International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802308

# Design of Low Power Modified Retiming LFSR Architecture

**Dr.N.Sureshkumar[1], K.S.Balaji[2], S.Ragul[3], K.Pavithran[4]**

Muthayammal Engineering College,Rasipuram, Tamil Nadu, India[1]

Department of Electronics and Communication Engineering, Muthayammal College of Engineering, Rasipuram, Tamil Nadu, India[2, 3, 4]

**Publication History:** Received: 25.02.2026; Revised: 20.03.2026; Accepted: 25.03. 2026; Published: 28.03.2026.

**ABSTRACT**: LFSR based PN Sequence Generator technique is used for various Steganography applications and for designing encoder, decoder in different communication channel. It is more important to test and verify by implementing on anyhardware for getting better efficient result. Here we propose Filter structure for parallel LFSR architecture and we also introduce pipelining and retiming technique to increase the speed of LFSR. In order to reduce power consumption in a digital system a set of strategies termed dynamic power management (DPM) is often used. The DPMs strategy consists in disabling the logic circuits that are not performing functional operations during a particular time frame, thus reducing power consumption. Steganography is the art of hiding information in a cover medium such that the existence of information is concealed. An image is a suitable cover medium for steganography because of its great amount of redundant spaces. One simple method of image steganography is the replacement of the least significant bit (LSB) of a cover image with a message bit. Therefore, a new LSB algorithm is proposed here which can effectively resist statistical analysis. In this novel algorithm, every two sample's LSB bits are combined using addition modulo 2 which is compared to the secret message. Built In Self-Test(BIST) application can run on steganography design, where parallel LFSR is the main module.

**KEYWORDS**-LSBsteganography,Built-in self-test (BIST), linear feedback shift register (LFSR)

## I. INTRODUCTION

In recent years, the design for low power has become one of the greatest challenges in high-performance very large scale integration (VLSI) design. As a consequence, many techniques have been introduced to minimize the power consumption of new VLSI systems. However, most of these methods focus on the power consumption during normal mode operation, while test mode operation has not normally been a predominant concern. However, it has been found that the power consumed during test mode operation is often much higher than during normal mode operation [1]. This is because most of the consumed power results from the switching activity in the nodes of the circuit under test (CUT), which is much higher during test mode than during normal mode operation [1]-[3].Several techniques that have been developed to reduce the peak and average power dissipated during scan-based tests can be found in [4] and [5]. A direct technique to reduce power consumption is by running the test at a slower frequency than that in normal mode. This technique of reducing power consumption, while easy to implement, significantly increases the test application time [6]. Furthermore, it fails in reducing peak-power consumption since it is independent of clock frequency. Another category of techniques used to reduce the power consumption in scan-based built-in self-tests (BISTs) is by using scan-chain-ordering techniques [7]-[13].Mostly LFSR is used as random number generator to give random inputs for testing. So for any BIST application LFSR will be main design module.

## II. PSEUDO-RANDOM NUMBER GENERATOR

Pseudo random number generator (PRNG) prevents invaders to find message bits easily. A secret key can be used as a seed for PRNGs. Using a seed causes PRNGs to generate the same random numbers on receiver side as on the sender side. In this paper, a linear feedback shift register (LFSR) is used as PRNG[14].

A. Basic LFSR

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802308

A LFSR is made of sequential shift-register with combinational feedback logic connected to it which can generate a sequence of binary values in a pseudo-random manner. A design modelled around LFSRs often has both speed and area advantages over a functionally equivalent design that does not use LFSRs.
Feedbacks around an LFSR's shift register are connected to the certain points (taps) of LFSR construction and constitute either XORing or XNORing these taps to provide taps back into the register. The selection of taps determines how many values can be generated in a given sequence before the sequence is repeated. Certain tap arrangement lead to maximal length sequences of (2n - 1).

B. IIR filter representation of LFSR

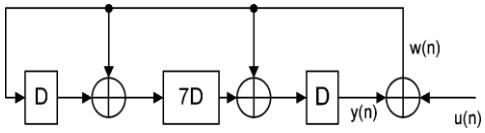



Figure 1.LFSRarchitectureforg(x) = $1+x+x^8+x^9$

We can derive parallel architectures for IIR filters using look ahead techniques. We use the same look-ahead technique to derive parallel system for a given LFSR. Parallel architecture for a simple LFSR described in the previous section is discussed first. Consider the design of a 3-parallel architecture for the LFSR in Fig. 1. In the parallel system, each delay element is referred to as a block delay where the clock period of the parallel system is 3 times the original sample period (bit period) [16].

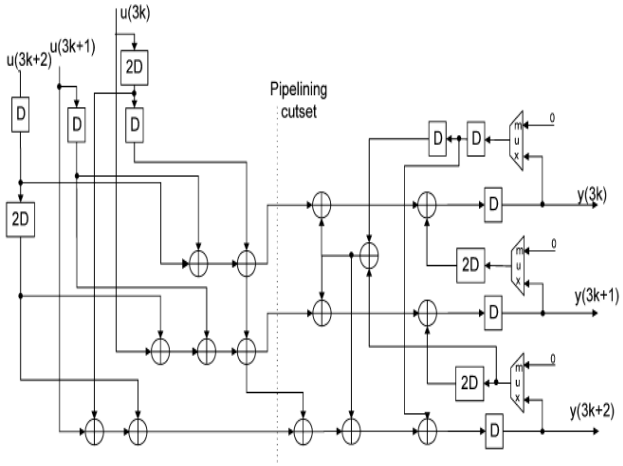
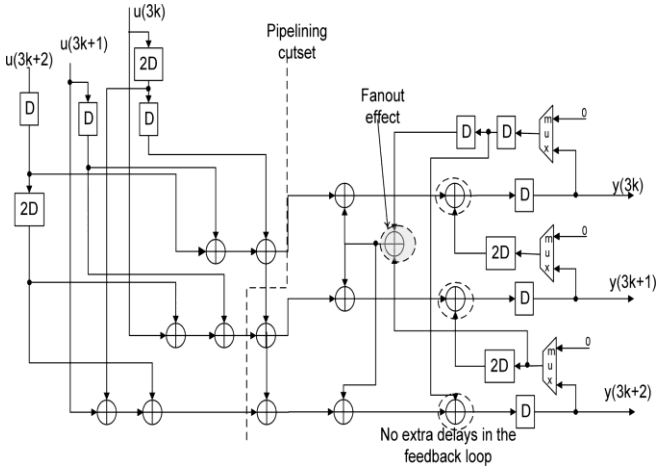



Figure 2.Block diagram of Three parallel LFSR architecture after pipelining



International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802308

Figure3.Retimingand pipeliningcutsetsinthreeparallelLFSRarchitecturetoreduceC.Pto for figure 1WecanseefromFigure 3that,whenwehaveadditionaldelaysatthefeedbackloops,wecanretimearoundthecommonlysharednodestoremovethelargefa nout effect.Wecanfurtherreduce thecritical pathbycombining parallelprocessingandpipeliningconceptsforIIRfilterdesign.

C. Gated-clock design of LFSRs

To reduce power consumption in a digital system a set of strategies termed dynamic power management (DPM) is often used. The DPMs strategy consists in disabling the logic circuits that are not performing functional operations during a particular time frame, thus reducing power consumption.

To analytically evaluate the power consumption of the gated clock approach applied to a LFSR, we have to take into account also the dissipation introduced by the extra gates that are employed to implement the gated clock circuits, as well as the load effects introduced by these gates with respect to the traditional one.

Proof: The sequence of 1s and 0s that is followed by one bit position of a maximal-length LFSR is commonly referred to as an msequence. Each bit within the LFSR will follow the same m-sequence with a one-time-step delay. The m-sequence generated by an LFSR of length n has a periodicity of 2n − 1. It is a well-known standard property of an m-sequence of length n that the total number of runs of consecutive occurrences of the same binary digit is 2n−1.

In order to evaluate the power reduction obtained by applying the gated-clock approach to a LFSR. As a preliminary results, we obtained that

$$C_{ck} > \frac{\alpha}{1-\alpha}(C_{inFF\_CK} + C_{NORNAND} + 4C_{inXOR} + (C_{INV} + C_{inINV})/n)$$

which defines the technological condition (and the circuital solutions for the gate's implementation) so that the gate-clock approach leads to an improvement in terms of power reduction compared to the traditional LFSR implementation.

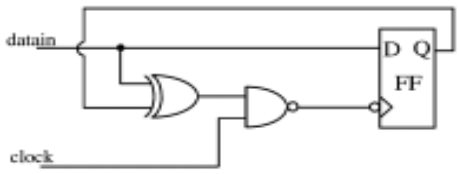



Figure 4.Block diagram of bit gatedclock FF

## III. STEGANOGRAPHY

In the modern world, information is converted from paper type to digital information. Therefore, security improvement in data saving and exchanging is important. Different techniques of cryptography are used for data encryption but all of these methods can be recognized by invaders. If the information can be embedded in a medium in such a way that it cannot be observable easily, it will not raise the suspicion of invaders. This is the main idea of steganography.

The image formats used typically in such steganographical methods are lossless and the data can be directly manipulated and recovered. Since bmp images use lossless compression, one form of LSB attempts to use bmp images. However, other image formats are used as cover image as well.

A. Data hiding process

Consider S = < x0, x1, … ,xn> be the set of pixels of an image which is selected by a pseudo-random number generator. Pseudo random number generator produces random numbers according to the value of seed (key). xis the gray value of each pixel. n is determined by the size of embedded message and the number of LSB bits in each pixel which can be used to embed messages. It can be calculated by

$n = \frac{k}{m}$

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802308

Where k is the length of bit stream of embedded message, and m is the number of bits used to embed messages in each pixel.

B. Message Bit Randomizer Module

This part of design changes message bits so that if invaders find them, they cannot construct the message without access to secret key and the LFSR architecture. In each clock cycle, message bits must be XORed by a random number. The result of XOR operation will be embedded in pixels. At receiver side, extracted LSBs of each pixel must be XORed with the same random bits to construct the message bits.

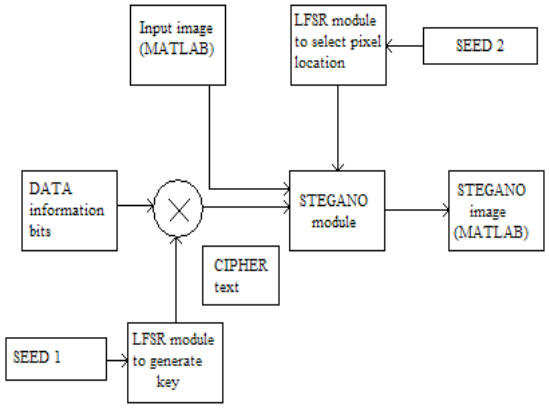



Figure 5.Block diagram of proposed steganography method in functional mode.

## IV. DISTORTION ANALYSIS

The images can be distorted in embedding process because of changing pixel bits. Distortion is measured by means of two parameters namely, Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR).

MSE can be calculated by

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}.\sum_{j=1}^{N}(Xij - Yij)^2$$

The PSNR is calculated using

$$PSNR = 10\log_{10}\{\frac{I^2max}{MSE}\}\ dB$$

Imax is the maximum intensity value of each pixel which is equal to 255 for 8 bit gray scale images. Higher value of PSNR leads to better image quality.

The size of these images is 256*256 pixels. As shown here, message embedding is done with no dramatic changes in image quality

## V. EXPERIMENTAL RESULTS

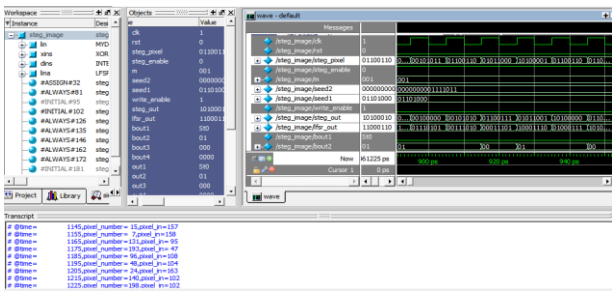


Figure 6.Simulated output

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802308

## VI. CONCLUSION

Finally we increase the Fmax operating frequency of LFSR with pipelining technique and one dynamic power management (DPM) is used to reduce the power dissipation. This proposed new LFSR type is used in steganography application with new algorithm approach. This algorithm can resist statistical analyses and enables the usage of LSB in a secure way. Therefore, it is more appropriate for hardware implementation. Furthermore, by using our pixel interleaver and message bit randomizer, protection against attacks is improved. User can select how many bits must be embedded in each pixel according to image quality and length of message.In this design, two separate keys are used as a seed value to our LFSR to improve security.

## REFERENCES

1. Y. Zorian, ―A distributed BIST control scheme for complex VLSIdevices, in Proc. 11th IEEE VTS, Apr. 1993, pp. 4-9.
2. A. Hertwig and H. J. Wunderlich, ―Low power serial built-in self-test, in Proc. IEEE Eur. Test Workshop, May 1998, pp. 49-53.
3. P. H. Bardell, W. H. McAnney, and J. Savir, Built-in Test for VLSI:Pseudorandom Techniques. New York: Wiley, 1997.
4. P. Girard, ―Survey of low-power testing of VLSI circuits, IEEE Des. TestComput., vol. 19, no. 3, pp. 80-90, May/Jun. 2002.
5. C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor &Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011. DOI: 10.1080/15325008.2010.541746
6. C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of Electrical Engineering, Vol.63 (6), pp.365-372, Dec.2012. DOI: 10.2478/v10187-012-0054-2
7. C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011. DOI 10.1007/s00202-011-0203-9
8. S.Tamilselvi, R.Prakash, C.Nagarajan,"Solar System Integrated Smart Grid Utilizing Hybrid Coot-Genetic Algorithm Optimized ANN Controller" Iranian Journal Of Science And Technology-Transactions Of Electrical Engineering, DOI10.1007/s40998-025-00917-z,2025
9. S.Tamilselvi, R.Prakash, C.Nagarajan," Adaptive sliding mode control of multilevel grid-connected inverters using reinforcement learning for enhanced LVRT performance" Electric Power Systems Research 253 (2026) 112428, doi.org/10.1016/j.epsr.2025.112428
10. S.Thirunavukkarasu, C. Nagarajan, 2024, "Performance Investigation on OCF and SCF study in BLDC machine using FTANN Controller," Journal of Electrical Engineering And Technology, Volume 20, pages 2675–2688, (2025), doi.org/10.1007/s42835-024-02126-w
11. C. Nagarajan, M.Madheswaran and D.Ramasubramanian- 'Development of DSP based Robust Control Method for General Resonant Converter Topologies using Transfer Function Model'- Acta Electrotechnica et Informatica Journal , Vol.13 (2), pp.18-31,April-June.2013, DOI: 10.2478/aeei-2013-0025.
12. C.Nagarajan and M.Madheswaran - 'DSP Based Fuzzy Controller for Series Parallel Resonant converter'- Springer, Frontiers of Electrical and Electronic Engineering, Vol. 7(4), pp. 438-446, Dec.12. DOI 10.1007/s11460-012-0212-0.
13. C.Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.
14. C.Nagarajan and M.Madheswaran, "Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation" has been presented in ICTES'08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007
15. Suganthi Mullainathan, Ramesh Natarajan, "An SPSS and CNN modelling based quality assessment using ceramic materials and membrane filtration techniques", Revista Materia (Rio J.) Vol. 30, 2025, DOI: https://doi.org/10.1590/1517-7076-RMAT-2024-0721
16. M Suganthi, N Ramesh, "Treatment of water using natural zeolite as membrane filter", Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022
17. K. M. Butler, J. Saxena, T. Fryars, G. Hetherington, A. Jain, and J. Lewis,―Minimizing power consumption in scan testing: Pattern generation And DFT techniques, in Proc. Int. Test Conf., 2004, pp. 355-364.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802308

18. Saxena, K. Butler, and L. Whetsel, ―An analysis of power reductiontechniques in scan testing, in Proc.Int. Test Conf.
19. V. Dabhholkar, S. Chakravarty, I. Pomeranz, and S. M. Reddy, ―Techniques for minimizing power dissipation in scan and combinational circuits during test applications, IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 17, no. 12, pp. 1325-1333, Dec. 1998.
20. Y. Bonhomme, P. Girard, L. Guiller, C. Landrault, S. Pravossoudovitch,and V. Virazel, ―Design of routing-constrained low power scan chains, in Proc. Des. Autom. Test Eur. Conf. Exhib., Feb. 2004, pp. 62-67.
21. W. Tseng, ―Scan chain ordering technique for switching activity reductionduring scan test, Proc. Inst. Elect. Eng.—Comput.Digit. Tech., vol. 152, no. 5, pp. 609-617, Sep. 2005.
22. C. Giri, B. Kumar, and S. Chattopadhyay, ―Scan flip-flop ordering withdelay and power minimization during testing, in Proc. Annu. IEEEINDICON, Dec. 2005, pp. 467-471.
23. Y. Bonhomme, P. Girard, C. Laundrault, and S. Pravossoudovitch, ―Powerdriven chaining of flip-flops in scan architectures, in Proc. Int. Test Conf.,Oct. 2002, pp. 796-803.
24. M. Bellos, D. Bakalis, and D. Nikolos, ―Scan cell ordering for lowpower BIST, in Proc. IEEE Comput. Soc. Annu. Symp. VLSI, Feb. 2004,pp. 281-284.
25. K.V.A. Reddy and S. Chattopadahyay, ―An efficient algorithm to reducetest power consumption by scan cell and scan vector reordering, in Proc. IEEE 1st India Annu. Conf. INDICON, Dec. 2004, pp. 373-376.
26. SaeedMahmoudpour, SattarMirzakuchaki - Hardware Architecture for a Message Hiding Algorithmwith Novel Randomizers, in International Journal of Computer Applications (0975 – 8887) Volume 37– No.7, January 2012
27. Cheng and K. K. Parhi, "High speed VLSI architecture for general linear feedback shift register (LFSR) structures," in Proc. 43rd Asilomar Conf. on Signals, Syst., Comput., Monterey, CA, Nov. 2009, pp. 713–717.
28. Manohar Ayinala and K. K. Parhi, "High-Speed Parallel Architectures for LinearFeedback Shift Registers" IEEE TRANSACTIONS on signal processing, vol. 59, no. 9, september 2011
29. **Kiran, A., Rubini, P., & Kumar, S. S. (2025).** Comprehensive review of privacy, utility and fairness offered by synthetic data. IEEE Access.
30. **Gopinathan, V. R. (2024).** Real-Time Financial Risk Intelligence Using Secure-by-Design AI in SAP-Enabled Cloud Digital Banking. International Journal of Computer Technology and Electronics Communication, 7(6), 9837-9845.
31. **Udayakumar, R., Elankavi, R., Vimal, R., & Sugumar, R. (2023).** Improved Particle Swarm Optimization with Deep Learning-Based Municipal Solid Waste Management in Smart Cities. Environmental & Social Management Journal, 17(4).
32. **Anand, L. (2023).** An Intelligent AI and ML–Driven Cloud Security Framework for Financial Workflows and Wastewater Analytics. International Journal of Humanities and Information Technology, 5(02), 87-94.
33. **Soundappan, S. J. (2020).** Big Data Analytics in Healthcare: Applications for Pandemic Forecasting. International Journal of Advanced Research in Computer Science & Technology, 3(1), 2248-2253.
34. **Rajasekar, M. (2024).** Real-Time Predictive DevOps Intelligence for Risk-Aware Digital Business Processes in Cloud and SAP Ecosystems. International Journal of Advanced Research in Computer Science & Technology, 7(4), 10713-10718.
35. **Poornima, G., & Anand, L. (2024, May). Novel AI Multimodal Approach for Combating Against Pulmonary Carcinoma. In 2024 5th International Conference for Emerging Technology (INCET) (pp. 1-6). IEEE.**
36. **Prabha, P. S., & Rengarajan, A. (2025).** Adaptive Cloud Resource Allocation Using Attention-Driven Deep Reinforcement Learning. Engineering, Technology & Applied Science Research, 15(6), 29334-29340.
37. **Jagadeesh, S., & Sugumar, R. (2017).** A Comparative study on Artificial Bee Colony with modified ABC algorithm. European Journal of Applied Sciences, 9(5), 243-248.
38. **Varma, K. K., & Anand, L. (2025, March). Deep Learning Driven Proactive Auto Scaler for High-Quality Cloud Services. In International Conference on Computing and Communication Systems for Industrial Applications (pp. 329-338). Singapore: Springer Nature Singapore.**
39. **Kumar, S. A., & Anand, L. (2025). A Novel EEG-Based Deep Learning Framework for Enhancing Communication in Locked-In Syndrome Using P300 Speller and Attention Mechanisms. KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS, 19(11), 3841-3855.**
40. **Poornima, G., & Anand, L. (2025). Medical image fusion model using CT and MRI images based on dual scale weighted fusion based residual attention network with encoder-decoder architecture. Biomedical Signal Processing and Control, 108, 107932.**
41. **Archana, R., & Anand, L. (2025). Residual u-net with Self-Attention based deep convolutional adaptive capsule network for liver cancer segmentation and classification. Biomedical Signal Processing and Control, 105, 107665.Kumar, S. A., & Anand, L. (2025).** A Novel EEG-Based Deep Learning Framework for Enhancing

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802308

Communication in Locked-In Syndrome Using P300 Speller and Attention Mechanisms. KSII Transactions on Internet and Information Systems, 19(11), 3841-3855.

42. **Rengarajan, A. (2025).** Cloud-Based AI-Driven Threat Detection Framework for Smart Grid Cybersecurity. International Journal of Future Innovative Science and Technology, 8(6), 16065.
43. **Murugeshwari, B., Sudharson, K., Panimalar, S. P., Shanmugapriya, M., & Abinaya, M. (2020).** SAFE–Secure Authentication in Federated Environment using CEG Key code.
44. **Raj A. A., & Sugumar, R. (2023).** Early Detection of COVID-19 with Impact on Cardiovascular Complications using CNN Utilising Pre-Processed Chest X-Ray Images. 2023 International Conference on Applied Intelligence and Sustainable Computing (ICAISC), IEEE.
45. **Jagadeesh, S., & Sugumar, R. (2017). A Comparative study on Artificial Bee Colony with modified ABC algorithm. European Journal of Applied Sciences, 9(5), 243-248.**
46. **Selvi, G. V., Anbarasan, A. B., Murthy, B. A., & Prabavathy, S. (2023).** An Application Oriented Integrated Unequal Clustering Algorithm for Wireless Sensor Network. In Underwater Vehicle Control and Communication Systems Based on Machine Learning Techniques (pp. 140-154). CRC Press.
47. **Sruthi, R. S., Ananya, S., & Murugeshwari, B. (2010).** Web Based Virtual Control System Laboratory and On-Line Temperature Control of Electrophoresis Equipment using LabVIEW. International Journal of Computer Applications, 975, 8887.
48. **Vimal Raja, G. (2021).** Mining Customer Sentiments from Financial Feedback and Reviews using Data Mining Algorithms. International Journal of Innovative Research in Computer and Communication Engineering, 9(12), 14705-14710.
49. MATHEW, A. R. (2025). Neurosecurity and Brain-Computer Interfaces.
50. Soundappan, S. J. (2024). AI-Driven Customer Intelligence in Enterprise Lakehouse Systems Sentiment Mining Governance-Aware Analytics and Real-Time Data Synchronization. International Journal of Advanced Engineering Science and Information Technology (IJAESIT), 7(5), 14905.
51. Mathew, A. (2025). Human–AI Collaboration in Security Operations: Measuring Alert Trust, Automation Bias, and Analyst Upskilling in AI-Augmented SOC Environments. International Journal of Computer Technology and Electronics Communication, 8(5), 11375-11380.
52. Soundappan, S. J. (2022). AI-Based Fault Detection and Isolation for Reliability in Modern Power Systems. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 5(4), 7106-7110.
53. **Poornima, G., & Anand, L. (2024, April). Effective Machine Learning Methods for the Detection of Pulmonary Carcinoma. In 2024 Ninth International Conference on Science Technology Engineering and Mathematics (ICONSTEM) (pp. 1-7). IEEE.Garg, V. K., Soundappan, S. J., & Kaur, E. M. (2020).** Enhancement in intrusion detection system for WLAN using genetic algorithms. South Asian Research Journal of Engineering and Technology, 2(6), 62–64.
54. Rengarajan, A., Jayakumar, C., & Sugumar, R. (2012). Optimization Of Recent Attacks Using Internet Protocol. National Journal of System and Information Technology, 5(1), 8.
55. Mathew, A. (2024). AI TRiSM: Trust, Risk, and Security Management in Cybersecurity. Cybersecurity, 4(3), 84-90.
56. Mathew, A. (2025). Deep seek vs. ChatGPT: A deep dive into AI Language mastery. Int J Multidisciplinary Res, 7(1), 1-5.