systems can obtain good performances. For example, the face recognition system in [96] can get the 1% FAR and 10% FRR, the fingerprint recognition system in [97] can get 1% FAR and 0.1% FRR, and the hand geometry recognition system in [98] can get 2% FAR and 0.1% FRR. Additionally, some other performances are also cared, including the ease of acquisition for measurement, the permanence against aging, the authentication speed, and ease of use of a substitute, etc. It is reported that, among the various biometrics (e.g., face, fingerprint, hand geometry, keystrokes, hand veins, iris, retinal scan, signature, voice, facial thermograph, odor, DNA, gait and ear canal), fingerprint, hand geometry, hand veins, iris, facial thermograph and ear canal can obtain the better tradeoff in various performances.

4.9.3 Open issues

A biometric system cannot always give provable results because of biometrics' complex properties such as variability. A solution is multi-mode authentication [94] that means either to combine several biometrics or to combine various authentication methods (i.e., possession-based method, knowledge-based method and biometrical method). Additionally, cancellable biometrics is also a hot topic, which is a way to inherit the protection and the replacement features of biometric data more seriously [99]. It is very essential for protecting biometrics in storage or in processing state.

4.10 Intrusion detection and prevention

In multimedia information system, intrusion detection [100] is the act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a resource. The system performing automated intrusion detection is called an Intrusion Detection System (IDS). An IDS can be either host-based, if it monitors system calls or logs, or network-based if it monitors the flow of network packets. Modern IDSs are usually a combination of these two approaches. When a probable intrusion is discovered by an IDS, typical actions to perform would be logging relevant information to a file or database, or generating an email alert. These automatic actions can be implemented through the interaction of Intrusion Detection Systems and access control systems such as firewalls. If intrusion detection takes a preventive measure without direct human intervention, then it becomes an intrusion-prevention system (IPS).When an attack is detected, it can drop the offending packets while still allowing all other traffic to pass. Generally, it is a network security device that monitors network and system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities. For example, a host-based IPS (HIPS) [101] is one where the intrusion-prevention

application is resident on that specific IP address, usually on a single computer. Differently, Network-based IPS (NIPS) [102] will operate in-line to monitor all network traffic for malicious code or attacks. Now, there are exist three kinds of NIPS, i.e., Content-Based IPS (CBIPS) that inspects the content of network packets for unique sequences, detects and prevents known types of attack such as worm infections and hacks, Protocol Analysis based IPS that natively decodes application-layer network protocols and evaluates different parts of the protocol for anomalous behavior or exploits, or Rate-Based IPS (RBIPS) that monitors and learns normal network behaviors and intends to prevent Denial of Service attacks.

The intrusion detection or prevention technology is immature and dynamic. For example, the accuracy and adequacy of IDS signatures cannot be determined [103]. The proprietary nature of the signatures for most commercial intrusion detection systems makes a detailed discussion of their accuracy and adequacy difficult. This may be adequate for very simple attacks, but are probably inadequate for sophisticated, multi-stage attacks. Additionally, it is necessary to identify unknown modes of attack continuously. Generally, intrusion detection systems can match patterns of behavior that represent signatures of known attacks, while difficult to recognize new attack strategies. The adaptive approaches are expected to solve this problem. Furthermore, intrusion detection systems could provide evidence to support prosecution in court but do not. With the rapidly growing theft and unauthorized destruction of computer-based information, the frequency of prosecution is rising, and it is urgent to use computer forensics to analyze the evidence provided by intrusion detection or prevention systems.

4.11 Performance comparison of different technical solutions

Actually, different technical solutions solve different security issues. The ten solutions mentioned above and their targeted security issues are listed in Table 1. As it can be seen, no solution can solve all the security issues. Thus, in practice, more than one solution is used together. For example, to provide a secure video-on-demand service over Internet, both Digital Rights Management technique and intrusion detection and prevention technique are used. Whether to or how to compound them together depends on the corresponding multimedia service system and its performance requirements.

Table 1: Targeted security issues of different technical solutions

Technical solutions	Targeted security issues				
	Eavesdropping	*Intrusion*	*Forgery*	*Piracy*	*Privacy*
Digital Rights Management	√			√	√
Confidentiality protection	√				
Ownership protection				√	
Traitor tracing				√	
Secure multimedia distribution based on watermarking	√			√	
Forgery detection			√		
Copy detection				√	
Privacy-preserving data mining					√
Secure user interface		√	√		
Intrusion detection and prevention		√			

5 Open issues and hot topics

In the previous section, we reconsidered some typical solutions for multimedia information system security. However, there are some other solutions, which focus on special applications. As various multimedia information systems are emerging, some new solutions are expected. Hereafter, we describe some of the interesting trends.

Trusted computing

Trusted Computing (TC) [104] is recently proposed to construct a fully trusted system. It aims to solve the security issues caused by software-only means, which enforces the trusted behavior by loading the hardware

with a unique ID and key. With Trusted Computing, the computer will consistently behave in specific ways, and those behaviors will be enforced by hardware and software. Generally, it will have the following components, i.e., endorsement key, secure input and output, protected execution, sealed storage, and remote attestation. Although it may cause consumers to lose anonymity in online interactions, it is regarded as a possible enabler for future versions of mandatory access control, copy protection, and digital rights management.

Steganography

Steganography [105] is used as a covert communication method, which hides secret information into multimedia content and thus sends it to receivers imperceptibly. Only the receiver partnered with the sender can extract the secret information from multimedia carrier. Different from watermarking, the third party can only detect whether the multimedia content is suspicious or not (i.e., steganalysis), and then decide whether to remove it. Better steganography algorithms are expected to resist the latest steganalysis methods.

Security in network or service convergence

Ubiquitous multimedia services are becoming more and more popular, and often converge several networks or services together. The challenge includes not only the exchange of network protocols, the bit-rate adaptation of multimedia content and the compliance of user terminals but also the security architecture covering all the involved networks. Interoperable DRM is not the only solution. The recent work reported in [106] shows that some potential application scenarios need to be investigated.

Security of content sharing in social networks

Nowadays, content sharing social networks enrich human being's life. Some typical networks include Blog, Video Blog, P2P sharing platforms, etc., where users can upload or post multimedia content freely. However, it is noted that, more and more unhealthy contents arise in these networks, e.g., the content related to legality, sex, privacy, piracy or terror. To detect, distinguish or prevent these contents' distribution is a new topic [107]. Some content analysis and classification techniques need to be used together with existing security solutions.

Privacy-preserving data processing

Privacy-preserving data mining addresses the necessary to protect privacy in data retrieval. However, it is now also urgent in other fields, such as multi-party interaction, remote diagnosis, content distribution [108], etc. Thus, the new protocols or operations need to be investigated, which aims to the new applications. The new technique, named signal processing in encryption domain [109], attempts to give a general solution by adopting homomorphic encryption and signal processing operations. It is still at the beginning.

Multimedia forensics

In Section 4, we review the forensicbased forgery detection techniques. However, multimedia forensics includes more valuable techniques, e.g., media source distinguish technique and device identification technique [110]. The former one denotes the technique to distinguish the devices (camera, scanner, cell phone, computer, etc.) that generate the multimedia content by investigating the content's properties. Differently, the latter one not only distinguishes the device type, but also identifies the device itself. These techniques may be useful to support prosecution in court.

Intelligent surveillance

Surveillance is now widely used in public security. With the increase of distributed surveillance cameras and collected data volumes, intelligent surveillance [111] becomes more and more urgent, as it processes the multimedia data automatically to extract usable information. The typical intelligent processing techniques include object tracking, activity analysis, crime detection, face extraction, etc. Generally, various basic techniques are required, such as video segmentation, semantic analysis, machine learning, etc.

6 Conclusions

In this paper, we introduced a general architecture of multimedia information system and addressed some important security issues. We reviewed some typical technical solutions, and proposed some hot research topics. The paper is expected to provide valuable directions to researchers working in multimedia information system security. Due to the diversity of multimedia information systems, the security issues and solutions are various and it is difficult to be included in one paper. Therefore, in this paper we considered only some important security issues such as: eavesdropping, intrusion, forgery, piracy and privacy, and reviewed only some typical solutions such as Digital Rights Management (DRM), confidentiality protection, ownership protection, traitor tracing, secure multimedia distribution based on watermarking, forgery detection, copy detection, privacy-preserving data mining, secure user interface, and intrusion detection and prevention. As more and more multimedia information systems arise, new security issues will be generated. We are inclined to the fact that the research community will solve emerging security issues by proposing novel approaches. For this reason, in the near future we will update this survey by adding the new issues and solutions.

7 Acknowledgement

The work was partially supported by Crypto project through the grant code of ILAB-PEK08-006

8 References

[1] M. C. Angelides and S. Dustdar. *Multimedia Information Systems* (The Springer International Series in Engineering and Computer Science), by Publisher: Springer, June 30, 1997.

[2] S. M. Rahman. *Design and Management of Multimedia Information Systems: Opportunities and Challenges*, Publisher: IGI Global, April 16, 2001.

[3] B. Thuraisingham. Security and privacy for multimedia database management systems, *Multimedia Tools and Applications*, 33(1): 13-29, April 2007.

[4] B. Thuraisingham. *Multimedia systems security*. Proceedings of the 9th *ACM workshop on Multimedia & Security*, Dallas, Texas, USA, Pages: 1-2, 2007.

[5] *Intrusion detection system*. http://en.wikipedia.org/wiki/Intrusion_detection_system.

[6] *Digital Rights Management*. http://en.wikipedia.org/wiki/Digital_rights_management.

[7] ISMACryp 2.0 (ISMA Encryption & Authentication Specification 2.0). http://www.isma.tv/.

[8] Open Mobile Alliance, Digital Rights Management 2.0 (OMA DRM 2.0), 03 Mar 2006.

[9] *Digital Video Broadcasting Content Protection & Copy Management* (DVB-CPCM), DVB Document A094 Rev. 1, July 2007.

[10] *HDCP (High-bandwidth Digital Content Protection System),* http://en.wikipedia.org/wiki/HDCP.

[11] *COPP (Certified Output Protection Protocol),* http://msdn2.microsoft.com/en-us/library/Aa468617.aspx

[12] *DTCP (Digital Transmission Content Protection),* http://en.wikipedia.org/wiki/DTCP

[13] W. Li. Overview of fine granularity scalability in MPEG-4 video standard, *IEEE Transactions on Circuits and Systems for Video Technology*, 11(3): 301-317, 2001.

[14] J. Y. Sung, J. Y. Jeong, and K. S. Yoon, "DRM Enabled P2P Architecture," 2006 *International Conference on Advanced Communication Technology (ICACT2006)*, pp. 487-490, 2006.

[15] J.-P. Andreaux, A. Durand, T. Furon, and E. Diehl, "Copy Protection System for Digital Home Networks," *IEEE Signal Processing Magazine*, March 2004, pp.100-108.

[16] *DMP - Digital Media Project* (http://www.dmpf.org/)

[17] R. A. Mollin, *An Introduction to Cryptography*. CRC Press. 2006.

[18] S. Lian, J. Sun, G. Liu, and Z. Wang. Efficient video encryption scheme based on advanced video coding, *Multimedia Tools and Applications*, Springer, 38(1): 75-89, 2008.

[19] S. Sridharan, E. Dawson, and B. Goldburg. Fast Fourier transform based speech encryption system. *IEE Proceedings of Communications, Speech and Vision*, 138(3): 215-223, 1991.

[20] L. Gang, A. N. Akansu, M. Ramkumar, X. Xie. Online Music Protection and MP3 Compression. In Proc. Of *Int. Symposium on Intelligent Multimedia, Video and Speech Processing*, May 2001, pp.13-16.

[21] M. Podesser, H. P. Schmidt, and A. Uhl, "Selective bitplane encryption for secure transmission of image data in mobile environments," In CD-ROM Proceedings of the *5th IEEE Nordic Signal Processing Symposium* (NORSIG 2002), Tromso-Trondheim, Norway, October 2002.

[22] R. Pfarrhofer and A. Uhl. Selective image encryption using JBIG. In *Proceeding of 2005 IFIP Conference on Communications and Multimedia Security*, pp. 98-107, 2005.

[23] R. Norcen and A. Uhl, "Selective encryption of the JPEG2000 bitstream," IFIP International Federation for Information Processing, *LNCS 2828*, pp. 194-204, 2003.

[24] S. Lian, J. Sun, D. Zhang, and Z. Wang. A selective image encryption scheme based on JPEG2000 Codec. *2004 Pacific-Rim Conference on Multimedia (PCM2004)*, Springer *LNCS, 3332*, 65-72, 2004.

[25] I. Agi and L. Gong. An empirical study of MPEG video transmissions. In *Proceedings of the Internet Society Symposium on Network and Distributed System Security*. San Diego, CA, Feb. 1996, pp. 137-144.

[26] L. Tang. Methods for encrypting and decrypting MPEG video data efficiently. In Proceedings of the Fourth *ACM International Multimedia* Conference (ACM Multimedia'96). Boston, MA, November 1996, pp. 219-230.

[27] C. Shi, and B. Bhargava. A fast MPEG video encryption algorithm. In Proceedings of the *6th ACM International Multimedia Conference*. Bristol: UK, September, 1998, pp. 81-88.

[28] J. Ahn, H. Shim, B. Jeon, and I. Choi. Digital Video Scrambling Method Using Intra Prediction Mode. 2004 Pacific-Rim Conference on Multimedia (PCM2004), Springer, *LNCS Vol.3333*, pp.386-393, November 2004.

[29] W. Zeng and S. Lei. Efficient frequency domain selective scrambling of digital video. *IEEE Trans on Multimedia*, 5(1): 118 –129, March 2003.

[30] S. Lian, Z. Liu, Z. Ren, and H. Wang. Secure advanced video coding based on selective encryption algorithms. *IEEE Transactions on Consumer Electronics*, 52(2): 621-629, 2006.

[31] S. Lian. *Multimedia Content Encryption: Techniques and Applications*. Auerbach Publication, Taylor & Francis Group, 2008.

[32] I. J. Cox, M. L. Miller and J. A. Bloom, *Digital Watermarking*, Morgan-Kaufmann, San Francisco, 2002.

[33] M. Wu, E. Tang, and B. Liu, Data hiding in digital binary images, In Proc. *IEEE Int'l Conf. on Multimedia and Expo*, Jul 31-Aug 2, 2000, New York, NY, 393-396.

[34] S. Bounkong, B. Toch, D. Saad, and D. Lowe, ICA for watermarking digital images, *Journal of Machine Learning Research*, 4(7-8): 1471-1498, 2004.

[35] Y. Bodo, N. Laurent, and J. Dugelay, Watermarking video, hierarchical embedding in motion vectors, *IEEE International Conference on Image Processing*, Spain, 14-17 Sept. 2003, vol. 2, pp. 739-742.

[36] D. Gruhl, A. Lu, and W. Bender, *Echo Hiding, Pre-Proceedings: Information Hiding*, Cambridge, UK, 1996, pp. 295-316.

[37] N. F. Maxemchuk, and S. H. Low. Performance comparison of two text marking methods, *IEEE Journal on Selected Areas in Communications*, 16(4): 561-572, May 1998.

[38] C. S. Collberg, and C. Thomborson, "Software watermarking: models and dynamic embeddings," In Proc. *ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL99),* San Antonio, Texas, 1999, pp. 311-324.

[39] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, A digital watermark, *Proc. of the IEEE Int. Conf. on Image Processing*, Vol. 2, pp. 86–90, Austin, Texas, Nov. 1994.

[40] W. Bender, D. Gruhl, N. Morimoto, and A. Lu. Techniques for data hiding, *IBM systems Journal*, 35(3-4): 313-316, 1996.

[41] D. Ye, Y. Mao, Y. Dai, and Z. Wang. A multi-feature based invertible authentication watermarking for JPEG Images, Proceedings of the *3rd International Workshop on Digital Watermarking (IWDW2004)*, Seoul, Korea, Oct. 2004, pp. 152-162.

[42] D. Coltue, and P. Bolon, "Watermarking by histogram specification," In Proc. SPIE Electronic Imaging'99, *Security and Watermarking of Multimedia Contents*, San Jose, 1999, pp. 252-263.

[43] P. M. Rongen, M. B. Macs, and C. Overveld, Digital image watermarking by salient point modification, In Proc. *SPIE Electronic Imaging'99, Security and Watermarking of Multimedia Content*, San Jose, 1999, vol. 3657, pp. 273-282.

[44] C. I. Podilchuk, and W. Zeng, "Image-adaptive watermarking using visual models," *IEEE Journal of Selected Areas in Communication*, 16(4):525-539, 1998.

[45] M. D. Swanson, B. Zhu, A. H. Tewfik, and L. Boney. Robust audio watermarking using perceptual masking. *Signal Processing*, 66(3): 337-355, 1998.

[46] M. J. Tsai, K. Y. Yu, Y. Z. Chen. Joint wavelet and spatial transformation for digital watermarking. *IEEE Trans. on Consumer Electronics*, 2000, 46(1): 241~245.

[47] H. Joumaa, F. Davoine, "An ICA based algorithm for video watermarking," In *Proc. 2005 International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2005*), Vol. 2, pp. 805-808.

[48] M. Wu, W. Trappe, Z. J. Wang, and R. Liu, Collusion-resistant fingerprinting for multimedia. *IEEE Signal Processing Magazine*, March 2004, 21(2): 15-27.

[49] Y. Wu, "Linear Combination Collusion Attack and its Application on an Anti-Collusion Fingerprinting," *IEEE International Conference on Acoustics, Speech, and Signal Processing, 2005* (ICASSP '05). March 18-23, 2005, Vol. 2, pp. 13-16.

[50] A. Herrigel, J. Oruanaidh, H. Petersen, S. Pereira, and T. Pun, "Secure copyright protection techniques for digital images," In *Second Information Hiding Workshop* (IHW), LNCS 1525, Springer-Verlag, 1998, pp. 169-190.

[51] Z. J. Wang, M. Wu, W. Trappe, and K. J. R. Liu, "Group-oriented fingerprinting for multimedia forensics," *EURASIP Journal on Applied Signal Processing*, 2004(4) 2153-2173, 2004.

[52] D. Boneh, and J. Shaw, Collusion-secure fingerprinting for digital data, *IEEE Trans. Inform. Theory*, 44 (5): 1897-1905, Sept. 1998.

[53] W. Kim, and Y. Suh, "Short N-secure fingerprinting code for image," *2004 International Conference on Image Processing*, 2004, pp.2167-2170.

[54] Y. Mao, and M. K. Mihcak, "Collusion-resistant international de-synchronization for digital video fingerprinting," *IEEE Conference on Image Processing*, 2005, vol. 1, pp. 237-240.

[55] N. Hayashi, M. Kuribayashi, and M. Morii, Collusion-resistant fingerprinting scheme based on the CDMA-technique, Second International Workshop on Security (IWSEC 2007), LNCS 4752, pp. 28–43, 2007.

[56] G. Tardos, Optimal Probabilistic Fingerprint Coding, in: Proceedings of the *35th Annual ACM Symposium on Theory of Computing*, 2003, pp. 116– 125.

[57] S. Lian. Traitor tracing in mobile multimedia communication. In "*Handbook of Research on Mobile Multimedia*" (2nd edition), edited by Ismail Khalil Ibrahim. IGI Global, 2008.

[58] D. Simitopoulos, N. Zissis, P. Georgiadis, V. Emmanouilidis and M. G. Strintzis. Encryption and watermarking for the secure distribution of copyrighted MPEG video on DVD, *ACM*

Multimedia Systems Journal, *Special Issue on Multimedia Security*, 9(3), 217-227, Sep. 2003.

[59] I. Brown, C. Perkins, and J. Crowcroft. Watercasting: Distributed watermarking of multicast media. In Proceedings *of International Workshop on Networked Group Communication*, Springer-Verlag LNCS, 1736, pp. 286–300, 1999.

[60] J. Bloom, "Security and rights management in digital cinema," in Proc. *IEEE Int. Conf. Acoustic, Speech and Signal Processing*, Vol. 4, pp. 712-715, 2003.

[61] R. Parnes and R. Parviainen, "Large scale distributed watermarking of multicast media through encryption," in Proc. IFIP Int. Conf. Communications and Multimedia Security Issues of the New Century, pp. 149-158, 2001.

[62] H. V. Zhao, K. J. R. Liu, Fingerprint multicast in secure video streaming. *IEEE Transactions on Image Processing*, 15(1), 12-29, 2006.

[63] R. Anderson and C. Manifavas. Chamleon – a new kind of stream cipher. *LNCS*, *Fast Software Encryption*, Springer-Verlag, pp. 107-113, 1997.

[64] D. Kundur and K. Karthik, "Video fingerprinting and encryption principles for digital rights management," *Proceedings of the IEEE*, 92(6): 918-932, 2004.

[65] S. Lian, Z. Liu, Z. Ren, and H. Wang, "Secure Distribution Scheme for Compressed Data Streams," 2006 *IEEE Conference on Image Processing* (ICIP 2006), Oct 2006, pp. 1953-1956.

[66] A. N. Lemma, S. Katzenbeisser, M. U. Celik, and M. V. Veen. Secure watermark embedding through partial encryption. *Proceedings of International Workshop on Digital Watermarking (IWDW 2006)*, Springer LNCS, 4283, 433-445, 2006.

[67] C.-Y. Lin and S.-F. Chang. A robust image authentication algorithm surviving JPEG lossy compression. In *SPIE Storage and Retrieval of Image/Video Databases*, Vol. 3312, pp. 296–307 (1998).

[68] H. T. Sencar and N. Memon, Overview of state-of-the-art in digital image forensics, Book chapter, Part of Indian Statistical Institute Platinum Jubilee Monograph series titled *'Statistical Science and Interdisciplinary Research*,' World Scientific Press (2008).

[69] A. C. Popescu and H. Farid. Exposing digital forgeries by detecting traces of re-sampling, *IEEE Trans. Signal Processing*, 53(2): 758-767 (2005).

[70] A. C. Popescu and H. Farid. Exposing digital forgeries in color filter array interpolated images, *IEEE Trans. Signal Processing*, 53(10): 3948-3959 (2005).

[71] W. Wang, and H. Farid. Exposing digital forgeries in video by detecting double MPEG compression, *Proceedings of the 9th workshop on Multimedia & security* (*MM&Sec'06)*, September 26–27, 2006, Geneva, Switzerland (2006), pp. 35-42.

[72] M. K. Johnson and H. Farid. Exposing digital forgeries by detecting inconsistencies in lighting, Proc. of *ACM Multimedia Security Workshop* (2005), pp. 1-10.

[73] B. Sankur S. Bayram, I. Avcibas and N. Memon. Image manipulation detection. *Journal of Electronic Imaging* – 15(4), 041102 (17 pages) (2006).

[74] J. Fridrich, D. Soukal, and J. Lukas. Detection of copy-move forgery in digital images. In *Proceedings of 2003 Digital Forensic Research Workshop (2003)*, Cleveland, OH, USA, 2003, http://www.ws.binghamton.edu/fridrich/Research/copymove.pdf.

[75] H. Farid. Exposing digital forgeries in scientific images. *ACM MM&Sec'06*, September 26–27, 2006, Geneva, Switzerland, pp. 29 - 36.

[76] A. Joly and O. Buisson. Discriminant local features selection using efficient density estimation in a large database, in Proc. *ACM Int. workshop on Multimedia information retrieval*, pp. 201–208, New York, 2005.

[77] L. Amsaleg and P. Gros. Content-based retrieval using local descriptors: Problems and issues from a database perspective, *Pattern Anal. Appl.*, 4(2-3): 108–124, 2001.

[78] E. Y. Chang, C. Li, J.-Z. Wang, P. Mork, and G. Wiederhold. Searching near-replicas of images via clustering, in Proc. *SPIE: Multimedia Storage and Archiving Systems* IV, 1999, vol. 3846, pp. 281–92.

[79] C. Kim. Content-based image copy detection, *Signal Processing: Image Communication*, 18(3): 169–184, 2003.

[80] M. Wu, C. Lin, and C. Chang. Image copy detection with rotating tolerance, In CIS 2005, Part I, *LNAI 3801*, Springer, pp. 464-469, 2005.

[81] M.-N. Wu, C.-C. Lin, C. Chang. A robust content-based copy detection scheme, *Fundamenta Informaticae* 71(2-3): 351–366, IOS Press, 2006.

[82] S. A. Berrani, L. Amsaleg, and P. Gros. Robust content-based image searches for copyright protection, in Proc. *ACM Int. Workshop on Multimedia Databases*, pp. 70–77, 2003.

[83] J.-H. Hsiao, C.-S. Chen, L.-F. Chien, M.-S. Chen. A new approach to image copy detection based on extended feature sets. *IEEE Trans. Image Process*, 16(8): 2069-2079, August 2007.

[84] V. S. Verykios, E. Bertino, I. N. Fovino, L. P. Provenza, Y. Saygin, Y. Theodoridis. State-of-the-art in privacy preserving data mining, *SIGMOD Record*, 33(1): 50-57, 2004.

[85] V. S. Verykios, A. K. Elmagarmid, E. Bertino, Y. Saygin, andE. Dasseni. Association rule hiding, *IEEE Transactions on Knowledge and Data Engineering*, 16(4): 434-447, 2004.

[86] Y. Saygin, V. Verykios, and C. Clifton, Using unknowns to prevent discovery of association rules, *SIGMOD Record,* 30(4): 45–54, 2001.

[87] L. Chang and I. S. Moskowitz, Parsimonious downgrading and decision trees applied to the inference problem, In Proceedings of the 1998 *New Security Paradigms Workshop* (1998), 82–89.

[88] J. Vaidya and . Clifton, Privacy preserving association rule mining in vertically partitioned data, In the *8th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (2002), pp. 639–644.

[89] M. Kantarcioglou and C. Clifton, Privacy-preserving distributed mining of association rules on horizontally partitioned data, In Proceedings of the *ACM SIGMOD Workshop on Research Isuues in Data Mining and Knowledge Discovery* (2002), 24–31.

[90] Y. Lindell and B. Pinkas, Privacy preserving data mining, In *Advances in Cryptology - CRYPTO 2000* (2000), 36–54.

[91] D. Agrawal and C. C. Aggarwal, On the design and quantification of privacy preserving data mining algorithms, In Proceedings of the *20th ACM Symposium on Principles of Database Systems* (2001), 247–255.

[92] A. Evfimievski, R. Srikant, R. Agrawal, and J. Gehrke, Privacy preserving mining of association rules, In Proceedings of the *8th ACM SIGKDDD International Conference on Knowledge Discovery and Data Mining* (2002), pp. 217-228.

[93] *Biometrics*. http://en.wikipedia.org/wiki/Biometrics.

[94] A. K. Jain, A. Ross, and S. Pankanti. Biometrics: A tool for information security. *IEEE Transactions On Information Forensics and Security*, 1(2): 125- 143, June 2006.

[95] M. Krause and H. F. Tipton. "Characteristics of Biometric Systems". In Handbook of Information Security Management. *CRC Press, pp. 39-41*.

[96] P. J. Philips, P. Grother, R. J. Micheals, D. M. Blackburn, E. Tabassi, and J. M. Bone. Face recognition vendor test 2002: Overview and Summary. http://www.frvt.org/DLs/FRVT_2002_Overview_and_Summary.pdf, March 2003.

[97] C. Wilson, A. R. Hicklin, H. Korves, B. Ulery, M. Zoepfl, M. Bone, P. Grother, R. J. Micheals, S. Otto, and C. Watson, *Fingerprint vendor technology evaluation 2003: summary of results and analysis report*, NIST Internal Rep. 7123, Jun. 2004.

[98] E. Kukula, and S. Elliott, *Implementation of Hand Geometry at Purdue University's Recreational Center: An Analysis of User Perspectives and System Performance*, IEEE 2005, The 39th Annual 2005 International Carnahan Conference on Security Technology (CCST'05), 11-14 Oct. 2005, pp. 83-88.

[99] N. K. Ratha, J. H. Connell, and R. M. Bolle. Enhancing security and privacy in biometrics-based authentication systems, *IBM systems Journal*, 40(3): 614-634, 2001.

[100] NIST SP 800-31, *Intrusion Detection Systems*.(Online) http://csrc.nist.gov/-publications/nistpubs/index.html

[101] Study by Gartner. *Host-based intrusion prevention systems (HIPS) update: Why antivirus and personal firewall technologies aren't enough.* (online) http://www.gartner.com/-teleconferences/attributes/attr_165281_115.pdf

[102] Study by Gartner. *Magic quadrant for network intrusion prevention system appliances, 1H08.(online)* http://www-935.ibm.com/-services/us/iss/pdf/esr_magic-quadrant-for-network-intrusion-prevention-system-appliances-1h08.pdf

[103] J. Allen, A. Christie, W. Fithen, J. McHugh, J. Pickel, and E. Stoner. *State of the Practice of Intrusion Detection Technologies*. TECHNICAL REPORT, CMU/SEI-99-TR-028, ESC-99-028, January 2000.

[104] R. Shane, "The Trusted Computing Platform Emerges as Industry's First Comprehensive Approach to IT Security", 2006. (online) https://www.trustedcomputinggroup.org/news/Industry_Data/IDC_448_Web.pdf.

[105] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker. *Digital Watermarking and Steganography,* 2nd Edition, The Morgan Kaufmann Series in Multimedia Information and Systems, 2007.

[106] S. Lian. Digital Rights Management for the Home TV based on scalable video coding. *IEEE Transactions on Consumer Electronics*, 54(3): 1287-1293, August 2008.

[107] *Social Networking Security. (online)* http://www.infosec.co.uk/files/KEY_22_1215_Social_Croft.pdf.

[108] S. Lian, Z. Liu, Z. Ren, and H. Wang. Commutative encryption and watermarking in compressed video data. *IEEE Circuits and Systems for Video Technology*, 17(6): 774-778, June 2007.

[109] *Signal Processing in the Encrypted Domain* (SPEED). (online) http://www.speedproject.eu/.

[110] J. Lukas, J. Fridrich and M. Goljan. Digital camera identification from sensor pattern noise, *IEEE Trans. Inf. Forensics and Security,* 1(2): 205-214 (2006).

[111] W. Hu, T. Tan, and S. Maybank. A survey on visual surveillance of object motion and behaviors. *IEEE Trans. on Systems, Man and Cybernetics-Part C: Applications and Reviews*, 34(3): 334–352, 2004.