**Copyright and Data Privacy**

14251205 Li Shiying

14252392 Sun Jingxuan

**1. Introduction**

Copyright, as a form of intellectual properties, grants rights to the creators to exclusively use and distribute their original works. Although the first copyright act did not emerge until the deployment of the Statute of Anne in 18th century Britain, the concept of protecting a work from being stolen by others dates back to 15th century, when the extensive usage of printing press made it easier for people to copy the creation of others [1]. However, nowadays, as the development in information technologies enables people to publish their original work online, these works become vulnerable to various cyberattacks. Therefore, technologies and laws must be applied to further protecting the copyright. In this paper, we will primarily focus on the latest data security technologies including DRM, watermark and data encryption which are frequently used in copyright protection as well as give a detailed explanation and evaluation of the two-fold problem on the scenarios of copyright violation and the prevention and recovery methods in a technological depth. In addition, laws regarding cyberattack and ethical issues will also be introduced.

**2. Content Protection Approaches**

Out of the concern of the data itself, confidentiality or secrecy refers to data belonging to certain individuals or institutions should never be obtained by unauthorized entities, which is highly related to copyright issues. Copyrighted data should not be altered in an unauthorized manner since the time it was created, transmitted or stored by an authorized source [21]. Common approaches are adding semantic information to original data. Along the history of dealing with copyright issues, two strategies are popularly utilised, namely data encryption and digital watermark.

**2.1 Encryption**

**2.1.1 Advanced Encryption Standard and Its Applications**

In the process of encryption, an algorithm is cast onto the original data and transform it into a more compact representation which is not comprehensible by human beings. Keys are generated for authorized party as it has the corresponding decryption algorithm, so that such scheme can insure the original data not to be altered by unauthorized party. Nowadays, various standards are used in data protection. AES, as is considered pretty secure, has been pervasively used in data protection since its first development in 2001 by U.S. National Institute of Standards and Technology and replaced the old Data Encryption Standard (DES) which is ineffective [23]. In this section, we will give a detailed view of AES algorithm as well as introduce its application in FairPlay developed by Apple Inc.

**2.1.1.1 AES Algorithm**

The basic scenario of an encryption method is to use a piece of plain text and a series of keys as input to generate the encrypted cipher text. Unlike DES which allows the block size of text to be any multiple of 32 bits, AES, on the other hand, although has various 3 key sizes, which are 128, 192 and 256 bits respectively, the block size is always 128 bits [3]. The basic steps of AES encryption are illustrated in Figure 1. As is shown below, input the plaintext and cipher key are transformed to the final ciphertext is generated after a series of rounds in a typical AES system. After being preprocessed to a 4 bytes \* 4 bytes’ matrix shown in figure 1, the data are further encrypted following a design principle call substitution-permutation network (SPN), in which they are encrypted using substitution boxes (S-boxes) and permutation boxes (P-boxes) [3]. During each round, the 4 bytes \* 4 bytes’ matrix will first be chopped into 128 small 8-bit blocks and go into 128 different S-boxes in which they will be substituted by another block of bits for encryption. The steps in S-boxes is invertible for the subsequent decryption, which means that the substitution should be one-to-one; therefore, a fixed-table storing the conversion principles is deployed.

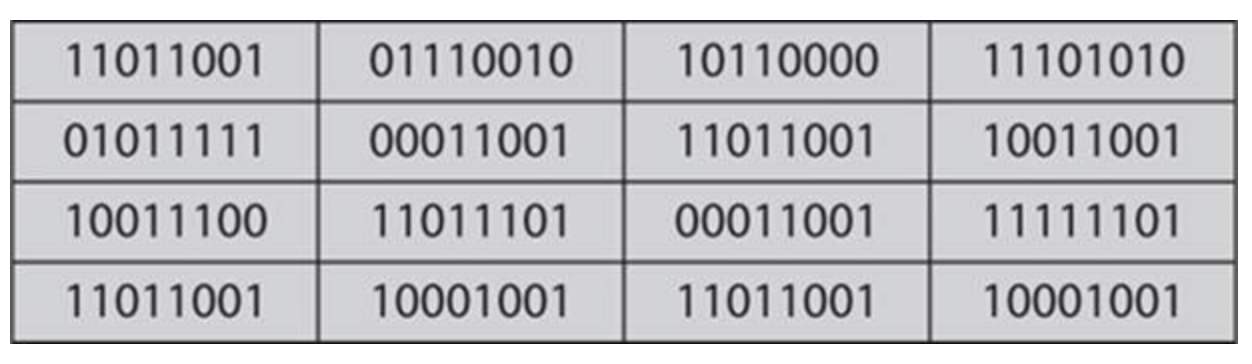


Figure 1 [3]

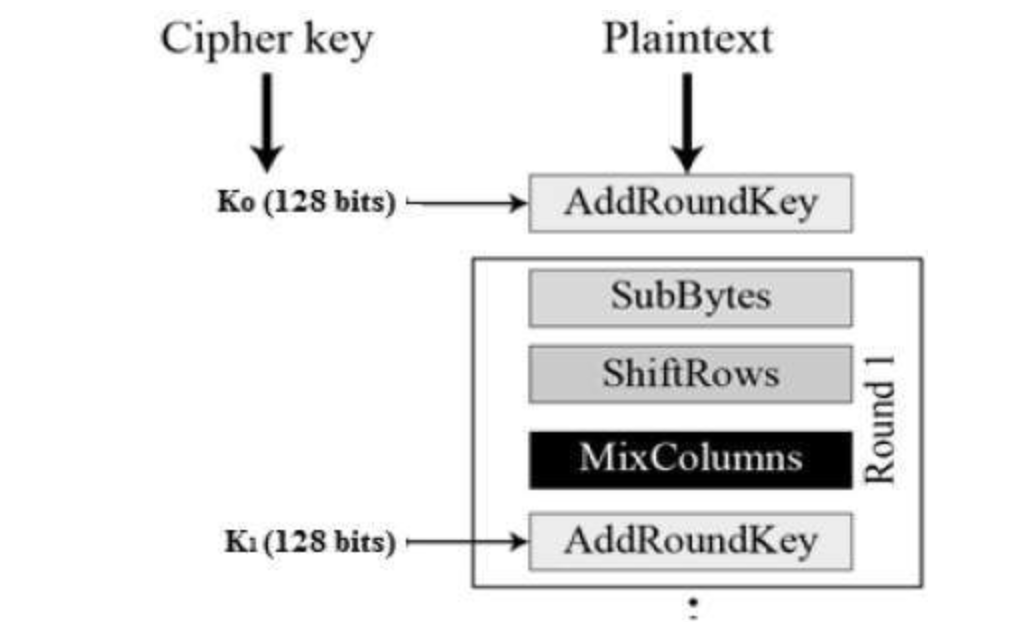
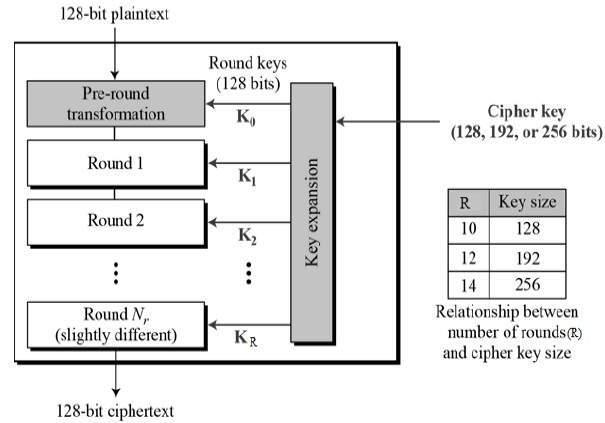


Figure 2 [4]

Then, the output data of S-boxes are feed to P-boxes for ShiftRows. As the data is still in a 4 bytes \* 4 bytes’ matrix format, we could consider it as a square with 4 columns \* 4 rows. As is illustrated in Figure 3, during the ShiftRows, the sequence of the first row will remain unchanged. However, the elements of the second is shifted 1 to the left: this makes the original sequence “2a”, “2b”, “2c” and “2d” become “2b”, “2c”, “2d” and “2a” from left to right. The units of shifting increment following the increment of the row index. Thus the elements are shifted 2 to the left in the third row and shifted to 3 in the fourth row. The output of ShifRows is still a 4\*4 matrix but with different element orders.

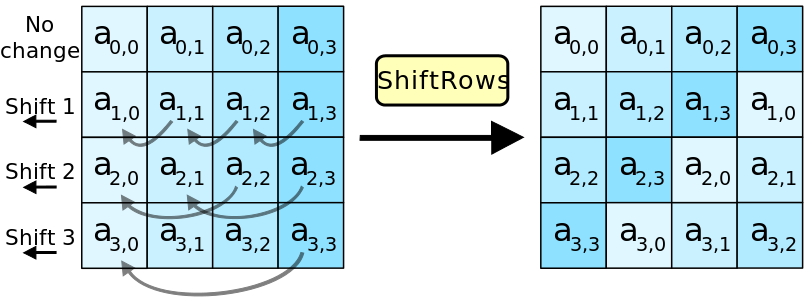


Figure 3 [2]

After processed by P-boxes, the permuted matrix will be further encrypted using MixColumns which, after a series of mathematical computation, could transform the input matrix to a totally new matrix. Initially, in the MixColumns step, each column of the matrix is treated as a four-term polynomial: *b(x) = b3x3 + b2x2 + b1x + b0* [13]. After multiplied with a fixed polynomial *a(x) = 3x3 + x2 + x + 2* modulo x4 + 1, the new matrix will be generated. The final step of one round is AddRoundKey, during which a subkey derived from the original input key will be used to combine each byte to give a further encryption [3]. Finally, the encryption process of one round will be finished and the data is feed to the next round until the end of the whole AES encryption.

**2.1.1.2 FairPlay: an AES Based Technology**

Nowadays, to prevent digital media copyrights from being violated by the third party, many digital media provider companies deployed certain Digital Rights Management (DRM) technologies, allowing only authorized users or devices to view or play the digital content [15]. Among them, one notable example is FairPlay developed by Apple Inc., which is used to protect the copyright of digital media sold in iTunes Store. It protects digital contents using AES encryption on the Advanced Audio Coding (AAC) layer [8]. In the following sections, we will go into details on the application of AES in FairPlay and the dilemmas such technology brings.

AAC is a coding standard for lossy digital audio encryption. Unless its predecessor MP3, it achieves better sound quality with high flexibility, allowing additional DRM to be used inside. It could solely exist as a format of audio files or integrated into MPEG-4 as the audio layer in a video file. In iTunes, all the music is in AAC format and all the videos are formatted according to MPEG-4 standard.

A cryptographic encryption in AAC ensures that only users purchased the specific digital file have right to view and play it. Although on the iTunes server, digital contents are not encrypted, after bought by users, iTunes will encrypt the purchased file and send the encrypted version to user’s local device. In FairPlay, two steps of encryption are used. The AAC data of a purchased digital file is encrypted using a master key following AES algorithm. After encryption, the audio content of AAC is encapsulated and stored in an atom called mdat [16]. Besides, in the purchased digital file, the master key used to encrypt the audio content will also be stored in an encrypted format using another key called “user key” generated by the local iTunes application. The atom of storing the encrypted master key is called priv. A protected AAC structure will then formatted as m4p (figure 4) and stored locally in the user’s devices for further view and play [32].

Although the mechanism of FairPlay is shown in the previous paragraph, it still couldn’t demonstrate what exactly would happen when a digital file is purchased by a user and how whole scenario works. Therefore, in the following part, the steps of purchasing a file from iTunes and playing the file will be described.

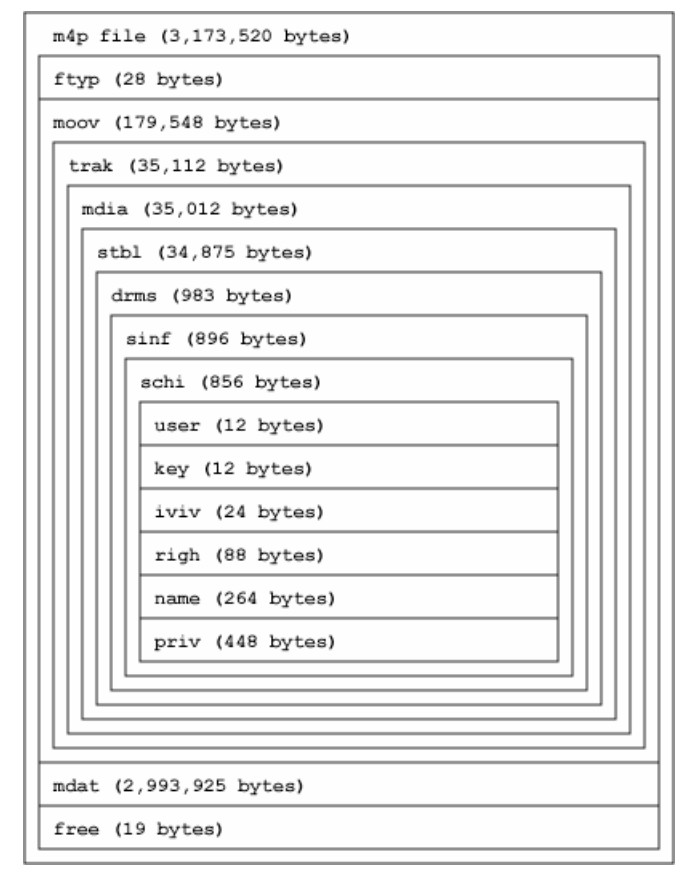


Figure 4 [32]

During the process of purchasing a movie on iTunes, for instance, after the “buy” button on the iTunes is clicked by the user, locally, a unique user key will be generated. The client-side iTunes will create a request with download request of the particular film and the user key which is then sent to server. After receiving the request, the iTunes sever will encrypted the target movie using master key, and send the encrypted version to the client. Arriving at the client side, the master key is further encrypted by user key.



Figure 5 [16]

When the user wants to play the movie he/she purchased from iTunes, iTunes will use the user key to unlock the master key and then use the master key to decrypt the AAC data [16]. The user then can freely view the file he/she purchased.

iTunes allows up to 5 devices of one user to be authorized and used to play iTunes media. When a user uses iTunes a new device, an id number of the device will also be generated and sent to iTunes server. The user then can use the new device to synchronize all the videos and audios he/she purchased from iTunes on other devices. The id of authorized devices of one user will stored in the iTunes Store server with the corresponding user information.

**2.1.1.3 FairPlay: Cons**

It seems that with the AES based FairPlay, files provided by iTunes are quite secure and is hard to be hacked by the third party. However, is FairPlay really secure? When it is undeniable that the AES encryption is pretty secure, and a file is impossible to be unscrambled without the key. Nonetheless, if the key used to encrypt the file is obtained, the file will also become vulnerable. As mentioned above, an iTunes media is encrypted using a master key which is then further encrypted using user key and stored in the media data. If the user key is obtained, it would be quite easy for cracker to decrypt the media file and steal its contents. The user key is stored both on iTunes application locally and on the iTunes Store server [16]. There will always be opportunities for hackers to steal the user key as long as they are in use. Also, digital data could also be stolen after they are decrypted and uncompressed by iTunes [16]. Until now, several methods of stealing a digital file from iTunes have been developed (table 1).

|  |  |
| --- | --- |
| Method | Mechanism |
| QTFairUse | Steal data after they are unlocked by iTunes |
| PyMusique | Pretends to be iTunes and download files from iTunes server |
| FairKeys | Pretends to be iTunes and download files from iTunes server |

Table 1 [16]

**2.1.2 Variations of Encryption-based DRM**

There is an intrinsic point of data itself, that essentially data can be represented with a variety of forms, which is not a consideration of data transmission. These forms include and not limited to text, audio, image, video and so on. Accordingly, the encryption of different types of data slightly diverts from each other, combining the related hardware or transmission channel. This set of different technologies of constraining access control unite into DRM. We provide a list of DRM encryption strategies for different data types, with several methods other than encryption but under the context of DRM [33].

|  |  |  |
| --- | --- | --- |
| Media/Data type | Major access control | Related strategies |
| Games | Production key encryption | Limit number of installation on different devices |
| Documents | Encryption | Remote manipulation (e.g. delete unauthorized copy) by encryption key |
| E-books | Encryption | File transmission through HTTPS protocol |
| Films | Encryption | Hardware (DVD player) build-in reverse DRM license  DRM metadata file |
| CDs (deprecated due to legal reasons) | Implicit installation of DRM software on users’ computer |  |

Table 2 [11]

**2.1.3 Evaluation and Current Situation of Encryption-based DRM**

Encryption can be carried out on almost all types of data and on the encryption/decryption key itself as dual encryption serving as a “double insurance”. However, along time, encryption-based DRM has gradually grown out of fond of users as for its cumbersomeness and ineffectiveness, and is partially substituted by digital watermark in multimedia area [14], which will be introduced in the next section.

A loophole intrinsic in encryption is that, theoretically, no matter how complicated it is, there is possibility that the encryption algorithm can be cracked. And as long as the algorithm is cracked, all the data protected by such algorithm can be accessed without authentication and will be free-at-hand of copyright violators. Although it is merely supposition, weighing the effort of cracking the algorithm against unblocked access to all copyright data, it is still profitable once and for all.

In real life situations, some companies focus on the additional profit brought by DRM rather than anti-piracy. As mentioned in the table, sometimes the hardware has to implement reverse DRM by certain company in order to get the content of files. As a consequence, users have to buy such hardware together with the films themselves, and the hardware is where the company gets extra profit [14].

One further notice is that, not as developed as in multimedia, encryption-based DRM is still the major practice of copyright protection of e-books and text files [14].

**2.2 Digital Watermark**

In the contrary to data encryption, which is the transformation of original data, digital watermark refers to a kind of marker embedded in a noise-tolerant signal such as an audio, video or image data [30]. The watermark itself is not extracted from the original data, but covertly added as a layer of the “packed” data ready for transmission. Applying digital watermark belongs to the category of information hiding [10]. The very information hidden within the watermark is copyright, license, authorship and so on [10].

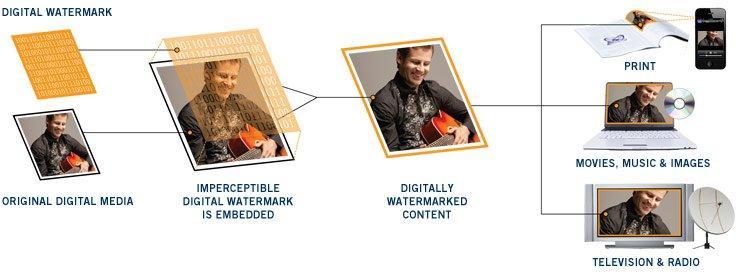


Figure 6

Three potential stages are involved in the life cycle of a digital watermark, namely embedding, attacking and extraction/detection [12]. In embedding process, a watermark signal generated from watermarking algorithms based on host signal is embedded to host signal, which refers to the original data.

In the transmission, a third party might modify the watermarked signal. The modification, referred to as “attack”, might be intended or unintended, as well as malicious or unmalicious. However, in the context of copyright violation, the action of modification itself might in some cases be wrongful practice. Extraction or detection is carried out by receiving party, who has the paired algorithm to extract the watermark information. Authentication is achieved by successful extraction of watermark or comparison between the extracted watermark and the original watermark.

Digital Watermarkis divided into two disciplines, robust digital watermark and fragile watermark, according to its usage, among which robust digital watermark is a permanent watermark used for denoting the copyright of authors in digital works [10]. A traditional and widely implemented watermarking system on image is the DCT-domain watermarking system proposed by Cox et al.

**2.2.1 DCT-domain Watermarking System [28]**

In the proposed system, the authors applied the idea of comparing the possibly corrupted image and the original watermarked image to calculate the distorted watermark in the corrupted image, and then comparing the extracted watermark with the original watermark. If the two watermarks are the same, the conclusion would be received image is not distorted and thus is an authorized copy of copyright image; if they are different, the conclusion would be otherwise. Along the base line we have introduced in Section 2.2, the system involves a two-fold algorithm of watermark casting and watermark extraction.

**2.2.1.1 DCT**

As mentioned, watermark signal is generated based on host signal, which is this case the copyrighted image. The essential information used is the coefficients after carrying out the Discrete Cosine Transform (DCT) on the original image.

DCT is the underlying compression methodology of JPEG lossy compression standard [19], which is carried out above a preprocessing step of transforming the coloured image from RGB colour model into a greyscale model YCbCr. The pixel information before the transform belongs to spatial domain, and the transformed coefficients belongs to frequency domain, or DCT domain, thus comes the name of the watermarking system. The magnitude of coefficients in the frequency domain reflects the degree of change in colour and illumination, specifically the larger the coefficient is, the more abrupt the change is. These differences are calculated based on the DC term, which is usually the left-most and up-most DCT coefficient.

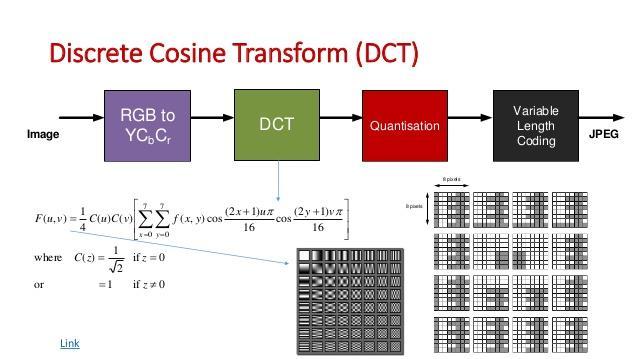


Figure 7

**2.2.1.2 Watermark Casting [28]**

After obtaining the DCT coefficients, the watermarking system takes the 1000 largest value except the DC term, denoted as T, and generates a random number for each coefficient. The set of random numbers falls in a normal distribution with a mean of 0 and variance of 1, denoted as X. The watermark is embedded by a function F of T with the coefficient set X (here coefficient refers to the coefficient of the function variable set T).

The image with the new 1000 largest DCT coefficients is the watermarked image. After a transformation from frequency domain back to spatial domain, the watermarked image is ready for transmission.

**2.2.1.3 Watermark Extraction [28]**

After transmission, receiving party obtains both host signal which is the original image and the watermarked image. For both image, the 1000 largest coefficients in the host signal is selected and according to the index, the 1000 coefficients in watermarked image is selected. With a reversed function of F, an estimate X\* is calculated and the similarity of X\* and X are measured by certain formula, denoted as sim(X, X\*). Intuitively, if similarity value is smaller than threshold, it implies the watermark is approximately the same, thus means the received watermarked image is an authorized copy.

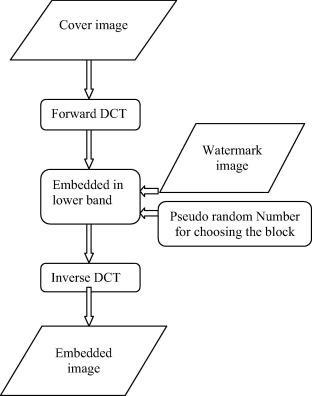


Figure 8

**2.2.2 Evaluation of Digital Watermarking**

A major advantage of information hiding over cryptography is that the illegal interceptors cannot distinguish if there is any secret message being hidden, which increases the difficulty of interception and decryption. Therefore, for digital watermarking, there does not exist the problem mentioned in the evaluation of encryption-based DRM. In real life applications, data encryption and digital watermark can be used as complementary techniques for content protection [12].

**2.3 Data Transmission**

On the other hand, the concept of authentication and anonymity often stand in each other’s way in typical data transmissionapproaches. We raise the example of P2P network to illustrate the possibility of copyright infringement during data transmission. While former sections of content protection focus on unauthorized modification of copyright data, here the emphasis will be on unauthorized distribution of copyright data.

**2.3.1 An Overview of P2P File Sharing Network**

Peer-to-peer networks are decentralised networks whose popularity is raised due to peer-to-peer resource sharing, the convenience of large file transmission and network anonymity. It acquires a virtual overlay network on top of the physical network topology [25], and each node within the overlay network is considered as a “peer”. Each peer belonging to the network is both file distributer and receiver, which makes the scheme reciprocated. File sharing is realized by searching the neighbours who own the desired files with the following step of file chunk sending through TCP/IP protocol. Decentralisation is the opposite to client-server model, in which files are sent by the server to the requiring node in the network. P2P networks have two models, namely unstructured and structured. Unstructured networks are easy to build while structured networks find neighbours faster and more reasonably.

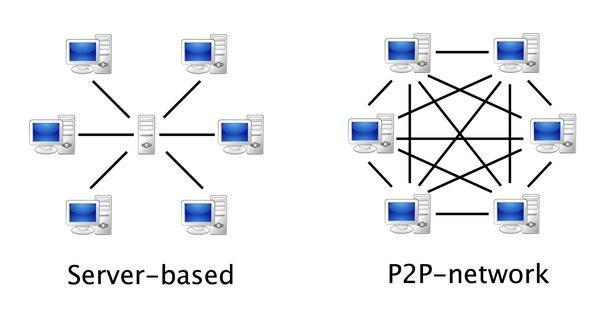


Figure 9

**2.3.2 Problem with P2P**

As file sharing are between neighbour nodes in P2P networks, which implies data transfer from one user to another is without using an intermediate server, there is no insurance whether the content is authorized or not. For example, in BitTorrent protocol, the Torrent files which serve as a pointer to the location of the copy of desired data, may or may not contain copyright information, or it can simply point to websites such as the Pirate Bay whose files are not authorized copy [5].

Another problem is, once unauthorized material is found, there is no possibility to find out the source of such material, as P2P networks are anonymous. The forte of P2P has fallen into the crux of itself.

**2.3.3 The Case of Spotify**

In the mp3 era, one of the most popular on-demand stream music service companies Spotify, utilised a hybrid network of server- and unstructured P2P networking strategy [20]. It originally had two servers located in London and Stockholm [20], and music was sent from both the servers and afterwards the peers themselves. The main consideration back then was decreasing the load on Spotify’s servers and bandwidth resources. Even for a nowadays tycoon, in the starting-up days it still needed to make the most use of open network as backup resource in order to achieving scalability of music streaming library while keeping the performance of low playback latency or jitter. Spotify also used TCP protocol to assist P2P, but only focusing on TCP’s ability of handling packet loss [29].

In 2014, Spotify began to remove the P2P portion of network and gradually moved to a full client-server model out of the consideration of security and company profile. Such change was enabled by the growing number of servers of the company [29], that there was no need to achieve scalability or seamless playback through peer-stocked resources. As TorrentFreak put it, “Spotify’s departure from P2P technology marks the end of an era”. Though most people wouldn't have noticed the change, the removal of P2P indeed enhances the copyright protection of the music industry.

**2.3.4 Solutions to P2P Network Copyright Infringement**

**2.3.4.1 Technical Approaches**

On technological spectrum, protocols such as Music2Share and other related works [31][34][24] are proposed to settle collusive piracy of P2P networks. But they are only derivations of the original network, adding elements of identification and authentication. Indeed, the risk of copyright infringement in P2P network is intertwined with its essential characteristics of decentralisation, and it is hard to find a satisfactory solution. As mentioned, technically, the openness and effectiveness of a reciprocated anonymous network always stands in opposition to and compromises strict authentication.

**2.3.4.2 Business Models**

From another point of departure, solutions to P2P network copyright infringement are found in business models, shifting the interest from prevention to recovery and from decreasing the loss to increasing the revenue.

***Advertising Model: YouTube*** Media sharing websites of TV, films, even music utilise such advertising model (usually with digital fingerprinting technology). The idea is playing ads before or in the middle of the media content is played. It is easy to understand where the revenue comes from and it will compensate the loss of being pirated in certain degree. But in users’ perspective, the service is completely free. Also, in the sense of reducing the time of users finding and downloading pirated items, such convenient service encourages users to legally access copyrighted data [17.

***Time-limited Streaming Service: Apple Music***Most on-demand streaming services nowadays offer time-limited access to large amount of copyright data on a monthly or yearly basis with proportional payment. The attracting aspect to the users as well as the preliminary for companies is the amount of data. That is, users may temporarily “own” the data they have never encountered before and ultimately users feel they are paying for the accessibility while they are actually paying for the songs they stream only. Even though piracy is leveraged, for example in the case of Apple Music [17], the extra revenue can still cover the loss and even create net income.

***Takedown: NEC***Still, except from the new models focusing on revenue, there are also new ways of tackling with piracy itself, but in a recovery approach instead of a protection one. Takedown services seek, identify and remove unauthorized copyright content from the internet, with underlying techniques including digital fingerprint [17]. Fingerprinting resembles encryption, referring to extract compact information from original content. The major difference is that fingerprints are generated with each copy of user data ignoring the identification of owner and only focusing on whether the copy is authorized. To enhance the effectiveness of takedown, a combination with revenue oriented approach is taken into practice for optimizing piracy loss and management effort [17].

**3. Ethics and Laws**

**3.1 Importance of Copyright and Related Laws**

Copyright protection could prevent the private interests from being infringed by others. An original work is an asset of its creator [1]. It is possible that in the future, this work will make substantial profit. Nonetheless, if the work is stolen by others, the profit brought by the work will no longer belong to its original creator. From the perspective of organizations and companies, a loss of an original work could result in a large number of loss in profit. From the perspective of an individual, on the other hand, even if the creator doesn’t intend to use his/her work to make profit, for him/herself, the work is still a precious product filled with a lot of effort. When someone steals this work, he/she does not only steal the work itself, but renders the creator’s effort void. The copyright issue is in essence an ethical issue. As according to Rousseau’s “the Social Contract”, one in natural state would deprive the private interest of others in order to make more interests for him/herself, without restrictions, malicious attack on copyright could be rampant [27]. And since the sophisticated technologies would also on the other hand enable thieves to confront copyright protection techniques and steal works from the internet, laws become truly necessary to further prevent the copyright infringement. In Hong Kong, there are several laws protecting copyrights; they grant copyright owners several rights including copying the work, issuing copies of the work to public, etc [18]. Once infringement happens, the owner can take civil legal action against infringers; the infringers, then, may be subject to a term of imprisonment and fine. The laws also consider using cyber-technology in unauthorized ways such as copying proprietary movies as crime [18]. Therefore, with the advanced technologies in data protection and certain laws in preventing copyright infringement, it is reasonable to believe that copyright in digital world would also be well protected.

**3.2 Pirated Content and Laws Dilemma**

It is common that in Hong Kong, one heard from his/her friend that the friend download pirated software such as Adobe Photoshop from a website offering pirated resources and download link. Such action is definitely illegal, as downloading pirated content is seen as copying other’s work without authorization. However, on the other hand, it is pretty seldom that people downloading pirated content are prosecuted: it seems to render that the copyright law is rather inviable and useless.

But the intellectual property ordinance in Hong Kong is still effective and according to it, one may find that it is quite reasonable that people simply downloading pirated software are not indicted for civil or criminal act. Act of duplicating unauthorized software and use it privately is illegal, but by no means a criminal offence, which means that victims of infringement only have right to trigger civil penalties [7]. However, as it is a civil case, whether to sue the infringer depends on the victim him/herself. If the victim chose not to sue the infringer or he/she is unaware that his/her work is copied by others without permission, the infringer will then not be charged [7]. This explains why in real life, many people download pirated software, music, movies and etc., but it is hardly heard that any of them are charged because of the infringement actions. And in the case mentioned previously, as long as Adobe doesn’t charge the friend of copying unauthorized Photoshop, he/she, even though doing things illegally, will not be penalized.

Illegal downloading happens highly frequently worldwide and it is really difficult for all the cases to be caught. Nowadays, it is rampant that people download pirated movies and TV series using BitTorrent rather than buy licensed recourses. In order to make more profit and better protect the copyright, some companies in film and related industry have already taken actions by hiring copyright trolls to prevent such infringements from happening [6].

For example, if a user starts downloading a pirated movie, the company troll hired by the movie producer company will identify the user’s IP by either getting a list of IP address from the pirated resource provider or using a torrent software to connect the user’s torrent software. The IP address of the user is then seen as an evidence of the user’s illegal action of downloading. The company then may send the user a settlement letter threatening legal action if the user doesn’t pay a number of settlement – which is typically around $2500 to $4500 [9]. If the user ignores the threat, he/she will then be sued as long as the company considers it is worth for suing.

One may find some confusing points in this case. Why after discovering the infringement, the victim company, instead of prosecuting the infringer directly, first send the infringer a settlement letter asking for money? Why there exists possibilities that the company decides not to sue the user even if he/she doesn’t pay the settlement?

There are two possible explanations to the first question. One is that an IP address is not a person; even if the company get the IP address, it is still likely that the it has no idea who exactly infringes its copyright by downloading unauthorized movies [6]. And as one cannot charge another without knowing the identity of the other, the letter is simply used as a way to increase profits through the settlement fee. Even though the company knows the identity of the infringer, it may still issue a settlement letter rather than directly sue the infringer since compared to put infringer into jail, the company prefers to earn more money. If it sues the infringer on a court and win the case, it will likely to get only hundreds of dollars for remedies. However, in the settlement, it can threat the infringer to give it thousands of dollars which is obviously more profitable.

Then, it would be easier to answer the second question: why finally infringers without paying settlement fee are not charged by the company. Suppose that a film company finds that 1000 users download pirated films produced by the company; the company will then send settlement letter to the 1000 users respectively threatening for money. Even if only 10% of them replies and pay for the settlement, the company earns the amount exceeding the profits brought by 1000 copies of authorized film CDs. And as the judicial proceedings is usually cumbersome, it won’t be necessary anymore for the company to further sue the remaining infringers.

With the fact that producer companies monitor the illegal downloading, it is reasonable to expect that the number of copying unauthorized movies through Internet would decrease. However, considering in the other way, it seems that the copyright owner of especially movies and TV series cares nothing other than money, otherwise they will continue sue the infringer after he/she refuse to pay the settlement amount. And after the infringer discovers that even if he/she doesn’t pay the settlement amount, he/she would not be charged, instead of stopping downloading unauthorized content, the infringer will possibly download pirated contents more rampantly without fear, making the copyright even harder to be protected.

**4. Conclusion**

In this paper, we reviewed the approaches of protecting copyright and intellectual property on the technical spectrum through history. The example of AES and variations have been raised to illustrate the encryption-based DRM, which is mostly deprecated currently or enhanced by other methods. Along time, digital watermarks show its convenience and high-efficiency in network transmission, thus grows its popularity. As for transmission, we gave a critical observation on the once popular P2P network configuration and pointed out the risk of copyright infringement. Finally, solutions are prompted from both technological and business, law perspective.

**Reference:**

[1]"A Brief History of Copyright", *Iprightsoffice.org*, 2017. [Online]. Available: http://www.iprightsoffice.org/copyright\_history/. [Accessed: 27- Nov- 2017].

[2]"Advanced Encryption Standard", *En.wikipedia.org*, 2017. [Online]. Available: https://en.wikipedia.org/wiki/Advanced\_Encryption\_Standard#/media/File:AES-ShiftRows.svg. [Accessed: 27- Nov- 2017].

[3]"Advanced Encryption Standard", *www.tutorialspoint.com*, 2017. [Online]. Available: https://www.tutorialspoint.com/cryptography/advanced\_encryption\_standard.htm. [Accessed: 27- Nov- 2017].

[4] *Announcing the ADVANCED ENCRYPTION STANDARD (AES)*. Federal Information Processing Standards Publication, 2017, pp. 17-18.

[5] "BitTorrent", *En.wikipedia.org*, 2017. [Online]. Available: https://en.wikipedia.org/wiki/BitTorrent. [Accessed: 26- Nov- 2017].

[6] Bischoff, P (2007) *Is Torrenting Safe? Is it illegal? Are you likely to be caught?.* compritech. Retrieved November 27, 2017 from the World Wide Web : <https://www.comparitech.com/blog/vpn-privacy/is-torrenting-safe-illegal-will-you-be-caught/>

[7] Community Legal Information Centre. The Law and Technology Centre, HKU. Retrieved November 27, 2017 from the World Wide Web : <http://www.clic.org.hk/en/topics/hkLegalSystem/criminalAndCivilLaw/answer12.shtml>

[8] *Computer Forensics: Investigating Network Intrusions and Cyber Crime*. Cengage Learning Ptr, 2009.

[9] Copyright Infringement Tips for Illegal Movie & Music Download Cases. Jux Law Firm. Retrieved November 27, 2017 from the World Wide Web : <https://jux.law/copyright-infringement-tips-for-illegal-movie-music-download-cases/>

[10] DAI Yuan jun, Information Hidding and Digital Watermark, <https://www.ibm.com/developerworks/cn/security/l-info/> 2002.1.1. [Accessed: 26- Nov- 2017].

[11] "Digital rights management", *En.wikipedia.org*, 2017. [Online]. Available: https://en.wikipedia.org/wiki/Digital\_rights\_management#Technologies. [Accessed: 26- Nov- 2017].

[12] "Digital watermarking", *En.wikipedia.org*, 2017. [Online]. Available: https://en.wikipedia.org/wiki/Digital\_watermarking#Digital\_watermarking\_life-cycle\_phases. [Accessed: 26- Nov- 2017].

[13] Easttom, C. “Modern Cryptography: Applied Mathematics for Encryption and Information Security,” New York: McGraw-Hill, 2016, pp.143-161.

[14] "Evaluation of DRM", 2017. [Online]. Available: https://www.quora.com/How-secure-are-DRM-documents-from-hacking. [Accessed: 26- Nov- 2017].

[15]"FairPlay Streaming - Apple Developer", *Developer.apple.com*, 2017. [Online]. Available: https://developer.apple.com/streaming/fps/. [Accessed: 27- Nov- 2017].

[16] *How FairPlay Works: Apple's iTunes DRM Dilemma.* Retrieved November 27, 2017 from the World Wide Web : <http://www.roughlydrafted.com/RD/RDM.Tech.Q1.07/2A351C60-A4E5-4764-A083-FF8610E66A46.html>

[17] H. Sudler, "Effectiveness of anti-piracy technology: Finding appropriate solutions for evolving online piracy", *Business Horizons*, vol. 56, no. 2, pp. 149-157, 2013.

[18] *Intellectual Property Protection.* GovHK. Retrieved November 27, 2017 from the World Wide Web : <https://www.gov.hk/en/residents/communication/infosec/intproperty.htm>

[19] "JPEG", *En.wikipedia.org*, 2017. [Online]. Available: https://en.wikipedia.org/wiki/JPEG. [Accessed: 26- Nov- 2017].

[20] Kreitz, G., & Niemela, F. Spotify--large scale, low latency, P2P music-on-demand streaming. In *Peer-to-Peer Computing (P2P), 2010 IEEE Tenth International Conference on* (pp. 1-10). IEEE, 2010.

[21] M. Arapinis, "Introduction in COMPUTER SECURITY", School of Informatics, University of Edinburgh, 2015.

[22] M. Barni, F. Bartolini, V. Cappellini and A. Piva, "A DCT-domain system for robust image watermarking", *Signal Processing*, vol. 66, no. 3, pp. 357-372, 1998.

[23] Nechvatal, J., Barker, E., Bassham, L., Burr, W., Dworkin, M., Foti, J., & Roback, E. (2001). Report on the Development of the Advanced Encryption Standard (AES). *Journal of Research of the National Institute of Standards and Technology*, *106*(3), 511–577.

[24] P. HE, M. CHEN and K. WU, "Decentralized fair multi-party exchange protocol under P2P environment", *Journal of Computer Applications*, vol. 29, no. 10, pp. 2606-2610, 2009.

[25] Peer-to-peer", *En.wikipedia.org*, 2017. [Online]. Available: https://en.wikipedia.org/wiki/Peer-to-peer. [Accessed: 26- Nov- 2017].

[26] "P2P still used or back in?", *Community.spotify.com*, 2017. [Online]. Available: https://community.spotify.com/t5/Desktop-Linux-Windows-Web-Player/P2P-still-used-or-back-in/td-p/1036003. [Accessed: 26- Nov- 2017].

[27] Rousseau, J. (1968). *The social contract* (Penguin classics). London, England ; New York: Penguin Books.

[28] S Cox, I. J., Kilian, J., Leighton, T., & Shamoon, T. Secure spread spectrum watermarking for images, audio and video. In *Image Processing, 1996. Proceedings., International Conference on* (Vol. 3, pp. 243-246). IEEE, 1996.

[29] "Spotify Starts Shutting Down Its Massive P2P Network - TorrentFreak", *TorrentFreak*, 2017. [Online]. Available: https://torrentfreak.com/spotify-starts-shutting-down-its-massive-p2p-network-140416/. [Accessed: 26- Nov- 2017].

[30] "数字水印技术\_百度百科", *Baike.baidu.com*, 2017. [Online]. Available: http://baike.baidu.com/view/369009.htm. [Accessed: 26- Nov- 2017].

[31] T. Kalker, D. Epema, P. Hartel, R. Lagendijk and M. Van Steen, "Music2Share - copyright-compliant music sharing in P2P systems", *Proceedings of the IEEE*, vol. 92, no. 6, pp. 961-970, 2004.

[32] Venkataramu, R (2007) *Analysis and Enhancement of Apple’s Fairplay Digital Rights Management.*  Retrieved November 27, 2017 from the World Wide Web : <https://www.comparitech.com/blog/vpn-privacy/is-torrenting-safe-illegal-will-you-be-caught/>

[33] "Windows Media DRM FAQ", *Web.archive.org*, 2017. [Online]. Available: https://web.archive.org/web/20101208173800/http://www.microsoft.com/windows/windowsmedia/forpros/drm/faq.aspx. [Accessed: 26- Nov- 2017].

[34] X. Lou and K. Hwang, "Collusive Piracy Prevention in P2P Content Delivery Networks", *IEEE Transactions on Computers*, vol. 58, no. 7, pp. 970-983, 2009.