ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
Indian Journal of Science and Technology, *Vol 9(47), DOI: 10.17485/ijst/2016/v9i47/106904, December 2016*

Privacy and Ownership Protection Digital Data Techniques: Comparison and Survey

H. Thakur* and G. Singh

Department of Electronics and Electrical Engineering, Lovely Professional University, Phagwara – 144411, Punjab, India;
harshul.thakur2007@gmail.com, gursharanjeet.singh@lpu.co.in

Abstract

Objectives: The main objective for writing this paper is to review about classification of various digital data hiding techniques, their types and along with their comparison. **Methods**: This paper provides the complete overview about the various types of data hiding techniques currently available and highlighted the important concepts behind each technique. A brief overview of the research work on studies related to DHT is considered and several research papers on these topics are cited. This paper reviews various recent advancement made in the field of DHT particularly the cryptography, steganography and digital watermarking. **Findings**: The various digital data hiding techniques have their own unique features and processing methods for hiding or maintaining the secrecy of the original information but watermarking is emerging as one of the most competent way to care for digital data at present. This paper also provides an effective source of information about the possible research gap in the field of creating robust and secure watermarking technique.

Keywords: Data Hiding Technique (DHT), Discrete Cosine transform (DCT), Discrete Wave late transform (DWT), Human Auditory System (HAS), Least Significant Bit (LSB) Coding, Watermarking (WM)

1. Introduction

Now days, almost each and every information is available to our door steps by just pressing an option search on Google. This information is called as digital information which is available in almost all formats on the internet. The available data in the form of video, audio and image have originally originated from a unique source, from whom we don't know or we don't want to experience. Most of us are simply copying that data without getting rights from the concerned owner of the same information. This is what we named with a term called digital piracy.

The internet age and the expansion of innovative technologies like P2P (peer to peer) file sharing have led to more chances for ethical violations like digital piracy. It is the use of work without permission which is protected by copyright law, the only copyright holder has the right to reproduce, display, distribute and do derivate of the information. The most important issue is academic property rights for digital media in terms of security and enforcement[1]. Digital piracy is also known as soft-lifting, It is of huge worry at present even after applying diverse approaches like creating awareness and using various technological means, but it didn't solve yet[2].

Due to the piracy, companies are bearing huge losses every year. Look on to the one of the scenario, as per the reports given by the UNITED STATES COPYRIGHT OFFICE, the piracy rate of file sharing in peta bytes per month (1 peta byte=1 million gigabytes=1.6 million CDs) is increased by 44% from year 2008 to 2014 in North America and it will reach up to 51% by the year 2019[3]. This also affects the sales of the US music industry; it may

**Author for correspondence*

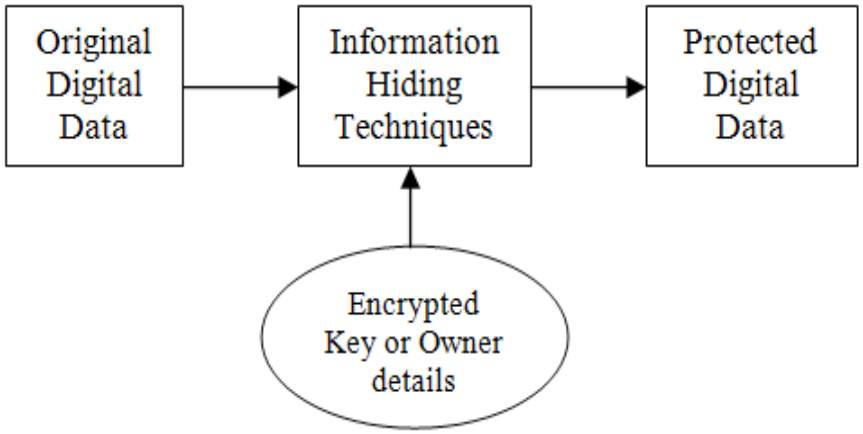

Figure 1. Process of protecting digital data.

happen that genuine consumers have to pay more money to buy the same music/video. If you think of remedy to this is not sell online, you may be wrong. Companies can't stop selling music/video online, as per the revenue details, In 2004 the maximum sales about 98.4% are done through physical purchase and 1.5% through digital download[4], but In 2015 the market scenario has been changed drastically, the maximum sales about 34% is done through Digital downloads, 34.3% from streaming, 28.8% by physical purchase, rest 2.9% is from synchronization and ringtones[5]. You would be surprised to know that US music industry revenue is facing a loss of $12.5 billion due to the global music piracy and the net revenue is just about $2.4 billion.

Due to the circulation of digital data over the internet, many authors and publishers get hesitate to show their work on the web due to security reasons. They may have fear of duplication of information and replication of copyright material. Many approaches are identified for protecting digital data; time stamping, authentication and encryption. Some more and efficient ways to prove the claim and to protect digital data from piracy, to protect copyright, digital audio and video data aredata hiding techniques like cryptography, steganography and digital watermarking.

These techniques help in hiding the encrypted key, name of owner or other related details into the original information in such a way that it remains undetectable without disturbing the quality of the original information as shown in Figure 1. A low level signal is to embed into the image or video, this signal is known as a digital watermark, which is uniquely identified by the owner and easily extracted from the image[6].

2. Data Hiding Techniques

2.1 Cryptography

A secret writing, word with Greek origins formed by combining two words, 'Kryto' means secret or hidden and 'graphene' means writing. As it became the need of the people to communicate secretly which in turn ensured the evolution of cryptography. This is the science of encrypting (Coding) and decrypting (decoding) information message so as to keep it secure, done by using a key that is ideally known to the sender and recipient sharing the message as shown on Figure 2.

Further it has three different mechanisms, they are Symmetric-Key encipherment (same key is shared by the sender and receiver to encrypt and decrypt the information message), Asymmetric-Key encipherment (Public and private key is used instead of one, for encryption public key of receiver is used by sender and for decryption receiver applies his own private key) and Hashing (a

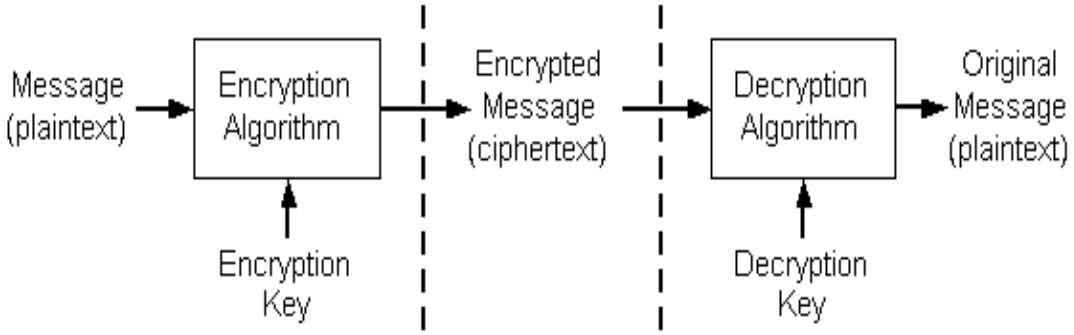

Figure 2. The process of cryptography (encryption and decryption).

fixed length message is sent along with the information message)[7]. Cryptography converts the secret information message into unreadable form (can't be read by human), but limitation of this technique is that the encrypted code is visible to everyone and intruders may apply some methods to decrypt the secret information.

2.2 Steganography

Steganography is actually a Greek word which is combination of two words Stegano (means hidden) and graphy (means writing). Steganography is a way of hiding the secret message in original media such as image, text, video and audio, so that it will get visible to anyone. In olden times, a special kind of invisible ink was used to write down the secret messages which can only be seen by heating the paper to a certain temperature otherwise the paper looks blank[8]. In cryptography, one can easy recognize that the message is encoded and can't be decoded without knowing the correct key and In Steganography, the secret message is not so much difficult to decode but no one can easily detects the presence secret message that means it protects the existence of encrypted data being detected. Steganography has strength to overcome the limitations of cryptography by hiding the secret message during communication. Different techniques of steganography are:

2.2.1 Text Steganography

In text steganography the secret message is hidden inside some other text file (cover text), so that it can easily be transmitted on unsecure channel[8]. The cover text is generated using random text sequences; This method is suffering from problems related to security and linguistic point of view[9].

Example:

i. Original Message: **S**ource **E**nhancement **C**onquer **R**andom **E**ffective **T**houghts.
ii. Secret Message: SECRET

2.2.2 Audio Steganography

In this technique of steganography the secret audio is hidden behind the other audio (in frequency may human can't hear)[10]. One audio contains the secret message and other audio act as cover media file as shown in Figure 3. It is a difficult task to hide additional information into the audio sequence as compared to images[11], due to supremacy of the HAS (Human Auditory System) over HVS (Human Visual System)[12]. Audio Steganography analysis is shown in Table 1[13].

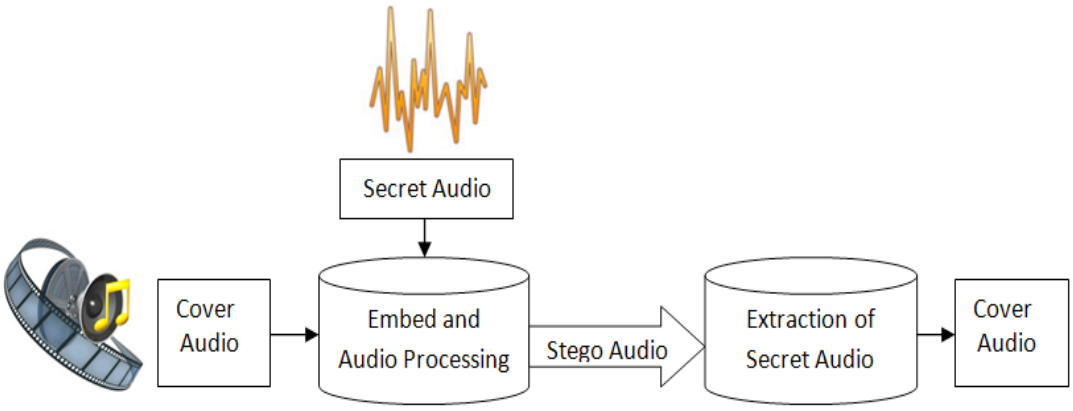

Figure 3. The process of audio steganography

Table 3. Audio steganography analysis

Domain	Methods	Hiding Rate	Strengths	Weakness
Wavelet Domain	Wavelet Coefficients	200Kbps	High embed Capacity	Lossy Data recovery
Temporal Domain	LSB	16Kbps	Simple Method	Easy to Extract
	Echo Hiding	40-50bps	Flexible to lossy data compression Algorithms	Low Security and Capacity
Frequency Domain	Tone Insertion	250bps	Imperceptibility of embedded data	Lack of Security and Transparency
	Phase Coding	333bps	Robust in Signal Processing	Low Capacity
	Spread Spectrum	20bps	Better Robustness	Weak in time scale changes

2.2.3 Video Steganography

In video steganography the secret data is hidden behind a video file, the capacity of storing secret data is more in Video Steganography[14]. Secret data can hide in audio as well as in video. This process of video steganography is shown in Figure 4.

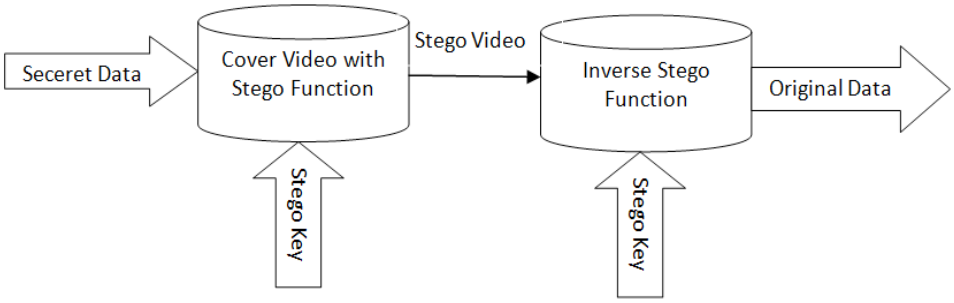

Figure 4. The process of video steganography.

2.2.4 Image Steganography

In this process of steganography, cover image is utilized to cover the secret data. Secret data can be in the form of image or text[15]. After the stego process, embedded picture is transferred through a unsecure channel. The secret message can be hidden in the pixels of the image[16,17]. Now a days, the internet home pages consist of steganography programs, image as cover for secret information is used by some of them[18].

These two techniques have their own significance, In combining above two provides double level of security to the digital data the process as shown in Figure 6. This technique is more robust than the security provide by the individual techniques[19]. The double security advantage is provided in terms of not to prevail the existence of secret data and decryption can't be done without Key.

Original Image

Original Image +Hidden Data

Figure 5. The process of image steganography[18].

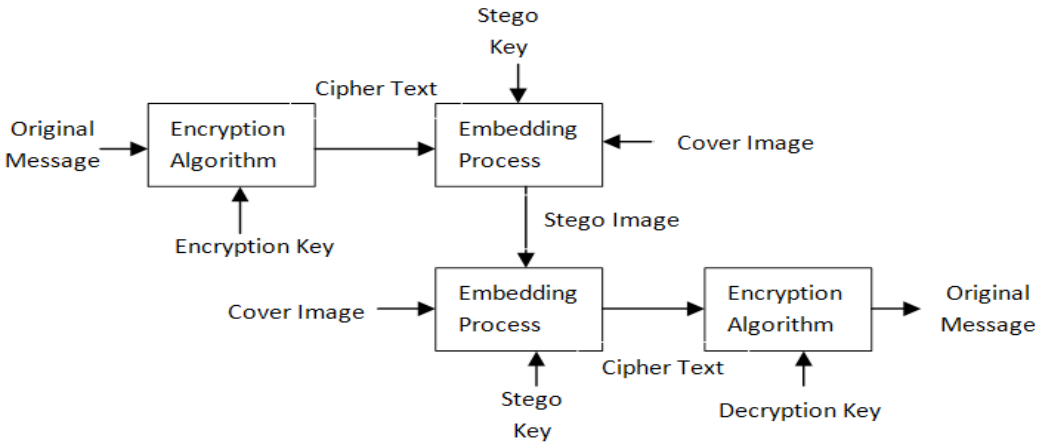

Figure 6. The process combining cryptography and stegnography.

2.3 Water Marking

Watermarking is the process of hiding the information or embeds secret information (watermark) in digital multimedia like images or photographs, digital audio and video, taking care of limitation related to the HAS (Human Auditory System) and HVS (Human Visual System)[20,21]. Cryptography and watermarking techniques are almost related techniques, but in watermarking encryption is not always present. To secure the digital content and protect data from unauthorized users digital watermarking is used, it also identifies the ownership right of digital data. Imperceptibility and robustness are the important characteristic of digital watermarking against various types of attacks like compression, filtering, cropping, rotation and scaling.

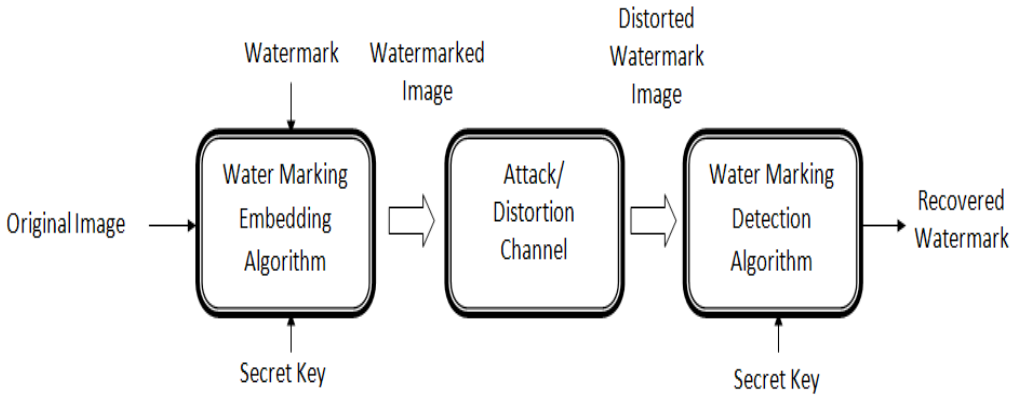

Figure 7. Embedding and extracting process of digital watermark .

Digital watermarking is one of the emerging technologies at present; it is the collection of technologies like network technology, processing of signal, cryptography, stochastic theory, algorithm design, probability theory etc.[22]. Robustness of watermark against different types of attacks is totally defined by the efficiency of digital watermarking algorithms, which provide protection from malicious attacks. A robust watermark is invisible to human eye or not even heard by human ear it is only detected through special detecting algorithms; with the process watermarking has proceeded. Only the authorized person can detect, extract and even modify the digital watermark. For authentication and tamper proofing again the Digital watermarking method is used[23].

Host image is the one in which watermark is to be encoded. In process of digital watermarking, a multimedia signal is embedded into a host signal keeping in mind that it should remain recoverable in order to claim the information. In all digital watermarking techniques two algorithms are surely present, one is embedding algorithm to embed watermark into the original signal and the other is detecting algorithm to retrieve or recover watermark form the signal again[24]. For watermarking techniques, these two processes are same and opposite but in between these two processes there is a transmission channel called as attack/distortion channel[25], where signal may undergo with modification due to removal, interference, compression, cropping, distortive, additive and filtering attacks, the embedding process and extracting process of digital watermarking is shown in Figure 7.

3. Types of Watermarking

3.1 The Types of Watermarked Document

3.1.1 Image Watermarking

Images can represent in terms of frequency in transform domain and in terms of pixels in spatial domain. Watermarks are embedded into the images by changing the values of the pixels and coefficients in time and frequency domain respectively[26].

3.1.2 Video Watermarking

The video watermarking is the extension of image watermarking. With this technique watermark is added to the real time video stream. This method has more robustness and real time quality extraction. Embedding in spatial and transform domain is almost similar to the image watermarking[27].

3.1.3 Audio Watermarking

The embedding of information in audio sequence is more tedious than embedding information in images. As audio signal is dimension less, very low amount of data is embedded into audio then the data embedded in images. The most popular area is audio watermarking, as large scale of piracy occurs due to internet music[28].

3.1.4 Text Watermarking

In text watermarking, watermark is inserted in font shapes, space between characters, and spaces between lines. It protects d doc, pdf and other text files from changes[29].

The text watermarking techniques are:

- Spread Spectrum Watermarking:- In this a generated signal "pseudo random noise" is inserted in to the host signal[30].
- Line Shift Coding:- In this technique even line is shifted down if bit is zero otherwise the line is shifted up, odd lines are used at decoding and they are also called as control lines[31].
- Word Shift Coding:- In this technique, the line is divided into group of words then groups shifted to left and right according to payload and for decoding, odd groups are used to measure distance between groups[32].
- Feature Coding:- In this technique certain text features are changed in a definite way to encode 0s and 1s of the payload. In comparing watermarked document with the original document, watermark can be detected.

3.2 According to Human Preception

3.2.1 Visible Watermark

In this, watermark is easily discovered over the digital data. It is like punching of stamp on the document. Another exam can be taken of Television channels; their channel logo is always present at one of the corners of the picture.

3.2.2 Invisible Watermark

In this watermarking, the watermark is not easily discoverable. No one even detects the presence of watermark inside the digital media. But it can be detecting with the correct detection algorithm[33].

- Invisible (Robust Watermark)
- Invisible (Fragile Watermark)
- Combination of Visible and Invisible WM (Dual Water Marking)

3.3 According to Working Domain

3.3.1 Spatial Domain Watermarking

In spatial domain process the static amplitude pseudo-noise is added into the image. This modifies the list significant bit of the original signal. The spatial watermarking can be applied only on one of the color bands by using color partition, but the watermark may appears during the separation of colors for printing. The watermark can be hidden into the data as assumed that the LSB data are visually inappropriate[34].

3.3.2 Frequency Domain Watermarking

In frequency domain watermarking, the low frequency components are modified to contain text or signal. It is also called as transform domain watermarking, because for to apply frequency domain watermarking techniques signal has to firstly transform to frequency domain and then modifications are applied to transformed coefficients then a watermarked image is formed by inverse transforming the coefficients. Many techniques have been purposed based on frequency domain watermarking. By transforming the original image in to frequency domain by using Discrete Fourier Transform (DFT), Discrete Wavelet transforms (DWT) and Discrete Cosine Transform (DCT) a high quality watermarking image can be produced[35].

3.4 According to Application

3.4.1 Source Based

A digital watermark is a source and destination based also depending upon application. In Source based watermark, a unique watermark is added at the point of source level, containing the information of owner to all distributed copies of original image. It is not used for authentication or verifying the image got tampered at the receiving end.

3.4.2 Destination Based

The watermark is destination based also where a unique watermark is given to the each distributed copy and it could be used to find the illegal buyer.

3.5 According to Extraction Process

It is divided into three extraction algorithms. These are:

3.5.1 Blind Algorithm

It is a process in which the original watermark image is not needed to detect or extract the watermark, it only requires the correct secret key.

3.5.2 Semi Blind Algorithm

In the extraction process of semi blind algorithm both watermark image and secret key is required to detect and extract the watermark.

3.5.3 Non Blind Algorithm

In non blind algorithm a original image is required to detect and extract the original watermark[36].

4. Comparison of Data Hiding Techniques

In cryptography, the content of the message is protected by encryption methods. During communication between

the two parties, it is very much secure in case if third party is also present. In cryptography process the plain text is converted into cipher text which is not understandable by the any other user. But one drawback of the cryptography is, it is not so robust against attacks because once message is decrypted, it will be seen by everyone, no further security remains after decryption. In Case of digital watermarking, the watermark always remains present in the image till the originator removes it from the image. So, it is more robust against attacks as watermark can be recovered with recovery algorithms and hackers can not even able to find the existence of watermark. With this the imperceptibility of the digital objects will increase[37].

In watermarking, the information is related to digital objects to be secured or to its owner. Steganography is used just to hide a message. Watermarking is one to many communications (for example, movies) while in case of steganography is one to one communication (for example, sender to receiver). Both are different in robustness criteria, steganography deals with detection of hidden message. But watermarking deals with removed by a piracy. The following Table 2. Shows the comparison between steganography and cryptography and Table 3 shows the comparison between steganography and Watermarking[38].

Table 2. Steganography vs cryptography

S.No.	Steganography	Cryptography
1	It does not alter the structure of secret data.	It alters the overall structure of the secret data
2	It hides the secret data.	It coverts secret data into other readable form.
3	Passing message is known	Passing message is unknown
4	Once detected anyone can easily decode the secret data.	Once detected, no one can easily decode the secret data.
5	Stego Media is the final output.	Cipher text is the final output.
6	It prevents the existence of secret data.	It prevents an unauthorized party from detecting the secret message

Table 3. Steganography vs watermarking

S.No.	Steganography	Watermarking
1	The secret data is embedded in any digital media is called stego file.	The watermark is embedded in any digital media is called Watermarked file.
2	The objective and concern of steganography is on capacity	The objective and concern of watermarking is on Robustness
3	In Detection process cover is not needed for recovery.	Data is retrieved from correlation and original cover is required for the same.
4	In relation to cover, it is never perceptible to the normal human eye.	Watermarks are some time visible to human eye but not in case of invisible watermarks.
5	In case of attacks, steganalysis detects the presence of information.	In case of attacks, image processing aid required for removal and replacement of watermarks.
6	Not easy to detect because it is hard to find the steganographic image.	Not at all easy to detect.
7	Steganography hides the message without altering it.	Watermarking extends the information and become and attribute of the cover image.
8	The techniques involved are like LSB, Phase Coding, Echo Hiding, Spread Spectrum etc.	The techniques involved are like DWT, DCT, DFT etc.

5. Conclusion

The present paper was intended to introduce diverse data hiding techniques including cryptography, steganography and watermarking. All have their unique features to protect original data and a comparison between them was carried out. It is found that a combination of cryptography and steganography gives better security to the digital data, but problem related to these techniques is the requirement of more space to hide the data. The most widely used technique is LSB but it has drawbacks. So one has to follow either the data compression measure or the robust method of data hiding technique i.e watermarking. Watermarking is having a potential and most robust approach for protection of ownership rights on digital data. According to types of document, working domain, applications, human perception and extraction process, there are different requirements of the watermarking systems. However, it is difficult to satisfy all the requirements at the same time. This paper provides the complete description of methods available for watermarking. Digital marking is still a challenging area of research with challenging problems, like it may or may not survive in

every possible attack. The future research points toward more robust and secure water marking technique to ensure about the secrecy of digital multimedia.

6. References

1. Edward J, Christine I. Digital watermarking: Applications and Algorithms. Proceedings of IEEE Signal processing Magazine. 2001 July.
2. Rekha A,Pillai R. Piracy in the digital age: Is ethical awareness turning into action? IEEE International Symposium on Ethics in Science, Technology and Engineering, 2014, Chicago, IL. 2014. p.1–4.
3. If You Think Piracy Is Decreasing, You Haven't Looked at the Data... - Digital Music News", Digital Music News. 2016 Aug 31. Available from: http://www.digitalmusicnews.com/
4. 2015 Aug 31 Available from: http://copyright.gov/policy/musiclicensingstudy/copyright-and-the-music-marketplace.pdf.
5. Friedlander J. 2016 Aug 31 Available from: https://www.riaa.com/
6. Chandra M, Pandey S,Chaudhary R. Digital watermarking technique for protecting digital images. 3rd International Conference on Computer Science and Information Technology (ICCSIT). 2010, Chengdu, 2010, 226-233.
7. Forouzan B.Introduction to cryptography and network security. Boston: McGraw-Hill Higher Education; 2008.
8. Mishra R, Bhanodiya P.A review on steganography and cryptography. International Conference on Advances in Computer Engineering and Applications (ICACEA),, Ghaziabad.2015. p. 119–22.
9. Bennett K. Linguistic Steganography: Survey, analysis, and robustness concerns for hiding information in text. Center for Education and Research in Information Assurance and Security. Purdue University, 2004.
10. Bhattacharyya S, Gautam S. A Robust Image Steganography using DWT Difference Modulation (DWTDM). International Journal of Computer network and Information Security.2012; ,4(7).
11. Jenkins N, Jean E.Steganography in audio.University of Cambridge CST Part II Dissertation. 2009.
12. Johnson N,Jajodia S. Exploring steganography: Seeing the unseen. IEEE Computer. 1998 Feb; 31(2):26–34.
13. Balgurgi P,Jagtap S. Audio Steganography Used for Secure Data Transmission. International Conference on Advances in Computing. Springer India. 2016; 174:699–706.
14. Bhagat AR,Dhembhare AB. An Efficient and Secure Data Hiding Technique-Steganography. International Journal of Innovative Research in Computer and Communication Engineering. 2015; 3(2): 941–9.
15. Singh H, Singh PK, Saroha K. A Survey on Text Based Steganography.Proceedings of the 3rd National Conference; INDIACom-2009 Computing For Nation Development. Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi. February 2009, 26–27.
16. Jain, Nitin, Ram SM, Dubey S. Image Steganography Using LSB and Edge Detection Technique. International Journal of Soft Computing and Engineering (IJSCE). 2012; 2231–307.
17. Amin M, Salleh M, Ibrahim S, Katmin MR, Shamsuddin MZI. Information Hiding using Steganography. Proceedings of 4th National Conference on Telecommunication Technology, Shah Alam, Malaysia. 2003.
18. Kaur N, Behal S. A Survey on various types of Steganography and Analysis of Hiding Techniques. International Journal of Engineering Trends and Technology. 2014; 11(8): 387–91.
19. Raphael A,Sundaram V. Cryptography and Steganography: A Survey. International Journal of Computer Technology 2011; 2(3): 626–30.
20. Husain F. A survey on digital watermarking techniques for multimedia data. MIT International Journal of Electronics and Communication Engineering. 2012; 2(1), 37–43.
21. Robert L, Shanmugapriya T. A Study on Digital Watermarking Techniques. International Journal of Recent Trends in Engineering. 2009; 2(1), 223–5.
22. Durvey M, Satyarthi D. A Review Paper on Digital Watermarking. International Journal of Emerging Trends and Technology in Computer Science.2014; 3(4): 99–105.
23. Tiwari N, Ramaiya MK,Sharma M. Digital watermarking using DWT and DES. 3rd International Advance Computing Conference. IEEE.2013.
24. Singh S. Digital Watermarking Trends. International Journal of Research in Computer Science. 2011; 1(1): 55–61.
25. Parashar P,Singh R. A Survey_Digital Image Watermarking Techniques. International Journal of Signal Processing, Image Processing and Pattern Recognition. 2014; 7(6): 111–26.
26. Potdar VM., Han S, Chang E. A survey of digital image watermarking techniques. 3rd IEEE International Conference on Industrial Informatics. INDIN '05. 2005. 2005 Aug; 10(12): 709–16.

27. Arnold M, Schmucker M, Wolthusen SD. Techniques and Applications of Digital Watermarking and Content Protection, 1st ed. Artech House: 2003 July.
28. Heidenheim, Germany. Digital Watermarking for Digital Media. Information Science Publishing. May 2005.
29. Mathapati R, Pujari J. Digital Video Watermarking. International Journal of Advanced Research in Computer Science and Software Engineering. 2012; 2(11): 1–8.
30. Cox IJ, Kilian J, Leighton FT, Shamoon T. Secure spread spectrum watermarking for multimedia. IEEE Transactions on Image Processing. 1997 Dec; 6(12): 1673–87.
31. Micic A, Radenkovic D, Nikolic S. Autentification of Text Documents Using Digital Watermarking. Telecommunications in Modern Satellite, Cable and Broadcasting Services. 2005 Sept; 503-505.
32. Brassil, Maxemchuk, Gorman O; Electronic marking and identification techniques to discourage document copying. Selected Areas in Communications, IEEE Journal. 1995 Oct; 13(8): 1495–504.
33. Singh P, Chadha RS. A Survey of Digital Watermarking Techniques, Applications and Attacks. Proceedings of International Journal of Engineering and Innovative Technology (IJEIT).2013; 2(9).
34. Shah JK. ECE Department, Temple University, PA 19122. Available from: http://astro.temple.edu/~shah
35. Mistry D. Comparison of Digital Water Marking methods. International Journal on Computer Science and Engineering. 2010; 2(9):2905–9.
36. Singh P, Chadha RS. A Survey of Digital Watermarking Techniques, Applications and Attacks. Proceedings of International Journal of Engineering and Innovative Technology (IJEIT). 2013 March; 2(9).
37. Kaur S, Copyright Protection of Data by using Video Watermarking. International Journal of Computer Application. 2015; 119(17): 14–18.
38. Diskin P, Lau S, Cummins, Parlett R. Steganography and Digital Watermarking Copyright. School of Computer Science. The University of Birmingham; 2004.