Research Article

Robust Digital Watermarking Techniques for protecting copyright Applied to Digital Data: A Survey

Lakshman Ji[a], Dr Shiv Kumar [b]

[a]Ph.D Research Scholar , [b]Assistant Professor
[a, b] Department of Computer Science and Engineering, Sarvepalli Radhakrishanan University,Bhopal, Hoshangabad Rd, Near Nissan Motors, Misrod, Bhopal, Madhya Pradesh 462026

Article History: Received: 10 November 2020; Revised 12 January 2021 Accepted: 27 January 2021; Published online: 5 April 2021

Abstract: The colossal prominence of the World Wide Web in the mid 1990's shown the business capability of offering media assets through the computerized networks. Since business intrigues look to utilize the advanced organizations to offer computerized media revenue driven, they have a solid interest in ensuring their proprietorship rights. Since the danger of utilizing media data, advanced fabrications, and unapproved sharing (robbery) of

computerized content has expanded among content makers, merchants and clients. Today mixed media data theft alone has exposed all the enterprises to multi-billion income misfortunes. Customary advanced substance security methods, for example, encryption and scrambling, alone can't give satisfactory insurance of copyrighted substance, in light of the fact that these advances can't ensure computerized content whenever they are decoded. One approach to debilitate illicit duplication is to embed data known as watermark, into possibly weak information so that it is difficult to isolate the watermark from the information. Computerized watermarking is the way toward embedding's an advanced sign or example inside a computerized picture, which gives proof of realness. This paper presents a study on different data concealing strategies and depicts characterization of advanced Watermarking procedures.

Keywords: water marking protecting act, invisible data hiding, conceptual techniques, visible techniques, copyright, video data, audio data, text data etc

1. Introduction

Altering, dissemination and proliferation of the private computerized mixed media are getting incredibly simpler and quicker with the presence of the web and the accessibility of inescapable and ground-breaking sight and sound apparatuses. The issues of unlawful duplication, counterfeit money, business security, ensuring licensed innovation and so on are getting increasingly significant. Advanced watermarking has arisen as a potential technique to handle these issues. Advanced pictures are the most mainstream transporter record design among different accessible organizations like sound documents, video documents, and text records on account of their recurrence on the Internet. As of recently, licensed innovation and worth has consistently been bound to some actual holder that couldn't be effectively copied, in this manner ensuring that the maker profits by his work. Accordingly, data concealing procedures assumes an imperative part for giving copyright verification.

2. History of informaton hiding:

This is basically methods of data hiding through digital water making techniques. This is basically signal work related to final information hiding technique:

1. Digital visible data hiding methods used.
2. Digital water making data invisible methods is also used.
3. Digital data hiding techniques based on algorithms also performed.
4. Data hiding technique is based n water marking concept.
5. Data hidden is used for conceptual define for protecting right of information.
6. Data hiding is basically concept of encryption and decryption method.
7. Watermarking technique is also work with encryption technique. and one step forward working.

3. Digital water marking:

Digital water marker is a typically kind of marker of embedded noise tolerant signal such as audio data, video data, text data, copy right form of data protecting act. Water marking is the process of hiding digital signal in form of carrier signal .it means digital information or raw information hiding in form of carrier signal form of data hiding.

The following points are remembering for digital water marker signal protecting but not related to:

1. Data contain in carrier signal but information should not contain related to carrier signal.

The data information is hiding form digital marking technique is Hiding messages using imperceptible ink was similarly standard. Old Romans used to make their secret messages between the unmistakable lines by intangible ink that is all things considered set up by natural item squeezes, milk, and pee, etc At the moment that warmed, the imperceptible ink would darken and gets self-evident. Ovid in his ―Art of Love‖ prescribes using milk to make imperceptibly. During World Clearlyunprejudiced dispute is inside and out restricted and dismissed. Ishan Hard hit. Bar issue impacts appearance for restriction on results, shooting suets and vegetable oils." By social occasion the second letter from each word the secret message uncovers:

The priest Johannes Trithemius, authors of current cryptography, depicted a broad framework for covering mystery messages inside harmless writings in his three volume work

4. Disciplines Of Information Hiding

In old occasions, the messages were sent on foots. There are just two choices to shroud a message: conceal it on the courier, or have the courier remember it. Powerful watermarking is the watermarking calculation that can endure not just such broad activities, for example, pressure, adding clamor, separating, A/D or D/A change, etc, yet in addition such mathematical assaults, for example, turn, scaling interpretation, shearing, etc.

A wide scope of issues past the installing messages in substance have been enclosed by the overall term Information covering up (or information stowing away). The term stowing away can allude to either for data mystery (Steganography) or data impalpability (Watermarking). Two significant sub orders of data covering up are Watermarking and Steganography [4] that are firmly identified with one another yet with various hidden properties, necessities and plans, subsequently bring about various and consider solution of techniques based performed.

Cateogries of digtal water marking: protectingcopy:

these are two types of digital water marking techniques;

1. Visible techniques used for data hiding.
2. Invisible techniques used by water marking for data hiding.
3. Create images by using techniques for water marking methods.

Various waysw of image as tag water mark:

The various method for adopting water marking protecting on image or video data. fist we will explain the various ways for protecting watermarking techniques:

1. Create your logo and put on transparent sheet as back ground save it as format of PNG file format.
2. Open the basic image when we want water mark on it.
3. Now the image is going watermark. so we will do click on image and put your logo to image where u want protecting.
4. Resize your image with logo and keep it corner side of your image right or left side of image.
5. Water marking the process where u can use to image or text data protecting from any kind of your logo and prototype image. So it is the process of copy right logo imposing of image or text data impose on corner or top size of data text format.
6. The various unique method of data secret as format used by water marking.

The general disciplines of information hiding [1], [3]-[9] are given in figure 1.

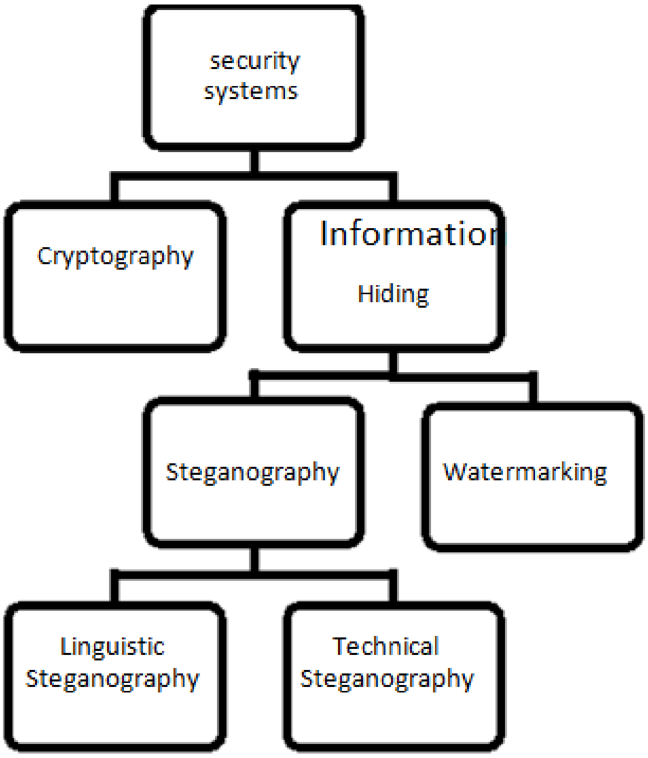


Fig. 1. Information hide porotype model

A. Cryptography

. The square blueprint of cryptography [1] is given in figure 2.

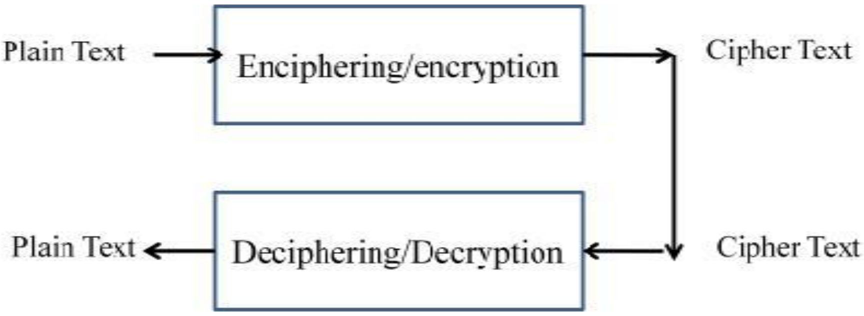


Fig. 2. Block Diagram of Cryptography

The strength of Steganography would accordingly have the option to be heightened by solidifying it with cryptography.

B. Steganography:

. This type of steganography is combine with cryptography and one more step for hiding the data with the help of secret file format. The steganography is the method of hiding data by using secret file format for protecting detection. The data file is extracted rom the place of receiver side. It is the better kid of steganography technique used with encryption step involved.

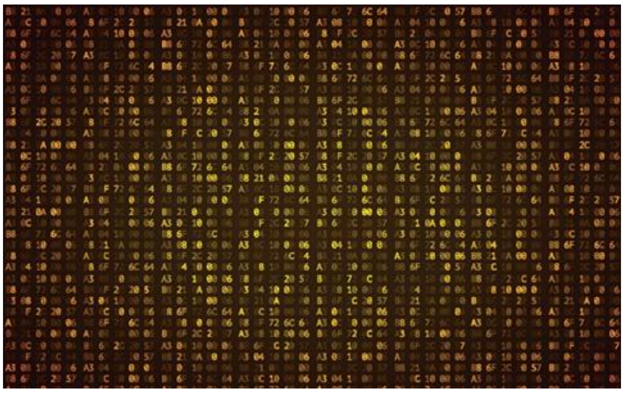


Fig 3. Example file of steganography.

Figure 3 shows the generic model of Steganography

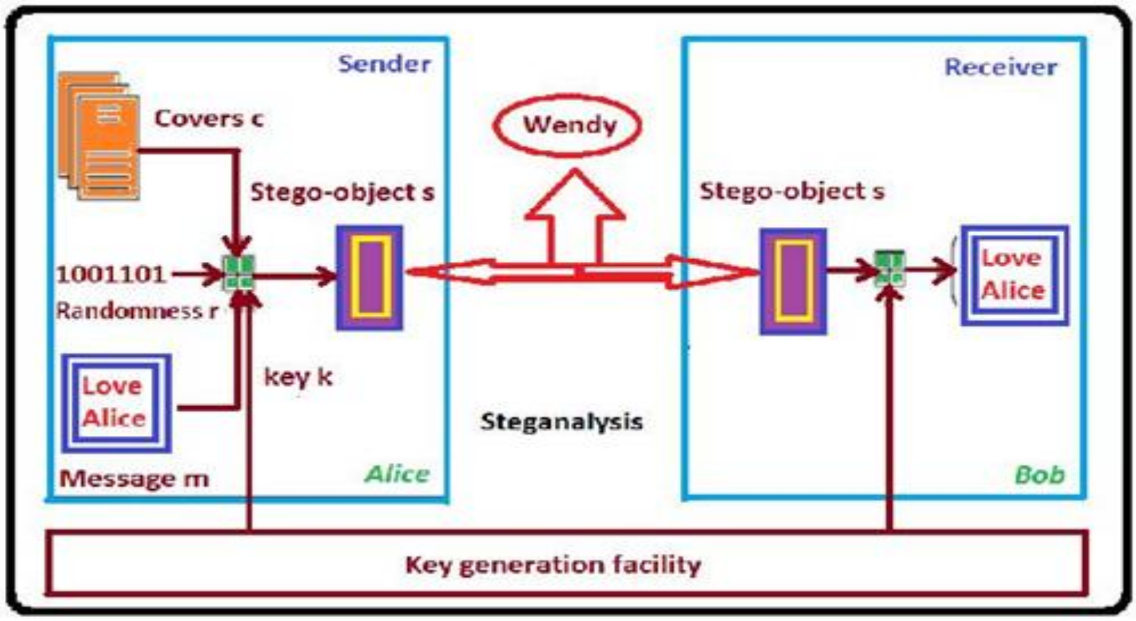
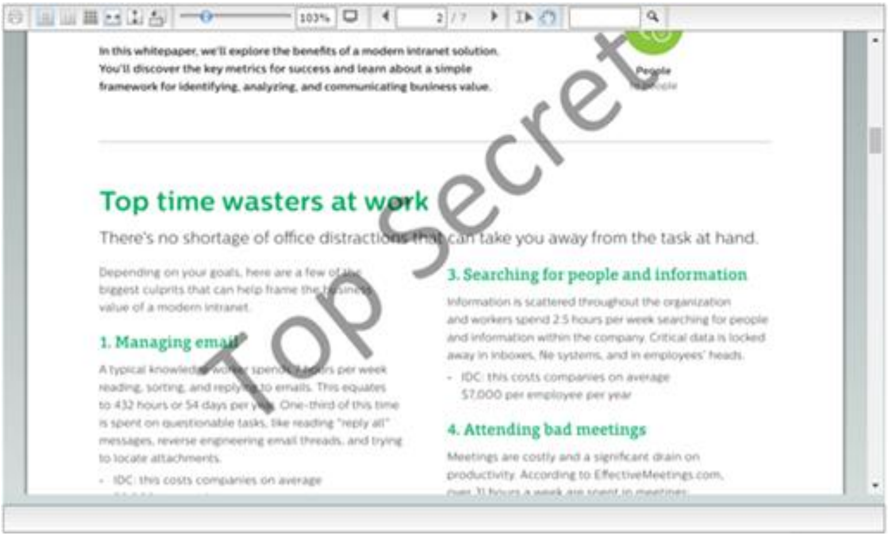


Fig. 4. The pro-type model Steganography

Watermarking

Progressed watermarking is typically used for ownership copy right techniques. It is hiding form of process.



In this whitepaper, we'll explore the benefits of a modern intranet solution. You'll discover the key metrics for success and learn about a simple framework for identifying, analyzing, and communicating business value.

Top time wasters at work

There's no shortage of office distractions that can take you away from the task at hand.

Depending on your goals, here are a few of the biggest culprits that can help frame the business value of a modern intranet.

1. Managing email

A typical knowledge worker spends 8 hours per week reading, sorting, and replying to emails. This equates to 432 hours or 54 days per year. One-third of this time is spent on questionable tasks, like reading "reply all" messages, reverse engineering email threads, and trying to locate attachments.

- IDC: this costs companies on average

3. Searching for people and information

Information is scattered throughout the organization and workers spend 2.5 hours per week searching for people and information within the company. Critical data is locked away in inboxes, file systems, and in employees' heads.

- IDC: this costs companies on average $7,000 per employee per year

4. Attending bad meetings

Meetings are costly and a significant drain on productivity. According to EffectiveMeetings.com, over 31 hours a week are spent in meetings.

Fig 5. Watermarking method represent

5 Comparisons Of Steganography, Watermarkingand Cryptography

Visibly water marks are also known as overt water marking.

In visible water marking is also known as covert water marking techniques. Simple one more water marking process is also vary famous and unique for investigation or research work done that is known as forensic water marking.

The novel approach is paper is that introduce the forensic water marking. The forensic water marking is the process in which hiding identifying information of particular video file, image file and test data file format.

detect the transmission of message and hence cannot try to decrypt it.

Criterion/method	**Stegano-graphy**	**Water-marking**	**Cryp-tography**
Carrier	**Digital media format**	**Video files and audio files**	**Text file format**
Secret Data	**Pay load format**	**Digital water marking**	**Simple text .**
Detection	**Blind**	**Open**	**blind**
Result	**Original file**	**Original file**	**Cipher text file**
Objective	**Secret communication**	**Copy right**	**Data protected**

TABLE 1 Comparison Of Steganography, Watermarking And Cryptography

6. Detailed Look At Watermarking

Human Visual System (HVS) to make the watermark indistinct. Like conventional actual watermarks, computerized watermarks are frequently just detectable under specific conditions, for example in the wake of utilizing some algorithm.[2] If a computerized watermark misshapes the transporter signal such that it turns out to be effectively recognizable, it could be viewed as less successful relying upon its purpose.[2] Traditional watermarks might be applied to noticeable media (like pictures or video), while in advanced watermarking, the sign might be sound, pictures, video, writings or 3D models. A sign may convey a few unique watermarks simultaneously. Dissimilar to metadata that is added to the transporter signal, an advanced watermark doesn't change the size of the transporter signal.

The required properties of an advanced watermark rely upon the utilization case in which it is applied. For checking media documents with copyright data, an advanced watermark must be fairly hearty against changes that can be applied to the transporter signal. All things being equal, if uprightness must be guaranteed, a delicate watermark would be applied.

Both steganography and computerized watermarking utilize steganography methods to install information secretively in boisterous signs. While steganography focuses on impalpability to human detects, computerized watermarking attempts to control the vigor as first concern.

I= F (I, W) ---------------------------------------(1).

V `= V+W.

V`1, V`2, V`3,V`4---------------------------------V`n.

If X As Expression Image Protection Then Watr Marking Expressed In.

For blind protection:

W= X. (I `) --------------------------------(2)

for non-blind protection:

W = X (I. I) ----------------------------------(3)

If the correlation function C= W. W`>=T.

where t is the thresh hold value

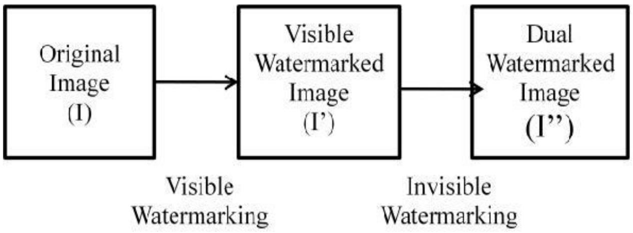


Fig. 7. Concept of Dual Watermarking

According to Application

alluring for proprietorship recognizable proof or verification where an extraordinary watermark distinguishing the proprietor is acquainted with all the duplicates of a specific picture being appropriated. The objective - based watermark could be utilized to follow the purchaser on account of illicit exchanging.

As Indicated By Watermark Detection/Extraction

Contingent upon the blend of sources of info and yields

watermarking is delegated visually impaired or non-daze strategies. Non-dazzle watermarking method requires unique picture for the discovery of watermark while daze strategy don't utilize unique picture for extricating the watermark. The upsides of non-dazzle method are lower blunder likelihood, higher limit and following exchange yet it might prompt numerous cases of possession.

Water marking protecting copyright:

- So-utilizing watermarks with ensured records offers numerous preferences to a distributer:
- as a replicating obstruction.
- As protecting copy right.
- Cipher text data file format protected.
- Unusual prospective informative file as used by water marking protecting techniques.
- Visible water marking methods used.
- Invisible water marking method as used.
- Bit map images as taken for protecting.
- as a method for distinguishing the wellspring of a printed report.
- as a method for deciding if a record has been changed.
- There are two kinds of computerized watermarking, noticeable and imperceptible.

A watermark is a blurred foundation picture that shows behind the content in a report. You can utilize them to demonstrate a record's state (private, draft, and so on), add an unobtrusive organization logo, or in any event, for a touch of imaginative pizazz. The water marking protecting method as working for various concern basis and new techniques. The protecting and copy right method or techniques is permed by cipher text file format or hiding file format or logo put on file format. these are various copy right and protecting methods are also used by applied water marking

7. Conclusion

One can see that there exists an enormous choice of ways to deal with shroud data in pictures. All the significant record designs have various strategies for concealing messages, with various solid and powerless focuses individually. Watermarking is the way toward concealing some information or data in a proper mixed media document concerning model picture, sound and video records. It goes under the proof that if the element is noticeable, the odds of assault is apparent, hence the objective of undetectable watermarking is consistently to cover the actual presence of the implanted information. It has been moved to the bleeding edge of current security methods by the surprising development in accessible computerized media through World Wide Web. Watermarking innovation assumes a significant part in getting business as it permits putting a vague imprint in the mixed media information to distinguish the real proprietor This paper represents the various survey view on water marking protecting ways and methods. and applied techniques

References

Dr.M.A.Dorairangaswamy, "A Novel Invisible and Blind Watermarking Scheme For Copyright Protection of Digital Images", International Journal of Computer Science and Network Security, VOL.9 No.4, April 2009.

Dr.M.Mohamed Sathik, S.S.Sujatha, "An Improved Invisible Watermarking Technique for Image Authentication", International Journal of Advanced Science and Technology Vol. 24, November, 2010.

Shivani Khurana, "Watermarking and Information-Hiding", International Journal of Computer Science and Information Technologies, Vol. 2 (4) ,1679-1681, 2011.

Mahmoud El-Gayyar and Prof. Dr. Joachim von zur Gathen , "Watermarking Techniques Spatial Domain Digital Rights Seminar", Media Informatics, University of Bonn, Germany, May 06.

S. Sinha, S. Pramanick, A. Jagatramka, P. Bardhan, D.K. Kole, A.Chakraborty, "Digital Video Watermarking using Discrete Wavelet Transform and Principal Component Analysis", International Journal of Wisdom Based Computing, Vol. 1 (2), 7-12, August 2011.

C.H. Li and S.S. Wang, "Transform-Based Watermarking for Digital Images and Video," IEEE, International Conference on Consumer Electronics, June1999.

Elham Shahinfard, Shohreh Kasaei, "Digital Image Watermarking using Wavelet Transform".

Saraswathi.M, "Lossless Visible Watermarking for Video", International Journal of Computer Science and Information Technologies, Vol. 2 (3) ,1109-1113, 2011

H. Liu, N. Chen, J. Huang, "A Robust DWT-Based Video Watermarking Algorithm", Proceedings of the International Conference on Signal and Image Processing Applications (ICSIPA), IEEE, pp. 352 – 356,2000.

T. JAYAMALAR, Dr. V. RADHA, "Survey on Digital Video Watermarking Techniques and Attacks on Watermarks", International Journal of Engineering Science and Technology, Vol. 2(12), 6963- 6967, 2010