May - June 2020
ISSN: 0193-4120 Page No. 11017 - 11025

Image Steganography for Hiding Text for Secure Data Transmission

M. Meghana Chowdary[1] , P.Radhika[2],Sk.Reshmi Khadherbhi[3], G.Vidya Lakshmi[4]

[1,2,3,4] Vignan's Nirula Institute of Technology & Science for Women, Peda Palakaluru, Guntur-522009, Andhra Pradesh, India

Article Info
Volume 83
Page Number: 11017 - 11025
Publication Issue:
May - June 2020

Article History
Article Received*: 19 November 2019*
Revised*: 27 January 2020*
Accepted*: 24 February 2020*
Publication*: 19 May 2020*

Abstract

Steganography is a system for the safe transmission of information over the system. Right now, mystery data is transmitted by concealing this behind a sign or picture or video. Picture stenography is another methodology which uses a picture for the protected transmission of information by concealing it behind a spread picture. Data security is a basic factor while transmitting mystery data between two elements. The strategies utilized for this reason for existing are Steganography and cryptography. Despite the fact that Cryptography scrambles the data, it unveils its reality. Steganography conceals the presence of the mystery data. In Steganography the mystery message to be imparted is inserted inside a bearer, consequently it is escaped the vindictive clients. Information is one of the most pertinent and significant term from the old Greek age to present day science and business. The measure of information and utilization of information change for hierarchical work is expanding. Thus, for security and to maintain a strategic distance from information misfortune and unapproved access of information we have structured a picture Steganographic calculation executing both Cryptography and Steganography. This calculation forced a figure message inside a spread picture to cover the presence of the figure content and the stego-picture is moved from sender to planned recipient by conjuring a dispersed association among them to accomplish the information realness.

Keywords : Image Steganography, Data hiding, Data transmission, Data secure, Cryptography.

I. INTRODUCTION

The word steganography originates from the Greek words "stegos" signifying "spread" and "grafia" signifying "stating" characterizing it as "secured composing". Steganography is one such pro security progression inside which puzzle data is embedded in an exceedingly spread [1] [2] [3]. Steganography is that the specialty of made sure about or concealed composition. The inspiration driving steganography is covert correspondence to cover a message from an untouchable [4]. This complexity from cryptography, the art of puzzle making, which is intended to make a message undefined by a pariah, anyway doesn't cover the nearness of the riddle correspondence [5] [6]. Regardless of the specific undeniable truth that steganography is part and exceptional from cryptography, there are various analogies between the two, and a couple of essayists mastermind steganography as an appearance of cryptography since covered correspondence is likewise a sort of secret forming [6] [7]. Regardless, this paper will regard steganography as a novel field. Steganography is characterized in light of the fact that the investigation of inserting touchy data in another medium commented in light of the fact that the blanket medium. It's simultaneously as old as cryptography [8] [9] [10]. Steganography includes stowing away of the data to maintain a strategic distance from location of the key data. The articles used to conceal the key data are called spread items [11]. The concealed data in addition to the blanket item is known as stego object. The blanket article is

Published by: The Mattingley Publishing Co., Inc.

May - June 2020
ISSN: 0193-4120 Page No. 11017 - 11025

mixed media records like sound, video or picture document. Pictures are famously utilized as spread items [12] [13] [14]. Gary scale pictures or shading pictures is utilized as spread articles. Shading pictures steganography is more well-known than dim scale picture steganography since its additional room for information covering up [15].

A colossal measure of secret information is being lost once every year during transmission by the interlopers [16]. Figuring procedures are broadly used to scramble and unscramble information. However, some of the time encryption doesn't appear to be sufficient and stowing away of the information itself is required more. The system utilized for this idea is named Steganography [17] [18] [19]. Steganography is that the strategy for disguising data in an exceedingly very bearer like content, picture, voice, video, or convention [20] [21]. Computerized pictures are one by and large the normal and most popular ones in light of their recurrence on the on the web and high limit of information transmission without corrupting impact on pictures quality. it is a high security system for long information transmission [22]. To a PC, a picture is additionally a gathering of numbers that comprise diverse light powers in a few territories of the picture [23].

This numeric portrayal frames a lattice and accordingly the individual focuses are referenced as pixels [24] [25]. Most pictures on the online comprises of an oval guide of the picture's pixels (spoke to as bits) where every pixel is found and its shading [26] [27] [28]. These pixels are shown on a level plane column by push. The quantity of bits in an exceedingly very mix, called the bit profundity, alludes to the quantity of bits utilized for every pixel [29]. The most popular Steganographic technique that works inside the spatial space is that the LSB, which replaces the smallest sum huge bits of pixels, chose to shroud the data [30] [31]. This strategy has a few usage forms that improve the calculation in specific angles.

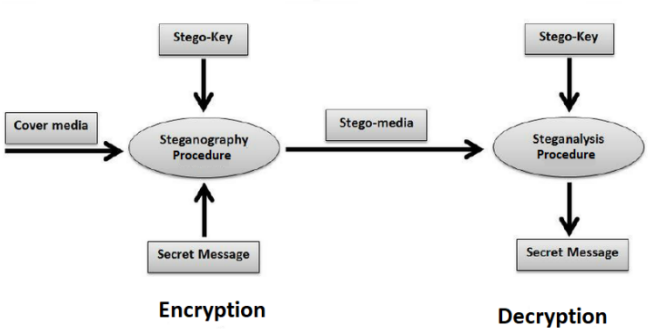

Fig 1: Block diagram of Encryption and Decryption

II. Literature Survey

In [32], Guo and Le estimated the quality factor of JPEG pictures by keeping up quantization tables and played out certain stages alongside this plan to transmit a concealed record. Creators in [33] joined cryptography with steganography by first encoding a message utilizing Vernam figure and afterward inserting it with a picture utilizing LSB method with moving. In [34] executed neural systems to recognize best areas in the host picture to install the mystery information. Patel and Meena superimposed powerful cryptography with steganalysis [35]. The LSB of the image component is altered with its MSB and pixel determination is finished utilizing pseudo arbitrary number. Joined picture cryptography with steganography [36]. Both encryption and decoding are finished utilizing RC4 stream figure and a hash work alongside RGB pixel rearranging are utilized for stego analysis. The creators in [37] proposed two quantum picture concealing systems. A steganography quantum approach is proposed to conceal a picture in another picture document [38] [39]. Also, a quantum watermarking approach is utilized to shroud a water-stamped dim picture to a bearer picture proposed a quantum steganography approach utilizing lattice coding for quantum shading pictures [40].

III. Proposed Method

An advanced picture comprises of various pixels. Right now, utilized shading picture. As we probably are aware, a shaded pixel can be spoken to as a

Published by: The Mattingley Publishing Co., Inc.

May - June 2020
ISSN: 0193-4120 Page No. 11017 - 11025

blend of red, green and blue shading with proper extents [41] [42]. In parallel documentation, a shading level is spoken to by a stream of 8 bits. In this manner altogether, 24 bits are required to indicate a pixel [43]. In this way a picture is an exhibit of numerous bytes each speaking to a solitary shading data lying in a pixel [44]. In the proposed strategy, a gathering of three successive bytes from such an exhibit is utilized to install a touch of the whole message. The proposed procedure has two fundamental parts: I. Changing the mystery message (plain content) to figure message by AES Cryptography ii. Concealing the figure into picture by a proposed Steganographic strategy 128 bits AES Cryptographic calculation takes a secret phrase and encodes the plain content to figure content. This figure content will be installed into a spread picture utilizing our Steganographic method [45] [46]. In the Steganographic method, a sifting calculation has been utilized to shroud the data. The MSB bit indicate the region where to implant the mystery message.

The proposed framework gives multilayered security to make sure about information move. LSB coding is utilized to insert mystery data in the spread items, for example, picture, sound or on the other hand video document [47] [48] [49]. In LSB coding the least huge piece of each inspecting point is subbed with a paired message. Perfect information transmission pace of 1kbps per 1 kHz is utilized for LSB coding. Once in a while to build the measure of information to be inserted the two Least Significant bits of the example are subbed with two message bits. The virtual products utilized right now Core java, jdk1.6.0_12, Computer with a Pentium processor, 256 MB RAM and about 2GB (approx.) of hard circle space. The client needs to make the collaborations to the framework through the client screens created as some portion of the framework utilizing Java Frames. The product runs on any Operating System which has java virtual machine. 256 MB RAM and circle space of 2GB (approx.) is required for this reason. Since this product is principally founded on JAVA, the most fundamental framework arrangement as determined will in all probability work. For execution reasons a potential negligible framework necessity would be a Pentium class processor, 256 MB RAM and circle space of 2GB (approx.).

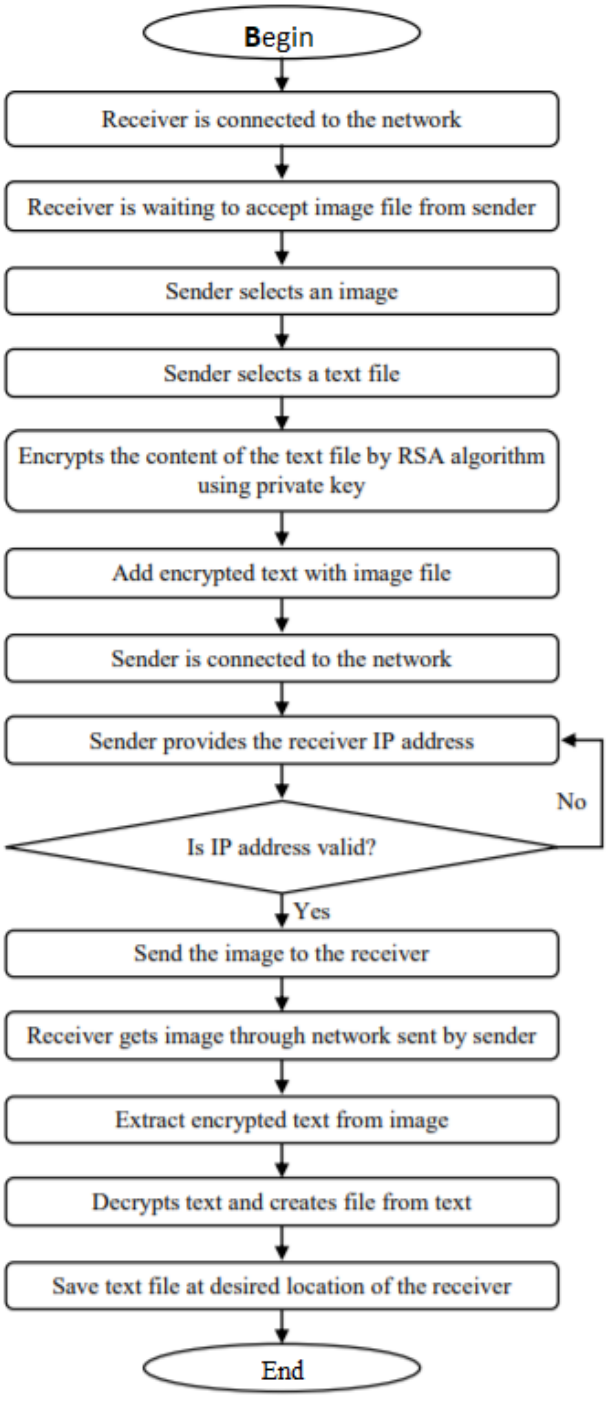

Fig 2: Architecture of the proposed method

Published by: The Mattingley Publishing Co., Inc.

May - June 2020
ISSN: 0193-4120 Page No. 11017 - 11025

This segment presents a bit by bit answer for the issue portrayed previously. The encryption calculation at the Sender's end also, unscrambling calculation at the Receiver's end are definite underneath.

Encryption Algorithm (Sender's end):

Stage 1: Select the content document where the first message has been composed.

Stage 2: Encrypt the substance of the content document utilizing the RSA calculation with the open key of the beneficiary.

Stage 3: Select a suitable spread picture (.jpeg position).

Stage 4: Read the header and footer of the chose picture in an exhibit cushion.

Stage 5: Add the scrambled information toward the finish of picture footer.

Stage 6: Sender and collector are associated with the system.

Stage 7: Sender gives the collector's IP address and afterward send the Stego-picture if the IP address is substantial.

Decryption Algorithm (Receiver's end):

Stage 1: Receive the Stego-picture.

Stage 2: Extract the encoded message from the finish of the stego image by perusing the picture footer.

Stage 3: Generate the private key and unscramble the removed message and afterward make a book document.

Stage 4: Save the content record at the ideal area.

Keys Used:

The protection of any cryptography or steganography calculation relies upon the size of the key utilized. In the proposed calculation, we have utilized the RSA calculation for encoding the content information. In RSA, two enormous irregular prime numbers are created and are prepared to make the private and open keys. These prime transmissions of the content document, sender applies a coordinated methodology by consolidating cryptography with picture steganography [50] [51] [52]. The sender initially scrambles the content record utilizing RSA cryptography calculation and afterward conceals the figure message behind a picture for secure spread. After approval of the recipient's IP address, the picture stego document is sent to the recipient [53] [54]. The last upon gathering extricates the scrambled instant message from the picture document also, unscrambles it to get the first message.

VI. Results

We performed recreation on MATLAB2010a, variant 7.10, under the Windows 7 proficient with double Core CPU and 4 GB RAM. The spread pictures of size 512x512 from USC SIPI picture database (openly accessible at http://sipi.usc.edu/database) are utilized. At first, we estimated the perceptual loyalty of stego pictures utilizing Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) at that point these stego pictures were exposed to normal picture preparing assaults to check the strength of the plan and the outcomes are demonstrated as follows. From the recreation results, it is clear that the proposed conspire is perfect for Secret information correspondence as it meets key prerequisites counting security, better perceptual fidelity and robustness [55] [56].

The Fig.1 shows the first picture we have utilized as spread picture to shroud the content and Fig.2 shows a similar picture after forcing the figure message inside it. Strangely, both unique and stego pictures are indistinct. Covering an encoded example to a precisely regular picture is expected for tricking busybodies. The quality elements of the first picture

Published by: The Mattingley Publishing Co., Inc.

May - June 2020
ISSN: 0193-4120 Page No. 11017 - 11025

is overseen by installing every pixel of the stego picture to a particular area.

Image Size	150kb					
Tools	File Size	50kb	File Size	100kb	File Size	200kb
	Encryption	Decryption	Encryption	Decryption	Encryption	Decryption
Proposed System	10.012	1.8	45	1.8	170	2.5
S-tool	4	2	5	3	can't do	
Openpuff	3	2	6	4	can't do	

Table 1: Comparison of existing Steganography tools test results

#	Features	LSB	Proposed Method
1	Image Types	Only selected image types	All image types
2	Data Size	Depend on image size	Independent of image size
3	Hiding Time	Fast	Slow
4	Retrieval Time	Fast	Fast
5	Statistical attack	HighPossibilities	No impact
6	Complexity	High	No impact

Table 2: Comparison Features between the LSB and proposed method

#	Features	S-Tools	Proposed Tool
1	Image Types(compatible)	.bmp, .gif	All image types
2	Image Size (maximum)	Unlimited	Unlimited
3	Data Size	Depend on image size	Independent of image size
4	Hiding Time	Fast	Slow
5	Retrieval Time	Fast	Fast
6	Statistical attack	High Possibilities	No impact

Table 3: Comparison features of S-Tools and proposed method

#	Attacks	S-Tool	Proposed Tool
1	Stego-only attack	Less impact	No impact
2	Known cover attack	High impact	No impact
3	Known message attack	High impact	Less impact
4	Chosen stego attack	High impact	Less impact
5	Chosen message attack	High impact	High impact
6	Known stego attack	High impact	Less impact

Table 4: Comparison of attacks in S-Tools and proposed method

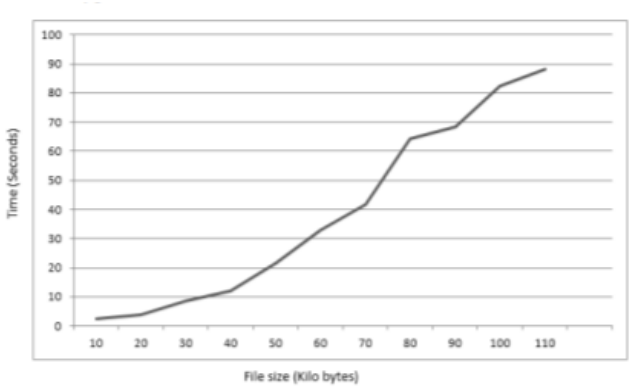

Fig 3: A line graph of Encryption Process

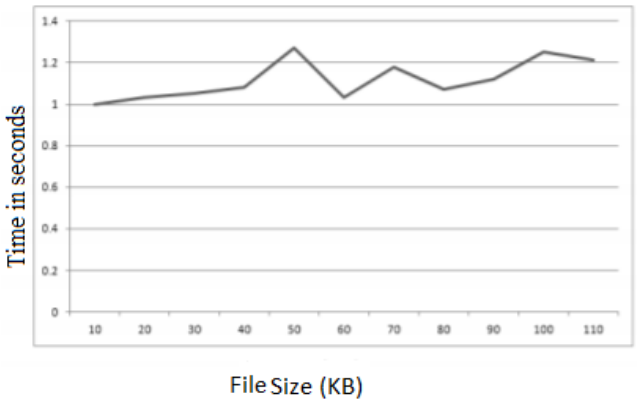

Fig 4: A line graph of Decryption Process

V. CONCLUSION

This paper proposes a novel system for mystery information correspondence that can obstruct particular figuring out strategies by settling the information capture attempt issue. During information transmission if information is caught it tends to be effectively removed by assaulting the cryptographic calculation. We proposed a picture steganography plot dependent on LSB calculation that covers up the encoded message inside spread pictures vaguely. Breaking the correspondence framework would include capturing, recognizing, separating, figuring out and deciphering. Along these lines consolidating cryptography with steganography offers a perfect framework for mystery information transmission with higher consistency as for remain solitary cryptographic strategies. Therefore, this plan gives two level protections, first utilizing cryptographic key and

Published by: The Mattingley Publishing Co., Inc.

May - June 2020
ISSN: 0193-4120 Page No. 11017 - 11025

second utilizing stego key where the mystery message is scrambled before installing and decoded after interpreting. The STEGO - picture is looking splendidly unblemished and has high pinnacle sign to commotion proportion esteem. Consequently, an unintended spectator won't know about the very presence of the mystery picture. The extricated mystery picture or mystery information is perceptually like the first mystery picture or information.

REFERENCES

[1]. Jing-Ming Guo and Thanh Nam Le, "Mystery Communication utilizing JPEG Double Compression", IEEE Signal Processing Letters, Vol. 17, No. 10, pp. 879-882, 2010.

[2]. Kamaldeep Joshi and Rajkumar Yadav, "A New LSB-S Image Steganography Method Blend with Cryptography for Secret Communication", Proceedings of third International Conference on Image Processing, pp. 86-90, 2015.

[3]. K.S. Seetha Lakshmi, B.A. Usha and K.N. Sangeetha, "Security Enhancement in Image Steganography utilizing Neural Networks and Visual Cryptography", Proceedings of International Conference on Computational Systems and Information Systems for Sustainable Solutions, pp. 396-403, 2016.

[4]. Nasarul Islam K V, Mohamed Riyas K V, "Analysis of Various Encryption Algorithms in Cloud Computing", International Journal of Computer Science and Mobile Computing, ISSN: 2320-088X, 2017, pp.90-97.

[5]. Sumitha J, S.Manjupriya, "Comparative Analysis of Homomorphic Encryption in Cloud Computing",International Journal of Management, Technology and Engineering, Vol.8, No12,2018,pp.1251-1255.

[6]. Arepalli, Gopi & Erukula, Suresh & Gopi, A.P. & Nagaraju, Chiluka. (2016). Secure multicast routing protocol in MANETs using efficient ECGDH algorithm. International Journal of Electrical and Computer Engineering (IJECE). 6. 1857-1865. 10.11591/ijece.v6i4.9941.

[7]. K. Sarada, V. Lakshman Narayana,(2020), “Improving Relevant Text Extraction Accuracy using Clustering Methods”, TEST Engineering and Management,Volume 83, Page Number: 15212 – 15219.

[8]. K. Sarada, V. Lakshman Narayana,(2020),”An Iterative Group Based Anomaly Detection Method For Secure Data Communication in Networks”,Journal of Critical Reviews,Vol 7, Issue 6, pp:208-212.doi: 10.31838/jcr.07.06.39.

[9]. Banavathu Mounika, P. Anusha, V. Lakshman Narayana,(2020), “Use of BlockChain Technology In Providing Security During Data Sharing”, Journal of Critical Reviews, Vol 7, Issue 6, pp:338-343. doi: 10.31838/jcr.07.06.59.

[10]. V. Lakshman Narayana, B. Naga Sudheer,(2020),”Fuzzy Base Artificial Neural Network Model For Text Extraction From Images”, Journal of Critical Reviews,Vol 7, Issue 6,pp:350-354,doi: 10.31838/jcr.07.06.61.

[11]. V. Lakshman Narayana, A. Peda Gopi,(2020),”Accurate Identification And Detection Of Outliers In Networks Using Group Random Forest Methodoly”, Journal of Critical Reviews, Vol 7, Issue 6,pp:381-384,doi: 10.31838/jcr.07.06.67.

[12]. Sandhya Pasala, V. Pavani, G. Vidya Lakshmi, V. Lakshman Narayana,(2020),”Identification Of Attackers Using Blockchain Transactions Using Cryptography Methods”, Journal of Critical Reviews, Vol 7, Issue 6,pp:368-375,doi: 10.31838/jcr.07.06.65

[13]. C.R.Bharathi, Vejendla. Lakshman Narayana , L.V. Ramesh, (2020),”Secure Data Communication Using Internet of Things”, International Journal of Scientific & Technology Research, Volume 9, Issue 04,pp:3516-3520.

[14]. Lakshman Narayana Vejendla and Bharathi C R,(2017),“Identity Based Cryptography for Mobile ad hoc Networks”, Journal of Theoretical and Applied Information Technology, Vol.95, Issue.5, pp.1173-1181. EID: 2-s2.0-85015373447

[15]. Lakshman Narayana Vejendla and A Peda Gopi, (2017),” Visual cryptography for gray scale images with enhanced security mechanisms”, Traitement du Signal,Vol.35, No.3-4,pp.197-208. DOI: 10.3166/ts.34.197-208

[16]. A Peda Gopi and Lakshman Narayana Vejendla, (2017),” Protected strength approach for image

Published by: The Mattingley Publishing Co., Inc.

May - June 2020
ISSN: 0193-4120 Page No. 11017 - 11025

steganography", Traitement du Signal, Vol.35, No.3-4,pp.175-181. DOI: 10.3166/TS.34.175-181

[17]. Lakshman Narayana Vejendla and A Peda Gopi, (2020)," Design and Analysis of CMOS LNA with Extended Bandwidth For RF Applications", Journal of Xi'an University of Architecture & Technology, Vol. 12,Issue. 3,pp.3759-3765. https://doi.org/10.37896/JXAT12.03/319.

[18]. Chaitanya, K., and S. Venkateswarlu,(2016),"DETECTION OF BLACKHOLE & GREYHOLE ATTACKS IN MANETs BASED ON ACKNOWLEDGEMENT BASED APPROACH." Journal of Theoretical and Applied Information Technology 89.1: 228.

[19]. Patibandla R.S.M.L., Kurra S.S., Mundukur N.B. (2012), "A Study on Scalability of Services and Privacy Issues in Cloud Computing". In: Ramanujam R., Ramaswamy S. (eds) Distributed Computing and Internet Technology. ICDCIT 2012. Lecture Notes in Computer Science, vol 7154. Springer, Berlin, Heidelberg

[20]. Patibandla R.S.M.L., Veeranjaneyulu N. (2018), "Survey on Clustering Algorithms for Unstructured Data". In: Bhateja V., Coello Coello C., Satapathy S., Pattnaik P. (eds) Intelligent Engineering Informatics. Advances in Intelligent Systems and Computing, vol 695. Springer, Singapore

[21]. Patibandla, R.S.M.L., Veeranjaneyulu, N. (2018), "Performance Analysis of Partition and Evolutionary Clustering Methods on Various Cluster Validation Criteria", Arab J Sci Eng ,Vol.43, pp.4379–4390.

[22]. R S M Lakshmi Patibandla, Santhi Sri Kurra and N.Veeranjaneyulu, (2015), "A Study on Real-Time Business Intelligence and Big Data",Information Engineering, Vol.4,pp.1-6.

[23]. K. Santhisri and P.R.S.M. Lakshmi,(2015), " Comparative Study on Various Security Algorithms in Cloud Computing", Recent Trends in Programming Languages ,Vol.2,No.1,pp.1-6.

[24]. K.Santhi Sri and PRSM Lakshmi,(2017), "DDoS Attacks, Detection Parameters and Mitigation in Cloud Environment", IJMTST,Vol.3,No.1,pp.79-82.

[25]. P.R.S.M.Lakshmi,K.Santhi Sri and Dr.N. Veeranjaneyulu,(2017), "A Study on Deployment of Web Applications Require Strong Consistency using Multiple Clouds", IJMTST,Vol.3,No.1,pp.14-17.

[26]. P.R.S.M.Lakshmi,K.Santhi Sri and M.V.Bhujanga Ra0,(2017), "Workload Management through Load Balancing Algorithm in Scalable Cloud", IJASTEMS,Vol.3,No.1,pp.239-242.

[27]. K.Santhi Sri, P.R.S.M.Lakshmi, and M.V.Bhujanga Ra0,(2017), "A Study of Security and Privacy Attacks in Cloud Computing Environment", IJASTEMS,Vol.3,No.1,pp. 235-238.

[28]. R S M Lakshmi Patibandla and N. Veeranjaneyulu, (2018), "Explanatory & Complex Analysis of Structured Data to Enrich Data in Analytical Appliance", International Journal for Modern Trends in Science and Technology, Vol. 04, Special Issue 01, pp. 147-151.

[29]. R S M Lakshmi Patibandla, Santhi Sri Kurra, Ande Prasad and N.Veeranjaneyulu, (2015), "Unstructured Data: Qualitative Analysis", J. of Computation In Biosciences And Engineering, Vol. 2,No.3,pp.1-4.

[30]. R S M Lakshmi Patibandla, Santhi Sri Kurra and H.-J. Kim,(2014), "Electronic resource management using cloud computing for libraries", International Journal of Applied Engineering Research, Vol.9,pp.18141-18147.

[31]. Ms.R.S.M.Lakshmi Patibandla Dr.Ande Prasad and Mr.Y.R.P.Shankar,(2013), "SECURE ZONE IN CLOUD", International Journal of Advances in Computer Networks and its Security, Vol.3,No.2,pp.153-157.

[32]. Patibandla, R. S. M. Lakshmi et al., (2016), "Significance of Embedded Systems to IoT.", International Journal of Computer Science and Business Informatics, Vol.16,No.2,pp.15-23.

[33]. AnveshiniDumala and S. PallamSetty. (2020),"LANMAR routing protocol to support real-time communications in MANETs using Soft computing technique", 3rd International Conference on Data Engineering and Communication Technology (ICDECT-2019), Springer, Vol. 1079, pp. 231-243.

[34]. AnveshiniDumala and S. PallamSetty. (2019),"Investigating the Impact of Network Size on LANMAR Routing Protocol in a Multi-Hop Ad

Published by: The Mattingley Publishing Co., Inc.

May - June 2020
ISSN: 0193-4120 Page No. 11017 - 11025

hoc Network", i-manager's Journal on Wireless Communication Networks (JWCN), Volume 7, No. 4, pp.19-26.

[35]. AnveshiniDumala and S. PallamSetty. (2019),"Performance analysis of LANMAR routing protocol in SANET and MANET", International Journal of Computer Science and Engineering (IJCSE) – Vol. 7,No. 5, pp.1237-1242.

[36]. AnveshiniDumala and S. PallamSetty. (2018), "A Comparative Study of Various Mobility Speeds of Nodes on the Performance of LANMAR in Mobile Ad hoc Network", International Journal of Computer Science and Engineering (IJCSE) – Vol. 6, No. 9, pp. 192-198.

[37]. AnveshiniDumala and S. PallamSetty. (2018),"Investigating the Impact of IEEE 802.11 Power Saving Mode on the Performance of LANMAR Routing Protocol in MANETs", International Journal of Scientific Research in Computer Science and Management Studies (IJSRCSMS) – Vol.7, No. 4.

[38]. AnveshiniDumala and S. PallamSetty. (2016),"Analyzing the steady state behavior of RIP and OSPF routing protocols in the context of link failure and link recovery in Wide Area Network", International Journal of Computer Science Organization Trends (IJCOT) – Vol. 34 No 2, pp.19-22.

[39]. AnveshiniDumala and S. PallamSetty. (2016),"Investigating the Impact of Simulation Time on Convergence Activity & Duration of EIGRP, OSPF Routing Protocols under Link Failure and Link Recovery in WAN Using OPNET Modeler", International Journal of Computer Science Trends and Technology (IJCST) – Vol. 4 No. 5, pp. 38-42.

[40]. VellalacheruvuPavani and I. Ramesh Babu (2019) ,"Three Level Cloud Storage Scheme for Providing Privacy Preserving using Edge Computing",International Journal of Advanced Science and Technology Vol. 28, No. 16, pp. 1929 – 1940.

[41]. VellalacheruvuPavani and I. Ramesh Babu,"A Novel Method to Optimize the Computation Overhead in Cloud Computing by Using Linear Programming" ,*International Journal of Research and Analytical Reviews* May 2019, Volume 6, Issue 2,PP.820-830..

[42]. Anusha Papasani and Nagaraju Devarakonda,(2016),"Improvement of Aomdv Routing Protocol in Manet and Performance Analysis of Security Attacks", International Journal Of Research in Computer Science & Engineering ,Vol.6,No.5, pp.4674-4685.

[43]. Sk.Reshmi Khadherbhi,K.Suresh Babu , Big Data Search Space Reduction Based On User Perspective Using Map Reduce ,International Journal of Advanced Technology and Innovative Research Volume.07, IssueNo.18, December-2015, Pages: 3642-3647

[44]. B.V.Suresh kumar,Sk.Reshmi Khadherbhi ,BIG-IOT Framework Applications and Challenges: A Survey Volume 7, Issue VII, JULY/2018 pg.no 1257-1264

[45]. P.Sandhya Krishna,Sk.Reshmi Khadherbhi,V.Pavani, Unsupervised or Supervised Feature Finding For Study of Products Sentiment ,International Journal of Advanced Science and Technology, Vol 28 No 16 (2019).

[46]. K.Santhi Sri, Dr.Ande Prasad (2013), "A Review of Cloud Computing and Security Issues at Different Levels in Cloud Computing" , International Journal on Advanced Computer Theory and Engineering Vol. 2,pp 67-73.

[47]. K.Santhi Sri, N.Veeranjaneyulu(2018), "A Novel Key Management Using Elliptic and Diffie-Hellman for Managing users in Cloud Environment", Advances in Modelling and Analysis B,Vol.61,No.2,pp 106-112.

[48]. K.Santhi Sri, N.Veeranjaneyulu(2019), "Decentralized Key Management Using Alternating Multilinear Forms for Cloud Data Sharing with Dynamic Multiprivileged Groups", Mathematical Modelling of Engineering Problems,Vol.6,No.4,pp511-518.

[49]. S.Sasikala, P.Sudhakar, "interpolation of CFA color Images with Hybrid image denoising", 2014 Sixth International Conference on Computational Intelligence and Communication Networks, DOI 10.1109/.53 193 DOI 10.1109/CICN.2014.53, pp. 193-197.

[50]. Me. Jakeera Begum and M.Venkata Rao, (2015), "Collaborative Tagging Using CAPTCHA"

Published by: The Mattingley Publishing Co., Inc.

May - June 2020
ISSN: 0193-4120 Page No. 11017 - 11025

International Journal of Innovative Technology And Research, Volume No.3, Issue No.5,pp,2436 – 2439.

[51]. L.Jagajeevan Rao, M. Venkata Rao, T.Vijaya Saradhi (2016), "How The Smartcard Makes the Certification Verification Easy" Journal of Theoretical and Applied Information Technology, Vol.83. No.2, pp. 180-186.

[52]. Venkata Rao Maddumala, R. Arunkumar, and S. Arivalagan (2018)"An Empirical Review on Data Feature Selection and Big Data Clustering" Asian Journal of Computer Science and Technology Vol.7 No.S1, pp. 96-100.

[53]. Singamaneni Kranthi Kumar, Pallela Dileep Kumar Reddy, Gajula Ramesh, Venkata Rao Maddumala, (2019), "Image Transformation Technique Using Steganography Methods Using LWT Technique" ,Traitement du Signalvol 36, No 3, pp. 233-237.

[54]. Chaitanya, K., and S. Venkateswarlu,(2016),"Detection of Blackhole & Greyhole Attacks In Manets Based on Acknowledgement Based Approach." Journal of Theoretical and Applied Information Technology 89.1: 228.

[55]. Sergei V. Jargin , and . "Drugs and dietary supplements with unproven effects in research and practice: Part 2." Journal of Complementary Medicine Research 10 (2019), 112-128. doi:10.5455/jcmr.20190314031843

[56]. G.V. Vidya Lakshmi, Y. Vasanthi, A. Suneetha, M. Nagaraju, (2020),"Imbalanced Data In Sensible Kernel Space With Support Vector Machines Multiclass Classifier Design",Journal of Critical Reviews,Vol 7, Issue 4, pp: 820-824.

[57]. Yang, G., Lucas, R., Caldwell, R., Yao, L., Romero, M., Caldwell, R.Novel mechanisms of endothelial dysfunction in diabetes(2010) Journal of Cardiovascular Disease Research, 1 (2), pp. 59-63. DOI: 10.4103/0975-3583.64432

[58]. C.R.Bharathi, Vejendla. Lakshman Narayana , L.V. Ramesh, (2020),"Secure Data Communication Using Internet of Things", International Journal of Scientific & Technology Research, Volume 9, Issue 04,pp:3516-3520.

Published by: The Mattingley Publishing Co., Inc.