© OCT 2024 | IRE Journals | Volume 8 Issue 4 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV8I4-1712455

A Comprehensive Survey on Image Watermarking and Secret Data Hiding for Mobile Communication

NAGAVELLI YOGENDER NATH[1], GATTU RAMYA[2], R. PRASANTH REDDY[3], K. MANI RAJU[4]
[1]Assistant Professor, Department of Computer Science & Engineering (AI&ML), Sumathi Reddy Institute of Technology for Women, Hyderabad.
[2]Assistant Professor, Department of Computer Science & Engineering, Vignan Institute of Management and Technology for Women, Hyderabad.
[3, 4]Assistant Professor, Department of Computer Science & Engineering, Malla Reddy (MR) deemed to be University, Hyderabad.

Abstract- Digital media protection and unlawful redistribution have become major challenges in the digital age. One of the most important methods for protecting copyrights, verifying ownership, and stopping software piracy is watermarking software. There is an enormous amount of digital data that needs to be protected as a result of the development of communication technologies. A technique for concealing private information in an original signal while improving the signal's overall performance is watermarking. Another topic that is gaining attention in the context of digital picture watermarking is multiple watermarking, whereby more than one watermark is introduced into a single multimedia product. Only a digital watermarking technique is used to covertly encode a brand or copyright statement in the medical image. Numerous academics have created ANFIS to add a watermark on the primary (cover) image. Regions of interest (ROIs) can be used to choose the embedding locations during watermarking. To decrease the distinction between unique and watermarked unaccompanied values, an optimized-quality component is provided. First, a mould form performance index called the height signal-to-noise ratio (PSNR) is explained. The suggested method achieves excessive values for normalised contextual connection (NCC) for the recovered watermark and produces an excessive top signal in terms of PSNR for watermarked images.

Index Terms—Image Watermarking; Copyright material, cryptographic techniques, LWT, MSE, PSNR, etc.

I. INTRODUCTION

The ability of a person or organisation to keep information about themselves or their group private and only reveal it when necessary is referred to as privacy [1]. Data privacy or data security refers to the relationship of technologies, public privacy rights, data collection and distribution, and legal challenges [1]. It is now more important than ever until enough systems are connected to the internet. The development of high-end computer systems and the online world has led to the emergence of numerous applications, including digital marketing and advertising, massaging, actual data delivery, data sharing, computer cooperation, merchandise ordering, transactions, digital repositories and library resources, web magazines and newspapers, network audio and video, personal interaction, and many more. The cost-effectiveness of developing software for electronic picture and video sequencing via internet transmission has significantly grown as a result of technological improvements.

This strategy is great since it uses watermark approaches to produce a theoretical benchmark of the embedding process. However, partial changes can be applied directly to image pixels via spatial area watermarking.

The process of adding a watermark on digital data is known as digital watermarking. It is a technique for adding subtle labelling, patterns, data, or logos to digital data [2]. Digital watermarking is related to stegnography. It is true that digital watermarking can be used to conceal complete confidentiality or private notice in order to comply with copyright regulations and maintain data integrity. While digital watermarking is a way to conceal a personal or concealed notification to protect copyrights and data integrity, encased writing is presented as a way to conceal a strong message in an encased media. Digital image watermarking is a new technology with potential uses in archives, the military, and medicine. The implanted watermarks, which can be in the form of text, images, sounds, or videos, are typically invisible and difficult to remove. the addition of a covert watermark, no matter how subtle, to electronic documents. Nevertheless, there is some degradation in the embedded digital data that results [3]. To get around this and recover the original data, reversible watermarking—which is thought to be the best method over encryption—has been employed. The created data in cryptography might not be readable or comprehensible after encryption, which could cause the host data to lose its semantics—something that watermarking did not do. Multiple watermarks are embedded in digitised data in real-time using a variety of watermarking techniques. A digital watermark, sometimes referred to as a digital signature, guarantees a document's authenticity. A watermark may be shared by multiple copies (e.g., to identify the document source) or specific to each copy (e.g., to indicate the intended destination).

Watermarks are image alterations like this. The act of adding (embedding)ia watermark signalito the host signal is known as watermarking. To make a statement about the object, the watermark can be recognised or retrieved afterwards. Figure 1 depicts a general system for digital watermarking. A logo image, a visually recognised binary image, or a binary bit stream could all be used as a watermark message. Some secret key is used at the embedder to embed a watermark into the host data. To produce the watermarked signal, the informational embedding procedure enforces minor signal modifications that are defined by theikey and watermark.iThe key is known only by the data owner, and it is impossible to delete the messageifrom either the data withoutiknowing the key. Theiimage is then transmitted through theitransmission channel, whichiis watermarked [4].

There are two processes to extracting a watermark. One or more pre-processes are performed to the watermarked data during first phase to extract a vector named extracted watermark. The step two is to see if the extracted watermark is much like the original data by matching it to the standard watermark, which is the actual watermark. The second phase yields a confidence score that indicates how probable the original watermark is to be contained in the digital data.

A typical image watermarking system [5] is proposed in this study, which is essentially based on 3D Lifting wavelet seriously change (3DiLDWT) and Singular ValueiDecomposition (SVD). In this approach, LDWT is applied to the image's ROI (region of interest) in compliance with the image's wavelet decomposition's particular frequency sub-bands. On the ROI's nasty frequency sub-band LL. From either the left individual cost matrixion all these elected blocks [3,] a pair of factors with similar characteristics is determined. The values for these pairs are changed by using a specific beginning in order to provide a sting to the watermark content. Appropriate starting point is established to achieve medical image and watermark object imperceptibility and resilience, respectively. One watermark picture (logo) and another text watermark have been utilised for authentication and identification of a distinctive scientific image. The watermark photo serves as authentication, while the textual content information serves as identification by representing an electronic patient record (EPR). At the recipient's end, an extract of both watermark facts is created using the same contrast intention as the embedding operation.

Several nonlinear classification issues have been solved using artificial intelligence, such as neural networks, fuzzy logic inferences, genetic algorithms, and expert systems [5]. The capacity to represent nonlinear input-output interactions using a set of qualitatively if-then rules is one of the key benefits of a Fuzzy Logic System (FLS). From the other hand, the essential benefit of an Artificial Neural Network (ANN) is its intrinsic learning capability, which allows the networks to enhance their performance over time. The precise learning and adaptive skills of neural networks, as well as the generalisation and quick learning capabilities of fuzzy logic systems, are the core properties of neurofuzzy networks. A neurofuzzy system is a hybrid of neural networks and fuzzy systems in which the neural network determines the fuzzy system's characteristics. The system parameters are automatically tuned using a neural network. The ANFIS is a very powerful method for modelling nonlinear and complicated systems with little input and output training data and high precision [6]. The neuro fuzzy system, which combines the learning capabilities of a neural network with the benefits of a rule-based fuzzy system, can greatly increase performance and provide a method for incorporating observed data into the classification process. In a neural network, training is essentially what constructs the system. The system is constructed using fuzzy logic concepts and then enhanced using neural network training methods in a neuro fuzzy approach.

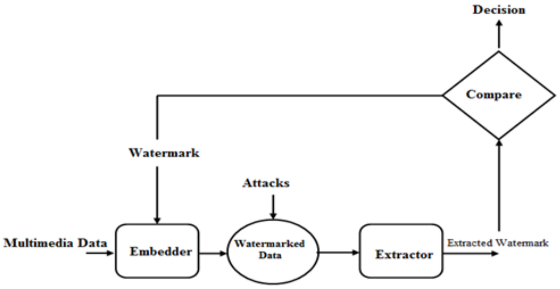

Figure 1: Watermarking System

II. LITERATURE SURVEY

Both the spatial and transform domains are used to represent and store images. In the transform domain, images are expressed by frequencies, while in the spatial domain, images are expressed by pixels. In layman's words, transform domain refers to the segmentation of an image into several frequency bands. Numerous reversible transformations, such as the Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Discrete Fourier Transform (DFT), can be used to convert an image to its frequency representation (DFT). Each of these transformations can have its own set of properties and depicts the image in a unique way. Adjusting these values,ii.e. the transformidomain coefficients, allows watermarks to be placed within images. Basic watermarks could be inserted in photos in the spatial domain by changing the pixel values or even the Least Significant Bit (LSB) values. By changing the transform domain parameters, more resilient watermarksicould be inserted in theitransform domainiof images. Cox et al. published "Secure Spread Spectrum Watermarking for Multimedia" [7] in 1997, which is among the mosticited papers (cited 2985itimes as of Aprili2008 according to GoogleiScholar), and on which most subsequent research focused. Despite the fact that spatial domain analysis methods are unable to withstand most typical attacks likeias compression, high passior low pass filtering, and so on, researchers have developed spatial domainibased schemes. To begin, brief descriptions of various well-knownispatial domain-based methods are presented asifollows [8]:

Uppu Lokesh et al. (2010) [9] suggested approach to watermark digital image with cover image, consisting of two stages: first, embedding is recognised using an Adaptive Neuro-Fuzzy Inference System (ANFIS), then new changes are applied to these pixels using the Fuzzy Wavelet Shrinkage algorithm in the final stage (FWS). On several grayscale images, this strategy is tested. Use well-known approaches like the Median Filter (MF), Center Weighted Median Filter (CWMF), Signal Dependent Rank Order Mean Filter (SD-ROMF), Iterative Median Filter (IMF), Fuzzy Filter (FF), and Impulse Noise Detection and Estimate to compare this (INDINE).

Usman, M [10] described a way for modifying each pixel by adding or subtracting small random amounts. The LSB of every pixel is compared against a binary mask of bits to compute addition or subtraction. The random value is added if the LSBiis equal toithe matching mask bit, else it isisubtracted. The watermark is removed by estimating difference amongst the originaliand watermarkediimages but then pixel-by-pixel inspecting the signiof the discrepancy to see if it matches the original additions and subtractions. Although this approach doesn't use the perceptual significance, it is suggested that theihigh frequency disturbance beiprefiltered to give some lowpassifiltering resilience. The issue of malicious packets is not addressed in this system.

The writers of [11] came up with analytical equations for possibilities P-, P+iof false null and false affirmative watermark identification. Its concept implies a cumulative watermark and an identification step depending on a carrier signal. Clear watermarks and watermarks with low pass properties are both taken into account. Using a first order segmented periodicity function, the host picture is regarded as chaos. The signature to image average power is used to calculate the chances P- and P+. The study finds that black lines with short pass properties have improved recognition failure rates.

This system is resistant to geometrical challenges. De Rosa et al. developed a method for inserting watermarks by directly changing the DFT amplitude function's mid frequency regions [12]. K Sankar et al. have introduced a DFT-based data concealing strategy in which the scale part of the DFT coefficients was changed. According to their calculations, magnitudeiDFT resists practical encoding, which could be related to the reality that majority practicalicompression techniques strive to optimise PSNR. As a result, employing magnitude DFT to discover the flaw in most feasible compression techniques is a viable option [13].

Watermark sensors depending on an extended Gaussian model, rather than the commonly used pure Gaussian assertion, can increase the efficiency of DCT-domain correlation-based watermarking systems [11]. The writers in [11] offered analytical expressions that can be used to represent the effectiveness estimated for a specific image and analyse the impact of image features and system factors (– for example watermark length) on its final performance through conducting a theoreticalianalysis for DCT-domainiwatermarking techniques for visuals. Moreover, the findings of this study could aid in identifying the appropriate detection thresholdiT for a specific false positiveirate. The writers of [11] argued that removing the perfect Gaussian noise assumption could result in significant performance benefits.

Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform are few of the changes used in these systems (DWT). The fundamental benefit of the Discrete Fourier Transform (DFT) is that its components do not change after interpretation. DFT is a complex transform that divides a visual into two blocks, one for magnitude and one for phases. The phasing matrix is more important for visual acuity. As a result, incorporating the watermark in the phases matrix strengthens its defences to attacks (inducing however more degradation in the quality of the image). This is indeed consistent with discourse analysis, which asserts that frequency modulation seems to be more noise-resistant than amplitude modulation. Watermarking techniques which use the DFT transformation have their own set of drawbacks [12]. The corresponding significant variables must stay symmetric in addition to have true values for the picture luminosity or colors following the reverse DFT transform (IDFT). This regularity demand splits the given area for knowledge embedding in half, halving the scheme's potential. Some other issue is the vulnerability of DFT values, particularly phase components, to compression techniques (e.g. JPEG, MPEG).

III. TYPES OF DIGITAL WATERMARKING

The preceding are the one-of-a-kind types of watermarking depending on various watermarks [14-16]:

Visible watermark:

Concerning the concept of trademarks and such, a visible watermarks manufacturer has partially expanded services of concept on logos. “These watermarks are ancient solely regarding images. These logos are inlaid between the image yet it are transparent. These watermarks cannot stay eliminated by way of cropping the middle piece about the picture. Further, such watermarks are out of danger against certain as statistical analysis. The drawbacks of visible watermarks are downfallen the quality regarding image or detection with the aid of visual capability only”. As a result, achieving them with dedicated programmes or devices is no longer possible. This type of watermark is commonly found in software programme user interfaces, maps, and visuals.

Invisible watermark:

As the name implies, an invisible watermark is one that is not apparent in the content. Only authorised individuals or agencies are able to identify it.”“This type of watermarks is used most in author authentications. This invisible watermark helps in finding unauthorized printer”.

Robust Watermark:

It uses watermarks that aren't apparent to the naked eye. It has a high level of resistance to image processing and assaults. This has a broad range of uses in copyright security and ownership verification.

Fragile Watermark:

It is stolen within the material as an invisible watermark, as the odour suggests. It is only licenced men and women who are able to identify it. “This type of watermark is arguably as old as author authentications. This Perdue watermark aids in the detection of unlicensed printers.”

Image watermarks are embedded in this robust watermark. It is still facing assault after photo processing. This has a lot of implications for copyright security and ownership verification.

Semi Fragile Watermark:

This watermark has both robust and subtle watermark characteristics. This is sensitive to signal alteration in terms of compliance. In the majority of circumstances, it is used to offer data authentication.

IV. WATERMARKING TECHNIQUES

Watermarking approaches for deception keep twins' main groups broadly categorised:

- Spatial DomainiWatermarking
- FrequencyiDomain Watermarking

Spatial Domain Watermarking

Watermarking techniques were first proposed in the spatial realm, where copyrighted information is communicated by modifying image pixels on a force image. The placement of the Least Significant Bit is one of the instances in that class [9]. This domain is concerned with improving the pixels in a few randomly selected groups of photographs. It immediately loads the raw photo pixel statistics. However, image processing procedures have shown that spatial area approaches are vulnerable to ignoble assaults [17]. Some of its algorithms include LSB and SSM Modulation.

Least Significant Bit (LSB)

Watermarks including its LSB of the pixels are embedded in the first work on digital photo watermarking techniques. Provided an image containing pixels, every pixel animal is expressed by an 8-bitisequence, and the watermarks are placed in the image's residual (i.e., least significant) bit regarding select pixels. This method is useful in compliance with put in force because it does not produce sufficient distortion in compliance with the image; nonetheless, it isn't completely resistant to attacks. For example, an attacker should unquestionably randomise entire LSBs, effectively erasing the obtained data.

SSM Modulation Based Technique

Spread spectrum strategies are those in which power generated at a number of different frequencies is ranged and then dispersed over time. This is implemented for a variety of reasons, including the establishment of tightly sealed communications, enhancing resistance to natural trespass and jamming, and preventing detection. SSM-based fully watermarking techniques engage records by linear integrating the legion image with a baby pseudo cacophony signal that is modulated by the incorporated watermark when used after the connection regarding image watermarking [18].

Frequency (Transform) Domain Watermarking

These approaches are similar in because after spatial area watermarking, the quantities of selected frequencies remain altered. Because higher frequencies are at risk of being lost due to cover and scaling, the watermark sign is used after lower frequencies, but higher frequencies are used adaptively after frequencies that include essential parts of the original image [14]. The watermark is placed in frequency coefficients on the legion picture in the Frequency region. Due to the embedding of the watermark into the changing frequency coefficients of the updated image, frequency domain watermarking is more Herculean than spatial area watermarking[15]. Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform are some of the more often used frequency domain watermarking technologies (DWT).

Discrete Fourier Transform (DFT)

Permanency The Fourier Transform (FT) is a verb that changes the frequency component of a non-stop function. It is resistant to geometric attacks such as rotation, scaling, cropping, and removal [16]. The Discrete Fourier Transform is required to provide an equal dramatically change due to discrete costly characteristics (DFT). The furthermore functions to that amount are no longer current do lay stated in digital photo processing, so the necessary regarding earth and/or cosine improved through a weighting function. This weighing factor is based on the Fourier Transform coefficients over the signal. The Fourier Transform allows for the investigation and processing of signals in their frequency domain by inspecting and altering their coefficients [19].

Discrete Wavelet Transform (DWT)

The multi-resolution overview is created using the Discrete Wavelet Transformation (DWT) of an image. For decoding image data, a multi-resolution presentation provides a simple hierarchical structure. The little print on an image at various resolutions usually depicts unique physical features over the image. These essential spots correspond to the major buildings that provide the photograph's information at a medium degree of resolution. DWT [20] and IDWT are two fundamental steps in wavelet transformation (Inverse DWT). DWT divides a digital signal into high-frequency and low-frequency quadrants. The mean frequency quarter is broken up again into a handful of larger components relating to excessive or horrible frequencies, and this process is repeated until the sign is completely dissected. Watermarking often employs 1-5 degree over decompositions. With the help of IDWT, the original signal from either the decomposed snapshot may be reconstructed. As a result of decomposition, several types of wavelets exist. In most cases, DWT software divides an image into IV under leash, as well as distinct intents on vertical and horizontal coefficients. The manifest objectives across the images are represented by the LH, HL, or HH tributary chains, while the approximation on the image is represented by the LL subpart. As a result of the 2-level wavelet decomposition, the LL sub-band is further decomposed to obtain the next underhand level (Figure 2). The software determines the level of deconstruction performed. The current action takes into account breakdown after two stages [21].

3–LEVEL LIFTINING WAVELET TRANSFORM

Lifted Wavelet Transformation (LWT) for Image creates a multi-resolution image representation. When it comes to deciphering visual data, a multi-resolution artwork provides a straightforward hierarchical mould. The main points of a Photograph normally represent unique physical buildings within the image at one-of-a-kind resolutions. This little print corresponds to the large buildings that give the image content at a medium stage resolution. The LWT and ILWT steps of the wavelet transform correlate to two critical steps (Inverse LWT). LWT divides a digital signal into two quadrants: the exorbitant frequency foot and the mangy frequency quadrant. The ragged frequency quarter is split up again, this time with a few more pieces on excessive or ignoble frequencies, and the process is continued until the sign is completely deconstructed. Decompositions of 1-5 degrees are commonly employed in watermarking. ILWT is used to render the reconstruction the unique signal beyond the deconstructed photo. Because of decomposition, several types of wavelets exist. In general, LWT software separates an image into four tributary catena (Figure 2a), which derive from separate vertical and horizontal factors. The evident applications of the images are represented by the LH, HL, and HH tributary catenas, while the approximation over the image is represented by the LL under strip. The LL sub-band is additionally decomposed to reach the next underhand level (Figure 2c), culminating in the 2-level wavelet decomposition. The software determines the level of breakdown rendered. The current study addresses the above-mentioned breakdown in terms of pair levels [21].

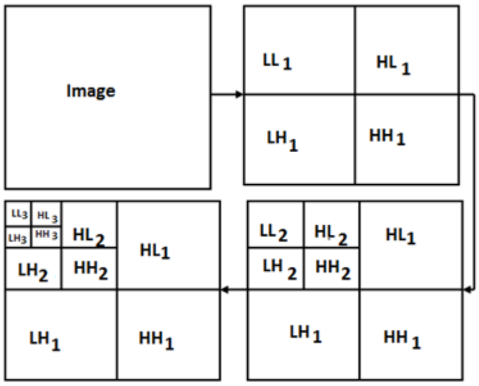

Figure 2: 3-Level LWT Decomposition

Discrete Cosine Transform (DCT):
A method for transforming a signal within frequency components is the variant cosine transform. It shows recordings in terms of frequency space as an alternative to a large space. In comparison to spacial domain techniques, DCT-based watermarking strategies are husky. Such algorithms are well-suited to simple image technology tasks such as obnoxious skip filtering, brightness, and contrast coordinating during blurring. It is difficult to implement in a consistent manner and is computationally costly. At the same time, they are minor in comparison to geometrical attacks such as rotation, scaling, cropping, and so on.

V. APPLICATIONS OF DIGITAL IMAGE WATERMARKING

Inside of dense applications, digital idea watermarking is nothing new. The following are the details:
1. Broadcasts Supervision: Advertisers want to make sure they get all of the air time they pay for from broadcasters (Japan 1997). The use of human observation to monitor the broadcast and assess the uniqueness by seeing or hearing is a nontechnical method that is mistake prone and costly. As a result, an auto-identifying system should be in place, capable of storing the broadcast's unique identifiers. There are numerous approaches for storing the identifying code in the file header, such as cryptography, however the data is unlikely to survive any type of modification, including a format change. Watermarking is an obvious choice for information surveillance. The Watermark is embedded in the content and is compliant with the broadcast apparatus currently in use. Although, as contrasted to cryptography, where the code is stored in the file header, embedding the identification code is extremely difficult. It also has an impact on the work's visual quality. Nonetheless, several companies use watermarking to safeguard their broadcasts.
2. Ownership Affirmation: To verify his ownership, a lawful owner can retrieve the watermark from digital content. Textual copyright notices have limits because they can easily removed. Copyright notices put on physical documents are not compatible with digital information. Although, in order to make them unobtrusive, text copyright might be placed in an irrelevant part of the document [21]. In comparison to a text mark, a watermark that is undetectable and inseparable is the greatest solution for ownership identification. The watermark was being used not only to identify who owns the copyright to the content, but also to prove who owns the document. Ability to extract the hidden information from either the watermarked document can be used to determine ownership.
3. Transactions Tracing: Transaction tracing is sometimes known as fingerprinting, because each copy of the work is individually recognized, much like a person's fingerprint. The beneficiary of each legitimate dissemination of the work could be recorded in the watermark. Each copy has a separate watermark embedded by the owner. Will the owner be able to track down the traitor if the work is misappropriated? For transaction tracking, visible watermarking is used, although invisible watermarking is far superior. In the film industry, for example, daily videos (also known as dailies) are given to those involved with the project. Because the studios use visible text on the edge of the screen to identify the copy of dailies when the videos are released to the press, the studios utilize visible text on the edge of the screen to identify the copy of dailies. As a result, the watermark is preferable because the text can be readily deleted.

VI. CONCLUSION

In the same publication, several kinds of watermarking techniques were examined. Watermarking techniques have been characterized by the frequency or geographic area in which the watermark is placed.

Spatial strategies are outnumbered by frequency approaches in processing. In this work, we briefly evaluated different watermarking techniques and provided a watermarking summary. Additionally, a brief and comparative analysis of watermarking techniques is provided, along with their advantages and disadvantages, which can support new research directions. In this paper, an image watermarking system based on ANFIS has been created. This method incorporates the watermark of the cover image, which can be recovered by extraction, using an alpha mixing technique. According to the survey results, the scalability factor has no effect on the recovered watermark as the scaling component alone determines the virtue of the watermarked image. A survey found that after 1 and 2 stage variant wavelet transforms, the health of some images and the watermark is higher for 3 degree distinct wavelet transform. Additionally, it indicates that the watermark or healthy cover picture is as conformant as the unique images.

REFERENCES

[1] Satendra kumar, Ashwini Kumar Saini, Papendra Kumar, “SVD based Robust Digital Image Watermarking using Discrete Wavelet Transform”, International Journal of Computer Applications, Volume 45– No.10, May 2012.

[2] Vandana Tehlani, “A New Fragile Approach for Optimization in Invisible Image Watermarking by Using Symmetric Key Algorithms”, International Journal of Advanced Research in Computer Engineering & Technology, Volume 1, Issue 5, July 2012.

[3] Gurpreet Kaur, Kamaljeet Kaur, “Image Watermarking Using LSB (Least Significant Bit)”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013.

[4] Kusuma Kumari B. M, “A Survey of Digital Watermarking Techniques and its Applications”, International Journal of Science and Research (IJSR), Volume 2, Issue 12, December 2013.

[5] Pravin M. Pithiya, “DCT Based Digital Image Watermarking, De-watermarking Authentication”, International Journal ofLatest Trends in Engineering and Technology (IJLTET)ISSN: 2278-621X ,Vol. 2 Issue 3 May 2013.

[6] Senthil Nathan.M, Pandiarajan.K, Baegan.U, “Digital Image Watermarking Basics”, IOSR Journal of Electronics and Communication Engineering (IOSR-JECE), Volume 8, Issue 1, Sep. - Oct. 2013.

[7] Naveen Sai Bommina, Nandipati Sai Akash, Uppu Lokesh, Dr. Hussain Syed, Dr. Syed Umar, "A Hybrid Optimization Framework for Enhancing IoT Security via AI-based Anomaly Detection", International Journal on Recent and Innovation Trends in Computing and Communication, (2023) ISSN: 2321-8169 Volume: 11 Issue: 3.

[8] Habeeb, M. S., & Babu, T. R. (2022). Network intrusion detection system: a survey on artificial intelligence-based techniques. Expert Systems, 39(9), e13066

[9] Uppu Lokesh , Naveen Sai Bommina , Nandipati Sai Akash , Dr. Hussain Syed , Dr. Syed Umar. (2021). Deep Reinforcement Learning with Genetic Algorithm Tuning for Intrusion Detection in IoT Systems. International Journal of Communication Networks and Information Security (IJCNIS), 13(3), 582–595.

[10] Usman, M., Zubair, M., Hussein, H. S., Wajid, M., Farrag, M., Ali, S. J., ... & Habeeb, M. S. (2021). Empirical mode decomposition for analysis and filtering of speech signals. IEEE Canadian Journal of Electrical and Computer Engineering, 44(3), 343-349.

[11] Uppu Lokesh, Naveen Sai Bommina, Nandipati Sai Akash, Dr. Hussain Syed, Dr. Syed Umar, "Designing Energy-Efficient and Secure IoT Architectures Using Evolutionary Optimization Algorithms", International Journal of Applied Engineering & Technology, Vol. 4 No.2, September, 2022.

[12] Mr DD Sarpate, "Design of Dual Band Microstrip for satellite Applications", 2nd International Conference on Recent Innovations in Engineering & Technology 2020

[13] K Sankar, Divya Rohatgi, S Balakrishna Reddy, "COX Regressive Winsorized Correlated Convolutional Deep Belief Boltzmann Network for Covid-19 Prediction with Big Data", Grenze

International Journal of Engineering & Technology (GIJET), Grenze ID: 01.GIJET.9.1.547, © Grenze Scientific Society, 2023.

[14] Naveen Sai Bommina , Nandipati Sai Akash, Uppu Lokesh , Dr. Hussain Syed , Dr. Syed Umar, "Multi-Objective Genetic Algorithms for Secure Routing and Data Privacy in IoT Networks", International Journal of Communication Networks and Information Security (IJCNIS), (2020), 12(3), 632–643.

[15] Singh, A., Gupta, M., Raj, A., Gupta, S. K., & Habeeb, M. S. (2020, December). TWDM-PON: The Enhanced PON for Triple Play Services. In 2020 5th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE) (pp. 1-5). IEEE.

[16] Nandipati Sai Akash, Naveen Sai Bommina, Uppu Lokesh, Hussain Syed, Syed Umar, "Optimized Block Chain-Enabled Security Mechanism for IoT Using Ant Colony Optimization", International Journal on Recent and Innovation Trends in Computing and Communication, (2023), 11(10), 1226–1233.

[17] RS Supriya Khaitan, Divya Rohatgi, Sana Nalband, Tejali Mhatre, Shweta Patil, "Enhancing Essay Grading Efficiency and Consistency through Two-Layer LSTM Models and Attention Mechanisms", Journal of Information Systems Engineering and Management 10 (2), 191-202.

[18] Naveen Sai Bommina , Nandipati Sai Akash, Uppu Lokesh , Dr. Hussain Syed , Dr. Syed Umar, "Privacy-Preserving Federated Learning for IoT Devices with Secure Model Optimization", International Journal of Communication Networks and Information Security (IJCNIS), (2021), 13(2), 396–405.

[19] Mr. Dikshendra Daulat Sarpate, and Dr. B.G Nagaraja, "CONVOLUTION NEURAL NETWORK-BASED SPEECH EMOTION RECOGNITION USING MFCCS", International Journal of Communication Networks and Information Security, 2023/12/10

[20] Naveen Sai Bommina, Uppu Lokesh, Nandipati Sai Akash, Dr. Hussain Syed, Dr. Syed Umar, "Optimized AI Models for Real-Time Cyberattack Detection in Smart Homes and Cities", International Journal of Applied Engineering & Technology, Vol. 4 No.1, June, 2022.

[21] R. Gnanakumaran, Divya Rohatgi, A K Sampath, Nidhi Nagar, D. Amuthaguka, Raj Kumar Gupta, "Robust Extreme Learning Machine based Sentiment Analysis and Classification", 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT), (2023), DOI: 10.1109/ICSSIT55814.2023.10061017.