International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-3, January 2020

Detection of Tampered Images using Watermarking Technique

Komali Dammalapati, Bhanu Kiran Devisetty, VVS Sasank, Arpita Ro, Sadhana Burla

Abstract*: Over the most recent couple of years there is a gigantic improvement in advanced innovation . Most the data is in the form of images, videos and audios. But there are various software's to modify these images. So the data we transmit through the digital images may not be secure. For example if we are using an image as an evidence then there may be a chance of modifying that image. There may be a risk of using a digital image as evidence. So, it's not secure to use digital images as evidence. So we decided to do a research on technology that provide security to tampered images. But there are many technologies to detect tampered images. Our project mainly focused on watermarking technique to detect tampered images.

Keywords: technology, steganography, digitalimage , tampering, security.

I. INTRODUCTION

In the present world digital images and digital videos are getting viral in social media like Instagram, Facebook etc. There is a chance of using those images for commercial purposes. Copyright of images had become common these days. Watermark is used for protection of copyright problems. Watermark help us to identify who used our image. Watermarks are also used for providing Authentication to Banknotes. Watermarking is also used for hiding digital information inside an image but does not contain any relation to that image. Digital Watermarks can provide security to evidences to identify the owner. The two sorts of watermarking are one is unmistakable watermarking and the other one is undetectable watermarking. Unmistakable Watermarking can be noticeable to all people who saw that picture. No figurings are required to see noticeable watermarked picture.

Revised Manuscript Received on January 30, 2020.
***** Correspondence Author
Bhanu Kiran Devisetty*, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.
VVS Sasank, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.
Arpita Roy, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.
Sadhana Burla, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.

Be that as it may, if there should arise an occurrence of see undetectable watermarking, a few computations are required to see watermark picture[5]. Invisible Watermarked image will look same as original image. To see invisible watermarking, watermark should be extracted from original image.

We cannot see watermark until the watermark is extracted from original image. Watermark is used for detection of tampered images. Modification of images has become common these days. One can identify whether the images are tampered or

not through Watermarking Technique. Our project mainly deals with the detection of tampered images using Watermarking Technique. Watermark is a straightforward picture or content that had been applied to a picture to shield the first picture from programmers. Watermarking is a procedure of concealing the data inside a picture for security reason. Digital videos, Images and Digital Text can be easily modified. So there is risk of using digital images as security purpose. But we can use digital images or videos or text as security purpose by using Watermarking Technique. Suppose one person committed a crime and police has fingerprints of that person as evidence to prove that he has committed crime. If the police want to send that fingerprints through email to other police station, then there will be a chance of hacking. If that person is expert at hacking or contact a person who can hack the email, then he may hack the mail and change the fingerprints of that person.There has been an enormous development in Information and Communication advances during the most recent decade. Web has become the predominant media for information correspondence. Yet, the mystery of the information is to be taken consideration. Steganography is a procedure for accomplishing mystery for the information conveyed in Internet.[4]To overcome this problem only watermark is used. Fingerprint is made as watermark image and embedded that image in another image. Watermark is added to an image by changing the pixel values. If the hacker hack the mail also then he will change the original image, but the watermark image remains constant. Through watermarking technique we can save the evidence from attacks. We can also embedded a text in an image. Suppose there is a secret code for military persons to perform the mission. That secret code should be confidential. It should not be known to other nationality members. If the military people are sending the code to navy person, then there is a chance of hacking[6]. At this situation also watermarking technique can be used. Watermarking is used for detection of tampered images. Watermarking Technique can also be used for Banknote Authentication. Medical pictures hold wellbeing data about a patient.

Because of their failure to show data plainly and absence of master specialists, spur patients to send their imaging reports utilizing unbound Internet[2]. The goal is to give security to medicinal pictures of patients going through unbound systems through watermarking techniques.

II. BACKGROUND WORK:

The data to be installed in a sign is known as an advanced watermark, in spite of the fact that in certain settings the expression computerized watermark implies the contrast between the watermarked signal and the spread sign. The sign where the watermark is to be implanted is called the host signal. A watermarking framework is normally isolated into three unmistakable advances, inserting, assault, and recognition. In implanting, a calculation acknowledges the host and the information to be installed, and creates a watermarked signal.By then the watermarked modernized sign is transmitted or set away, by and large transmitted to somebody else[8]. In case this individual makes an adjustment, this is called an attack. While the change may not be pernicious, the term ambush rises up out of copyright security application, where outcasts may attempt to oust the propelled watermark through modification. There are various potential alterations, for example, lossy weight of the data (in which objectives is diminished), cutting an image or video, or purposely including racket.

III. LITERATURE SURVEY:

The fitting foundation of writing and the idea of advanced picture watermarking are investigated in this section. The copyright insurance of sight and sound substance has become a basic issue now days because of simple duplicating, the most recent advancements in computerized transmission and far reaching of broadband systems and the web. The transmission of data happens in various structures and is utilized in numerous applications, where the correspondence must be done stealthily shape. Suchmystery correspondence strategies incorporate the exchange of medicinal information, bank moves, corporate interchanges, obtaining utilizing bank cards, a lot of data through messages and so forth. Steganography, cryptography and watermarking are the various procedures used to perform mystery correspondence.

IV. EXISTING SYSTEM:

Today the majority of us are utilizing advanced pictures, computerized recordings and so on. Altering of computerized pictures is exceptionally simple. Our venture predominantly manages discovery of Tampered pictures. There are numerous Techniques to distinguish altered pictures however we selected watermarking procedure to identify altered pictures. First we will take an advanced picture and we will isolate it into three parts: Red, Green and Blue. Red, Green and Blue parts are one uncommon highlights of images[25]. They are utilized for recognizable proof reason. Later we will separate the picture into L_L3, L_H3, H_L3 and H_H3 utilizing DWT Technique[9]. Later we will implant a picture into another picture. We are utilizing non-unmistakable watermarking Technique, so the inserted picture isn't noticeable until we use unscrambled code. This Technique is utilized for concealing the confirmation of confirmations. For instance an individual has carried out wrongdoing and his fingerprints are utilized as confirmation of confirmations. We utilized a key to install watermark picture in unique picture. The fingerprints of the individual who carried out wrongdoing will be watermarked picture and other any unique mark we will take as unique picture. Assume if that individual had rolled out any improvements additionally the watermarked picture will be secure. We utilize a similar key to unscramble the watermarked picture. In the event that the key got checked, at that point the picture isn't altered, generally the picture is altered. The introduction of a steganographic strategy can be evaluated by three parameters; (I) covering limit, (ii) twisting measure and (iii) security.[3]

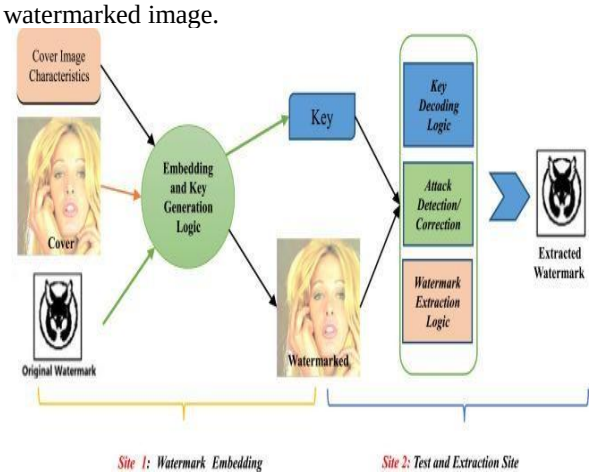
V. PROPOSED METHOD

My proposed calculation comprises of two phases. First arrange comprises watermark installing process and second organize is confirmation arrange which comprises of watermark extraction and validation and confinement utilizing separated watermark[24]. 3-level DWT based watermarking is utilized.

Watermark Embedding Stage:

Watermark embedding steps are given below:

1) Take original image and divide it into 3 components.
2) Perform 3DWT on 3 components to decompose it into four non-overlapping coefficient sets: L_L3, L_H3,H_L3, H_H3.
3) Take watermark image/ logo and resize it as L_L3 by using bilinear interpolation.
4) Encrypt watermark using chaos based encryption algorithm. And call the encrypted watermark as “W E”.
5) Embed shuffled watermark with L_L3 decomposed level of original image using scaling factor. Where,scaling factor value is consider as 0.01
6) Use inverse DWT(I3DWT) on 3DWT transformed image and produced final watermarked image.



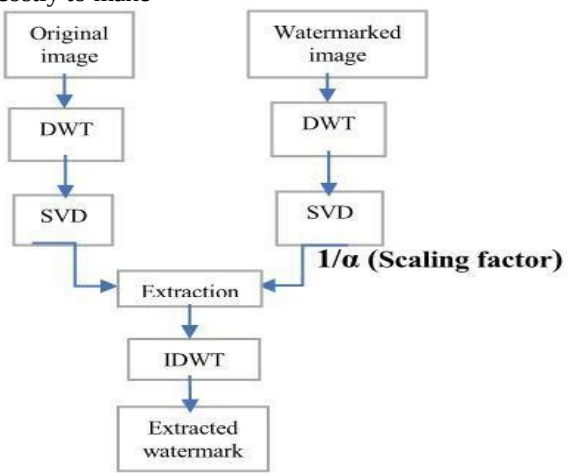
Watermark extraction stage:

Watermark extraction steps are given below:

1) Take watermarked image and divide it into 3 components.

2) Apply 3DWT on watermarked image.
3) Extract watermark by using scaling factor which is embedded in watermarked image.
4) Combine watermarks of all 3 components.
5) Decrypt extracted encrypted watermark WEXE using chaos based decryption algorithm by entering right key which is used in encryption. And call the decrypted watermark as "WEXD".
6) Resize secret watermark "W" and get final extracted decrypted watermark "WEXD" to the same size of cover image and round their values to be 8bit binary values.
7) Compare "WEXD" with secret watermark "W" to identify tampered regions in image using XOR operation between them.

The picture nature of the watermarked picture is one of the most significant factors in assessing data stowing away techniques[10]. In the investigation we have applied calculation to 100 pictures to check its proficiency. We have applied various sorts of assault on the pictures. Separated watermark is unscrambled in the wake of entering right keys implies estimations of x0,y0 and z0 are considered as key.difficult to actualize. There is another kind of wavelet change for example Consistent Wavelet Transformation. The fundamental bit of leeway of Discrete Wavelet Transformation is that it enables sign to be put away more viably. The weakness of Discrete Wavelet Transformation is costly to make



The picture nature of the watermarked picture is one of the most significant factors in assessing data stowing away techniques[10]. In the investigation we have applied calculation to 100 pictures to check its proficiency. We have applied various sorts of assault on the pictures. Separated watermark is unscrambled in the wake of entering right keys implies estimations of x0,y0 and z0 are considered as key.

Image Tampering Detection Algorithms:

Discrete Wavelet Transformation:

Discrete Wavelet Transform gives required data both on investigation and combination. Discrete Wavelet Transformation is utilized to frame quicker change of wavelets[11]. Discrete Wavelet Transformation deteriorate discrete Wavelet signals. DWT utilizes various flag and used to break down the sign at various scales. Discrete Wavelet Transformation is anything but difficult to actualize. There is another kind of wavelet change for example Consistent Wavelet Transformation. The fundamental bit of leeway of Discrete Wavelet Transformation is that it enables sign to be put away more viably. The weakness of Discrete Wavelet Transformation is costly to make

Discrete Cosine Transformation:

Discrete Cosine Transformation is same as Spatial Domain Watermarking with the exception of the picture bit pixel LSB. Discrete Cosine Transformation is strong against assault[12]. To avoid the extraction of the concealed records legitimately from the changed over zone, for the most part the watermarks are installed through altering the relationship of neighboring squares of center recurrence coefficients of the first photograph, instead of utilizing an added substance activity. The fundamental favorable position of DCT is usage of Discrete Cosine Transformation is done insingle circuit and DCT has superb vitality compaction properties. The hindrances of Discrete Cosine Transformation is costly to make.

Chaos Based Image Encryption:

For watermark picture disarray based picture encryption is finished. Bedlam hypothesis portrays the conduct of certain nonlinear unique frameworks that under explicit conditions display elements that are exceptionally delicate to introductory conditions[13]. The turmoil based encryption has recommended another and effective approach to manage the recalcitrant issue of quick and profoundly secure picture encryption. It gives a decent mix of speed, high security, multifaceted nature, sensible computational overheads and computational power.Turmoil based encryption calculations are normally made out of two procedures by and large:

(I) Chaotic disarray of pixel positions by stage process and

(ii) Diff usion of pixel dim qualities by dispersion process.

$x(i+1)\ \ s*(yi-xi)$- (1)

$y(i+1)= r*xi-yi-xizi$ - (2)

$z(i+1)=xiyi-b*zi$-(3)

where, s,r and b are framework control parameters and think about estimations of it as 10, 28 and 8/3 individually. x0, y0 and z0 are introductory conditions and set their qualities for encryption and unscrambling[14]. The condition produces arrangement in the scope of 0 and 1 with confused conduct.

Particular Value Decomposition:

SVD is vigorous and solid symmetrical network decay strategy. Due to SVD calculated and strength reasons, it turns out to be increasingly more well known in signal handling region. SVD is an appealing mathematical change for picture handling. SVD has conspicuous properties in imaging. This segment investigates the principle SVD properties that might be used in picture handling. Albeit some SVD properties are completely used in picture handling, regardless others needs more examination and added to[15]. A few SVD properties are profoundly invaluable for pictures, for example, its most extreme vitality pressing, tackling of least squares issue, registering pseudo reverse of a framework and multivariate investigation . A key property of SVD is its connection to the position of a lattice and its capacity to estimated networks of a given position. Advanced pictures are frequently spoken to by low position grids and, in this way, ready to be depicted by an aggregate of a generally little arrangement of eigenimages.

This idea rises the controlling of the sign as two particular subspaces[16].

A few theories will be given and confirmed in the accompanying segments. For a total audit, the hypothetical SVD related hypotheses are initially outlined, and afterward the pragmatic properties are looked into related with certain examinations[17].

Stage Ordered Binarynumber System

POB number framework called, Permutation requested double number framework is a general number framework with two nonnegative fundamental parameters, n and r, where $n \geq r$ created by A. Sreekumar over the span of his exploration work. This number framework is seen as helpful and more productive than the ordinary number framework under use[18]. They have utilized POB number framework in a recently presented mystery sharing plan. The framework is meant by POB (n, r). In this number framework, it is conceivable to speak to all whole numbers in the range 0, . . .,

- 1 as twofold string, say B =b n-1b n-2 … ..b0, of length n, and having precisely r 1s.

Techniques In Watermarking:

Steganography is a procedure for incognito correspondence. It tends to be finished with picture, sound, and video transporters[1]. Picture steganography systems can be grouped into two significant classes, for example, spatial space procedures and recurrence area strategies.

Spatial Domain Watermarking:

Spatial Domain Watermarking Techniques are of two types. They are

Least Significant Bit:

Least Significant Bit is a simple approach to embedding information in an image. An image is in pixels and each pixel is represented by 8-bit sequence. The Watermarks are embedded in the last bit of original image. Last significant bit changes with bit of the secret message[19]. If we are using a 24-bit image, a bit of each red, green and blue components are used because they are represented by a Byte. Least Significant Bit is easy to implement. The main advantage of Least Significant bit is we can store large amount of information and there is a less chance of deviation from original image. The disadvantage of Least Significant Bit is the hidden data can be easily hacked by using simple attacks and there is a change of losing the hidden data with image manipulation[20].

Ssm Modulation:

Pread Spectrum Techniques Are Methods In Which Energy Generated At One Or More Frequency Domains Are Distributed In Frequency Domains. Spread Spectrum Modulation Is Used For Many Purposes Including Secure Communications. The Watermark Message Is Over A Wide Bandwidth. The Watermarking Provides A Solution To Communication Problem[21]. Spread Spectrum Techniques Is Also Good For Military Communication Problems. The First Spread Spectrum Technique Based On Discrete Wavelet Transform. Spread Spectrum Modulation Is Easy To Store And Transmit Noise Free Digital Signals. The Main Advantage Of Spread Spectrum Is Protecting The Privacy And Can Share The Same Frequency Band With Other Users. The Main Disadvantage Of Ssm Modulation Is Watermarks Can Be Easily Removed.

Frequency Domain Watermarking:

Frequency Domain Watermarking Techniques are of two types. They are

Discrete Cosine Transformation:

Discrete Cosine Transformation is same as Spatial Domain Watermarking except the image bit pixel LSB. Discrete Cosine Transformation is robust against attack. To prevent the extraction of the hidden records directly from the converted area, usually the watermarks are embedded via modifying the relationship of neighbouring blocks of middle-frequency coefficients of the original photo, in place of using an additive operation[22]. The main advantage of DCT is implementation of Discrete Cosine Transformation is done in single circuit and DCT has excellent energy compaction properties. The disadvantages of Discrete Cosine Transformation is expensive to manufacture.

Discrete Wavelet Transformation:

Discrete Wavelet Transform provides required information both on analysis and synthesis. Discrete Wavelet Transformation is used to form faster transformation of wavelets. Discrete Wavelet Transformation decompose discrete Wavelet signals. DWT uses different signals and used to analyse the signal at different scales. Discrete Wavelet Transformation is easy to implement. There is another type of wavelet transformation i.e. Continuous Wavelet Transformation[23]. The main advantage of Discrete Wavelet Transformation is that it allows signals to be stored more effectively. The disadvantage of Discrete Wavelet Transformation is expensive to manufacture.

Attacks On Watermarking:

- Removal Attacks: Tries to removes the Watermark signal without breaking the security of watermark.
- Passive Attacks: In this attack ,
- attackers just try to find out whether the watermark is present or not. They will not try to eliminate the watermark.
- Active Attacks: In this type of attack, attackers try to eliminate the watermark and try to remove that watermark.

VI. RESULTS:

RESULT DESCRIPTION	OBSERVED RESULT IMAGE
Original image on to which we apply watermarking	
Apply DWT on three components of original image and convert into L_L3, L_H3, H_L3 and H_H3.	
Watermark image	
Watermark tampered image	 
Watermark extraction image	

VII. CONCLUSION:

In this paper we exhibited a proficient technique for recognition of altering utilizing watermarking. Computerized Watermarking is extremely valuable strategy for identification of altering, restriction and recuperation of picture. We performed 3-level DWT on RGB parts and tumult based encryption for security reason. Trial results shows that proposed strategy work proficiently and identify altered zones successfully. High PSNR values shows less picture quality corruption by utilizing proposed strategy. The proposed strategy likewise gives low estimation of BER contrasted with existing technique. The proposed technique is likewise fit for finding the altered territories when picture is assaulted by aggressor.

REFERENCES

1. Error! Not a valid link.
2. Amarendra Babu, V., Anitha, T., & RamyaSwetha, R. (2017). Introduction to vagu e topology. Journal of Advanced Researchin Dynamical and Control Systems, 9(Special Issue 18), 768-780.
3. Bangare, S. L., Pradeepini, G., & Patil, S. T. (2017). Brain tumor classification using mixed method approach. Paper presented at the 2017 International Conference on Information Communication and
4. Embedded Systems, ICICES 2017, doi:10.1109/ICICES.2017.8070748
5. Bharath Kumar, T., Chandra Sekhar, O., RamamoortyM., Koteswara Rao, S., & Venkata Bhaskar Rao, D(2017). Comparitive study on wind forecasting models for day ahead power markets. Paper presented at the
6. 2017 IEEE International Conference on Signal Processing, Informatics Communication and Energy Systems, SPICES 2017, doi:10.1109/SPICES.2017.8091273 Retrieved from www.
7. Gouthami, K., Sukanya, D. V. N., Lakshminarayana, S., & Devi, Y. U.(2016). Study of optical switching characterstics in nano doped liquid crystal. Paper presented at the IFIP International Conference on Wireless and Optical Communications Networks, WOCN, , 2016-November doi:10.1109/WOCN.2016.7759877
8. Chandra Prakash, V., Sastry, J. K. R., Kantharao,V., Sriharshini, V., Sriram, G., & Ganesh, C.H.V.S.(2017).An expert system to assess memory power of a studenttt fselection of a suitable career. Journal of Advanced Research in Dynamical and Control Systems, 9(Special Issue 6), 309-321.
9. Chilukuri, S. S., & Madhav, V. V. (2017). Empirical evaluation of non-performing assets: A studyon PACs, SCARDBs and PCARDBs. Journal of Advanced Research in Dynamical and Control Systems, 9(Spec ial Issue 18), 3204-3218.
10. Hema Latha, S., & Subrahmanyam, K(2016).Extractionand processingof situation spatiotemporal traffic using SVM algorithm with big data. Journal of Theoretical and Applied Information Technology, 88(3), 632-637.
11. Gayathri, P., Umar, S., Sridevi, G., Bashwanth, N., & Srikanth, R. (2017). Hybrid cryptography for random-key generation based on ECC algorithm. International Journal of Electrical and Computer Engineering, 7(3), 1293-1298. doi:10.11591/ijece.v7i3.pp1293-1298 10.Jyothi, B., & Venu Gopala Rao, M. (2017) Performance analysis of 3-level 5-phase multilevel inverter topologies.International Journal of Electrical and ComputerEngineering, 7(4), 1696-1705. doi:10.11591/ijece.v7i4.pp1696-1705
12. Gangadhar, M. N. S., & Sreedevi, M. (2016). Regular pattern mining on dynamic databases using vertical formate on given user regularity threshold. Journal of Theoretical and Applied Information Technology, 86(3), 360-364.
13. Chandana, K., Prasanth, Y., & Prabhu Das, J. (2016). A decision support system for predicting diabetic retinopathy using neural networks. Journal of Theoretical and Applied Information Technology, 88(3), 598-606. 13.Girika, J., & Ur Rahman, M. Z. (2017)Adaptive speech enhancement techniques for computer based speaker recognition.Journal of Theoretical and AppliedInformation Technology, 95(10),2214-222
14. Jena, S. R., Lavanya, D. R., & Gadde,S.S.(2017).Minimization of execution ti me over cloud computing environment using fuzzy technique.Journal of Advanced Research in Dynamical and Control Systems, 9(Special Issue 18)
15. Jithendra Prasad, M. G. G., & Shameem, S. (2016). Design and analysis of micro-cantilever based biosensor for swine flu detection. International Journal of Electrical and Computer Engineerin\g, 6(3), 1190-1196. doi:10.11591/ijece.v6i3.9446
16. Kanaka Durga, K., & Rama Krishna, V. (2016). Automatic detection of illegitimate websites with mutual clustering. International Journal of Eletrical and Computer Engineering, 6(3), 995-1001.doi:10.11591/ijece.v6i3.9878
17. Koppula, S., & Muthukuru, J. (2016). Secure digital signature scheme based on elliptic curves for internet of things. International Journal of Electrical and Computer Engineering, 6(3), 1002-1010 doi:10.11591/ijece.v6i3.9420
18. PremaLatha, V., & Sreedevi, E. (2017)Cogitation on agents of things (AOT)of internet of things (IOT). Journalof Advanced Research in Dynamical andControl Systems, 9(18), 654-663.
19. Ramanath, S., & Suresh Babu, K.(2017).Experimental evaluation of an LTE cognitive radio network. Paper presented atthe 2017 9th International Conference on Communi cation Systems and Networks, COMSNETS 2017, 381382doi:10.1109/COMSNETS.2017.7945403.
20. Shahabuddin, S. M., & Yalla, P. (2017). Impact oflean software development into agile process model with integration testing prior to unit testing.Journal of Theoretical and Applied Information Technology, 95(22), 6163-6175.
21. Jammalamadaka, K., & Ramakrishna, V. (2016). A model to quantify and improve software test automation. International Journal of Control Theory and Applications, 9(34), 273-282.

22. Sajana, T., & Narasingarao, M. R. (2017). Machine learning techniques for malaria disease diagnosis - A review. Journal of Advanced Research inDynamical and Control Systems, 9(Special Issue 6),349-369.
23. Sasidhar, T., Manadeep, T. B., Siva Kishore, I.,& Surjana, N. (2017). Analysing and designing ofa high rise building (G+10) by STAAD.pro. International Journal of Civil Engineering and Technology, 8(4), 654-658.
24. Vishwanath, M., & Habibullakhan. (2017). Systematic analysis of T-junctions using plasmonic MIM waveguide. Journal of Advanced Research inDynamical and Control Systems, 9, 1862-1868.
25. Raju, K. N., Rao, M. V. G., & Ramamoorthy, M. (2016). Hybrid modulation technique for neutral point clamped inverter to eliminate neutral point shift with minimum switching loss. Paper presented at the IEEE Region 10 Annual International Conference, Proceedings/TENCON, , 2016-January doi:10.1109/TENCON.2015.7373101
26. Vurukonda, N., & Thirumala Rao, B. (2017). Secure sharing of outsourced data in cloud computing with comparison of different attribute based encryption schemes: A review. Journal of Advanced Research in Dynamical and Control Systems, 9(Special Issue 14), 680-698.
27. Salman, M. N., Trinatha Rao, P., & Ur Rahman, M. Z. (2017). Adaptive noise cancellers for cardiac signal enhancement for IOT based health care systems. Journal of Theoretical and Applied Information Technology, 95(10), 2206-2213.
28. Ravi, P., Haritha, D., & Polala, N. (2016). Computing iceberg queries having non anti monotone constrains with bit map number. Journal of Theoretical and Applied Information Technology, 84(2), 283-286.

AUTHORS PROFILE

Ms D Komali, M. Tech. working as Asst.Professor in CSE department of Koneru Lakshmaiah University.Her research area is cloud computing .

.

B.Sadhana, received B.Tech degree from VR. Siddhartha Engineering College, Vijayawada, Andhra Pradesh in 2015.She has received MS degree from IIIT-Hyderabad, Telangana in 2017.Her area of research include IoT and AI. Email id: sadhanaburla@gmail.com.

Mr V.V.S Sasank is working as Asst.prof in CSE Dept from Koneru lakshmaiah University, Vaddeswaram, Guntur Dt. Currently he is Pursuing Ph.D part time in Koneru lakshmaiah University,Vaddeswaram,Guntur Dt. He actively Participate in various workshops and seminars and presented technical papers related to Computer Science field. His area of interests are Data Mining,Image Processing,Machine Learning

Bhanukiran Devisetty. i had done my Masters of Science from Texas A&M Kingsville, USA in Computer Science Department back in 2016-17. i am currently working as an Assistant Professor in Computer Science and Engineering Department at KL University.Interested areas of research are : machine learning, cloud computing, software engineering, geo-spatial computing,bioinformatics,data-mining.