iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 9 **Issue:** VII **Month of publication:** July 2021

**DOI:** https://doi.org/10.22214/ijraset.2021.37028

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429*
*Volume 9 Issue VII July 2021- Available at www.ijraset.com*

# A Review on Counterfeit Detection of Products and Electronic Devices

Aasawari Tayade[1], Rajesh Patil[2], Anilkumar Shripad[3]
[1]*Post Graduate Student of Electronics and Telecommunication, Electrical Engineering Department, Veermata Jijabai Technological Institute.*
[2]*Professor, Electrical Engineering Department, Veermata Jijabai Technological Institute.*
[3]*Mechanical Architect System PU, Philips India Ltd.*

***Abstract:*** ***The problem of using unauthorized parts, components or products is widespread all around the world. These problems eventually cause a huge loss to the brands. To reduce such malpractices, brands are working on to find out a solution to overcome counterfeit. Counterfeit is basically a non-genuine or a non-brand product. The counterfeit device carries false information and can mislead us claiming about its good performance. The device infringes the intellectual property rights of the registered owner. We need to ensure that the equipment is manufactured and developed according to the requirements. Procurement team members need to establish and maintain robust obtainment processes to minimize the risk of buying non-submissive and counterfeit devices parts and find out a solution that detects the counterfeit parts. RFID tags and readers, DNA and PUF technologies, Cryptography techniques, labeling barcodes can provide a solution to counterfeit product detection problem. This paper compares the parameters and performance criteria of some of the detection techniques.***
***Keywords: Counterfeit Detection, Electronic Device, Security, Authentication, Unauthorized products***

## I. INTRODUCTION

It is common for manufacturers and distributors, as well as suppliers, to sell replacement parts that may not be authorized, due to increasing competitive pressures that are often driven by cost. This is a common problem for businesses dealing in serviceable or replaceable parts and components. Therefore, a need exists to discourage customer acceptance of will-fit, reconditioned, and counterfeit product components and prevent or at least minimize against the impact of such activity. Around 8 percent of medical devices are counterfeit and only 20 per cent of the countries in the world have worked on to counter the spread for preventing the loss to business and its reputation.

The application herein generally reflects to detection of serviceable product parts to prevent counterfeits. The various methods used in the industries for detection of fake products quotes all the brief technologies. Establishing and maintaining a robust procedure to deal with counterfeit is the solution for a brand.

Various authors have proposed a solution related to the detection of unauthorized parts and various industries that have successfully implemented the solution for avoiding the counterfeit. In this paper we will be taking about various technologies and the two considered technologies RFID, DNA and PUF based authenticators. While selecting a technology before implementation few parameters are needed to be taken into consideration like, integration efforts, deploy ability and security where integration efforts means- design overhead(power/ cost/ area), effect on yield and real time, maturity of technique, design effort and cost of intellectual property.

Deploy ability includes deployment and maintenance cost per user, cost of recycling, ease of use and testing., compatibility. Security includes resiliency to testing attacks, reverse engineering, probability of successful exploitation, ease of counterfeit detection and recovery of loss [10].

A product detection system which compares data representing various authentication markers of items supposed to be produced or sourced by a distinguished entity with the data stored where the authentication markers (encrypted) may represent inherit physical characteristics of an item.

The data can be captured by high resolution camera or scanner (RFID or BAR code scanners) and then communicated to unauthorized -product detection system [2]. There are various anti-counterfeiting techniques and since the supply chain and brands are affected and what kind of counterfeits happens, the counterfeit techniques are taken into consideration. So, there is a need for industries to focus on make a robust chain by adopting hardware security measures [10].

## II. TECHNOLOGIES

### A. RFID

The RFID has two important parts tag and reader and can be integration and implementation process are as follows: 1) RFID is a platform to detect unauthorized product, this can be done by placing the RFID tag on necessary product part. 2) The reader is placed on the system within the given range. 3) The tag can set the access password where the people can't read or modify the tags embedded information. 4) The reader on the other hand checks the tags and compares it with the data stored in database if there's a match it allows the part to function fully and if not, the emergency operations are restricted. 5) On detection of non-genuine part, the information is displayed on local monitoring screen. Kun (2015) focuses on system counterfeit detection and traceability, where CST is composed of various on chip sensors and in-system structures that helps to detect counterfeit IC's. This is possible by implementing RDIF tags. RFID tags with fingerprints based on their minimal power responses, measured at multiple frequencies, have been proposed to uniquely identify the objects to which they are attached [6].

Kwok (2018) states a self-visualization and self-valuation system by integrating the RFID technology and EPC concept to protect products from counterfeiting by the means of mobile platform. System using mobile devices with RFID technology and EPC standard, provides an effective and efficient approach to self-validated product and part authentication. Also, He stated the issues of standardization of RFID tag and reader and the implementation roadmap [11].

### B. PUF

Another approach is PUF- based. The PUF- based authentication to detect counterfeit IC can provide a strong and robust challenge response-based authentication mechanism for detection of product parts. The part of the system is provided with a unique physical fingerprint and provides great security benefits against counterfeiting. Physically Unclonable Function technology provides us with unsurpassed protection against the security attacks and DNA is a technology which uses random variations in the device characteristics which naturally occurs during the fabrication of the MOSFET wafers, these variations generate unique cryptographic keys which helps you separate your brand device from a non-genuine one. The cryptography authentication solution strengthens the security of the parts. These solutions provide strong security and authenticity to the brands.[7] Ujjwal (2014) tells about the major counterfeit challenges faced in the 21$^{st}$ century, where he stated various problem in counterfeit of IC's and mentioned taxonomy of counterfeit types and quoted the detection methods which includes physical and electrical detection methods. He also mentioned the counterfeit avoidance methods of which generation chip ID through PUF. Extracting unique features and parameters from a circuit are few techniques to generate chip ID to help uniquely distinguish each chip or embedding a unique ID into the chip. For doing so the multiple methods are described [3]. Rainer (2016) proposed a method and a device for generating a key derived from a cryptographic key using the physically unclonable function. One request value is assigned to the cryptographic key and one to derivation parameter. A response value is generated on a circuit unit using the physically unclonable function dependent on respective request value. The derived key is derived from the response value [7]. Yingjie (2016) states a physically unclonable function for extracting chip-unique signatures from IC's. For hardware security services these chips can be used for anti-counterfeiting, authenticity, signature generation, IC metering. Here he put various authentication PUF based methods and how the process of PUF based local authentication takes place [8].

### C. DNA

Lawrence (2014) stated a method of marking an item, which provides naturally-derived as well as synthetic non-natural polymeric marker molecules such as a DNA or Peptide marker in union with rapid scan or optional visible reporters for authenticating or tracking, in which the method includes providing an item for marking, and applying a medium including a DNA marker to the item and also provides a method of marking a part or a product with a DNA marker for authentication or tracking, wherein the technique consists of offering an object DNA marker, and molding the medium including the DNA marker to provide all or part of the item. The information is encoded uniquely to the item or to the model of the item as desired by using the DNA marker [4].

### D. On- Device Signature

A method, system, and computer usable program product for detecting a counterfeit device where he mainly focused on on-device signature for the plurality of device as the best suitable method for detection of a counterfeit device where a set of parameters are associated with the device are determined .The computer implemented method claims the on-device signature stored in the repository is compared to the computing signature of the product that enters the system. Detecting the part as the counterfeit part when compared to the computed signature not matching the on-device signature [1].

*E. QR code*

QR code an image-based authentication, based on trademark for a type of matrix barcode designed for automotive industries, it is a two-dimensional symbol. The code contains information in both x and y axis made up of four standardized kind of data. Many industries want to protect their sensitive data from external world or hide from unauthorized users. So, this QR code system generated a unique code image as a password. Where the comparison of username will be done with other users, if the match is found the message is displayed on the screen. A password is put and QR code is generated using an algorithm. User enters username and brows QR code image, if there's a match in the repository then the user is authorized.[9]

David (2019) proposed an invention which provides an apparatus and methods for the labelling and production of objects in a manner which help to the prevent and detect counterfeiting. Where he claimed a self -authenticable object containing an imprinted message having derived through use of an asymmetric key cryptographic authentication algorithm comprises of information which selectively allows to change and deviate the state of the set of optically readable, non-deterministic characteristics [12].

*F. Performance Criteria*

The comparative table contains data from various sources.

Table 1: Comparative Table and the kind of analytics supported

| Technology | Supported Analytics | | | |
|---|---|---|---|---|
| | Real time | Predictive | Trust | Security |
| RFID | Low | Medium | Medium | High |
| DNA, PUF | Medium | Medium | Medium | Medium |
| QR code, Bar code | High | High | High | Low |
| On- device signature | High | Medium | Medium | High |

1) *Real Time Analytics:* This refers to the capability of analysing, processing and knowledgeable or intelligent information as soon as the prevalent data is available to the system.
2) *Predictive Analysis:* This analysis is used to make advanced prediction about unidentified future events. This may include numerous techniques.
3) *Trust Analysis:* This is used to find out how trustworthy the technology is based on levels and it gives belief that it keeps commitments and promises.
4) *Security Analysis:* This analysis increases the level of protection and security of a product against counterfeit.

## III.SUMMARY

This paper has presented multiple technologies which helps to detect or identify the unauthorized products and it's tracing and tracking. Here in this paper an overview of counterfeit product detection with their usage in the industries in various fields is mentioned. Since counterfeit is products are increasing exponentially with the extraordinary amount of online and Gray market. The manufacturing and electronic device local service industries are unguarded to the counterfeiting attacks. Counterfeiting attacks of products starts from simple relabelling attack to vast reverse engineering to fabrication engagements. So, there is a strong requirement to mention the challenges of identification and detection of counterfeit products and designing suitable technology to improve accuracy in detection. The paper has presented overview of available electronic device / product security solutions to fight against counterfeit. A short comparative table of comparison of techniques in terms of real time, predictive, security and trust has been put forward. The technologies mentioned would assist a brand to adopt any of these security measures in safeguarding the products against counterfeiting. The paper specifically focuses on RFID, PUF, DNA, on-device signature like technologies which are commonly used in the industries, the reason behind is they provide a very suitable, feasible and strong solution against counterfeiting.

## REFERENCES

[1] [1] US20110295908A1 - Detecting counterfeit devices- Google Patents, Publication date 2011-12-01.Inventor, Dang Tu To, Michael C. Elles, Eric Thomas Gamble, Ketan Bachubhai Patel, Rupert P. Walker

[2] [2] Unauthorized Product Detection, Prior Publication Data US 2014/0201094 A1 Jul. 17, 2014,Inventors: Douglas James Herrington, Shehzad Mevawalla, Rajiv Chopra, Joseph Sirosh, Sachin Chouksey,

[3] [3] Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead, Ujjwal Guin Auburn University, Mark Tehranipoor, University of Florida (February 2014) ECE Dept., University of Connecticut, Honeywell Inc.

[4] [4] US20140272097A1-DNA marking of previously undistinguished items for traceability, Inventor Lawrence Jung, James A. Hayward, Minghwa Benjamin Liang, Year of Publiction -2014-09-18.

[5] [5] CH709353A2 - A method of checking the authenticity of an object, Inventor- Eric Bauer, - Google Patents, Authority, CH, Switzerland, Prior art date-2014-03-12, Publication date- 2015-09-15.

[6] [6] An RFID based Technology for Electronic Component and System Counterfeit Detection and Traceability, Kun Yang, Domenic Forte, Mark Tehranipoor,. 978-1-4799-1737-2 2015 IEEE.

[7] [7] US20160006570A1 Generating a key derived from a cryptographic key using a physically unclonable function, Inventor Rainer Falk, Steffen Fries, Publication date-2016-01-07.

[8] [8] Reliable PUF-based Local Authentication with self-Correction, Yingjie Lao, Bo Yuan, Chris H. Kim, Keshab Parhi, 0278-0070-2016 IEEE.

[9] [9] Strength of QR Code Over Design And Implementation of Authentication System, Lokesh Khedekar, Prajakta Kale, IEEE, International Conference on Communication an Signal Processing, April 6-8, 2016, India.

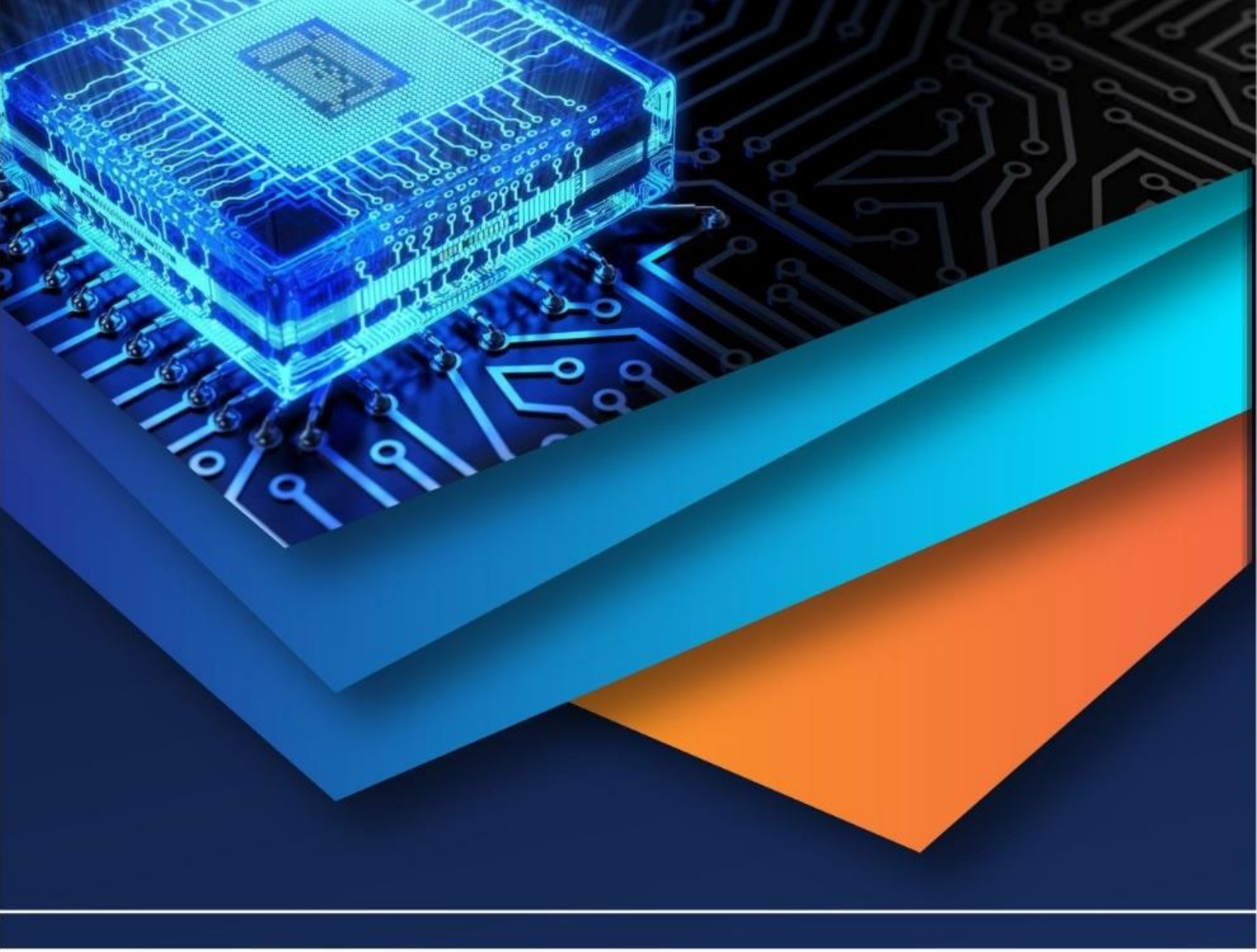
[10] [10] Hardware- Based Anti-counterfeiting Techniques for Safeguarding Supply Chain Integrity Md Tanvir Arfain, Andrew Stanley, Praveen Sharma, Maryland, Massachusetts, Massachusetts 978-1-4673-6853-/17 2017 IEEE.

[11] [11] Design and development of a mobile EPC-RFID-based self-validation system (MESS) for product authentication , S.K. Kwok ,Jacky S.L. Ting, Albert H.C. Tsang, W.B. Lee, Benny C.F. Cheung, - Department of Industrial and Systems Engineering, The Hong Kong Polytechnic University, Hung Hom, Hong Kong, Hong Kong, China.(2018)

[12] [12] US10291411B1 - Authentication method and system - Google Patents, Inventor-David I. Durst, Norman Kaish, Jay Fraser, Authority -USA, Publication date 2019-05-14.

[13] [13] The Impact of Counterfeiting on Genuine-Item Consumers' Brand Relationships, © 2009, American Marketing Association ISSN: 0022-2429 (print), 1547-7185 (electronic), Journal of Marketing Vol. 73 (May 2009), 86–98.

.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY