IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 2, February 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2023 ||

| DOI:10.15680/IJIRSET.2023.1202067 |

Study of Steganography and Digital Watermarking Scheme for Security Application

Deepali Paswan[1], Prof. (Dr.) Vikas Gupta[2]

M. Tech. Scholar, Department of Electronics and Communication, TIT, Bhopal, India[1]

Professor & Head, Department of Electronics and Communication, TIT, Bhopal, India[2]

ABSTRACT: Everything revolves around the use of Internet like online bill payment, online shopping, online trading, internet banking and even online dating and matrimonial. The rate at which online activities are increasing is overwhelming and so are online fraudulent activities. In this modern era of technology, computer network provides an easy and effective way to share and distribute files and digital information to the masses within a short span of time. With the advancement in the networking technology, many new ways to share the digital data is cropping up like mushrooms. With the tremendous growth in technology and ways to share information, security and authentication of the information shared becomes a major issue. But the major issue with the transmission of digital information is that innumerable copies can be made and is more susceptible to be misused if it lands in the hands of malicious users. This leads to the problem of authentication of content and copyright protection. Information Security deals in protecting the integrity and confidentiality of the information shared over the internet.

KEYWORDS: Steganography, watermarking, Carrier, robustness and information

I. INTRODUCTION

Internet is a boon to modern society. It provides a platform to obtain a variety of services including information gathering, online chats, emails and financial services like online shopping, bill payments, e-banking and many more. With internet cost coming down quickly and speed rocketing, a wide variety of jobs can be done easily and in comfort without any constraints of distance, time or space. Surfing the Internet is a simple and effortless task. Internet is readily available in all geographic locations including villages, towns and cities across the globe [1, 2].

Internet surfing can be done with the help of browsers such as Windows Explorer, Google Chrome and many more. In this modern era of technology, computer network provides an easy and effective way to share and distribute files and digital information to the masses within a short span of time. With the advancement in the networking technology, many new ways to share the digital data are cropping up like mushrooms. With the tremendous growth in technology and ways to share information, security and authentication of the information shared becomes a major issue [3].

But the major issue with the transmission of digital information is that the innumerable copies can be made and is more susceptible to be misused if it lands in the hands of malicious users. The organizations that are responsible for providing the Internet services to end-users are called as Internet Services Providers (ISPs). The major ISPs of India are BSNL, Vodafone, Airtel, Idea and Aircel. With the phenomenal growth in Internet technology, the crimes associated with it too grow exponentially. These are different from the regular crimes that come under the penal law code [4, 5].

II. LITERATURE REVIEW

Seddeq. E. Ghrare et al. [1], presented a DWT and SVD based hybrid image watermarking scheme using Self-adaptive Differential Evolution (SDE) algorithm. The scaling factors used in watermarking are optimized using SDE to gain the maximum achievable robustness and imperceptibility.

Nazir A. Loan et al. [2], the digital images are represented or stored either in spatial domain or in transform domain. In spatial domain image is represented by pixels or grey values where as in transform domain image is represented in terms of its frequencies. In simple terms, transform domain means the image is segmented into multiple frequency bands. To transfer an image to its frequency representation, we can use several reversible transforms like Discrete

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2023 ||

| DOI:10.15680/IJIRSET.2023.1202067 |

Cosine Transform (DCT), Discrete Wavelet Transform (DWT), or Discrete Fourier Transform (DFT). Each of these transforms has its own characteristics and represents the image in different ways. Watermarks can be embedded within images by modifying these values, i.e. the transform domain coefficients. In case of spatial domain, simple watermarks could be embedded in the images by modifying the pixel values or the Least Significant Bit (LSB) values. However, more robust watermarks could be embedded in the transform domain of images by modifying the transform domain coefficients.

Baharak Ahmaderaghi et al. [3], briefly discussed the issue of watermarking digital images as part of a general survey on cryptography and digital television. The authors provided a description of a procedure to insert a watermark into the least significant bits of pixels located in the vicinity of image contours. Since it relies on modifications of the least significant bits, the watermark is easily destroyed. Further, their method is restricted to images, in that it seeks to insert the watermark into image regions that lie on the edge of contours. Addition or subtraction is determined by comparing a binary mask of bits with the LSB of each pixel. If the LSB is equal to the corresponding mask bit, then the random quantity is added, otherwise it is subtracted. The watermark is subtracted by first computing the difference between the original and watermarked images and then by examining the sign of the difference, pixel by pixel, to determine if it corresponds to the original sequence of additions and subtractions. This method does not make use of perceptual relevance, but it is proposed that the high frequency noise be profiteered to provide some robustness to low-pass filtering. This scheme does not consider the problem of collusion attacks.

Aleksei Zhuvikin et al. [4], they described two watermarking schemes. The first is a statistical method called patchwork. Patchwork randomly chooses pairs of image points and increases the brightness at one point by one unit while correspondingly decreasing the brightness of another point. The second method is called “texture block coding” wherein a region of random texture pattern found in the image is copied to an area of the image with similar texture. Autocorrelation is then used to recover each texture region. The most significant problem with this scheme is that it is only appropriate for images that possess large areas of random texture. The scheme could not be used on images of text. The proposed well known patch watermarking method, inserted a message by supposing that two sets randomly selected pixels are Gaussian distributed with zero mean. The patch method is sensitive to desynchronization operations because the water mark is highly related to the position of those marked patches.

Etti Mathur et al. [5], proposed a method that embeds a binary watermark image in the spatial domain. A spatial transform that maps each pixel of the watermark image to a pixel of the host image, is used. Chaotic spread of watermark image pixels in the host image is achieved by “toralautomorphisms”. For watermark embedding, the intensity of the selected pixels is modified by an appropriate function that takes into account neighborhood information in order to achieve watermark robustness to modifications. For detection, a suitable function is applied on each of the watermarked pixels to determine the binary digit (0 or 1) that has been embedded. The inverse spatial transform is then used to reconstruct the binary watermark image.

Morteza Heidari et al. [6], the image is split into two random subsets A and B and the intensity of pixels in A is increased by a constant embedding factor k. Watermark detection is performed by evaluating the difference of the mean values of the pixels in subsets A and B. This difference is expected to be equal to k for a watermarked image and equal to zero for an image that is not watermarked. Hypothesis testing can be used to decide for the existence of the watermark. The above algorithm is vulnerable to low-pass operations.

N. Senthil Kumaran et al. [7], proposed a method for watermarking images. In that method, they break up an image into 8x8 blocks and compute discrete cosine transform (DCT) of each of these blocks. A pseudorandom subset of the blocks is chosen and then in each such block, a triplet of frequencies is selected from one of 18 predetermined triplets and modified so that their relative strengths encode a ‘1’ or ‘0’ value. The 18 possible triplets are composed by selection of three out of eight predetermined frequencies within the 8x8 DCT block. The choice of the eight frequencies to be altered within the DCT block is based on a belief that the “middle frequencies have moderate variance,” i.e., they have similar magnitude. This property is used to allow the relative strength of the frequency triplets to be altered without requiring a modification that would be perceptually noticeable.

Ranjeet Kumar Singh et al. [8], watermark is a pseudorandom sequence of fixed length and is produced using Gaussian distribution with zero mean and unit variance. It is embedded into the first one thousand largest AC coefficients. An objective measurement was proposed to evaluate the similarity between the original and extracted watermark. Block based watermarking algorithms differ either in block selection criteria or coefficient selection

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2023 ||

| DOI:10.15680/IJIRSET.2023.1202067 |

criteria. Pseudorandom subsets of the blocks are chosen, and a triplet of midrange frequencies is slightly altered to encode a binary sequence. Embedding of watermark information which is a pseudorandom sequence is performed by using inter block correlation of the DCT coefficients of the brightness of a color image. The strength of the watermark information to be embedded was varied with the visual features of the image.

III. STEGANOGRAPHY

Researchers have worked on the concept of hiding messages inside an image using steganographic techniques in the Spatial Domain. Some of the theories were reviewed and presented here. It [16] have researched on designing an image steganographic algorithm called Steganography Imaging System (SIS) that has two layers of security, username – password and encoding. They have worked only with .bmp files. They have shown the results based on the PSNR values. They claimed that their proposed methodology has higher PSNR value. The process flow of SIS is shown in the Figure 1.

Many steganographic algorithms can be used for these tasks but these are not perfect applications of steganography. In Steganography, generally some secret data embed into an innocuous looking simple image as a cover image and create a Stego image file. The Stego image visually seems to be same as cover image but hides the secret data inside it and transmitted to the recipients over the communication channels. When the desired recipient receives the Stego image, then follow the data extraction process to recover the secret data.

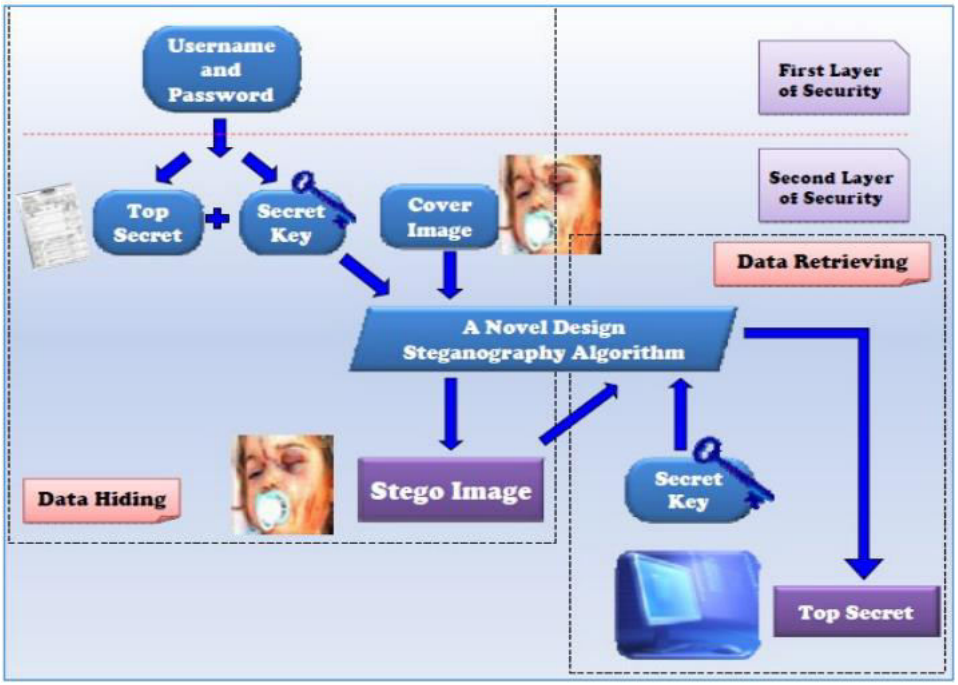

Figure 1: Steganography system

IV. DIGITAL WATERMARKING

The online transmission and distribution of multimedia content over the Internet have increased exponentially because of the availability of high-speed digital data networks and increased Internet usage. Security, authentication, and copyright protection of multimedia data have become a major concern, because such data can be duplicated, modified, and re-transmitted easily. Steganography and watermarking are two different techniques that are used to address these issues by hiding and protecting vital information in an undetectable manner. Steganography mainly aims in concealing the very existence of the information whereas watermarking tries to protect the hidden message. Watermarking is a mechanism in which copyrighted information is embedded by slightly altering the original content; this is usually achieved by transforming the domain space in such a manner that the change is unnoticeable to the human visual system. The embedded information can be detected and extracted at any time for authentication, ownership identification, copy protection, and control. The watermarking technique can be employed for secure communication of multimedia data, which may include images, audio, and video data, over the Internet. The digital watermarking method

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2023 ||

| DOI:10.15680/IJIRSET.2023.1202067 |

is not only a solution to address the security concerns of digital media, but also facilitates copyright protection and authentication. It is also an important branch of information hiding, as it can be applied to high-strength secure communication. In watermarking, a sequence of information called a watermark is embedded into the original data before transmission over an insecure channel. Subsequently, at the receiver end, the watermark is extracted and verified to ensure that the received data was not tampered with during transit. A general digital watermarking procedure is shown in Figure 2.

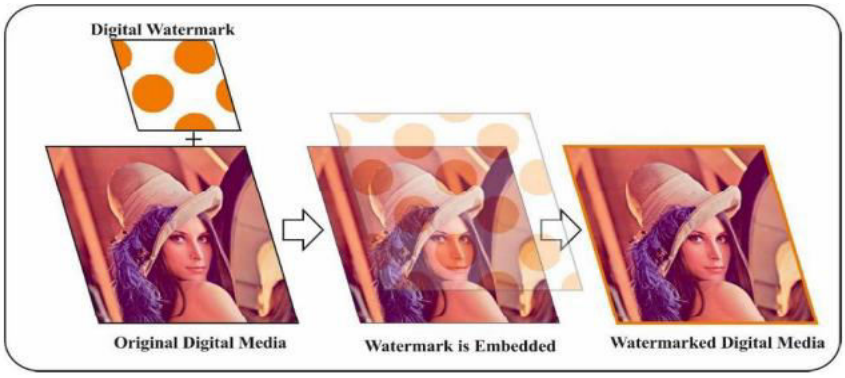

Figure 2: General procedure for digital watermarking

Characteristics of Digital Watermarking:-

Digital watermarking system has following properties.

Robustness: Robustness means the watermark embedded in a data can survive under various attacks and processing operations like rotation, scaling, compression etc. It should be robust against different geometrical and non-geometrical attacks.

Non-perceptibility: Watermark object can neither be seen by a human eye nor be caught by a human ear, it can only be find out through special processing or dedicated circuits. The watermark should be processed in such a way that it does not affect the quality of embedded data.

Security: Only the authorized users can detect, extract and modify the watermark and thus an owner can achieve the purpose of copyright protection.

Payload capacity: The payload limit of watermark portrays greatest measure of information that can be installed as a watermark into an advanced media. The span of the implanted data is frequently essential the same number of frameworks require a major payload to be inserted. As a big payload also provide a security to a digital media.

Verifiability: The watermark should be embedded in such a way that it able to give the full and reliable proof of the ownership of copyright protected information products. It can be used for protecting data from illegal distribution as the data is being protected by the watermark. It is also used for identifying the authenticity.

Fidelity: When we add a watermark into an image there is a large possibility that it will affect the quality of original image. We must keep this property of the image's quality to a minimum, so that the fidelity of an image should be maintained.

V. COMBINED WATERMARKING AND STEGANOGRAPHY

To protect the authenticity of the document, watermarking can be applied to it. This watermarked document can be embedded in cover image using a stego-key and transmitted over the communication medium. At the receiver end, the information can be first decrypted using the reverse procedure and then it can be validated for its authenticity using the watermarking. This combined approach will satisfy all four goals of data hiding: security, capacity, robustness and perceptibility.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2023 ||

| DOI:10.15680/IJIRSET.2023.1202067 |

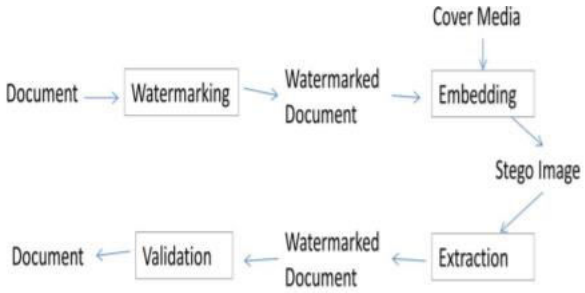

Figure 3: Watermarking with Steganography

Pure steganography – it does not require the exchange of cipher such as a stego-key but the sender and receiver must have access to embedding and extraction algorithm. The cover for this method is c hosen such that it minimizes the changes caused by embedding process. These systems are not very secure as the security depends on the presumption that no other party is aware of this secret message.
Secret key steganography – this method uses a key to embed the secret message into the cover. The key is only known to sender and the receiver and is known prior to communication. Also, the key should be exchanged in a secure medium. The disadvantage of this approach is that it is susceptible to interception.
Public key steganography – it utilizes two keys, open key put away out in the open database and is utilized for installing process and the mystery key is known just to correspondence parties and is utilized to reproduce the first message [8].

Attacks on Digital Watermarking
Watermarked multimedia data may undergo various means of processing before it finally reaches the intended receiver. This processing can be in the form of compression, enhancement, etc. In watermarking parlance, such processing of broadly classified into intentional and unintentional attacks. A watermarking scheme is said to be robust if it withstands any attack and can retrieve the watermark within acceptable noise limits. Attacks can be categorized into the following four classes:

Removal Attacks: These types of attack tend to remove or damage the watermark in the data without processing. A removal attack may tamper with the watermark, but will maintain the quality of the attacked watermarked data. Such attacks include noising, blurring, sharpening, and histogram equalization.
Geometric Attacks: These types of attack alter the watermark instead of removing or damaging it. Rotation, scaling, and translation are examples of such attacks. It is theoretically possible to recover the original watermark, provided information on the type of attack and its countermeasures are available.

Cryptographic Attacks: These attacks are similar to attacks in cryptography. Most watermarking schemes are based on secret keys. These attacks tend to break the keys, thereby cracking the security to discover the secret information or to insert misleading information. Brute force attacks or oracle attacks are such kinds of attack.

Protocol Attacks: These types of attack destroy the original watermark and insert the attacker's watermark leading to ambiguity of the ownership rights with regard to copyright protection.

VI. CONLUSION

The performance of these schemes was evaluated in terms of the robustness and imperceptibility using different parameters; e.g., the peak signal-to-noise ratio, correlation coefficient, and structural similarity index. The other parameters include the entropy, image fidelity, histogram analysis, bit error rate, and bit correction rate. Various experiments performed using intentional and nonintentional attacks showed that the proposed schemes possess relatively high robustness and imperceptibility. Comparative analysis of each of the proposed schemes with existing state-of-the-art algorithms demonstrated their advantages. The results show that the proposed watermarking schemes may be used for realtime applications such as copyright protection and authentication

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2023 ||

| DOI:10.15680/IJIRSET.2023.1202067 |

REFERENCES

[1] **SEDDEQ. E. GHRARE, A. ADIM MOHAMAD ALAMARI AND HAJER ABDULHKIM EMHEMED, "DIGITAL IMAGE WATERMARKING METHOD BASED ON LSB AND DWT HYBRID TECHNIQUE", IEEE 2ND INTERNATIONAL MAGHREB MEETING OF THE CONFERENCE ON SCIENCES AND TECHNIQUES OF AUTOMATIC CONTROL AND COMPUTER ENGINEERING (MI-STA), IEEE 2022.**

[2] Nazir A. Loan, Nasir N. Hurrah, Shabir A. Parah, Jong Weon Lee, Javaid A. Sheikh, and G. Mohiuddin Bhat, "Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption", Received January 4, 2018, accepted February 7, 2018, date of publication March 16, 2018, date of current version April 25, 2018.

[3] Baharak Ahmaderaghi ; Fatih Kurugollu ; Jesus Martinez Del Rincon ; Ahmed Bouridane, "Blind Image Watermark Detection Algorithm based on Discrete Shearlet Transform Using Statistical Decision Theory", IEEE Transactions on Computational Imaging, Volume: 4 , Issue: 1, Page s: 46 – 59, IEEE 2018.

[4] Aleksei Zhuvikin, "Selective Image Authentication using Shearlet Coefficients Tolerant to JPEG Compression", Page s: 681 – 688, IEEE 2017.

[5] Etti Mathur and Manish Mathuria, "Unbreakable Digital Watermarking using combination of LSB and DCT", International Conference on Electronics, Communication and Aerospace Technology ICECA 2017.

[6] Morteza Heidari1, Nader Karimi, and Shadrokh Samavi, "A Hybrid DCT-SVD Based Image Watermarking Algorithm", Iranian Conference on Electrical Engineering (ICEE), IEEE 2016.

[7] N. Senthil Kumaran, and S. Abinaya, "Comparison Analysis of Digital Image Watermarking using DWT and LSB Technique", International Conference on Communication and Signal Processing, April 6-8, 2016, India.

[8] Ranjeet Kumar Singh, Dilip Kumar Shaw and M. Javed Alam," Experimental Studies of LSB Watermarking With Different Noise", Eleventh International Multi- Conference on Information Processing-2015 (IMCIP-2015).

[9] Baharak Ahmaderaghi ; Jesus Martinez Del Rincon ; Fatih Kurugollu ; Ahmed Bouridane, "Perceptual Watermarking for Discrete Shearlet Transform", 5th European Workshop on Visual Information Processing (EUVIP), IEEE 2014.

[10] Bidyut Jyoti Saha, Kunal Kumar Kabi and Arun, "Non Blind Watermarking Technique using Enhanced One Time Pad in DWT Domain", International Conference of Digital Signal and Processing, ICCCNT, IEEE 2014.

[11] M. Kim, D. Li, S. Hong, "A Robust Digital Watermarking Technique for Image Contents based on DWT-DFRNT Multiple Transform Method", *International Journal Multimed. Ubiquitous Eng.,* vol. 9, no. 1, pp. 369-378, Jan. 2014.

[12] Jiann-Shu Lee and Fei-Hsiang Huang, "A New Image Watermarking Scheme Using Non-dominated Sorting Genetic Algorithm II", International Symposium on Biometrics and Security Technologies, IEEE 2013.

[13] Baloshi Mathews and Madhu S. Nair, "Modified BTC Algorithm for Gray Scale Images using max-min Quantizer", Automation, Computing, Communication, Control and Compressed Sensing, PP. 01-05, 2013 IEEE.

[14] Wang Santosh, U. V. S. Sitarama Varma, K. S. K Chaitanya Varma, Meena Jami, V. V. N. S Dileep, "Absolute Moment Block Truncation Coding For Color Image Compression," International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-2, Issue-6, PP. 53-59, May 2013.

[15] Lee, J. S., Huang, F. H., & Kuo, H. C., "A New Image Watermarking Scheme Using Non-dominated Sorting Genetic Algorithm II," In Biometrics and Security Technologies (ISBAST), International Symposium, pp. 56-61, IEEE 2013.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details