IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10451

A REVIEW INTEGRATING WATERMARKING AND STEGANOGRAPHY

Vibha Kashyap[1], Kavya C. Ezhuthachan[2], Dr. Sameera Khan[3]

Student, Department of Computer Science, Amity School of Engineering and Technology, Chhattisgarh, India[1]

Student, Department of Computer Science, Amity School of Engineering and Technology, Chhattisgarh, India[2]

Assistant Professor, Department of Computer Science, Amity School of Engineering and Technology, Chhattisgarh, India[3]

ABSTRACT - As of now-a-days, a huge segment of people like to use web to send data beginning with one spot then onto the following across the world. The fast advancement of internet came to fruition into a critical interest in moving the information secured and careful. In any case the information can be hacked while sending data over the web. And the first substance that is available in this advanced world can be effortlessly replicated and shown. Also, to beat this kind of issue copyright security is required. To move the data to the customer at objective without any modifications and replication, there are various techniques open like Cryptography, Watermark, Steganography of the privileged information has been a test when the huge measure of information is traded on the web. Steganography is an instrument for concealing data inside a picture. It is the craftsmanship and study of concealing a mysterious message in a cover media like picture, text, signals or sounds so that nobody, with the exception of the expected beneficiary knows the presence of the information. Watermark is a message which is installed into advanced substance (sound, video, pictures or text) that can be recognized or removed later. Such messages generally convey copyright data of the substance. This innovation implants into the information an unperceivable advanced code, in particular the watermark, conveying data about the copyright status of the work to be secured. We have attempted to clarify the intergration of Steganogarphy and Watermark although this paper is just a literature review of both.

1. INTRODUCTION

In the present data innovation time, the internet has had a vital impact within the correspondence and data sharing. Due to the fast advancement in Data Innovation and Correspondence and also the Web, the protection of the information and also the data has raised concern.

Since the ascent of the web, perhaps the most variables of knowledge innovation and correspondence has been the protection of knowledge. This is often cultivated through concealing data in other data, subsequently concealing the presence of the imparted data. In image Steganography the info is roofed up solely in pictures. The thought and practice of concealing data includes a long history. Pictures are the foremost mainstream objects utilized for Steganography. Watermarking is a part of data concealing which is employed to shroud exclusive data in computerized media like photos, music and video. Protected material is effortlessly traded over distributed organizations, and this has made significant concerns those substance suppliers who produce digital content. Watermarking could be a technique conversant in shroud data or unmistakable information at spans computerized mixed media framework.

2. HISTORY –

2.1 History of Steganopgraphy -

The word Steganography comes from the Greek beginning that signifies "hidden (covered) composing". Steganography consequently not just accentuate on the craft of concealing data yet additionally the craftsmanship and study of concealing the correspondence that occur. Steganography can be followed back to old Greek hundreds of years when the message is inked on the couriers shaved heads. Their head will be shaved when they arrive at the beneficiary of the message. Another Steganography technique that was utilized during those days is tablet wax. To shroud the message, the tablet was deleted by wax and text was scratched on and afterward again covered it by wax and seemed clear upon reviews. During the century, the strategies for utilizing imperceptible inks were very well known. During the World War II where individuals utilized ink for composing covered up messages, this was valid. Microdots were likewise covered up in body parts including nostrils, ears, or under fingernails. The military and a few administrative organizations are investigating Steganography for their own mysterious transmissions of data. Following examinations concerning the Al Qaeda assault, Steganography was associated to be made use within their assault of the World Trade Center.

2.2 History of Watermarking –

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10451

With more than 300 years of paper impacting the world forever Arjowiggins offers an abundance of involvement and ability. Watermarking is as significant today as it has consistently been staying at the core of our creation. Albeit the craft of papermaking can be followed back to the start of the main century it was not until the thirteenth century that watermarks arose. The principal models given by Italian papermakers. Watermarks were made by bowing bits of wire into filigree plans, taken from the French word " filigrane " and got to the wire network. Any plan would dislodge strands conferring a weak clear picture into the sheet especially obvious when held to the light. It was accepted these early watermarks served to distinguish crafted by singular paper creators. This was an amazingly laborious action and wages were procured on a piecework premise. Later watermarks became to fill in as pointers of one or the other sort, size or class of paper, going about as the main brand names. Around 1700 when banknotes initially started to show up from the recently established public and national banks of Europe watermarks were acquainted in an endeavor with obstruct forging. The development of the Fourdrinier paper machine in the late eighteenth Century made a need to make watermarks on the persistent reel of paper. The dandy roll developed around 1825 was considered to establish a connection by turning over the outside of the paper while in a liquid state dislodging filaments and making the thickness varieties important to shape a watermark.

3. LITERATUTRE REVIEW –

3.1 Steganography –

In the time of 2013 Prabakaran, G.; Investigated on Medical records are incredibly delicate patient data a multi secure and power of clinical picture based Steganography conspire is proposed. This approach gives a productive and capacity security instrument for the assurance of computerized clinical pictures. Creators proposed a suitable Steganography technique utilizing Integer Wavelet Transform to ensure the X-ray clinical picture into a solitary holder picture. The patient's clinical analysis picture has been taken as mystery picture and Arnold change was applied and mixed secret picture was acquired. For this situation, the mixed secret picture was installed into the spurious holder picture and Inverse IWT was taken to get a spurious mystery picture. It has been seen that the quality boundaries are improved with adequate PSNR contrasted with the current calculations.

Mehdi Hussain et al, (2013), In this paper the creator characterizes Steganography as a method which gets the classified information from unapproved client. It is utilized worldwide to get the information while transmission. Regularly the information can be implanted in sound, video, picture, sound, text and so on The application of steganography is military correspondence. In this as a matter of first importance a cover picture is utilized to implant the information behind it and subsequent to embeddings the information the picture becomes stego picture. In this paper creator utilizes different Steganography strategies and application or characterizations are likewise characterized.

Morkel et al, The creator in this paper expresses that Steganography is an innovativeness to conceal the information behind a picture, an sound, video or text. Many record designs are utilized for Steganography like .jpeg, .png. The computerized picture is more best for Steganography because of its recurrence over the web. There are numerous strategies for Steganography. The decision of the strategy is based on the idea of the application for which it is being utilized like some application requires significant degree of classification while a few requests for medium level mystery in their application. In this paper the fundamental spotlight is on checking the similarity of the strategy of Steganography for application and afterward the most reasonable method is applied to the application for Steganography.

3.2 Watermarking –

Sam Kwong , Jiwu Huang and Yongjian Hu : In 2004(ICAs) introduced a writing overview on Watermark security by utilizing an imperceptible Watermark to ensure apparent watermarked picture to beat the issue of watermarking expulsion and unapproved addition. in this the watermark is picked as paired picture of the inserted watermark so that extricated logos can show the proprietor transport without extra registering and the security of imperceptible watermark picture is rearranged with some turbulent planning method prior to installing (here Arnolds feline guide is utilized to change the parallel logos). Ali Al-Haj, Tuqa Manasrah In 2007 proposed a writing overview on Non-Invertible Copyright Protection of Digital Pictures Using DWT and SVD and proposed a non-daze subtle and strong computerized picture watermarking calculation.

Tieniu Tan and Ruizhen Liu and Tieniu Tan: In 2002 introduced a SVD Based Watermarking Scheme for Protecting Rightful Possession. To exhibit the strength of proposed watermarking the obstruction of the calculation to different twists was concentrated in a progression of analyses on dim scale pictures and the strategy is contrasted and the Spread Range Communication strategy to put the execution examination of the calculation in appropriate setting. This technique uses the wavelet coefficients of the cover picture to install the watermark in which any of the four arrangements of wavelet coefficients can be utilized to watermark the picture. The particular upsides of the cover picture and watermark are added to shape the changed particular upsides of the watermarked picture. In request to ensure the computerized sound and video items copyright in the organization, an improved sound visually impaired Watermarking calculation conspire dependent on discrete wavelet change (DWT) and particular worth disintegration (SVD) is proposed. The straightforwardness of the proposed calculation is better, and power is solid against the

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10451

mainstream sound sign assault, for example, resampling, Low-pass separating, requantization, Gaussian repetitive sound, pressure and other well known sound sign assaults.

4. ACTIVE DIAGRAM –

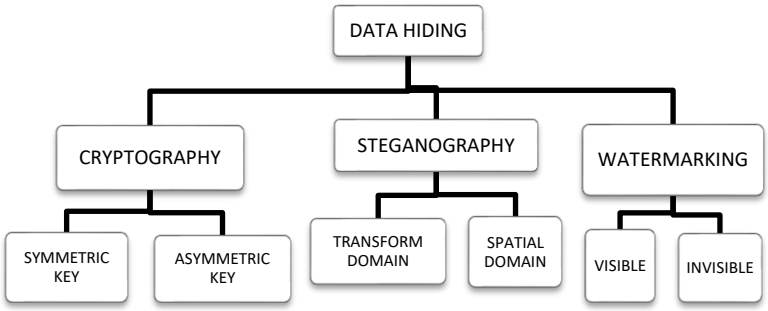

Fig.3.1 DATA HIDING AND IT'S TYPES

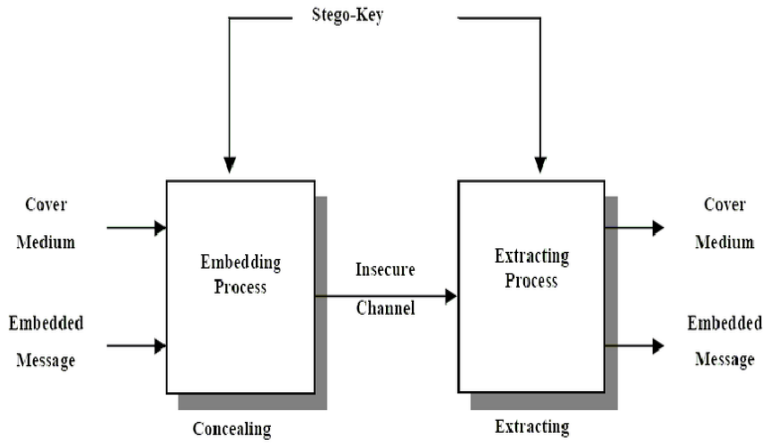

Fig. 3.2 PROCESS OF STEGANOGRAPHY

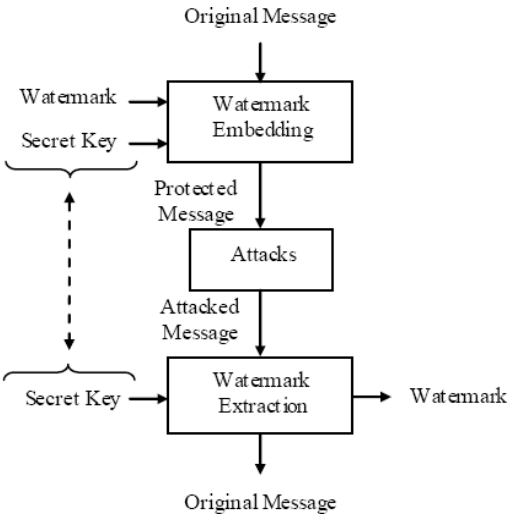

Fig. 3.3 PROCESS OF WATERMARKING

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10451

5. APPLICATION –

5.1 Applications of Steganography –

Steganography can be utilized whenever you need to shroud information. There are numerous motivations to conceal information yet they all bubble down to the craving to keep unapproved people from getting mindful of the presence of a message. In the business world Steganography can be utilized to shroud a mysterious substance equation or plans for another development. Steganography can likewise be utilized for corporate undercover work by conveying proprietary innovations without anybody at the organization being any the shrewder. Fear mongers can likewise utilize Steganography to stay quiet and to facilitate assaults. The entirety of this sounds genuinely accursed and truth is told the conspicuous employments of Steganography are for things like reconnaissance. The easiest and most established are utilized in map making, where map makers once in a while add a minuscule anecdotal road to their guides, permitting them to arraign copycats. A comparable stunt is to add anecdotal names to mailing records as a check against unapproved affiliates.

The majority of the more up to date applications use Steganography like a watermark, to ensure a copyright on data. Photograph assortments, sold on Cd, frequently have covered up messages in the photographs which permit recognition of unapproved use. A similar procedure applied to DVDs is much more successful, since the business assembles DVD recorders to identify and refuse duplicating of secured DVDs.

5.2 Applications of Watermarking –

Copyright Protection -Watermarking can be accustomed to securing reallocation of protected material over the untrusted network like Internet or on the other hand distributed (P2P) organizations. Content mindful organizations (p2p) could fuse watermarking innovations to report or on the other hand sift through protected material from such organizations.

Content Archiving -Watermarking can be utilized to embed computerized object identifier or on the other hand chronic number to help file advanced substance like pictures, sound or video. Typically advanced substance are identified by their record names; Henceforth implanting the item identifier inside the actual article decreases the possibility of tampering and hence can be effectively used in archiving systems.

Meta data Insertion- Meta alludes to the information that portrays information. Pictures can be named with its substance and can be utilized in web search tools. Sound documents can convey the verses or the name of the artist.

Broadcast Monitoring -Broadcast Monitoring alludes to the strategy of cross-confirming whether the substance that should be communicated (on TV or Radio) has truly been communicated or not. This has significant application is business notice broadcasting where the element who is promoting needs to screen whether their ad was really broadcasted at the ideal time and for right length.

Temper Detection - In the event that the delicate Watermark is obliterated or on the other hand corrupted, it demonstrated the presence of altering and subsequently the advanced substance can't be trusted. Alter recognition is likewise helpful in official courtroom where computerized pictures could be utilized as a criminological device to demonstrate whether the picture is altered or not.

Advanced Fingerprinting -Advanced Fingerprinting is a procedure used to recognize the proprietor of the advanced substance. Subsequently a solitary advanced article can have various fingerprints since they have a place with various clients.

6. CONCLUSION –

In this paper we attempted to incorporate the terms Steganography and Watermarking. In this paper we have clarified the writing about both Steganography and Watermarking. Due to space limit we have barred the specialized enumerating of our work, as we were attempting to clarify a technique which includes both the terms adding increasingly more security while moving information. The proposed technique which included the incorporating of the two added a greater amount of security from the aggressors.

7. REFRENCES –

1) T. Morkel , J.H.P. Eloff and M.S. Olivier “An Overview of Image Steganography”.
2) Amanpreet Kaur, Renu Dhir, and Geeta Sikka “A New Image Steganography Based On First Component Alteration Technique” (IJCSIS) International Journal of Computer Science and Information Security,Vol.6, No. 3, 2009.
3) Nagham Hamid, Abid Yahya, R. Badlishah Ahmad and Osamah M. Al-Qershi “ImageSteganography Techniques: An Overview” International Journal of Computer Science and Security (IJCSS), Volume (6): Issue (3): 2013.
4) Amir Ahmad Nasr. My Isl@m: How Fundamentalism Stole My Mind --- and Doubt Freed My Soul. Page 147. 2013.
5) "Executive Summary". The Future of the Global Muslim Population. Pew Research Center. 27 January 2011. Retrieved 1 November 2013.
6) "Region: Asia-Pacific". The Future of the Global Muslim Population. Pew Research Center. Retrieved 1 November 2013.
7) "Region: Middle East-North Africa". The Future of the Global Muslim Population. Pew Research Center. Retrieved 1 November 2013.
8) "Region: Sub-Saharan Africa". The Future of the Global Muslim Population. Pew Research Center. Retrieved 1 November 2013.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10451

9) "Region: Europe". The Future of the Global Muslim Population. Pew Research Center. Retrieved November 2013.
10) "Region: Americas". The Future of the Global Muslim Population. Pew Research Center. Retrieved 1 November 2013.
11) Tom Kington (31 March 2008). "Number of Muslims ahead of Catholics, says Vatican". The Guardian. Retrieved 1 November 2013.
12) "Muslim Population". IslamicPopulation.com. Retrieved 1 November 2013. "Field Listing - Religions". Retrieved 1 November 2013.
13) "Muslim Population by Country". The Future of the Global Muslim Population. Pew Research Center. Retrieved 1 November 2013.
14) 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.
15) Angela D. Orebaugh " Steganalysis: A Steganography Intrusion Detection System" , George Mason University
16) R. Krenn, "Steganography and steganalysis," An Article, Santa Barbara, California, January 2004, available from: http://www.krenn.nl/univ/cry/steg/article.pdf [Last accessed on 1 November 2013]
17) J.C. Ingemar, M.L. Miller, J.A. Bloom, J. Fridrich, and T. Kalker, "Digital watermarking and steganography", Burlington: Morgan Kaufmann; 2008.
18) J. Fridrich, "Steganography in Digital Media: Principles",Algorithms, and Applications, Cambridge, England: Cambridge University Press; 2009.
19) N.F. Johnson, and S. Jajodia, "Exploring steganography: Seeing the unseen," Computer, IEEE, Vol. 31, pp. 26-34, 1998.
20) T. Morkel, J.H.P. Eloff, and M.S. Olivier, "An overview of image steganography" in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, pp. 1-12, 29 Jun.-1 Jul. 2005.
21) M. Bachrach, and F.Y. Shih, "Image steganography and steganalysis,"Wiley Interdisciplinary Reviews: Computational Statistics, Vol. 3, pp. 251-9, 2011.
22) Petitcolas, F.A.P." Introduction to information hiding". In S. Katzenbeisser & F. A. P. Petitcolas (Eds.), Information hiding techniques for steganography and digital watermarking (pp. 1-12). Boston, London: Artech House,2000.
23) Farid, H. "Image forgery detection". Signal Processing Magazine, IEEE, 26(2): 16-25. doi: 10.1109/msp.2008.931079, 2009.
24) Cheddad, A., J. Condell, K. Curran, & P. Mc Kevitt. "A skin tone detection algorithm for an adaptive approach to steganography". Signal Processing, 89(12): 2465-2478. doi: 10.1016/j.sigpro.2009.04.022, 2009.
25) Arvind Kumar and Km. Pooja "Steganography- A Data Hiding Technique", International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010.
26) 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.
27) Banasthali Vidyapith, Rjasthan "Image Steganography Techniques: A Review Article", Bulletin of Engineering, Faculty of Engineering, Hunedoara, Romania, July-September,2013.
28) 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.
29) Ali Al-Ataby, Fawzi Al-Naima, "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform,"The International Arab Journal of Information Technology, Vol. 7, No. 4, October 2010.
30) M. Hassan Shirali-Shahreza, Mohammad Shirali-Shahreza, "Arabic/Persian Text Steganography Utilizing Similar Letters With Different Codes," The Arabian Journal for Science and Engineering,
31) Yongjian Hu, Sam Kwong, Jiwu Huang.USING INVISIBLE WATERMARKS TO PROTECT VISIBLY WATERMARKED IMAGES. Proceedings of the 2004 International Symposium on Circuits and Systems, 2004. ISCAS '04
32) Ali Al-Haj, Tuqa Manasrah. Non-Invertible Copyright Protection of Digital Images Using DWT and SVD. 2nd International Conference on Digital Information Management, 2007. ICDIM '07
33) W. Bender, D. Gruhl, N. Morimoto, Techniques for data hiding, Proc. SPIE 2420 (1995) 40.
34) O. Bruyndonckx, J.-J. Quisquater, B. Macq, Spatial method for copyright labeling of digital images, Proc. IEEE Workshop on Nonlinear Signal and Image Process- ing, Neos Marmaras, Greece, 20—22 June 1995, pp. 456—459.
35) J. Zhao, E. Koch, Embedding robust labels into images for copyright protection, Technical Report, Fraunhofer Institute for Computer graphics, Darmstadt, Germany, 1994.
36) Zhao, Y., Campisi, P., Kundur, D., "Dual Domain Watermarking for Authentication and Compression of Cultural Heritage Images", in IEEE Transactions on linage Processing, vol. 13, no. 3, pp. 430-448, March 2004.
37) Xie, L., Boncelet, G., Acre, G.R., "Wavelet transform based watermarking for digital images".