Sub-threshold Leakage Current Differential Age Sensor for Identifying Reused Integrated Circuits

Mahesh Kumar Singh[1,*,†], Palaka Uma Maheswara Rao[1,†] and Vella Satyanarayana[1,†]

[1]*Department of ECE, Aditya Engineering College, Surampalem, India*

Abstract

All the electronic components can fall under the untrusted portion in the semiconductor supply. It has made the world wide spread for the reduction of their cost in markets and to increase their productivity rapidly. This article mainly focuses on the recycled ICs which is being manufactured by different semiconductor firms, and this article also explains the difference between recycled ICs and new ICs. At present, these reused ICs have become a major issue, due to these counterfeit parts, the lifetime of the products manufactured using these parts decreased, and their reliability and performance are also affected badly. The power-up state of the chip is used as the basis for the new SRAM detection method that has been implemented here for integrated circuits. Integrated circuits that have been recycled can be located using this method effectively ICs. But it is difficult to detect these reused ICs which were already been previously for a certain period.

Keywords

Counterfeit, Deep learning, Counterfeit ICs, Aging sensor, Discharge time sensor

1. Introduction

Counterfeit integrated circuits (ICs), which are a major source of concern in the supply chain of electronic components due to reliability and security issues, are having an effect on a wide variety of industrial sectors, such as computers, telecommunications, automotive electronics, and even military systems [1, 2]. These concerns are brought about by the fact that counterfeit ICs pose a threat to the chain of distribution of electronic components. This is as a result of the issues that are brought about by the use of counterfeit ICs [3, 4]. A significant number of systems began to operate improperly as a direct result of the use of these counterfeit components. According to the research that was presented by M. Pecht and S. Tiku, a number of electronic companies have been compelled to suffer a loss of roughly 100 billion USD of global income each year as a direct result of this counterfeiting [5, 6]. This loss was presented as a direct effect of the counterfeiting. When talking about the counterfeiting of integrated circuits (ICs), the term ”recycled” refers to a component that has been retrieved from an old component and then modified so that it can be passed off as a new component that has been delivered by the original component manufacturer [7]. In other words, a recycled component is an old component that has been repurposed. Recycling and remarketing are the two most prevalent

ACI'23: Workshop on Advances in Computational Intelligence at ICAIDS 2023, December 29-30, 2023, Hyderabad, India

*Corresponding author.

†These authors contributed equally.

mahesh.092002.ece@gmail.com (M. K. Singh); 20A91A04P1@aec.edu.in (P. U. M. Rao); vasece[underscore]vella@aec.edu.in (V. Satyanarayana)

ways that fake identification cards are made [8, 9, 10]. Together, these two methods account for 80% of all instances of counterfeiting that take place across the world [11, 12]. According to a report that was published by the information handling Services in 2011, it is anticipated that these components will have a yearly cost of around $169 billion for the market that is involved in the semiconductor supply chain [13, 14]. The horizontal process of the once vertical IC supply chain has resulted in a change to the chip manufacturing process, which has led to the formation of a new security risk. This risk is due to the fact that the chip manufacturing process has been altered. In times past, one and the same company would frequently be responsible for both the design and fabrication of integrated circuits [15]. This was because it was considered acceptable to establish a foundry at a cost that, despite being a pricey investment, was considered to be acceptable. Since 1976, there has been a growth of sixty percent in the transportation of semiconductors throughout Asia, which has resulted in substantial alterations in the markets [16]. According to a recent survey on the semiconductor industry that was carried out by Semiconductor Equipment and Materials International (SEMI), 90% of the companies have been the victims of intellectual property (IP) infringement at some point in their history. Furthermore, 54% of the companies that were victims of IP infringement reported that the infringement was either serious or extremely serious [17, 18**? ?**]. Overproduction of integrated circuits and a lack of respect for intellectual property rights are common problems in the horizontal semiconductor business model. In this model, the company and other entities on the production chain have access to the designer's intellectual property, but neither the company nor the other entities respect the designer's intellectual property rights [19]. As a result of the escalating costs associated with keeping their technology up to date and maintaining their infrastructure, many businesses that deal in semiconductors have shifted their focus to the counterfeiting industry. This is due to the fact that counterfeiting is a highly profitable industry. They made a lot of their designs "fabless" by using third-party service providers to manufacture a lot of their designs, so that's what they mean when they say that. Several separate design firms, all of which have a history of fabricating their ideas in-house, have banded together in order to reduce costs and share the effort [20, 21, 22, 23, 24].

2. Related Work

Due to the numerous problems that recycling ICs can bring about for both government and business, such as the potential for a shorter lifetime, decreased reliability, and subpar performance, etc., numerous people have conducted various studies and discovered various solutions to identify these recycled ICs over the years [24, 25]. A few of these are: In 2000, the cost of a plant to manufacture 300mm silicon discs using 65nm technology would have been around $3 billion. Due to the fact that very few companies can afford these expenses, the industry has begun to specialize. Some of these niche players have since developed products with such astounding success that IC developers have licensed their patents application specific integrated circuit (ASIC) designs. Some IC manufacturing firms put their hands on third-party IP along with their own IC creation [1, 2, 26, 27, 28, 29]. In an effort to curb the spread of counterfeit components in the aerospace and defense industries, the Aerospace Industries Association (AIA) Counterfeit Components-Integrated Project Team published a number of recommendations

in May of this year [3, 4, 5, 30]. The AIA's goal is to reduce the risks associated with buying counterfeit components by raising awareness of those concerns. Mechanical, electronic, or even completely other kinds of components could be involved. These components initially posed a threat to the aerospace and defense industries because of their potential to lower product performance, reliability, and safety shown in table 1.

Table 1
. Top 5 most counterfeit semiconductors in 2011

Ranks	Type of the component	Reported incidents (%)
1	Transistor	7.6%
2	Programmable IC	8.3%
3	Memory IC	13.1%
4	Microprocessor IC	13.4%
5	Analog IC	25.2%

In 2015 a method that is based on low Ring Oscillators (RO) negative bias temperature instability (NBTI) awareness was proposed. This method is performed in the 90nm technology Generation node [7, 8]. This allows you to identify ICs that can only be used for a few hours. We propose simpler CDIR variations with RO-pairs, where the designer can pick from a variety of pairs appropriate to their area of expertise in finance. These CDIRs give improved estimation accuracy in comparison to N-CDIRs. In 2017, a technique was proposed to detect the recycled ICs called 'Bias Temperature Instability' (BTI) by using the infrastructure for power metering and control. This BTI method relied on the discharge time of virtual private networks during standby operations. The values of this time were determined by the threshold voltage of the CMOS devices in a given circuit. Power-gated design (PGD) [11, 13**?**]. On simulating the design of this BTI technique on SPICE software, they meet a value of estimating error of BTI aging as <1% and <6.2% for PGD. They've also found that the cost of this technique is less. The researchers came to a result that this aging technique is having some advantages as listed below:

- They do not require any distributed sensors in this technique, since a virtual private network is already presented in PGDs.
- It achieved a higher average aging estimation of around 97%.
- They don't require any mission profiles like high temperature, altitudes etc.

The Minimum Idle Time (MIT) cost is induced by consuming the energy to observe the discharge time is evaluated on two different models using either x86 or ARM architecture. It was found that less than <30% in x86 architecture and 45% in ARM architecture than the original power gating MIT. This problem was achieved by using the ARM Cortex M0 processor, which was made with a 65nm CMOS technology [13, 11, 15]. It was also proposed that a novel approach could be to use coarse-grained aging sensors to identify reused chips. As a result, we'll have to modify our approach slightly before it can be used in low-power devices. This sensor detects longer power-rail discharge periods when the target circuit goes into sleep mode and communicates that information [16, 17]. It was demonstrated by HSPICE simulation that the discharge time of the power network is age-dependent. This means it can help us figure out which ICs have been recycled and which haven't. After a year of use, the discharge time of

recycled integrated circuits was found to have increased by a factor of seven from its initial value after only three months. Time spent discharging was found to have increased following the first year of use [23**?**]. By allowing complete tracking of components from fabrication to final assembly, researchers in 2019 [8] uncovered a low-cost and dependable method for evaluating reused ICs. By doing so, the amount of recycled IC may be calculated. which helps us to detect the recycled ICs [26]. This method uses Radio Frequency Identification (RFID) to verify the originality of any chip. The researchers had concluded that this can assure trust among the manufacturers, distributors, and system integrators [1, 3, 4]. And also stated that it is unnecessary to supply power to the chip in the verification process at the distributor. But for the measurement of RO frequency, it needs to be powered up in the final verification in the system integrator's site. This can be applied to all chips practically [5]. In An alternative detecting method was developed, and it was made in such a way that it can be utilized on both large digital circuits and older components existing in the supply chain. This is because the scan chains provide direct access to the power ON mode of the circuit's flip flops (FF). Notably, the netlist of the circuit is not required, nor is any other information beyond scan testing of the component. This is a major perk [7, 8]. In 2021, scientists came up with an innovative answer they termed the "Differential Aging Sensor [13]." This sensor keeps an eye on the discharge time (dv), which grows with the age of the chips in the design and is reliant on the subthreshold leakage current. After that, the Global Foundries assisted with running the simulations by utilizing a hybrid of BTI and Hot Carrier Injection (HCI) shown in table 2. As an added bonus, it is said that the discharge time is sensitive to aging, which increases the frequency with which its previously used ones may be detected, and that it is also resistant to process, voltage, and temperature changes [11, 13, 15]. A reliable discharge time lends credence to these assertions (PVTs). Upon completing the simulation, the following occurred:

Table 2
Nominal temperature measured using Highest simulated temperature

Discharge Time	Nominal temperature (%)	Highest simulated temperature (%)
After 15 days	14.72%	55.93%
After 3 years	60.49%	310.17%

3. Methodology for IC Identification Circuit

Procedures on the circuit level (such as EPROM) and the water level (such as laser link cutting) necessitate the employment of very expensive and very efficient technology. In order to retrieve unique and repeatable data, ICID uses the inherent unpredictability of silicon fabrication. They may be manufactured with no additional steps or external programming, and they are compatible with all standard sub-micron CMOS processes. The building blocks of this ICID are a collection of addressable MOSFETs including high load resistance, standard gate and source topologies, and drains. Because of the incompatibility between the devices, the drain currents will be highly irregular, causing the load to generate a distinct sequence of irregular voltages for each die.

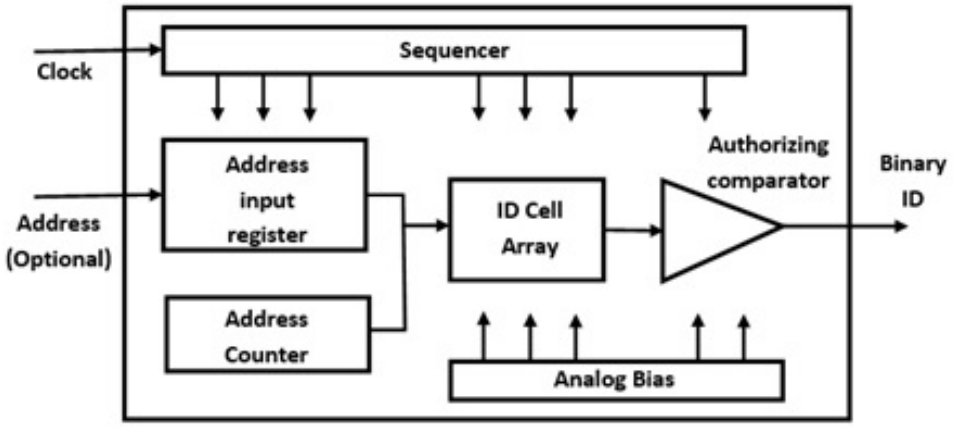

Figure 1: Block Diagram of ICID

ICID uses these varying patterns of consistently occurring random voltages to generate unique traces. Block diagram of ICID is shown in figure 1

In this method, to determine the previous usage of the ICs we use the FFs which are in power-up state. But due to its built-in asymmetry, the FF will be skewed. In this method, we'll build two FF groups which are mostly aged 0 and 1. This process consists of two phases namely 1. Characterization and 2. Authentication. In Phase-I two FF groups were selected so that we can determine whether the selected chip is new or recycled in Phase-II.

Phase-I (Characterization): The primary task of this characterization phase is to identify and group the FFs with the ages 0 and 1. At the first stage, we'll gather the information (FF input) from the Cut under test (CUT). Then we'll apply a random number of inputs and by using the scan chains we'll capture the response in FFs. Later on, based upon the probabilities of responses we'll split the FFs into two groups such that one of two groups consists of the FFs with the age of 'logical 0' and the other group consists of the FFs with the age of 'logical 1' shown in fig 2.

Phase-II (Authentication): Determining the recycled IC is a simple process. It is a must to measure the starting values of FFs for any CUT tests. To select the slave latches of the D-Flip flops (DFF), we need to encounter the clock with logic 0 and to select the master latches we need to encounter a clock with logic 1. Till now the FFs were arranged into groups based on their phase values so that their percentage of 1's difference is calculated. If the difference is lies within Δ, then the chip is identified as new, else the chip is recycled. The aging sensor consists of mainly 2 identical ring oscillators (RO), Stress RO (SRO), and Reference RO (RRO) which are in the same size and kept aside to maintain the same operating temperature and for the minimal process variations (PV). This design consists also a counter, a comparator, and a Non-volatile memory (NVM). In this, we're sending 2 additional signals that were already proposed and modified. It is constructed with only one RO, and an NVM makes use of the discharge time. This sensor is extremely accurate and focuses on the identification of recycled integrated circuits as well as the frequent difficulties that occur in the aging sensors that could diverge from the

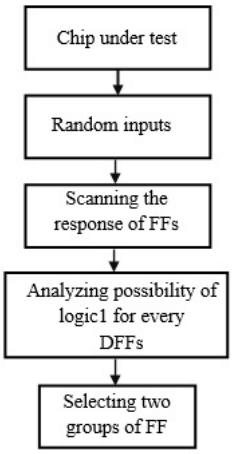

Figure 2: Proposed method based on the Power-up state of Flip flops

detection findings. It does both of these things in order to ensure that it provides correct results. Through the process of multiplexing, it is possible to obtain access to the readings of the RO's output. The comparator compares the RRO and SRO produces their difference as its output. The RRO discharge time and the discharge time difference between the RRO and SRO measurements are both stored in the NVM, however the NVM cannot be utilized to access either of these times.

4. Results and Discussion

Due to globalization, electronic component supply chains are getting more intricate, with parts sourced from a diverse set of manufacturers. This increased complexity has made the issue of fake electronics a pressing one that requires immediate solutions. There are currently a limited number of standards and algorithms available for detecting counterfeit components, but this is expected to change soon. But there hasn't been enough study done to address the detection and avoidance of all counterfeit parts that are currently permeating the electronic component supply chain. Counterfeit components may be any combination of recycled, noted, overproduced, cloned, out-of-specification/defective, and falsified paperwork. There is a higher chance of reliability concerns and a shorter lifespan for each of these components, even if they initially perform adequately. In this session, we will discuss some of the methods now in use to spot fake products and avoid buying them. Moreover, we will discuss the challenges that will need to be overcome in order to put these tactics into effect, as well as the development of novel detection and avoidance technologies shown in table 3.

Catastrophic failures in the manufacturing phase can be caused by deficiencies in the design, large swings in the manufacturing process, or isolated errors in individual devices. Devices may malfunction after manufacture due to flaws discovered after regular use that were missed during manufacturing testing. Infant mortality is the sad premature death brought on by external, preventable causes. Integral circuit failure can be caused by a variety of factors over

Table 3
Result discussion for sub-threshold leakage current differential

Detection Methods	Re-cycled	Observed	Over-produced	Out of Defective	Duplicated
Visual Inspection with Low Power	High	High	—	—	—
X-Ray	Low	—	—	—	—
Micro Blast Analysis	High	Medium	—	—	—
Scanning Acoustic Microscopy (SAM)	High	—	—	—	Medium
Scanning Electron Microscopy (SEM)	Medium	Low	—	—	Low
Material Analysis	Low	Medium	—	—	—
Parametric Tests	High	Low	Low	Medium	Low
Functional Tests	Low	Low	Low	Medium	Low
EFR Analysis	Low	High	Low	Low	Low
Path-Delay Analysis	High	High	Medium	High	Medium

Table 4
Methods for Avoiding Counterfeit Products and Component types

Avoidance Methods	Re-cycled	Ob-served	Over-produced	Out of Defec-tive	Dupli-cated	Obso-lete	Active	New
CDIR Sensors	Medium	Low	—	—	—	—	—	Medium
Secure Split Testing (SST)	—	—	High	High	Low	—	—	Medium
Hardware metering	—	—	Low	—	Low	—	—	Medium
Split Manufacturing	—	—	Low	—	Low	—	—	Medium
IC Camouflaging	—	—	—	—	Low	—	—	Medium
Hardware Watermarking	—	—	—	—	High	—	—	High
Physically Unclonable Func-tions (PUF)	—	—	Low	—	Low	—	—	High
Package ID	High	Low	N/A	—	—	Medium	Medium	Medium

Table 5
Increase in Discharge Time at 25°C due to 13 and 51

RO Stage	Time Age (Months)	Renewed τ_{dv} (ns)	Matured τ_{dv} (ns)	$\Delta\tau_{dv}$ (ns)	$\Delta\tau_{dv}$ % Growth
13	0.5	13.3	15.12	1.85	13.94
	1	-	15.28	2.01	15.15
	4	-	16.3	3.02	21.48
	8	-	16.72	3.45	25.66
	12	-	16.97	3.70	27.88
	16	-	17.01	3.81	28.85
	20	-	17.47	4.13	31.55
	24	-	17.67	4.40	33.16
51	0.5	10.5	12.08	1.55	14.72
	1	-	12.60	2.07	19.66
	4	-	13.82	3.05	30.42
	8	-	14.70	4.18	38.92
	12	-	15.29	4.76	45.20
	16	-	15.80	5.24	52.73
	20	-	16.01	5.42	53.01
	24	-	16.15	5.62	53.37

time, such as aging, wear and tear, hostile surroundings, heavy usage, etc. The breakdown that happens when a material or component performs above what is believed to be its inherent capabilities is referred to as intrinsic reliability failure mechanisms shown in table 4 and table 5.

Electrical tests are not reliable for producing correct results due to their numerous flaws. The results of the parametric tests for lower technical nodes are questionable due to increased process variability and environmental changes. This is because a component's electrical characteristics might vary greatly. Functional tests are useless as a result since it is extremely challenging, if not impossible, to gather data or manufacturer test fixtures for active and outdated parts. This is due to the need for test program generation for those components whose operation is less understood.

5. Conclusion and Future Scope

A chip aging sensor is used in the preceding article to measure the discharge time of recycled integrated circuits in order to identify them. This sensor was made by IBM. The second sensor design uses an SRO and RRO to measure the discharge time variation due to age, whereas the first sensor design depends on a single NVM and RO placed during manufacture. In this paper, we have to also represent various taxonomy of counterfeit detection and avoidance methods. Finally, we conclude that without taking proper precautions and proper detection techniques, using of counterfeit parts causes serious problems in many areas like in defense and aerospace industries. Physical and electrical testing are summarized. Then, we discussed counterfeit avoidance methods and how to discover counterfeit components proactively, rather

than reactively. We covered detecting and avoiding counterfeit goods, as well as recent research opportunities.

References

[1] K. Lofstrom, W. R. Daasch, D. Taylor, Ic identification circuit using device mismatch, in: 2000 IEEE International Solid-State Circuits Conference. Digest of Technical Papers (Cat. No. 00CH37056), IEEE, 2000, pp. 372–373.

[2] S. Wei, F. Koushanfar, M. Potkonjak, Integrated circuit digital rights management techniques using physical level characterization, in: Proceedings of the 11th annual ACM workshop on Digital rights management, 2011, pp. 3–14.

[3] U. Guin, D. Forte, M. Tehranipoor, Design of accurate low-cost on-chip structures for protecting integrated circuits against recycling, IEEE Transactions on Very Large Scale Integration (VLSI) Systems 24 (2015) 1233–1246.

[4] V. Tenentes, D. Rossi, S. Yang, S. Khursheed, B. M. Al-Hashimi, S. R. Gunn, Coarse-grained online monitoring of bti aging by reusing power-gating infrastructure, IEEE Transactions on Very Large Scale Integration (VLSI) Systems 25 (2016) 1397–1407.

[5] D. Rossi, V. Tenentes, S. Khursheed, S. M. Reddy, Recycled ic detection through aging sensor, in: 2018 IEEE 23rd European Test Symposium (ETS), IEEE, 2018, pp. 1–2.

[6] M. K. Singh, S. Manusha, K. Balaramakrishna, S. Gamini, Speaker identification analysis based on long-term acoustic characteristics with minimal performance, International Journal of Electrical and Electronics Research 10 (2022) 848–852.

[7] M. Alam, S. Chowdhury, M. M. Tehranipoor, U. Guin, Robust, low-cost, and accurate detection of recycled ics using digital signatures, in: 2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), IEEE, 2018, pp. 209–214.

[8] M. K. Singh, A text independent speaker identification system using ann, rnn, and cnn classification technique, Multimedia Tools and Applications (2023) 1–13.

[9] P. Agrawal, H. Kaur, G. Kaur, Multi lingual speaker identification on foreign languages using artificial neural network, International Journal of Computer Applications 57 (2012).

[10] P. Agrawal, A. Shukla, R. Tiwari, Multi lingual speaker recognition using artificial neural network, Advances in Computational Intelligence (2009) 1–9.

[11] M. K. Singh, Feature extraction and classification efficiency analysis using machine learning approach for speech signal, Multimedia Tools and Applications (2023) 1–16.

[12] A. Shankhdhar, P. K. Verma, P. Agrawal, V. Madaan, C. Gupta, Quality analysis for reliable complex multiclass neuroscience signal classification via electroencephalography, International Journal of Quality & Reliability Management 39 (2022) 1676–1703.

[13] G. Veerendra, R. Swaroop, D. Dattu, C. A. Jyothi, M. K. Singh, Detecting plant diseases, quantifying and classifying digital image processing techniques, Materials Today: Proceedings 51 (2022) 837–841.

[14] S. Chauhan, P. Agrawal, V. Madaan, E-gardener: building a plant caretaker robot using computer vision, in: 2018 4th International Conference on Computing Sciences (ICCS), IEEE, 2018, pp. 137–142.

[15] U. Padma, S. Jagadish, M. K. Singh, Recognition of plant's leaf infection by image processing approach, Materials Today: Proceedings 51 (2022) 914–917.
[16] P. M. Satya, S. Jagadish, V. Satyanarayana, M. K. Singh, Stripe noise removal from remote sensing images, in: 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC), IEEE, 2021, pp. 233–236.
[17] A. Nandini, R. A. Kumar, M. K. Singh, Circuits based on the memristor for fundamental operations, in: 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC), IEEE, 2021, pp. 251–255.
[18] R. Anushka, S. Jagadish, V. Satyanarayana, M. K. Singh, Lens less cameras for face detection and verification, in: 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC), IEEE, 2021, pp. 242–246.
[19] R. Nainvarapu, R. B. Tummala, M. K. Singh, A slant transform and diagonal laplacian based fusion algorithm for visual sensor network applications, in: High Performance Computing and Networking: Select Proceedings of CHSN 2021, Springer, 2022, pp. 181–191.
[20] K. R. S. Reddy, C. Satwika, G. Jaffino, M. K. Singh, Monitoring of infrastructure and development for smart cities supported by iot method, in: Proceedings of Second International Conference in Mechanical and Energy Technology: ICMET 2021, India, Springer, 2022, pp. 21–28.
[21] P. Agrawal, V. Madaan, A. Sharma, D. K. Sharma, A. Agrawal, S. Kautish, Trust-based communication systems for internet of things applications, 2022.
[22] V. Walia, V. Madaan, P. Agrawal, A. Mohan, C. Gupta, A. Sharma, A. Agrawal, Blockchain in iot and limitations, in: Trust-Based Communication Systems for Internet of Things Applications, John Wiley & Sons, Inc., 2022, pp. 17–27.
[23] Y. Zhang, U. Guin, End-to-end traceability of ics in component supply chain for fighting against recycling, IEEE Transactions on Information Forensics and Security 15 (2019) 767–775.
[24] W. Wang, U. Guin, A. Singh, A zero-cost detection approach for recycled ics using scan architecture, in: 2020 IEEE 38th VLSI Test Symposium (VTS), IEEE, 2020, pp. 1–6.
[25] M. K. Singh, P. M. Satya, V. Satyanarayana, S. Gamini, Speaker recognition assessment in a continuous system for speaker identification, International Journal of Electrical and Electronics Research 10 (2022) 862–867.
[26] S. Urmila, R. A. Kumar, M. K. Singh, Cardiac surveillance system using by the modified kalman filter, in: International Conference on Artificial Intelligence and Data Science, Springer, 2021, pp. 112–122.
[27] A. S. B. Musa, S. K. Singh, P. Agrawal, Suspicious human activity recognition for video surveillance system, in: International Conference on Control, Instrumentation, Communication & Computational Technologies ICCICCT-2014, IEEEXplore, 2014.
[28] N. Mohod, P. Agrawal, V. Madaan, Yolov4 vs yolov5: Object detection on surveillance videos, in: International Conference on Advanced Network Technologies and Intelligent Computing, Springer Nature Switzerland Cham, 2022, pp. 654–665.
[29] N. Mohod, P. Agrawal, V. Madan, Human detection in surveillance video using deep learning approach, in: 2023 6th International Conference on Information Systems and Computer Networks (ISCON), IEEE, 2023, pp. 1–6.
[30] K. Krishna, P. Manohar, N. Radha, M. Singh, Rectifier acoustical cardiac activity detection

analysis of ecg signal, International Journal of Electrical and Electronics Research 10 (2022) 438–441.