IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 10, October 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 10, October 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1010014 |

Review of Optimization of Secure Data for Steganography using Reversible Data Hiding

[1]Mohit Tripathi, [2]Prof. Deepak Kumar Mishra

M. Tech Scholar, Department of Computer Science and Engineering, VNS Group of Institutes-Faculty of Engineering, Bhopal, India[1]

Assistant Professor, Department of Computer Science and Engineering, VNS Group of Institutes-Faculty of Engineering, Bhopal, India [2]

ABSTRACT:- Steganography system assumes an imperative job in data stowing away in any computerized cover object. Security of data on web against unapproved get to has turned into a prime issue. Because of this, steganography method turns out to be progressively mainstream. Steganography is the science which incorporates mystery correspondence in a proper advanced cover objects viz. sound, picture, content and video records. The fundamental target of steganography strategy is to shroud the nearness of the installed data in transporter record and different goals are power, Un-perceptibility and limit of the disguised information. Steganography is independent from other related methods viz. watermarking and cryptography in term of heartiness and Un-perceptibility of data. Watermarking is a procedure that conceals data in advanced picture to secure scholarly properties and copyright, for example, logo for demonstrating possession. Steganography and watermarking are vital systems to disguise critical information in cover object an imperceptible and irremovable way. The two methods are the quick creating zone of data covering up. This paper conveys a relative report on advanced pictures steganography and watermarking strategies and noteworthy research developments are additionally talked about.

KEYWORDS: -Steganography, watermarking, Carrier, robustness and information

I. INTRODUCTION

These days sight and sound information has been moved speedily and comprehensively to the goals through the web into different structures, for example, picture, sound, video and content. In advanced correspondence over the web, everything is obvious and open to each client. In this way, security of data is a vital and essential assignment. There are three goals of network or information security such as confidentiality, integrity and availability (CIA) [1]. Confidentiality means that information is secure and not available to the unauthorized person. Integrity refers to the accuracy of information and availability means that information is in time access to authorized person. System security isn't adequate for dependable correspondence of data like content, sound, video and advanced pictures. There are numerous procedures to anchor pictures including encryption, watermarking, advanced watermarking, reversible watermarking, cryptography, steganography and so on. In this paper a review on encryption, steganography and watermarking is presented [2]. In this exploration think about we proposed a half and half security approach that is a combination of encryption, steganography and watermarking. A brief introduction of each technique has been discussed in the following sections [3, 4].

Video based stenographic techniques are broadly classified into temporal domain and spatial domain. In recurrence area, pictures are changed to recurrence segments by utilizing FFT, DCT or DWT and afterward messages are inserted in a few or the majority of the changed coefficients. Installing might be bit level or in square dimension. Besides in spatial space the bits of the message can be embedded in power pixels of the video in LSB positions. The preferred standpoint in the strategy is that the measure of information (payload) that can be inserted is more in LSB strategies. Anyway the vast majority of the LSB strategies are inclined to assault as depicted in [5] and [6]. This makes explore brotherhood keen on planning new techniques. Systems other than LSB substitution likewise exist in writing and have been talked about in the following area. In this paper a hash based LSB Techniques is proposed in spatial area. A use of the calculation is shown with AVI (Audio Video Interleave) document as a cover medium.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 10, October 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1010014 |

II. LITERATURE REVIEW

Nazir A. Loan et al. [1], have proposed DCT domain watermarking can be classified into global DCT watermarking and block based DCT watermarking. Applying global DCT on image segregates the image into different frequency bands. He proposed spread spectrum based approach for watermark embedding using global DCT transform. Signal energy present in any frequency band is undetectable if a narrowband signal is transmitted over a much broader bandwidth. In this approach watermark is a narrow band signal which is spread over all frequencies so that the energy in any single frequency component is very small and is undetectable. 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 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.

Tomas Denemark et al. [2], it is widely recognized that incorporating side-information at the sender can significantly improve steganography security in practice. Presently, most side-educated plans use a high caliber "pre cover" picture that is in this manner handled and after that mutually quantized and inserted with a mystery. In this paper, we research an elective type of side-information– a lot of various JPEG pictures of a similar scene – for applications when the sender does not approach a pre-cover. The extra JPEG pictures are utilized to decide the favored extremity of implanting changes to regulate the expenses of changing individual DCT coefficients in a current inserting plan. The proposed exactly decided regulation of inserting costs is advocated utilizing Monte Carlo recreations by demonstrating that subjectively a similar adjustment limits the Bhattacharyya remove between a quantized summed up Gaussian model of cover and stego DCT coefficients ruined by AWG procurement commotion.

Morteza Heidari et al. [3], every day, people share their digital media on the virtual networks; therefore, protecting them against piracy is worthy of consideration. Advanced watermarking is a technique to accomplish this objective. In this paper, we propose a watermarking technique in Discrete Cosine Transform (DCT) area. For this reason, DCT coefficients of the entire picture are determined. It displays a framework without square ness impacts. We use scaling factors for watermark installing to enhance subtlety of the watermark. A vector of settled components, which is determined experimentally, is utilized as a lot of scaling factors. We install the watermark with a four-time repetition in the cover flag. It is helpful to take advantage of voting method for improving performance of the system in extraction phase. Trial Results show higher execution of the proposed strategy in correlation with comparative works in this area.

N. Senthil Kumaran et al. [4], the unlimited growth in internet and multimedia leads to large usage of images resulting in huge storage and distribution of multimedia contents. With expanding utilization of advanced transmission systems the potential dangers for mixed media content is high which lead to need of assurance for credibility and privacy. To ensure the classification, once cushion should be the most secure calculation. This paper proposes a safe calculation to ensure the watermark picture over an open system in computerized watermarking and is implanted in Discrete Wavelet Transformation (DWT). The special key same as size of watermark is produced from the cover picture. Once cushion is connected utilizing created special key to scramble the watermark picture. The encoded picture so shaped is inserted into cover picture in DWT area. The trial results demonstrate the adequacy and power of the calculation utilizing PSNR and NC figurings.

Bidyut Jyoti Saha et al. [5], in recent years, singular value decomposition has become a popular tool for image watermarking. In this paper, we propose another visually impaired watermarking plan by quantizing the solitary estimations of wavelet part. To upgrade the framework execution, we treat the picture watermarking as a multi-target enhancement issue dependent on non-overwhelmed arranging hereditary calculation II. In light of this new point of view, the inalienable clash existing in picture loyalty and watermark heartiness for picture watermarking can be equitably dealt with. The experimental study shows that our methods indeed provide superior performance.

Jiann-Shu Lee et al. [6], we present a new non-blind digital image watermarking method for embedding a binary logo in an image, based on the dual-tree complex discrete wavelet transform (DT-CDWT) and interval arithmetic (IA). As our experimental results demonstrated, since the high-frequency components obtained by using DT-CDWT and IA contained a low-frequency component, we may expect that the image quality and robustness is maintained even if we

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 10, October 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1010014 |

embed the watermark into the high-frequency components. A watermark was embedded in several high-frequency components. We describe our watermarking procedure in detail and report experimental results demonstrating that our method gives watermarked images that have better quality and that are robust against attacks such as marking, clipping, contrast tuning (MATLAB histeq and imadjust commands), addition of Gaussian white noise, addition of salt & pepper noise, JPEG and JPEG2000 compression, and rotation.

Teruya Minamoto et al. [7], initially, researchers worked with watermark encryption using a single chaotic map. The proposed a novel DCT-based watermarking, in which a binary visually meaningful information is embedded into the cover image to detect temperament. This technique is used to embed each byte information of watermark image in each DCT block by shifting any random coefficient to have a mapped value in a binary mapping coefficient function which is same as watermark bit.

III. STEGANOGRAPHY

Steganography strategy is the craft of hiding data subtly in a computerized cover medium, for example, picture, sound, and video. The word Steganography derived from the Greek words which mean covered writing in any object [7]. The principle goal of steganography is to disguise the presence of the data in the cover medium. Steganography, Cryptography and Watermarking are mostly used to hide the message in image and these techniques are closely related to each other [8]. The strong point of steganography over cryptography is that the hidden messages do not attract attention of third party when it transmitted to the desired recipients because of robustness and undetectably. As watched, amid the most recent quite a few years, an exponential development of utilization of interactive media information over the Internet as Digital Images, Video and Audio documents. The ascent of computerized information on the web has additionally upgraded the examination work committed to steganography. The few uses of steganography like secure mixed media watermarking, military interchanges and fingerprinting applications for the validation assurance to control the issue of advanced theft.

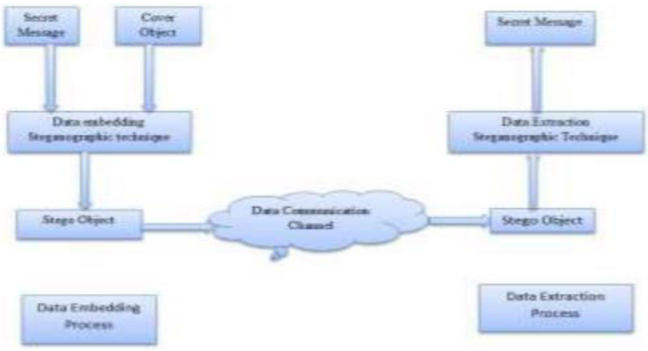

Fig. 1: Steganography system

Numerous steganographic calculations can be utilized for these undertakings yet these are not ideal utilizations of steganography. The Stego picture outwardly is by all accounts same as cover picture however conceals the mystery information inside it and transmitted to the beneficiaries over the correspondence channels. At the point when the ideal beneficiary gets the Stego picture, at that point pursue the information extraction procedure to recoup the mystery information.

TYPES OF STEGANOGRAPHY:-

The sender composes a harmless message and after that covers a mystery message on a similar bit of paper. The principle objective of steganography is to impart safely in a totally imperceptible way and to abstain from attracting doubt to the transmission of concealed information. It isn't to shield others from knowing the shrouded data, yet it is to shield others from suspecting that the data even exists. The information can be obvious in fundamental configurations like: Audio, Video, Text and Images and so forth. These types of information are perceptible by human stowing away, and a definitive arrangement was Steganography. The different kinds of steganography include:

Image Steganography: The Image Steganography is method in which we shroud the information in a picture so that there won't be any adjustment in the first picture.

b. Audio Steganography: Sound Steganography can be utilized to shroud the data in a sound document. The sound record ought to be imperceptible.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 10, October 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1010014 |

c. Video Steganography: Video Steganography can be utilized to conceal the data in video records. The video records ought to be imperceptible by the aggressor.

d. Text files Steganography: Content Steganography is utilized to shroud the data in content records. The general procedure of steganography i.e., setting up a stego object that will contain no change with that of unique item is arranged yet utilizing content as a source.

IV. DIGITAL WATERMARKING

Watermarking system mainly consist of two modules; Watermark embedding, Watermark extraction Watermark embedding and extraction process has a cryptographic key which could be either a public key or a secret key. The key is utilized for security reasons, which keep it from unapproved parties [4]. Cover object is the first picture to be watermarked. Watermark is another picture use for watermarking on the cover picture. Watermarked information is yield information which is get by superimposing of unique picture and watermark picture. Embedding process of watermark image is shown in figure 2.

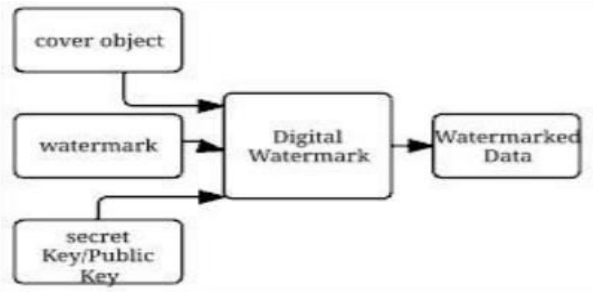

Fig. 2: Digital watermarking: Embedding process

Watermark, cover item and mystery key or open key are given as the contribution to watermark implanting process. Either content or a picture can be utilized as a watermark object. The yield information got is the separated watermark information. Extraction process of digital image watermarking is shown in Figure 3.

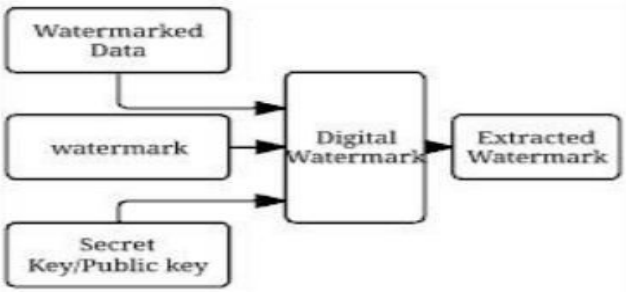

Fig. 3: Digital Watermarking: Extraction process

For extraction process Watermark or the original data, the Watermarked data and the secret key or the pubic key are the input data. The output is recovered watermark.

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 article can nor be seen by a human eye nor be gotten by a human ear, it must be discover through unique preparing or committed circuits. The watermark ought to be prepared so as to not influence the nature of implanted information.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 10, October 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1010014 |

Security: Just the approved clients can recognize, separate and change the watermark and therefore a proprietor can accomplish the motivation behind copyright insurance.
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 ought to be inserted so that it ready to give the full and solid verification of the responsibility for ensured data items. It tends to be utilized for shielding information from illicit conveyance as the information is being ensured by the watermark. It is additionally utilized for distinguishing the credibility.
Fidelity: When we include a watermark into a picture there is an expansive plausibility that it will influence the nature of unique picture. We should keep this property of the picture's quality to a base, with the goal that the loyalty of a picture ought to be kept up.

Applications of Digital Watermarking:-
Watermarking system can be used in different areas and some of the application of digital watermarking are:
Broadcast Monitoring: The Broadcast observing framework can secure business ads and profitable TV items. This use of advanced watermark distinguishes that when and where works are communicated by recognizing watermark installed in these works. There are diverse advances which can screen playback of sound recorded amid transmission. The computerized watermarking is an option in contrast to these advances because of its solid computerization identification.
Information Hiding: In advanced watermarking information covering up is a standout amongst the most widely recognized applications. Information stowing away is the strategy in which information is sent subtly so that no unapproved individual can recognize it.
Confirmation of Ownership: To keep the unapproved adjustment of information, the approved individual distinguishing proof is watermarked into the first information.
Information Authentication: The picture can be effectively intruded without being identified. The Watermark like content, mark, and set of words can be implanted into the picture to stay away from this temper and to keep up the inventiveness. Interfering of picture can without much of a stretch be recognized now, as the pixel estimation of the implanted information would change and does not coordinate with the first pixel esteems.

V. COMBINED WATERMARKING AND STEGANOGRAPHY

To secure the validness of the report, watermarking can be connected to it. This watermarked record can be installed in cover picture utilizing a stego-key and transmitted over the correspondence medium. At the recipient end, the data can be first decoded utilizing the turnaround strategy and after that it tends to be approved for its realness utilizing the watermarking. This consolidated methodology will fulfill every one of the four objectives of information concealing: security, limit, heartiness and detectable quality.

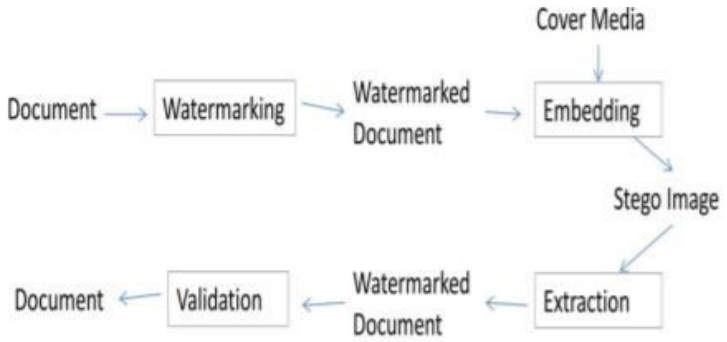

Fig. 4: Watermarking with Steganography

Pure steganography – it doesn't require the trading of figure, for example, a stego-key yet the sender and collector must approach implanting and extraction calculation. The cover for this technique is c hosen with the end goal that it limits the progressions brought about by implanting process. These frameworks are not extremely anchor as the security relies upon the assumption that no other gathering knows about this mystery message.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 10, October 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1010014 |

Secret key steganography – this strategy utilizes a key to implant the mystery message into the cover. The key is just known to sender and the collector and is known before correspondence. Likewise, the key ought to be traded in a safe 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].

VI. PARAMETER

It is most commonly expressed in terms of means squared error (MSE) or peak-signal-to-noise ratio (PSNR). The performance of image compression systems is measured by the metric defined in equations (1) and (2). It is based on the assumption that the digital image is represented as $N_1 \times N_2$ matrix, where N_1 and N_2 denote the number of rows and columns of the image respectively. Also, $f(i,j)$ and $g(i,j)$ denote pixel values of the original image before compression and degraded image after compression respectively.

Mean Square Error (MSE)

$$= \frac{1}{N_1 N_2} \sum_{j=1}^{N_2} \sum_{i=1}^{N_1} (f(i,j) - g(i,j))^2 \qquad (1)$$

Peak Signal to Noise Ratio (PSNR) in dB

$$= 10 \times \log_{10}\left(\frac{256^2}{MSE}\right) \qquad (2)$$

Evidently, smaller MSE and larger PSNR values correspond to lower levels of distortion. Although these metrics are frequently employed, it can be observed that the MSE and PSNR metrics do not always correlate well with image quality as perceived by the human visual system.

VII. CONCLUSION

It has been proved that the use of DWT-LSB with fusion method has improved the security of the watermarking scheme. Specific consideration is given to the proposed plan to ensure secure watermark installing and simple extraction. The watermark is intangible to the human eye and recoverable more often than not. The watermarked pictures were evaluated for loyalty by utilizing PSNR and MSE. The new methods could offer noteworthy focal points to the advanced watermark field and give extra advantages to the copyright security industry.

REFRENCES

[1] 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.

[2] Tomas Denemark, and Jessica Fridrich, "Steganography with Multiple JPEG Images of the Same Scene", IEEE Transactions on Information Forensics and Security, Volume: 12, Issue 10, 2017.

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

[4] 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

[5] 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.

[6] 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.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 10, October 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1010014 |

[7] Teruya Minamoto and Ryuji Ohura, "A non-blind digital image watermarking method based on the dual-tree complex discrete wavelet transform and interval arithmetic", Ninth International Conference on Information Technology- New Generations, IEEE 2012.

[8] 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.

[9] 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.

[10] Chen and K. V. Karthik, "A Modified Three Level Block Truncation Coding _or Image Compression", International Conference on Pattern Analysis and Intelligent Robotics, PP.31-35, June 2011 IEEE.

[11] Fan, Arpana Parakale, Bharamgonda Madhuri Mahavir, Bharamu Ullagaddi, "Image Compression using Absolute Moment Block Truncation Coding", International Conference on Pattern Analysis and Intelligent Robotics, PP.97-102, June 2011, Putrajaya, Malaysia.

[12] Bin and Hon-Hang Chang, "A Data Hiding Scheme for Color Image Using BTC Compression Technique," Proc. 9th IEEE International Conference on Cognitive Informatics, PP.845-850, 2010 IEEE.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details