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 11, Issue 8, August 2022

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: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 8, August 2022||

| DOI:10.15680/IJIRSET.2022.1108129 |

Study of Steganography and Digital Watermarking Scheme for Security Application

Gaurav Gadge[1], Prof. Satyarth Tiwari[2]

M. Tech. Scholar, Department of Electronics and Communication, Bhabha Engineering Research Institute, Bhopal, India[1]

Guide, Department of Electronics and Communication, Bhabha Engineering Research Institute, Bhopal, India [2]

ABSTRACT— Steganography technique plays an important role in information hiding in any digital cover object. Security of information on internet against unauthorized access has become a prime problem. Due to this, steganography technique becomes more popular. Steganography is the science which includes secret communication in an appropriate digital cover objects viz. audio, image, text and video files. The main objective of steganography technique is to hide the presence of the embedded information in carrier file and other objectives are robustness, Un-detectability and capacity of the concealed data. Steganography is separate from other related techniques viz. watermarking and cryptography in term of robustness and Un-detectability of information. Watermarking is a technique that hides information in digital image to protect intellectual properties and copyright, such as logo for proving ownership. Steganography and watermarking are important techniques to conceal important data in cover object an undetectable and irremovable way. Both techniques are the fast developing area of information hiding. This paper delivers a comparative study on digital images steganography and watermarking techniques and significant research growths are also discussed.

KEYWORDS— Steganography, watermarking, Carrier, robustness and information

I. INTRODUCTION

Nowadays multimedia data has been moved expeditiously and broadly to the destinations through the internet into various forms such as image, audio, video and text. In digital communication over the internet, everything is visible and accessible to every user. Therefore, security of information is a necessary and important task. 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. Network security is not sufficient for reliable communication of information like text, audio, video and digital images. There are many techniques to secure images including encryption, watermarking, digital watermarking, reversible watermarking, cryptography, steganography etc. In this paper a review on encryption, steganography and watermarking is presented [2]. In this research study we proposed a hybrid security approach that is a fusion 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 frequency domain, images are transformed to frequency components by using FFT, DCT or DWT and then messages are embedded in some or all of the transformed coefficients. Embedding may be bit level or in block level. Moreover in spatial domain the bits of the message can be inserted in intensity pixels of the video in LSB positions. The advantage in the method is that the amount of data (payload) that can be embedded is more in LSB techniques. However most of the LSB techniques are prone to attack as described in [5] and [6]. This makes research fraternity interested in designing new methods. Techniques other than LSB substitution also exist in literature and have been discussed in the next section. In this paper a hash based LSB Techniques is proposed in spatial domain. An application of the algorithm is illustrated with AVI (Audio Video Interleave) file as a cover medium.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 8, August 2022||

| DOI:10.15680/IJIRSET.2022.1108129 |

II. LITERATURE REVIEW

Wenguang He et al. [1], in reversible watermarking for image authentication, less degradation of the marked image is always desirable. For minimum distortion, the pairwise prediction-error expansion (PEE) technique was recently proposed to modify errors jointly. Although its superiority over conventional PEE has been verified, its potential has not been fully exploited yet. In this paper, we focus on optimal modification and propose an enhanced pairwise PEE. First, it is observed in PVO-based pairwise PEE that the histogram peak varies with relative location when predicting the largest/smallest two pixels. Then, a more effective 2D mapping is proposed by content-dependently selecting the expansion bin after introducing spatial location into prediction. Next, the 2D mapping is further extended considering prediction in non-smooth region tends to produce errors with large magnitude. Finally, we also propose to flexibly define the spatial location to achieve content-dependent prediction and further enhancement. Experimental results demonstrate that the proposed scheme achieves better capacity-distortion trade-off and outperforms several state-of-the-art schemes.

Awdhesh K. Shukla et al. [2], a high capacity data hiding method using lossless compression, advanced encryption standard (AES), modified pixel value differencing (MPVD), and least significant bit (LSB) substitution is presented. Arithmetic coding was applied on a secret message for the lossless compression, which provided ~22% higher embedding capacity. The compressed secret message is subjected to AES encryption; this provides higher security in the cases of steganalysis attacks. After compression and encryption, the LSB substitution and MPVD are applied. In MPVD, the adaptive non-overlapping 3×3 pixel blocks or a combination of 3×3 and 2×2 blocks are used in raster fashion. It is experimentally established that with the proposed method, significant enhancement in embedding capacity was achieved and 214 132 extra bits than existing methods could be embedded due to the use of arithmetic compression and MPVD. The MPVD and arithmetic coding together resulted into 25% enhanced embedding capacity than the earlier methods. The proposed method also provides high levels of visual quality with an average of 36.38 dB at 4.00 bpp. The proposed method is also proved to be secure against regular/singular (RS) steganalysis.

A. Bose et al. [3], in the age of digital world, the wide dissemination of images need bandwidth (BW) efficient transmission as well as ownership protection during transmission over radio mobile channel. Compressed sensing (CS) nowadays finds a potential application for BW efficient transmission over wireless network while digital watermarking, more specifically, spread spectrum (SS) watermarking is found to be efficient for copyright protection. To this aim, an SS watermarking scheme on CS images is proposed in presence of both multiplicative and additive impairments that support a general framework of radio mobile channel. First a mathematical form of watermark detection threshold in log-likelihood ratio model is derived followed by an optimization framework to minimize the visual distortion that includes CS reconstruction and watermark embedding distortion while satisfying some certain detection reliability constraints. An approximate closed form solution to the optimization problem in terms of embedding strength and a set of appropriate host samples selection for a given number of CS measurements is derived. A large set of simulation results on Rayleigh distribution as multiplicative degradation and Gaussian distribution as additive noise are reported. Performance comparison with the existing works validate the efficacy of the proposed method in terms of imperceptibility and improved detection reliability against a large set of diverse signal processing operations.

Nazir A. Loan et al. [4], it is widely recognized that incorporating side-information at the sender can significantly improve steganography security in practice. Currently, most side-informed schemes utilize a high quality “pre cover” image that is subsequently processed and then jointly quantized and embedded with a secret. In this paper, we investigate an alternative form of side-information– a set of multiple JPEG images of the same scene –for applications when the sender does not have access to a pre-cover. The additional JPEG images are used to determine the preferred polarity of embedding changes to modulate the costs of changing individual DCT coefficients in an existing embedding scheme. The proposed empirically determined modulation of embedding costs is justified using Monte Carlo simulations by showing that qualitatively the same modulation
minimizes the Bhattacharyya distance between a quantized generalized Gaussian model of cover and stego DCT coefficients corrupted by AWG acquisition noise.

Baharak Ahmaderaghi et al. [5], every day, people share their digital media on the virtual networks; therefore, protecting them against piracy is worthy of consideration. Digital watermarking is a method to achieve this goal. In this paper, we propose a watermarking method in Discrete Cosine Transform (DCT) domain. For this purpose, DCT coefficients of the whole image are calculated. It helps to present a system without block ness effects. We use scaling

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 8, August 2022||

| DOI:10.15680/IJIRSET.2022.1108129 |

factors for watermark embedding to improve imperceptibility of the watermark. A vector of fixed elements, which is calculated empirically, is used as a set of scaling factors. We embed the watermark with a four-time redundancy in the cover signal. It is helpful to take advantage of voting method for improving performance of the system in extraction phase.
Experimental Results show higher performance of the proposed method in comparison with similar works in this domain.

W.-H. Ko et al. [6], the unlimited growth in internet and multimedia leads to large usage of images resulting in huge storage and distribution of multimedia contents. With increasing use of digital transmission techniques the potential risks for multimedia content is high which lead to necessity of protection for authenticity and confidentiality. To protect the confidentiality, one time pad is supposed to be the most secure algorithm. This paper proposes a secure algorithm to protect the watermark image over a public network in digital watermarking and is embedded in Discrete Wavelet Transformation (DWT). The unique key same as size of watermark is generated from the cover image. One time pad is applied using generated unique key to encrypt the watermark image. The encrypted image so formed is embedded into cover image in DWT domain. The experimental results show the effectiveness and robustness of the algorithm using PSNR and NC calculations.

M. Hosseini et al. [7], in recent years, singular value decomposition has become a popular tool for image watermarking. In this paper, we propose a new blind watermarking scheme by quantizing the singular values of wavelet component. To optimize the system performance, we treat the image watermarking as a multi-objective optimization problem based on non-dominated sorting genetic algorithm II. Based on this new perspective, the inherent conflict existing in image fidelity and watermark robustness for image watermarking can be objectively handled. The experimental study shows that our methods indeed provide superior performance.

Ahmed et al. [8], 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 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.

Y.-H. Fung et al. [9], 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 technique is the art of concealing information imperceptibly in a digital cover medium such as image, audio, and video. The word Steganography derived from the Greek words which mean covered writing in any object [7]. The main objective of steganography is to conceal the existence of the information 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 observed, during the last several decades, an exponential growth of use of multimedia data over the Internet in the form of Digital Images, Video and Audio files. The rise of digital data on the internet has further enhanced the research work devoted to steganography. The several applications of steganography like secure multimedia watermarking, military communications and fingerprinting applications for the authentication determination to control the problem of digital piracy.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 8, August 2022||

| DOI:10.15680/IJIRSET.2022.1108129 |

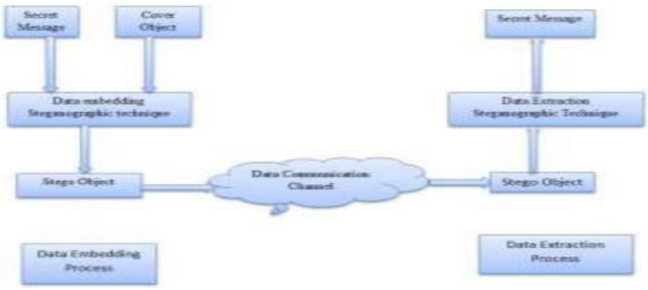

Figure 1: Steganography system

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.

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.

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: Text Steganography is used to hide the information in text files. The general process of steganography i.e., preparing a stego object that will contain no change with that of original object is prepared but using text 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 used for security reasons, which prevent it from unauthorized parties [4]. Cover object is the original image to be watermarked. Watermark is another image use for watermarking on the cover image. Watermarked data is an output data which is obtain by superimposing of original image and watermark image. Embedding process of watermark image is shown in figure 2.

The process of embedding a watermark during a multimedia object is termed as watermarking. Watermark is considered as a sort of a signature that reveals the owner of the multimedia object. Content suppliers want to enter watermarks in their multimedia objects (digital content) for several reasons like copyright protection, content authentication, tamper detection etc. A watermarking algorithmic program embeds a visible or invisible watermark in a given multimedia object

The embedding method is guided by use of a secret key that determines the locations inside the transmission object (image) where the watermark would be embedded.

Once the watermark is embedded it will experience many attacks as a result of the multimedia object being digitally processed. The attacks are often unintentional (in case of pictures, low pass filtering or gamma correction or

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 8, August 2022||

| DOI:10.15680/IJIRSET.2022.1108129 |

compression) or intentional (like cropping) therefore the watermark needs to be very robust against these possible attacks. When the owner desires to see the watermarks within the probably attacked
and distorted multimedia object, s/he relies on the key that was used to embed the watermark. Using the key, the embedded watermark sequence is often extracted. This extracted watermark may or may not resemble the first watermark as a result of the attack.
Hence to validate the existence of watermark, either the original object is used to match and find out the watermark signal (non-blind watermarking) or a correlation measure is used to detect the strength of the watermark signal from the extracted watermark (blind watermarking). In the correlation based detection the first watermark sequence is compared with the extracted watermark sequence.

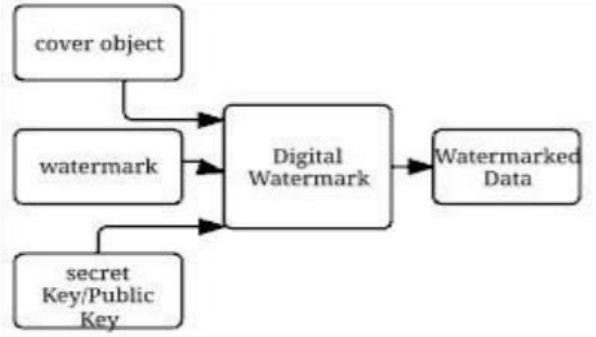

Figure 2: Digital watermarking: Embedding process

Watermark, cover object and secret key or public key are given as the input to watermark embedding process. Either a text or an image can be used as a watermark object. The output data received is the extracted watermark data. Extraction process of digital image watermarking is shown in Figure 3.

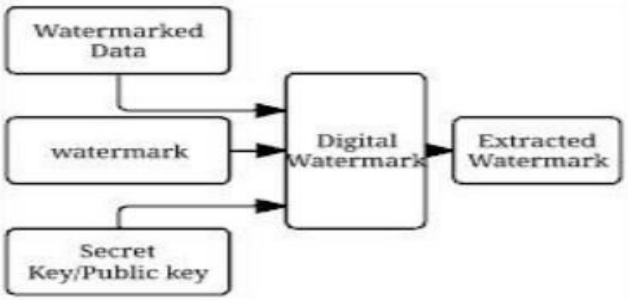

Figure 3: Digital Watermarking: Extraction process

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 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.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 8, August 2022||

| DOI:10.15680/IJIRSET.2022.1108129 |

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.

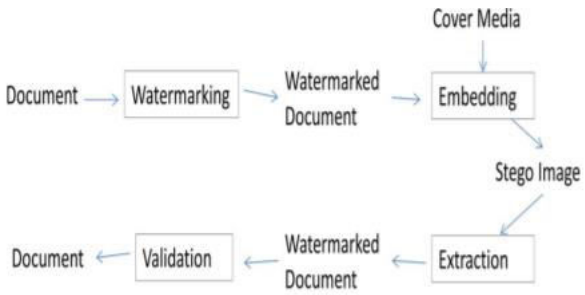

Figure 4: Watermarking with Steganography

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].

VI. METHODOLOGY

Cover-Image: A picture in which the mystery data will be covered up. The expression "cover" is utilized to depict the first, pure message, information, sound, still, video and so forth. The cover picture is some of the time called as the "host".

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 8, August 2022||

| DOI:10.15680/IJIRSET.2022.1108129 |

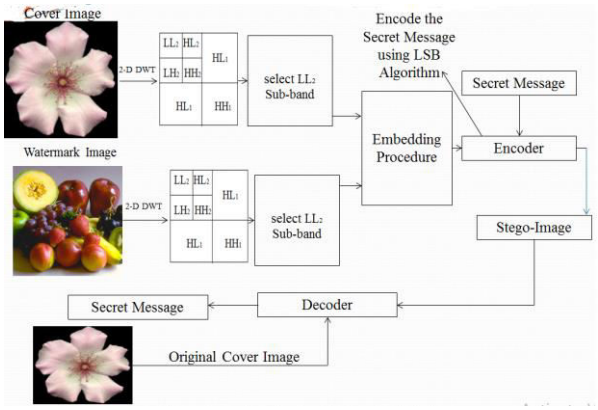

Figure 5: Flow Chart of Methodology

Stego-Image: The medium in which the data is covered up. The "stego" information is the information containing both the cover picture and the "inserted" data. Legitimately, the handling of concealing the mystery data in the cover picture is known as inserting.

Payload: The data which is to be covered. The data to be covered up in the cover information is known as the "inserted" information.

This system works best when the record is longer than the message document and if picture is grayscale.

While applying LSB method to every byte of a 24 bit picture, three bits can be encoded into every pixel.

If the LSB of the pixel value of cover image C(i, j) is equal to the message bit SM of secret message to be embedded C(i, j) remain unchanged; if not, set the LSB of C(i, j) to SM.

VII.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.

REFRENCES

[1] WENGUANG HE, ZHANCHUAN CAI AND YAOMIN WANG, "HIGH-FIDELITY REVERSIBLE IMAGE WATERMARKING BASED ON EFFECTIVE PREDICTION ERROR-PAIRS MODIFICATION", IEEE TRANSACTIONS ON MULTIMEDIA, IEEE 2020.

[2] AWDHESH K. SHUKLA, AKANKSHA SINGH, BALVINDER SINGH AND AMOD KUMAR, "A SECURE AND HIGH-CAPACITY DATA-HIDING METHOD USING COMPRESSION, ENCRYPTION AND OPTIMIZED PIXEL VALUE DIFFERENCING", IEEE ACCESS, OCTOBER 8, PP. 51130-51139, 2018.

[3] A. BOSE AND S. P. MAITY, "SPREAD SPECTRUM IMAGE WATERMARK DETECTION ON DEGRADED COMPRESSED SENSING MEASUREMENTS WITH DISTORTION MINIMIZATION," MULTIMEDIA TOOLS APPL., VOL. 77, NO. 16, PP. 20783–20808, AUG. 2018.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 8, August 2022||

| DOI:10.15680/IJIRSET.2022.1108129 |

[4] 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; Information Security Solutions for Telemedicine Applications, Vol. 6. No. 3. pp. 19876-19 897. IEEE, 2018.

[5] 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, Vol. 4, No. 1. pp. 46–59. IEEE, 2018.

[6] W.-H. Ko B. Satchidanandan P. R. Kumar; Theory and implementation of dynamic watermarking for cybersecurity of advanced transportation systems; Proc. IEEE Conf. Commun. Netw. Security (CNS) pp. 416-420, IEEE 2016.

[7] M. Hosseini T. Tanaka V. Gupt; Designing optimal watermark signal for a stealthy attacker; Proc. Eur. Control Conf. (ECC) pp. 2258-2262 Jun. 2016.

[8] Ahmed, F. and Moskowitz, I.S.; Composite Signature Based Watermarking for Fingerprint Authentication; ACM Multimedia and Security Workshop, pp. 137-142. 2005.

[9] Y.-H. Fung and Y.-H. Chan; Tone-dependent noise model for high-quality halftone; Journal Electron. Image, Vol. 22, No. 2, IEEE 2013.

[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, 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, 2014.

[12] 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.

[13] 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.

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