Difference of Watermarking & Steganography

J. Priscilla Sasi, P. Arul

Abstract*: *In the current world, the sensitive data are being transferred from source to destination in a much secured way in a common internet is inexorable. There are various technological aspects involved among the data world to protect the sensitive information or data hiding. Watermarking and Steganography are such important techniques which plays a prominent role in such data hiding. Earlier various techniques are been widely used like finger printing, Cryptography for encryption and decryption etc. But in the recent days the Digital Watermarking and Steganography are two range of techniques in such information hiding in a covered or secret way embedding to any host data which can be extracted with proper algorithms after the receiver receives the information. The combination of all these techniques can also bring a change in the internet industry. The information can be concealed and send across in a platform to the receiver with all these hidden techniques whereas the receiver of the data also need to know on the extraction techniques so that the information is been securely sent and received in a two-way communication. This paper deals about the comparing the common factors or attributes among the Watermarking and Steganography techniques.

***Keywords* : *Watermarking, Steganography, Encryption, Decryption, Data hiding, Data security*.**

I. INTRODUCTION

In the recent days the growth of internet and people interacting in the cyberspace is phenomenal. As long as the internet era is growing there is essential need of data transfer from sender to receiver in various modes. Especially the high data transfers happening, the potential risks are also emerging. The ease of data being hacked is more common. However in the Digital world, there are some of the techniques followed during such transfers where the data traversing from one to another can be hidden and made a secret transfer from a sender to receiver. Once such technology is Cryptography acts as a key for converting the actual messages or data into a different format and pass on to the receiver and the receiver again coverts the format received to a readable or understandable format so that the message or data is being transferred effectively. Another method is Steganography, where the message we are passing from a sender is being kept secret or embedded into another means of digitalization. There is one another method which is also widely used namelydigital watermarking where the data is hidden by digital signals. We will briefly discuss about the various attributes on each of these techniques, the main differences, and the key factors in this paper.

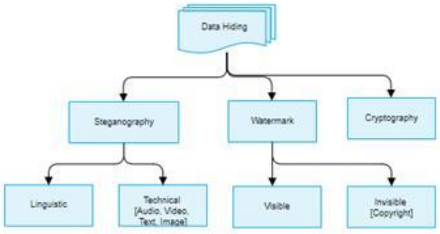

Fig. 1 – Basic types of Information Hiding

II. LITERATURE SURVEY

Zhicheng Niet. al. (2004) suggested how the data loss can be addressed when data is compressed and hidden in a JPEG format. The image is converted in to meaningful blocks and every block is represented as the arithmetic average done in the pixel values for each block. The secret information is associated with the pixel values or blocks of image [1].

Posanta Gopeet. al (2010) suggested steganography can be achieved through enhanced JPEG formats suitable for encryption and decryption methods. The Discrete Cosine Transform concept is applicable in each blocks. The encryption of data is done based on the Bit Error rate, MSE and PSNR parameter values. The main advantage on this approach is the added security when encryption concepts are applied [2].

M. B. Ould MEDENI et. al. (2010) suggestedthe errorinside the codesin the embedded data using steganography processes. The maximum embedded code is calculated in an optimal code.This improvises the efficiency during the embedding processand also helps to improvised security [3].

C.H. Yang et. al. (2010) suggested that new algorithm for improving the histogram based on the predictions in the reversibledata hiding approach. The pixels are predicted mostly used column based or chess board based approach. The column wise predictions are based on the pixels. During the predictions if any error occurs, the odd values in the columns are helpful in generating the histogram with the secret data embedded in it [4].

Shweta Singhal et. al (2011) suggested that steganography is used in a new image proposed in the spatial domain. In this process, the image pixels were replaced by the bits of the each text to hide the secret information and shared. The steganography key is used for digital security purposes. This process is used mainly for the better image quality is being securely transferred [5].

Revised Manuscript Received on December 05, 2019.
***** Correspondence Author
J. Priscilla Sasi*, Research Scholar, Department of Computer Science, Government Arts College, Trichy, India
P. Arul, Assistant Professor, Department of Computer Science, Government Arts College, Trichy, India

B. Sharmila et. al. (2012) suggested an algorithm that works in JPEG format of color images. The algorithm is very robust because to hide data in the images, the sharpen edges of the color image were chosen. In this method, it is difficult to found out the changes madein the sharper edges. During the data embed process, the components of RBG of the image are separated based on the sharp key. Every block is rotated in a same direction forcertain degrees to identify the secret key. In this process around 630 pixels can be embedded in a 256 x 256 image [6].

Frank Y.Shih suggested in his theory that using watermark we can easily identify the source, creator, owner, distributor and the customer who is the author for document or the image. In the Watermarking process the watermark can be embedded into a digital signal and can be extracted from the original image [7].

In the Digital WatermarkingPrinciples ad Practice by theMorgan Kaufmann Series suggested that the watermarking helps in informing the copyright protection into the software and hardware devices where copyright protection is enabled. The watermarkhelps in identifying the copyright owner and restrict the copyright process [8].

Jobenjit Singh et al in this paper describes how to check the Robustness and the imperceptibility of the system with the help of image watermarking process, it defines the various applications, properties and parameters like (PSNR) and Normalized Cross correlation (NCC) for data security[9].

Manpreet Kaur et al suggested the comparison on the watermarking techniques with the limitation of each technique. Kaur also suggest the image watermarking techniques for the data security [10].

Jaishri guru et al (2014) suggested about the detailed study of the watermarking algorithms which provides and the robustness of the process and the security factors used in digital imagewatermarking [11].

Mohan Durvey et al (2014)] suggested the challenges, limitations, performance and quality of the watermarking techniques [12].

III. PROCESS MODEL OF STEGANOGRAPHY AND DIGITAL WATERMARKING

Steganography is defined as an art of covering the sensitive information hidden through a digital media. It is extracted from the Greek word as covered writing. In the Steganography process, the sender embeds the secret information with another image while the receiver extracts the information hidden in it through various algorithms.

Generally the Steganography works in two kinds of principles.

(i). The Digital media namely the images or audio or video files can be altered without any change in the functionality.

(ii) The Change in the media files cannot be determined by the human vision as the changes appears minor.

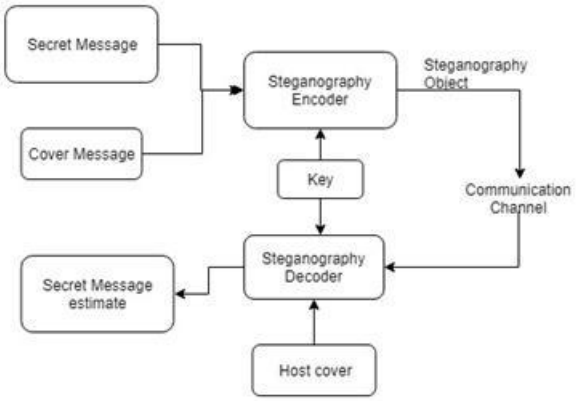

Fig. 1 – Steganography Process Model

Watermarking is defined as the technique for inserting the data into any image, text or videos either visible or invisible forms. The secret data is inserted into the media with watermark and the key is generated and shared to the sender and the receiver and the watermarked data is extracted with the secret key from the receiver's end.

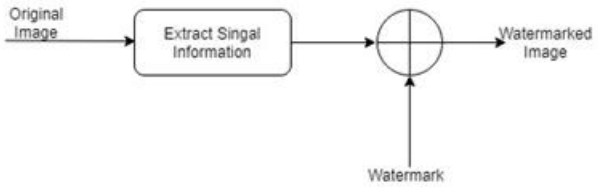

Fig. 2 – Watermark Transmission

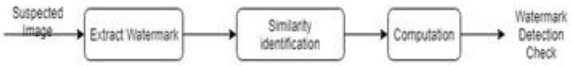

Fig. 3 – Watermark Detection

The above pictorial representations in Fig [1], Fig [2] and Fig [3] indicates the working process of steganography and watermark.

IV. COMPARATIVE STUDY ON STEGANOGRAPHY AND DIGITAL WATERMARKING

Attribute	Watermarking	Steganography
Definition	Art of embedding into Digital media.	Art of sharing hidden information. Also knownas covered writing.
Carrier	Paper, Images, Text.	Text, Audio, Video.
Communication	One to Many.	One to One.
Techniques	Spatial and Frequency.	LSB, Spatial, Block complexity and Transform domain.
Secrete Data	May be used.	May be used.
Motive	Owner identification.	Existing messages are covered.
Outcome	Watermarked image.	Stegano image.

Attribute	Watermarking	Steganography
Keys	(a) Blind Vs Non blind. (b) Spatial Vs Frequency (c) Public Vs Private.	(a)Pure Steganography. (b) Secret Key Steganography. (c) Public Key Steganography.
Tools	(a) Checkmark. (b) Optimark. (c) Certimark.	(a) Stegoshare. (b) Openstego. (c) Camouflage.
Robustness	Robust.	May or may not be robust.
Visibility	Can be visible or invisible.	Always invisible.
Application	Copyright protection, Source Tracking.	Modern Printers, intelligent services.

V. CONCLUSION

In this paper the Steganography is used widely for the data hiding which is helpful in carrying the secret digital information and it is difficult to track the information shared for the investigators.

However the digital watermarking is very much helpful in the data authorization and authentication and helps to track the real identity of the message being shared by adding a watermark on it. Our further work will be more focused on study on the increase in the data security and robustness of the watermarking techniques.

REFERENCES

1. Zhicheng Ni, Yun Q.Shi, Nirwan Ansari, Wei Su, Qibin Sun & Xiao Lin – Robust Lossless Image Data Hiding, IEEE Article (2004).
2. Prosanta Gope, Anil Kumar and Gaurav Luthra, - An Enhanced JPEGimage Steganography Scheme with Encryption Technique, inInternational Journal of Computer and Electrical Engineering, (2010), Vol.2.No.5, 924-930.
3. M.B.Ould MEDENI and El Mamoun SOUIDI, (2010) –Steganography and Error Correcting Codes, International Journal of Computer Science and Information Security, (2010), Vol.8.No.8, 147-149.
4. C.-H. Yang and M.-H. Tsai, -Improving Histogram-based Reversible Data Hiding, by Interleaving Predictions, IET Image Processing, (2010), Vol.4. Issue. 4. 223-234.
5. Shweta Singhal, Dr.Sachin Kumar and Manish Gupta, A New Steganography Technique Based on Amendment in Blue Factor, International Journal of Electronics Communication and Computer Engineering,(2011), Vol.2, Issue 1, 52-56.
6. B. Sharmila and R.Shanthakumari, Efficient Adaptive Steganography For Colour Images Based on Least Significant BitMR Algorithm, ICTACT Journal on Image and Video Processing, (2012), Vol. 2, Issue: 03,387-392.
7. Frank Y.Shih,Digital watermark and steganography,CRC Press,Taylor and Francis Group
8. Digital_Watermarking_Principles_amp Practice_The_Morgan_Kaufmann_Series_in_Multimedia_Information_and_Systems.
9. Jobenjit Singh Chahal, -A Review on Digital Image Watermarking, International Journal of Emerging Technology and Advanced Engineering Website,(2013), Volume 3, Issue 12, 482-484.
10. Manpreet Kaur – Review Paper on Digital Image Watermarking Technique for Robustness, International Journal of Advanced Research in Computer Science and Software Engineering, (2014), Volume 4, Issue 5, 948-952.
11. Jaishri Guru - A Review of Watermarking Algorithms for Digital Image, International Journal of Innovative Research in Computer and Communication Engineering,(2014), Vol.2, Issue 9, 5701- 5708
12. Mohan Durvey - A Review Paper on Digital Watermarking International Journal of Emerging Trendsand Technology in Computer Science, (2014), Volume 3, Issue 4, 99- 10

AUTHORS PROFILE

Mrs. J. Priscilla Sasi, ccompleted her B.Sc., (Physics) and M.Sc (Computer Science) degree respectively from Indira Gandhi Arts & Science College and Bishop Heber College, Bharathidasan University, Tiruchirappalli, Tamil Nadu in April 2000 and April 2003. She completed her M.Phil degree in Bharathidasan University, Tiruchirappalli during March 2008.After M.Phil studies she worked as Assistant Professor in Bishop Heber College, Tiruchirappalli for 2 years and worked as Assistant Professor in Guru Nanak College, Chennai for 8 years. Currently she is pursuing her Ph.D degree in Government Arts College, Thuvakudi, Tiruchirappalli, affiliated to Bharathidasan University for research work in Network Security. Her research mainly focused on to prevent Data theft which is based on human factor information security.

Dr. P. Arul obtained his B.Sc., (Computer Science) and MCA., degree from Hans Rover Arts College, Perambalur, Tamil Nadu, in 1988 and 1994 respectively. He received his M.Phil, from Bharathiyar University , Coimbatore, Tamil Nadu, in the year 2000. He received his Ph.D., from Vinayaka Mission, Salem, Tamil Nadu, in the year 2010. He has published more than 10 research papers in national and international journals. For 2 years worked as Assistant Professor in the Department of Computer Science, Cheran Arts and Science College, Erode. For a decade he worked as Assistant Professor in the Department of Computer Applications of Kongunadu Arts and Science College, Coimbatore. He also worked as Assistant Professor in the Department of Computer Science, CMS Arts and Science College, Coimbatore for 3 years. Currently he is working as Assistant Professor in the Department of Computer Science, Government Arts College, Thuvakudi, Trichy. He is supervising four doctoral works in Computer Applications. His mission is to impart qality, concept oriented education and mould younger generation.