Volume 4, No. 4, March-April 2013
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
REVIEW ARTICLE
Available Online at www.ijarcs.info

Information Hiding - Steganography & Watermarking: A Comparative Study

Gunjan Chugh
M.Tech Student
Deptt. of Computer Science
Banasthali University Rajasthan,India
gunjan.chugh17@gmail.com

Abstract: Information Hiding has emerged as a multidisciplinary field and is getting large support from the research community during the last two decades. The reason for the tremendous growth in this field is most obvious: to secure the communication, authentication and to provide copyright protection. Cryptography, alone doesn't provide security as the communication takes place in presence of 3rd parties and thus message can easily be decrypted by the intruders. Steganography, Watermarking & Fingerprinting have come up as sub-disciplines of Information Hiding, and are being employed in many application areas which includes military, defence, market applications, intelligence agencies, industries, biometrics, banking system and many more. This paper gives an overview on Steganography and Watermarking. The paper concludes with a brief comparison on Steganography and Watermarking on the basis of some parameters.

Key Words: Steganography, Watermarking, Cover Source, Stego File, Watermarked File

I. INTRODUCTION

Humans have continually sought new and efficient ways to communicate. Most of the time, users on the internet have to send, share or receive confidential information. As more and more communication is conducted electronically, new needs, issues, and opportunities are born. Thus, with the rapid development of the internet technologies, digital media needs to be transmitted conveniently over the network [1]. One problem that occurs when we are communicating over the channel is that it may have many eavesdroppers, either passive or active by nature. A passive eavesdropper may be one who just listens and an active one will listen and modify the message. Thus, we prefer that only the intended recipient have the ability to decipher the contents of the communication & we want to keep the message secret. Information Hiding and Cryptography have emerged as two solutions for the above problem. The search of a safe and secret manner of communication is very important now a days, not only for military purposes, but also for commercial goal related to the market strategy as well as the copyright rights [2,3].

Cryptography deals with the encryption of text to form cipher (encrypted) text using a secret key. However, the transmission of cipher text may easily arouse attackers suspicion, and the cipher text may thus be intercepted, attacked or decrypted violently. In order to overcome the shortcomings of cryptographic techniques, Information Hiding strategy was adopted. Information Hiding is a multi disciplinary field that provides hiding of secret data in some cover source. Consider a sender who wants to convey information to a recipient but does not want anyone else to know that the two parties are communicating. The sender could use steganography to hide information within innocuous information, for example, an image that covers the existence of the communication. The image would then be made available on an open channel for anyone to access, but only the intended recipient is aware of the hidden information, and has the ability to extract it.

II. INFORMATION HIDING CLASSIFICATION

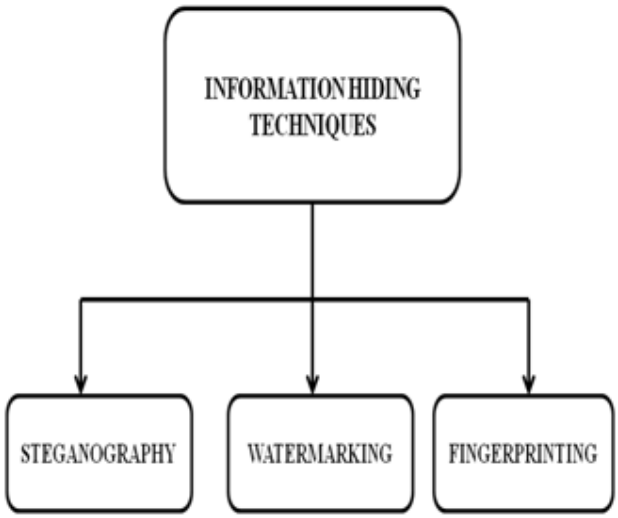

Figure 1: Classification of Information Hiding

Information hiding techniques can be classified into three categories:

a. Steganography:

Steganography is an art and science of hiding information in some cover media. The term originated from Greek roots literally mean "covered writing". The main purpose of steganography is to hide the fact of communication. The sender embeds a secret message into digital media (e.g. image) where only receiver can extract this message [2]. Steganography is discussed in detail in Section 3

b. Watermarking:

Watermarking is defined as a process of embedding information like owner name, company logo etc. in the host data. It is a data hiding technique that protects digital documents, files or images against removal of copyright

information. Section 4 covers Digital Watermarking in detail.

c. Fingerprinting:

Fingerprinting is the user-unique markings of the data for the purpose of tracing the origin of a discovered, illegal copy of data: The core idea of fingerprinting is that each user receives a copy of the object in question, containing a unique marking. The marking can be used to identify the object and thereby also the user if his identity is linked to the fingerprint in some way, for example by distributing copies only to users who identify themselves. Other scenario includes distributing sensitive information (images, videos) to several deputies and trying to trace down a traitor who leaks information to the enemy. The marks must be perceptually invisible and must be present in every frame or image that is being distributed. The marks must be embedded in a robust way so that multiple copying or editing cannot remove them[2,4] .

Figure 2 shows classification of Steganography.

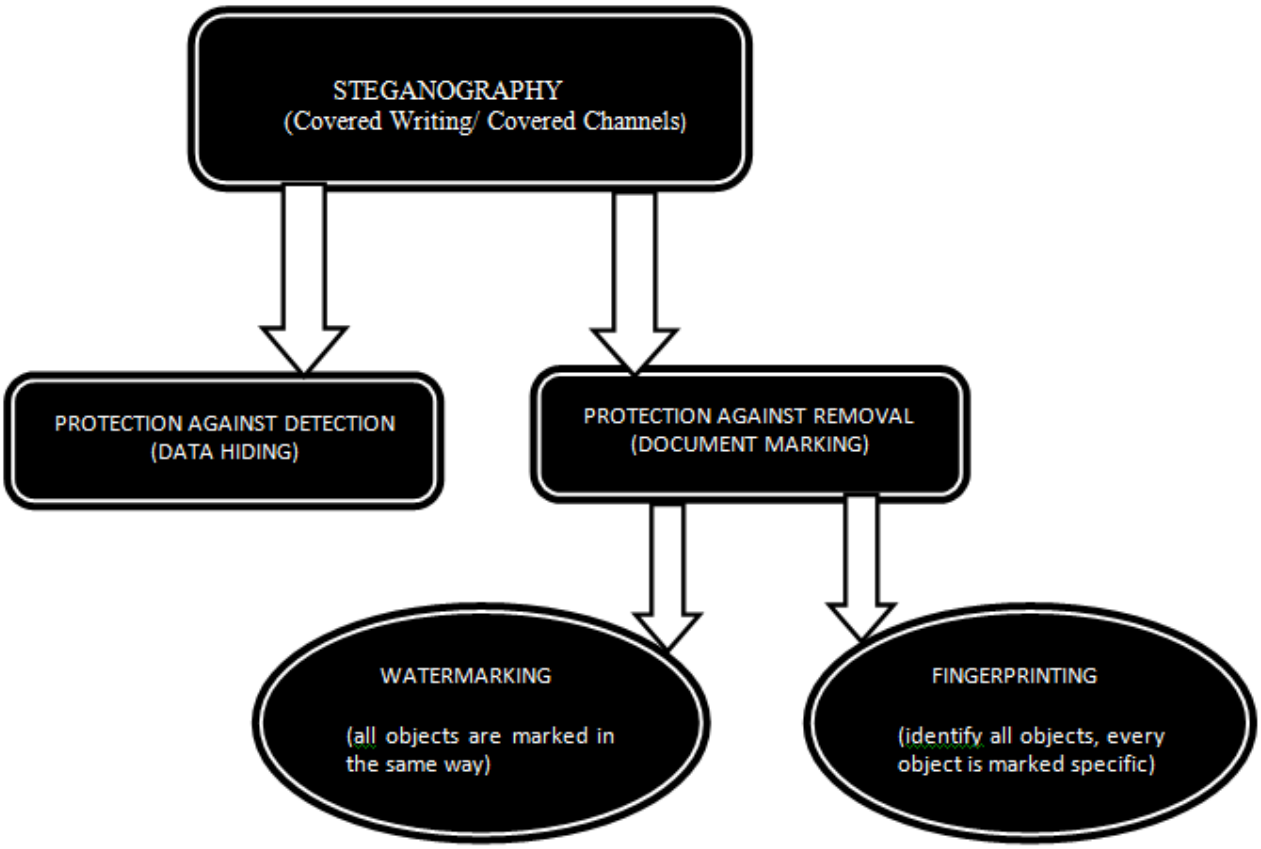

Figure 2 [5]

III. STEGANOGRAPHY

The word ‘steganos’ means “covered or protected” and ‘graphie’ means “writing” [6]. Steganography is thus, not only the art of information hiding, but also the art and science of hiding the fact that communication is even taking place [7].

Privacy is not the only motivation for steganography. By embedding one piece of data inside of another, the two become a single entity, thus eliminating the need to preserve a link between the two different pieces of data, or risk the chance of their separation. One application than exhibits the advantage of this facet of steganography is the embedding of patient information within the medical imagery. By doing so a permanent association between these two information objects is created [8]

The goal of steganography is to avoid drawing suspicion to the transmission of the secret message. The concept of “What You See Is What You get (WYSIWYG)” which we encounter sometimes while printing images or other materials, does not always hold true. Images can be more than what we see with our Human Visual System (HVS); hence they can convey more than merely 1000 words. For decades people strove to create methods for secret communication [9]. A Steganographic system has two main aspects: Steganographic capacity and imperceptibility. However, these two characteristics are at odds with each other. Furthermore, it is quite difficult to increase the Steganographic capacity and simultaneously maintain the imperceptibility of a Steganographic system[10]

A. Requirements of a Steganographic System:

a. The most important requirement for a steganography system is that the presence of the hidden message be undetectable. This means that images with and without secret messages should appear identical to all, irrespective of the possible statistical tests that can be carried out.

b. Another important requirement is the capacity of the communication channel. The challenge is to embed as much information as possible.

c. The last important requirement is that it must be possible to detect the hidden message without the original image[11]

B. Steganography Process:

a. Message Insertion(Sender's end):

a) Cover source (e.g. image, audio, video) and secret message which is to be hidden are given as input to the Message Insertion Algorithm.

b) Use the secret key & Steganographic Algorithm to hide the message in the cover source

c) Stego Output is produced as result of step 2

b. Message Retrieval(Receiver's end):

a) Stego Output send by sender is given as input to the Message Retrieval algorithm.

b) Use the Message retrieval algorithm and secret key to retrieve the message from the Stego output

c) Secret message is retrieved as a result of step 2

Secret key is to be shared between sender &receiver. Even if intruder breaks the Steganographic algorithm, then also message can't be retrieved because of the secret key which is only shared between sender & receiver.

Steganography process is shown in Figure 3 below

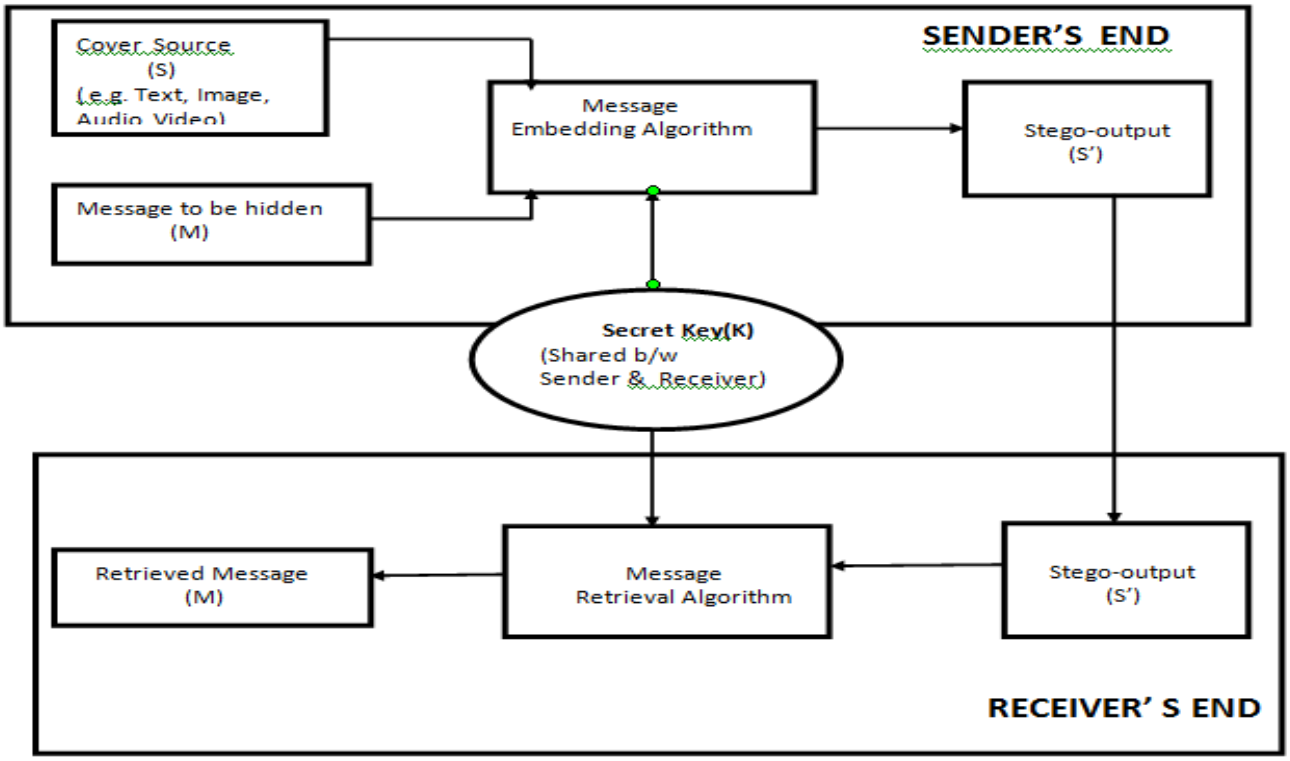

Figure 3

C. Types of Steganography:

a. Text Steganography:

An obvious method of text steganography is to hide a secret message in every *nth* letter of every word of a text message [8].A variety of different techniques exist of hiding data in text files. Text steganography using digital files is not used very often since text files have a very small amount of redundant data.

b. Image Steganography:

Images are very popular cover source for digital steganography. An image is represented as an array of pixels and pixels have a large amount of redundant bits where data can be hidden.

c. Audio/Video Steganography:

Audio/Video files can also be used for hiding secret data. One different technique unique to audio steganography is masking, which exploits the properties of the human ear to hide information unnoticeably. A faint, but audible, sound becomes inaudible in the presence of another louder audible sound [8].This property creates a channel in which to hide information. The larger size of meaningful audio files makes them less popular to use than images.

d. Protocol Steganography:

The term protocol steganography refers to the technique of embedding information within messages and network control protocols used in network transmission [12]. In the layers of the OSI network model there exist covert channels where steganography can be used [13]. An example of where information can be hidden is in the header of a TCP/IP packet in some fields that are either optional or are never used.

D. Applications of Steganography[14,15,16,17]:

a. Secret Communication

Using Steganography, two parties can communicate secretly without anyone knowing about the communication.

Cryptography ,only encode the message but its presence is not hidden and thus draws unwanted attention , Steganography ,thus, on the other hand , hides the existence of message in some cover media.

b. Copyright Protection:

This is basically related to watermarking i.e. a secret message is embedded in the image which serves as the watermark and thus identify it as a intellectual property which belongs to a particular owner.

c. Digital Watermarking:

This is one of the most important applications of Steganography. It basically embed a digital watermark inside an image. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyright infringements and for banknote authentication

d. Use by terrorists[14]:

Steganography at a large scale can also be used by terrorists, who hide their secret messages in innocent cover sources to spread terrorism across the country. Rumours were spread about terrorists using steganography when the two articles titled "Terrorist instructions hidden online" and "Terror groups hide behind Web encryption" were published in newspaper. Other media worldwide cited these rumours many times, especially after the terrorist attack of 9/11, without ever showing proof.

e. Feature Tagging:

Captions, annotations, time stamps and other descriptive elements can be embedded inside an image, such as the name of the individuals in a photo or location in a map. Copying the stego image also copies all of the embedded features and only parties who possess the decoding stego key will be able to extract and view the features

IV. WATERMARKING[21,22,23]

A. What is Watermark?:

Watermarks are identification marks produced during the paper making process. The first watermarks appeared in Italy during the 13th century, but their use rapidly spread across Europe. They were used as a means to identify the papermaker or the trade guild that manufactured the paper. Watermarks continue to be used today as manufacturer's marks and to prevent forgery.

A watermark is a “secret message” that is embedded into a “cover source”. Usually, only the knowledge of a secret key allows us to extract the watermark. Thus, the effectiveness of any watermarking technique depends on how robust the watermark is i.e. Even if someone knows that a watermark is exist (i.e. visible watermarking) in a given object, it should be impossible to remove the watermark from the watermarked object without causing a distortion or destroying the original (watermarked) object[16,17].

Figure 4: Watermark embedded in an Image

B. Types of Watermark[24]:

Watermarks can be categorised into 3 categories as follows:

a. ***Fragile Watermarks***: Fragile watermark comes under those category of watermarks that can be broken or distorted under slight changes.
b. ***Semi Fragile Watermarks***: These are the watermarks that can be broken under all changes that exceed a user specified threshold.
c. ***Robust watermarks***: These are the most effective watermarks. Robust watermarks can tolerate moderate to severe signal processing attacks (compression, rescaling, filtering)

C. Properties of Watermark[22,25,26,27]:

a. Imperceptible:

The watermark should be imperceptible in such a way that it may not effect the cover image or the audio quality of the original signal.

b. Undeletable:

It should be difficult or impossible for the intruder to remove the watermark without degrading the quality of image or original signal.

c. Robust to Lossy Data Compression:

The watermark should be embedded in such a way that it should survive the lossy compression techniques like JPEG and MPEG which are commonly used for transmission and storage.

d. Robust to Signal Manipulation and Processing operations:

The watermark should still be retrievable even if common signal processing operation arc applied, such as signal enhancement, geometric image operations, noise, filtering, etc.

D. What is Watermarking?:

Digital watermarking is a technique for inserting information (the watermark) into a cover source for e.g. an image, which can be later extracted or detected for variety of purposes including identification and authentication purposes

Thus, Digital watermarking is a method which helps for copyright, to authenticate data, identify illegal copies and detect illegal changes made in the data. The purpose of digital watermarks is to provide copyright protection for intellectual property that’s in digital format. Watermarking has become the key method for protecting digital elements such as image, audio and video[2,4].

E. Types of Watermarking[26]:

a. Visible Watermarking:

As the name suggests, visible watermarking refers to the information visible on the image or video or picture. Visible watermarks are typically logos or text. For example, in a TV broadcast, the logo of the broadcaster is visible at the right side of the screen.

b. Invisible Watermarking:

Invisible watermarking refers to adding information in a video or picture or audio as digital data. It is not visible or perceivable, but it can be detected by different means. It may also be a form or type of steganography and is used for widespread use. It can be retrieved easily.

F. Factors affecting Watermarking[20,22]:

- ***a. Tranparency*:** Transparency defines the invisibility of the watermark. The watermark must not be visible in the image under typical viewing conditions.
- ***b. Capacity*:** Capacity defines the amount of watermark i.e its size that can be embedded in an image. It also defines the ability to detect watermarks with a low probability of error as the number of watermarked versions of the image increases
- ***c. Robust*:** If the watermarking technique used is robust then watermark can easily be extracted even after the image has undergone some linear or non linear operations
- ***d. Perceptibility*:** A watermark is called imperceptible if the original cover signal and marked signal are indistinguishable and is called perceptible if the presence of marked signal is noticeable.

G. Verification/Detection Methods[28]:

For the purpose of verification or detection, watermarking can be categorized as follows;

a. Non-blind:

In this case, the watermarking scheme requires the use of the original image

b. Semi-Blind:

In this method, the watermarking scheme requires the watermark data and/or the parameters used to embed the data

c. Blind:

In this method, the watermarking scheme does not require the original image or any other data

H. Watermarking Process:

a. Watermark Embedding System :

a) Input to the system are Cover Data (I), Watermark (W) and Secret Key(K).
b) Secret Key is shared between Sender and Receiver.
c) Watermarked Data(I') is produced as output(as shown in Figure)

b. Watermark Recovery System :

a) Input to the system is Watermarked Data(I') and Secret Key(K)
b) Same key is used for Embedding as well as recovery of watermark
c) Watermark is produced as output(as shown in Figure)

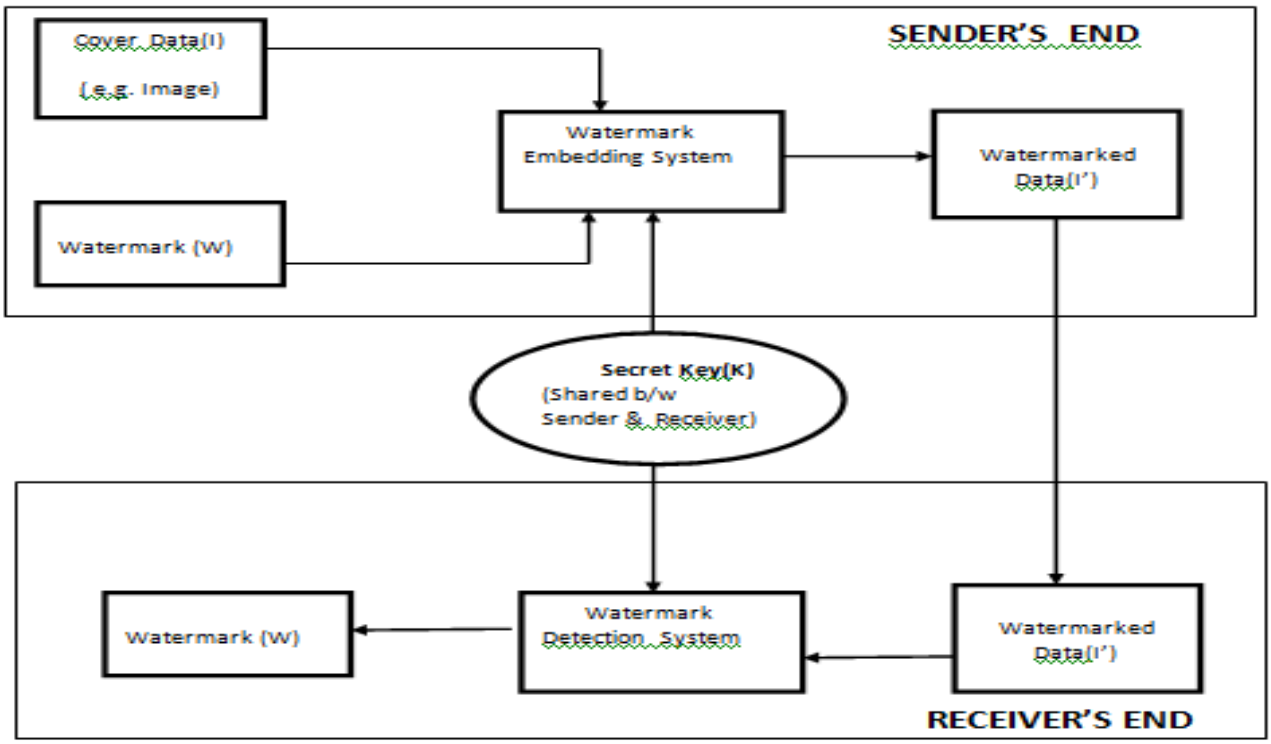

Figure 5

I. Applications of Watermarking[20,23,25,26]:

a. Copyright Protection:

Copyright Protection is one of the most important application of Watermarking. By embedding owner's information, logo in the original data it helps to prevent others from claiming the copyright and to disallow unauthorized copying of the cover. It also requires very high level of robustness

b. Content Authentication:

Watermarking is also widely used for the proof of authenticity of documents. The surfaces of ATM cards, ID cards, personal checks and credit cards could be watermarked with company's/ organisation's logo which serves as a authentic document belonging to that particular person/company or organisation

c. Forensic Applications:

For embedding digital watermarks, digital still pictures and video cameras can be used, that have integrated modules for embedding watermarks so that pictures and videos are fingerprinted with the time and device identifier of creation. Thus, printer, scanners and photocopiers may refuse the operations of those documents which are not authorized

d. Secure & Invisible Communication:

By using invisible digital watermarking, data can be communicated secretly to the destination with high level of robustness. This concept is widely used in defence & military, intelligent sectors and different organisations.

e. Transaction Monitoring or Tracking:

Embedding a watermark, helps to convey information about the legal recipient of the cover source. This can be useful to monitor or trace back illegally produced copies of the cover. This is usually referred as 'Fingerprinting'

f. Hidden Annotations:

Watermarking can be used in medical applications, for unique identification of patient's records. Patient's records can be embedded directly in the image for each patient which helps in efficient retrieval of patient's records and mismatch of patient's and their records.

g. Automatic Auditing of Radio Transmissions:

A robot can "listen" to a radio station and look for marks, which indicate that a particular piece of music, or advertisement, has been broadcasted.

V. STEGANOGRAPHY V/S WATERMARKING[29,30]

a. Objective:

The main aim of Steganography, is to hide the message (M) in some cover source (S) to produce a stego output (S') , in such a way that ***presence of M can't be detected*** by the intruder. It can also be regarded as one-to-one communication.

Watermarking aims to embed a watermark (W) in some cover data (D) to obtain new data (D'), in such a way that the ***watermark W can't be replaced or removed*** by the intruder. It can also be regarded as one-to-many communication.

b. Secret Data:

In Steganography, ***Payload*** works as secret data embedded with carrier without knowing its presence.

In Watermarking, ***Watermark*** is the secret data which is embedded with carrier with or without knowing its presence.

c. Failure Condition:

Steganography fails if the presence of hidden message is detected by the intruder. So, the failure condition in this case is ***"Detection"***

Watermarking fails if the intruder is able to remove or replace the watermark from the original data. Failure condition here is ***"Removal"***

d. Output/Result:

"Stego-File" is produced as output in case of Steganography which contains hidden message.

Watermarking produces ***"Watermarked File"*** as output with embedded watermark which can be visible or invisible.

e. Ownership:

Steganography ***does not*** provide ***any proof of ownership*** i.e. by using steganography alone one cannot tell anything regarding the authenticity of the document. It only embeds secret data in some cover source but does not tell to whom that data belongs.

On the other hand, **Watermarking** provides ***proof of ownership***. Embedding a watermark in the cover data helps in authenticity of the document i.e. it let us know that this particular document/image belongs to a particular company, person or organisation.

f. Robustness:

The purpose of Steganography is to provide covert communication between two parties whose existence is unknown to possible attacker, a successful attack consists in detecting the existence of this communication (e.g., using statistical analysis of images with and without hidden information). Robustness does not play an important role in case of Steganography as the main motive here is only to protect the message against detection.

Watermarking, on the other hand, embeds a watermark which acts as a proof of ownership like company's logo, owner's information. Thus, watermarking has an additional requirement of ***robustness against possible attacks***. Watermarks can be visible or invisible which may vary for different applications. Thus, robustness of the watermark plays a very important role. A watermark is considered as robust if , it can be extracted even after image has undergone several linear or non linear operations and survives some lossy compression techniques.

VI. CONCLUSION

This paper gives an overview on Steganography and Watermarking and also provides a comparison between them on the basis of some parameters. Steganography, a

branch of Information Hiding deals with hiding the secret data in some cover source (text, image, audio, video) to produce a stego file with embedded data. Watermarking, on the other hand, deals with copyright protection by embedding a watermark in some cover data to produce a watermarked file. Steganography fails if the hidden message can be detected by any person other than receiver. Watermarking, on the other hand, is not considered as robust if the embedded watermark can be removed or replaced by the intruder. Thus, Robustness of the watermark plays a very important role in watermarking. Both Steganography and Watermarking are being used in many real life scenarios because of wide variety of applications they address.

VII. REFERENCES

[1]. Arvind Kumar and Km. Pooja "Steganography- A Data Hiding Technique" , International Journal of Computer Applications (0975 – 8887) ,Volume 9– No.7, November 2010

[2]. Rajkumar Yadav "Study of Information Hiding Techniques and their Counterattacks: A Review Article" , International Journal of Computer Science & Communication Networks,Vol 1(2), 142-164, Oct-Nov 2011

[3]. Mehdi Kharrazi, Husrev T. Sencar and Nasir Memon "Image Steganography : Concepts and Practices "Polytechnic University, Brooklyn, NY 11201, USA

[4]. Adel Almohammad "Steganography-Based Secret and Reliable Communications: Improving Steganographic Capacity and Imperceptibility" A thesis submitted for the degree of Doctor of Philosophy, Department of Information Systems and Computing , Brunel University, August, 2010

[5]. R. Popa, An Analysis of Steganographic Techniques, The "Politehnica" University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering, (http://ad.informatik.unifreiburg.de/mitarbeiter/will/dlib_bookmarks/digital-atermarking/popa/popa.pdf, 1998)

[6]. Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn "Information Hiding A Survey"Proceedings of the IEEE, special issue on protection of multimedia content, 87(7):1062{1078, July 1999.

[7]. Angela D. Orebaugh " Steganalysis: A Steganography Intrusion Detection System" , George Mason University

[8]. Lisa M. Marvel "Image Steganography for Hidden Communication" A Dissertation Submitted to the Faculty of the University of Delaware in partial fulfilment of the requirements for the degree of Doctor of Philosophy in Electrical Engineering ,Spring 1999

[9]. T. Morkel , J.H.P. Eloff and M.S. Olivier "An Overview of Image Steganography"

[10]. Abbas Cheddad , JoanCondell, KevinCurran, PaulMcKevitt "Digital image steganography: Survey and analysis of current methods" Signal Processing 90 (2010) 727–752

[11]. Rajkumar Yadav "Analysis of Incremental Growth in Image Steganography Techniques for Various Parameters" Int. J. Comp. Tech. Appl., Vol 2 (6),1867-1870, NOV-DEC 2011

[12]. W Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," IBM Systems Journal, Vol. 35, No. 3 and 4, pp. 313-336, 1996.

[13]. Abbas Cheddad " Strengthening Steganography in Digital Images" ,School of Computing and Intelligent Systems, Faculty of Engineering, University of Ulster, Magee

[14]. http://en.wikipedia.org/wiki/Steganography

[15]. "Applications of Steganography" http://www.datahide.com/BPCSe/applications-e.html

[16]. http://en.wikipedia.org/wiki/Steganography

[17]. Khan, Mohammed Minhajuddin , "Steganography"

[18]. Abbas Cheddad " Strengthening Steganography in Digital Images" ,School of Computing and Intelligent Systems, Faculty of Engineering, University of Ulster, Magee

[19]. Rosziati Ibrahim and Teoh Suk Kuan "Steganography Algorithm to Hide Secret Message inside an Image" Computer Technology and Application 2 (2011) (102-108)

[20]. http://en.wikipedia.org/wiki/Digital Watermarking

[21]. M..M. Yeung, F.Mintzer, "An invisible Watermarking technique for image Verification", Proceedings of ICIP'97, Santa Barbara, CA, USA, October 26- 29, 1997, Vol II, pp. 680-683

[22]. Dr. Mohammed Al-Mualla and Prof. Hussain Al-Ahmad " Information Hiding : Steganography and Watermarking" , Multimedia Communication and Signal Processing (MCSP) Research Group, Etisalat College of Engineering , P.O.Box: 980, Sharjah, UAE

[23]. Chiou-Ting Hsu and Ja-Ling Wu, Senior Member, IEEE, "Hidden Digital Watermarks in Images" IEEE Transactions on Image Processing, VOL. 8, NO. 1, January 1999

[24]. Eda Ormanci, Ebru Arisoy "Image Adaptive and Fragile Watermarking"

[25]. Jonathan Cummins, Patrick Diskin, Samuel Lau and Robert Parlett " Steganography and Digital Watermarking" , School of Computer Science, The University of Birmingham

[26]. Nasir Memon, "Information Hiding, Digital Watermarking and Steganography" Polytechnic University, Brooklyn

[27]. Avani Bhatia, Mrs. Raj Kumari "Digital Watermarking Techniques", U.I.E.T, Panjab University, Chandigarh

[28]. Adam Day, "Invisible Digital Watermarking"

[29]. Manoj Kumar Sharma, Dr. P. C. Gupta, "A Comparative Study of Steganography and Watermarking" IJRIM ,Volume 2, Issue 2 (February 2012) (ISSN 2231-4334)

[30]. J. O'Ruanaidh, W. Dowling, F. Boland, \Watermarking digital images for copyright protection", IEEE Proceedings on Vision, Image and Signal Processing, 143(4), pp 250-256, August 1996.