Comparative Study on Video Steganography in Spatial and IWT Domain

Rizwana ali[1], Nilesh Bodne[2]

[1]*M.Tech student, Department of Electronics & Communication Engg., Vidarbha Institute of technology Nagpur, India*

[2]*Assistant Professor, Department of Electronics & Communication Engg., Vidarbha Institute of technology, Nagpur, India*

Abstract: Data Hiding has risen as a multidisciplinary field and is getting extensive help from the exploration network amid the most recent two decades. The explanation behind the enormous development in this field is most self-evident: to verify the correspondence, validation and to give copyright insurance. Cryptography, alone doesn't give security as the correspondence happens in nearness of outsiders and along these lines message can without much of a stretch be unscrambled by the interlopers. Steganography, Watermarking and Fingerprinting have come up as sub-controls of Information Hiding, and are being utilized in numerous application regions which incorporates military, barrier, showcase applications, insight organizations, ventures, biometrics, banking framework and some more. This paper gives a diagram on Steganography and Watermarking. The paper finishes up with a short examination on Steganography and Watermarking based on certain parameters.

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

1. INTRODUCTION

People have constantly looked for new and productive approaches to impart. More often than not, clients on the web need to send, share or get private data. As increasingly more correspondence is directed electronically, new needs, issues, and openings are conceived. Therefore, with the fast improvement of the web advances, computerized media should be transmitted advantageously over the system [1]. One issue that happens when we are conveying over the channel is that it might have numerous busybodies, either detached or dynamic naturally. An inactive spy might be one who just tunes in and a functioning one will tune in and alter the message. Along these lines, we incline toward that just the planned beneficiary can interpret the substance of the correspondence and we need to keep the message mystery. Data Hiding and Cryptography have risen as two answers for the above issue. The inquiry of a sheltered and mystery way of correspondence is imperative now a days, for military purposes, yet additionally for business objective identified with the market procedure just as the copyright rights [2,3].

Cryptography manages the encryption of content to shape figure (encoded) content utilizing a mystery key. In any case, the transmission of figure content may effectively stir assailants doubt, and the figure content may accordingly be blocked, assaulted or unscrambled fiercely. So as to beat the weaknesses of cryptographic procedures, Information Hiding system was embraced. Data Hiding is a multi disciplinary field that gives stowing away of mystery information in some spread source. Consider a sender who needs to pass on data to a beneficiary however does not need any other individual to realize that the two gatherings are imparting. The sender could utilize steganography to shroud data inside harmless data, for instance, a picture that covers the presence of the correspondence. The picture would then be made accessible on an open channel for anybody to get to, yet just the expected beneficiary knows about the shrouded data, and can remove it.

2. INFORMATION HIDING CLASSIFICATION

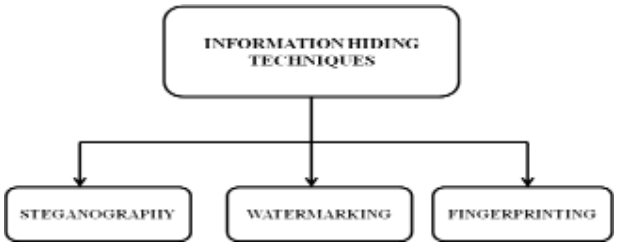


Figure 1: Classification of Information Hiding

Information hiding techniques can be classified into three categories:

a. Steganography:

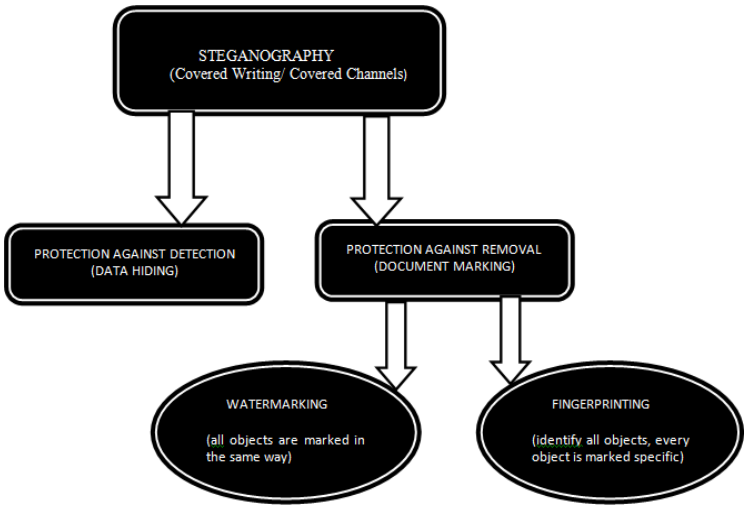
Steganography is a craftsmanship and investigation of concealing data in some spread media. The term began from Greek roots actually signify "secured composition". The principle reason for steganography is to conceal the reality of correspondence. The sender implants a mystery message into advanced media (for example picture) where no one but collector can remove this message [2]. Steganography is talked about in detail in Section 3Watermarking:

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.***

b. 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.



3. STEGANOGRAPHY

Figure 2 [5] 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);

The word 'steganos' signifies "secured or ensured" and 'graphie' signifies "expressing" [6]. Steganography is in this way, the specialty of data stowing away, yet in addition the workmanship and exploration of concealing the way that correspondence is notwithstanding occurring [7]. Security isn't the main inspiration for steganography. By inserting one bit of information within another, the two turn into a solitary element, in this manner dispensing with the need to save a connection between the two distinct bits of information, or hazard the opportunity of their division. One application than displays the upside of this aspect of steganography is the implanting of patient data inside the therapeutic symbolism. By doing as such a perpetual relationship between these two data objects is made [8]

The objective of steganography is to abstain from attracting doubt to the transmission of the mystery message. The idea of "What You See Is What You get (WYSIWYG)" which wehence 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 essential necessity for a steganography framework is that the nearness of the concealed message be imperceptible. This implies pictures with and without mystery messages ought to seem indistinguishable to all, independent of the conceivable factual tests that can be completed.

B. Another imperative prerequisite is the limit of the correspondence channel. The test is to install however much data as could be expected.

C. The last imperative prerequisite is that it must be conceivable to identify the concealed message without the first image[11]

Steganography Process:

Message Insertion(Sender's end): Cover source (for example picture, sound, video) and mystery message which is to be covered up are given as contribution to the Message Insertion Algorithm. Use the mystery key and Steganographic Algorithm to conceal the message in the spread Stego Output is produced as result of step 2

B. Message Retrieval(Receiver's end):

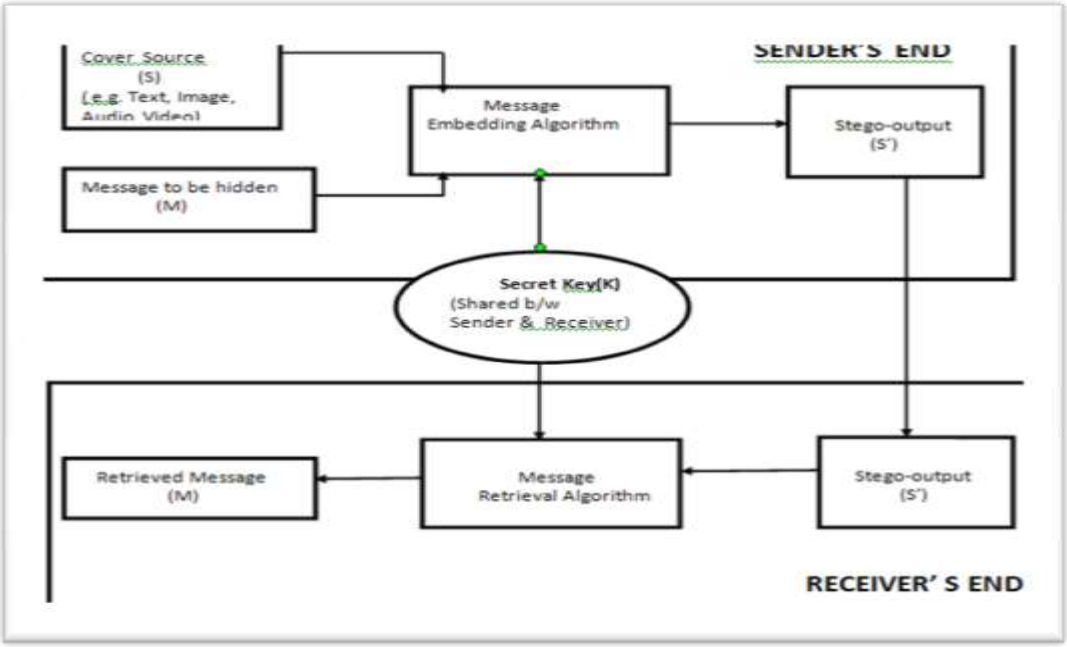
a) Stego Output send by sender is given as contribution to the Message Retrieval calculation.

b) Use the Message recovery calculation and mystery key to recover the message from the Stego yield

c) Secret message is recovered because of stage 2 Secret key is to be shared between sender &receiver.

Regardless of whether gatecrasher breaks the Steganographic calculation, at that point additionally message can't be recovered in light of the mystery key which is just shared between sender and recipient.

Steganography process is appeared in Figure 3 beneath



4. Types of Steganography:

A. Text Steganography:

An undeniable strategy for content steganography is to shroud a mystery message in each nth letter of each expression of an instant message [8].A wide range of methods exist of concealing information in content documents. Content steganography utilizing computerized records isn't utilized frequently since content documents have a little measure of repetitive information.

Image Steganography:

Pictures are exceptionally mainstream spread hotspot for advanced steganography. A picture is spoken to as a variety of pixels and pixels have a lot of repetitive bits where information can be covered up.

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 Figure 3 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.

B. Protocol Steganography:

The term convention steganography alludes to the method of inserting data inside messages and system control conventions utilized in system transmission [12]. In the layers of the OSI organize display there exist secretive channels where steganography can be utilized [13]. A case of where data can be covered up is in the header of a TCP/IP parcel in certain fields that are either discretionary or are never utilized.

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

C. 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.

D. 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.

E. Digital Watermarking:

This is a standout amongst the most imperative utilizations of Steganography. It fundamentally insert a computerized watermark inside a picture. Computerized watermarks might be utilized to confirm the realness or honesty of the transporter flag or to demonstrate the personality of its proprietors. It is unmistakably utilized for following copyright encroachments and for banknote verification

5. WATERMARKING[21,22,23]

A. What is Watermark?:

Watermarks are ID marks delivered amid the paper making process. The main watermarks showed up in Italy amid the thirteenth century, yet their utilization quickly spread crosswise over Europe. They were utilized as a way to recognize the papermaker or the exchange organization that produced the paper. Watermarks keep on being utilized today as maker's imprints and to forestall phony.

A watermark is a "mystery message" that is installed into a "spread source". Typically, just the information of a mystery key enables us to separate the watermark. Consequently, the adequacy of any watermarking procedure relies upon how hearty the watermark is for example Regardless of whether somebody realizes that a watermark is exist (for example unmistakable

watermarking) in a given article, it should be difficult to expel the watermark from the watermarked object without causing a contortion or pulverizing the first (watermarked) object

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. Factors affecting Watermarking:

A. Tranparency: *Transparency characterizes the intangibility of the watermark. The watermark must not be obvious in the picture under run of the mill seeing conditions.*

B. Capacity: *Capacity characterizes the measure of watermark i.e its size that can be implanted in a picture. It likewise characterizes the capacity to recognize watermarks with a low likelihood of blunder as the quantity of watermarked adaptations of the picture increments*

C. Robust: *If the watermarking strategy utilized is powerful then watermark can undoubtedly be removed even after the picture has experienced some direct or non straight activities*

D. Perceptibility: *A watermark is called subtle if the first spread flag and stamped flag are vague and is called recognizable if the nearness of checked flag is observable.*

a. Applications of Watermarking

b. 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

c. 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

d. 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

e. 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.

f. 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'

g. 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.

h. 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.

6. CONCLUSION

This paper gives a review on Steganography and Watermarking and furthermore gives an examination between them based on certain parameters. Steganography, a part of Information Hiding manages concealing the mystery information in some spread source (content, picture, sound, video) to create a stego record with installed information. Watermarking, then again, manages copyright assurance by inserting a watermark in some spread information to deliver a watermarked document. Steganography comes up short if the shrouded message can be distinguished by any individual other than collector. Watermarking, then again, isn't considered as powerful if the implanted watermark can be evacuated or supplanted by the interloper. Consequently, Robustness of the watermark assumes an imperative job in watermarking. Both Steganography and Watermarking are being utilized in numerous genuine situations on account of wide assortment of utilizations they address.

7. REFERENCES

- Arvind Kumar and Km. Pooja "Steganography- A Data Applications (0975 – 8887) ,Volume 9– No.7, November 2010
- 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-Nov2011
- Mehdi Kharrazi, Husrev T. Sencar and Nasir Memon "Image Steganography: Concepts and Practices "Polytechnic University, Brooklyn, NY 11201, USA
- 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
- 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_bo okmarks/digital-atermarking/popa/popa.pdf, 1998)
- 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.
- Angela D. Orebaugh "Steganalysis: A Steganography Intrusion Detection System" , George Mason University
- Lisa M. Marvel "Image Steganography for Hidden Communication" A Dissertation Submitted to the Faculty of the University of Delaware in partial fulfilment of the Electrical Engineering, Spring 1999
- T. Morkel , J.H.P. Eloff and M.S. Olivier "An Overview of Image Steganography"
- "Techniques for data hiding," IBM Systems Journal, Vol. 35, No. 3 and 4, pp. 313-336, 1996.
- http://www.datahide.com/BPCSe/applications-e.html

- http://en.wikipedia.org/wiki/Steganography
- Khan, Mohammed Minhajuddin , "Steganography"
- 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
- 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.
- Abbas Cheddad "Strengthening Steganography in Digital Images" ,School of Computing and Intelligent Systems, Faculty of Engineering, University of Ulster,Magee
- http://en.wikipedia.org/wiki/Steganography
- "Applications of Steganography" http://www.datahide.com/BPCSe/applications-e.html
- Abbas Cheddad " Strengthening Steganography in Digital Images" ,School of Computing and Intelligent Systems Faculty of Engineering, University of Ulster, Magee Rosziati Ibrahim and Teoh Suk Kuan "Steganography Algorithm to Hide Secret Message inside an Image" Computer Technology and Application 2 (2011) (102-108)
- http://en.wikipedia.org/wiki/Digital Watermarking
- 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
- 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
- Chiou-Ting Hsu and Ja-Ling Wu, Senior Member, IEEE, "Hidden Digital Watermarks in Images" IEEE Transactions on Image Processing, VOL. 8, NO. 1, January1999
- Eda Ormanci, Ebru Arisoy "Image Adaptive and Fragile Watermarking"
- Jonathan Cummins, Patrick Diskin, Samuel Lau and Robert Parlett " Steganography and Digital Watermarking" , School of Computer Science, The University of Birmingham
- Nasir Memon, "Information Hiding, Digital Watermarking and Steganography" Polytechnic University, Brooklyn
- Avani Bhatia, Mrs. Raj Kumari "Digital Watermarking Techniques", U.I.E.T, Panjab University, Chandigarh Adam Day, "Invisible Digital Watermarking"
- Manoj Kumar Sharma, Dr. P. C. Gupta, "A Comparative Study of Steganography and Watermarking" IJRIM,Volume 2, Issue 2 (February 2012) (ISSN 2231-4334)
- J. O'Ruanaidh, W. Dowling, F. Boland, \Watermarking digital imagesfor copyright protection", IEEE Proceedings on Vision, Image and Signal Processing, 143(4), pp 250-256, August 1996.