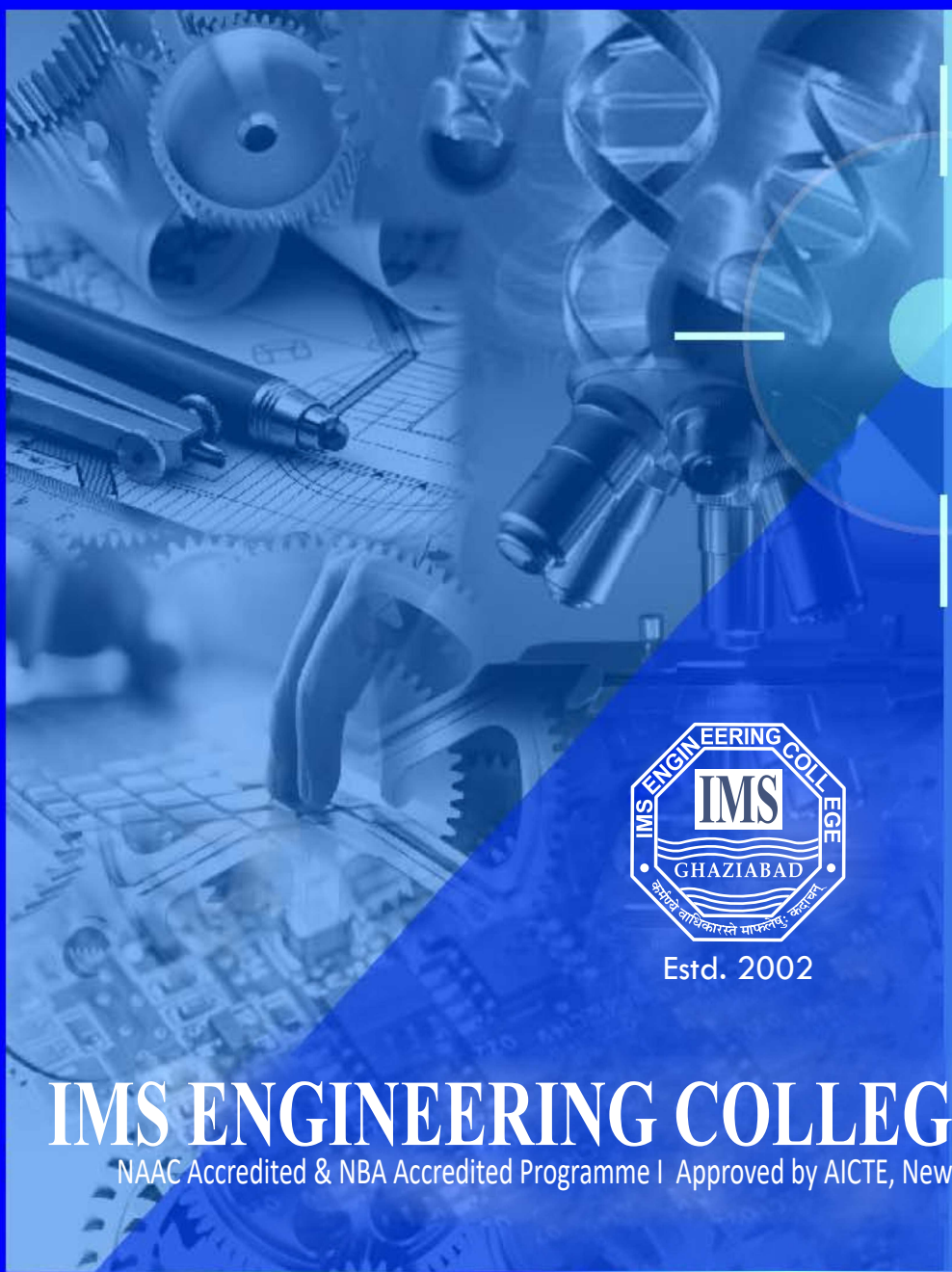
VIVECHAN INTERNATIONAL JOURNAL OF RESEARCH

Volume 12, Issue 1 | December - 2023 | ISSN No. :0976-8211



Estd. 2002

IMS ENGINEERING COLLEGE, GHAZIABAD

NAAC Accredited & NBA Accredited Programme I Approved by AICTE, New Delhi & Affiliated to AKTU, Lucknow

Owned & published by: IMS Engineering College, NH-24, Delhi-Hapur Bypass Road, Adhyatmik Nagar, Ghaziabad 201015 (UP)

Ph.: 0120-4940000, Fax: 0120-4940094

Approved by UGC, AICTE, New Delhi & affiliated to Dr APJ Abdul Kalam Technical University, Lucknow

NAAC Accredited & NBA Accredited Programme
Email: imsec@imsec.ac.in, Website: www.imsec.ac.in

Published by IMS Engineering College, Ghaziabad NH-24, Delhi-Hapur Bypass Road, Adhyatmik Nagar, Ghaziabad 201015 (U.P.). Editor Dr. Sonali Mathur

Contents

Editorial

Scientific research is a critical tool for successfully navigating our complex world. Without it, we would be forced to rely solely on intuition, other people's authority, and blind luck. The world's top scientists and researchers are always pushing to discover, prove, and create innovations in the world of science and technology. These discoveries are the result of critical thinking and continuous research efforts. Their breakthroughs alter life on earth and change our perception of reality. Each year, scientists make incredible discoveries. Scientists managed to make some pretty awesome breakthroughs and discoveries in recent years from space travel to the machine to medicine, nutrition, and Earth sciences.

Vivechan International Journal of Research has a strong emphasis on interdisciplinary issues as we are conscious that many complex problems in the built environment require multi-disciplinary solutions. Aim of this issue is to give the researchers an opportunity to share the results of their academic studies. This issue has papers from different domains including biotechnology, speech recognition, software engineering, recommendation system, internet of things, artificial intelligence, etc.

Vivechan International Journal of Research (VIJR) is published bi-annually by IMS Engineering College, Ghaziabad. It includes a wide range of research topics from science, engineering & management. It is a matter of great pleasure that we are successfully publishing the Volume 12 issue 1 of VIJR. This issue includes five articles from researchers from various disciplines. These articles have been summarized below to give a glimpse of the topics discussed in these articles.

In the first article authors Amol Prakash and Rahul Charles Francis presented a useful discussion of the manufacturing various components related to the engineering field, it is ordinary to utilize the identical tools regularly for coordinating dissimilar portion as outcome degrade manifest on the exterior flank surface and crater surface. This article proposes a technique to analyze or monitor flank wear with the help of image processing using MATLAB R2020a Software.

Author Ajay Gupta presented in his article to compare all the phishing website detection techniques. Phishing attack is an attempt to obtain confidential information or data, such as credit / debit card details, username, passwords, etc. by creating a fake website which is very much similar to genuine website. Because of visual similarity of website, users are not able to distinguish between a legitimate and phishing websites. Phishing attack often targets users to enter their personal information at a phishing website. Then that information is directly sent to attackers.

In the next article authors, Arshi kumari & Sunanda Gupta presented a useful discussion of the daily use of the internet increases, the myriad malware attacks are increasing day by day which leads to purloin of crucial data of individual, company, or organization. Various malware detection systems

or software are build and used, and are the first status must be established in order of importance or urgency for the prevention of the purloin of data. Traditional malware detection method uses feature selection and extraction (like in data mining, we have feature selection and extraction, which are different stages), which are time-consuming. Thus, keeping in view these vulnerabilities, many researchers used artificial intelligence paradigms i.e. machine learning (also used feature extraction and classification as different stages), deep learning for the improvement of the system.

Dinesh Singh presented in this article, a useful discussion of the theme of Internet of Things protection technologies by incorporating blockchain IOT applications. To address both cryptographic security and privacy concerns, the proposed IOT-based smart city architecture uses BC technologies. Furthermore, BC has a very low overhead on the IOT network. The new system is a block chain based fully distributed access management framework for IOT. This article discusses the similarities and differences between block chain and IOT technologies, as well as a general reference framework that can be used to build a variety of block chain based community IOT applications.

In the last Article Author Ashish Dixit talk about, image fusion techniques gain popularity because they combine the most appropriate features of different source images in order to generate a single image that contains more information and is more beneficial. In this paper, initially, we have studied the analysed the conventional spatial and transform domain image fusion techniques. These techniques face numerous challenges, and to overcome them, optimization algorithms are deployed. These algorithms search for the optimal solution for the image fusion technique based on the objective function. Therefore, the main focus of this article is to study and analyse the optimization algorithms based on various factors.

We wish to express our gratitude to the researchers for their valuable submissions and to the ones who showed their interest in our journal. The submitted articles have been carefully reviewed by a team of active researchers in interdisciplinary domains. We hope that the articles presented in this issue will enrich the knowledge of our esteemed readers. The editorial team wishes to thank reviewers for their time and valuable comments, which helped to maintain the standard of the journal.

We welcome your valuable comments and suggestions for the betterment of our journal. We look forward to receiving your contributions for the upcoming issue of VIJR in Jan 2024.

Analysis of Flank Wear in Turning Operation Using Digital Image Processing Technique

Amol Prakash[1] and Rahul Charles Francis[2]

[1,2] Department of Mechanical Engineering, Vaugh Institute of Agricultural Engineering and Technology, Sam Higginbottom University of Agriculture, Technology and Sciences, Prayagraj, Uttar Pradesh, India.

[1]Amolprakash001@gmail.com, [2]Rahul.francis@shiats.edu.in

Abstract:

While manufacturing various components related to the engineering field, it is ordinary to utilize the identical tools regularly for coordinating dissimilar portion as outcome degrade manifest on the exterior flank surface and crater surface. Flank wear is the most commonly seen wear while machining. It must be monitor because it causes the loss of materials as well as productivity which directly or indirectly affects the economy. This paper proposes a technique to analyze or monitor flank wear with the help of image processing using MATLAB R2020a Software. The image of the tool having flank wear is captured by a digital camera and then processed in the software. The processing of images involves gray level imaging, threshold image, filtering, edge detection. With the help of these processing parameters, monitoring of flank wear had been done.

Keywords: MATLAB, Image Processing, Flank wear, carbide insert.

1. Introduction

In the current Era, the machining industry is undergoing many trends. The leading trend is regarding the reduction of production cost [1]. These trends lead to a hard production parameter like an increase in cutting speed, feed, etc., and a decrease in human guidance. These parameters result in unmannered machining conditions. This is a fact that the economy of a country depends on production rate but because of the unmannered machining conditions, failures occur in the basic operations like turning, milling, drilling and due to this failure economy crashes. To overcome the failure a proper analysis of machining as well as machining components should be done.

Cutting operations like turning and milling play a vital role in today‘s leading manufacturing processes [2]. It is important to monitor the tools which are involved in these operations.

As industrialization is increasing day by day there is a need for flexibility of manufacturing systems. This helps in maintaining the competitiveness of industrial production [3]. To obtain flexibility monitoring or analysis of the components is very much important. There are many methods to monitor tools involve in machining which are direct methods and indirect methods [4].

1.1. Direct Measurement Methods

Different studies had been made in both direct and indirect methods for the analysis as well as the measurement of tool wear. Some of the direct measurement methods are: [4]

Tool Maker‘s Microscope

Proximity Sensors

1.2. Indirect Measurement Methods

It utilize distinct variables and indicators of the cutting procedure . The primary focus of this technique to find out level of decay . Some of the Indirect methods are as follows: [4]

Vibration

Acoustic Emission

Neural Network Sensor Fusion

Cutting Force

Indirect Measurement Methods are not very sensitive in comparison to Direct Measurement Methods. This results in errors while measurement of wear [2]. On the other hand, Direct Measurement Methods are free from any process parameters and measures the value more accurately and precisely. Both approaches can be utilize alternatively within a procedure or during a cycle .

The primary focus of the study to evolve a technique concerning tool wear within a cycle analysis using digital image processing.

Generally, there is a vast range of tool inserts for turning operation. But the most common as well as the conventional tool is the carbide tool. In this research, a tungsten carbide tool insert had been used for turning operation. The wear mechanism of the tungsten carbide tool insert is subjugated by adhesion and/or abrasion in continuous machining of carbon steels [5].

The main reason for choosing the digital image processing technique is- it is perhaps one of the easiest and most comfortable ways to detect any major or minor wear in the tool. Due to the increasing demand of cutting down the production costs under market pressure, unattended, machining is the main feature in most of the manufacturing industries. Major factors of economic losses are material loss and machine downtime caused mainly by continuously degrading tool edges. So, it is very much essential to analyze the wear to avoid hazardous effects on surface integrity and damage to the workpiece or machine tools [6].

2. Methodology

The following includes study work :

Appropriate choosing of Tool
Capturing of the image of the tool before machining
Image processing of the image of the tool before machining
Turning operation
Capturing of the image of the tool after machining
Image processing of the image of the tool after machining
Comparing the images of the tool i.e., before and after machining
Analysis of the wear on the tool

2.1.Selection of tool

In turning operation, axially symmetric profiles are formed by driving a tool along with a profile as the workpiece rotates. Some factors must be considered when selecting a tool for turning operation [7]. Following are the factors to be considered:

Type of workpiece
Shapes of internal and external profile
Amount of material to be removed

The desired finish of the part surface

Capabilities of the machine

All the above-mentioned factors indicate the carbide tool as a good tool for turning operation. Firstly, a carbide insert shown in figure 2 had been selected. The basic configuration of the carbide insert is mentioned in the Table 1 and Figure 1.

Parameter	Value
SAP Material number	2028799
ISO Catalog Number	TPKN2204PDR
Grade	TTR
Cutting Edges Per Insert	3
[D] Insert IC Size	12.7000
[L10] Insert cutting Edge Length	21.9970
[S] Insert Thickness	4.7600
[BS] Corner Face Length	1.4000
Average Chip Thickness	0.1800

Table 1: Configuration of carbide insert (all numeric values are in metric)

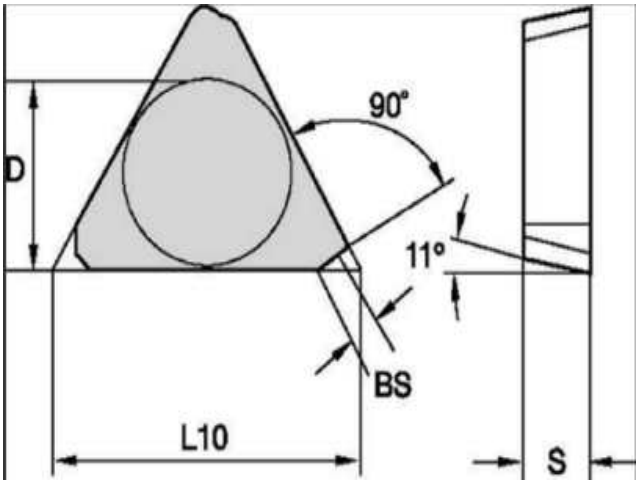


Fig. 1. Dimensional View of the insert

Fig. 2. Carbide Insert

2.2. Capturing of the image of the tool before machining

After the selection of the insert, the second step is to capture the image of the tool before machining. But for this, the insert is welded with an iron shank shown in figure 3 with help of gas welding.

Fig. 3. Carbide insert welded with the iron shank

2.3. Image processing of the image of the tool before machining

It is very important to process the image before machining so it will be easier to compare the image before and after the wear. Image processing is done by MATLAB software. Processing of image shown in figure 4 includes gray level image, threshold image, filtering of the image, and edge detection.

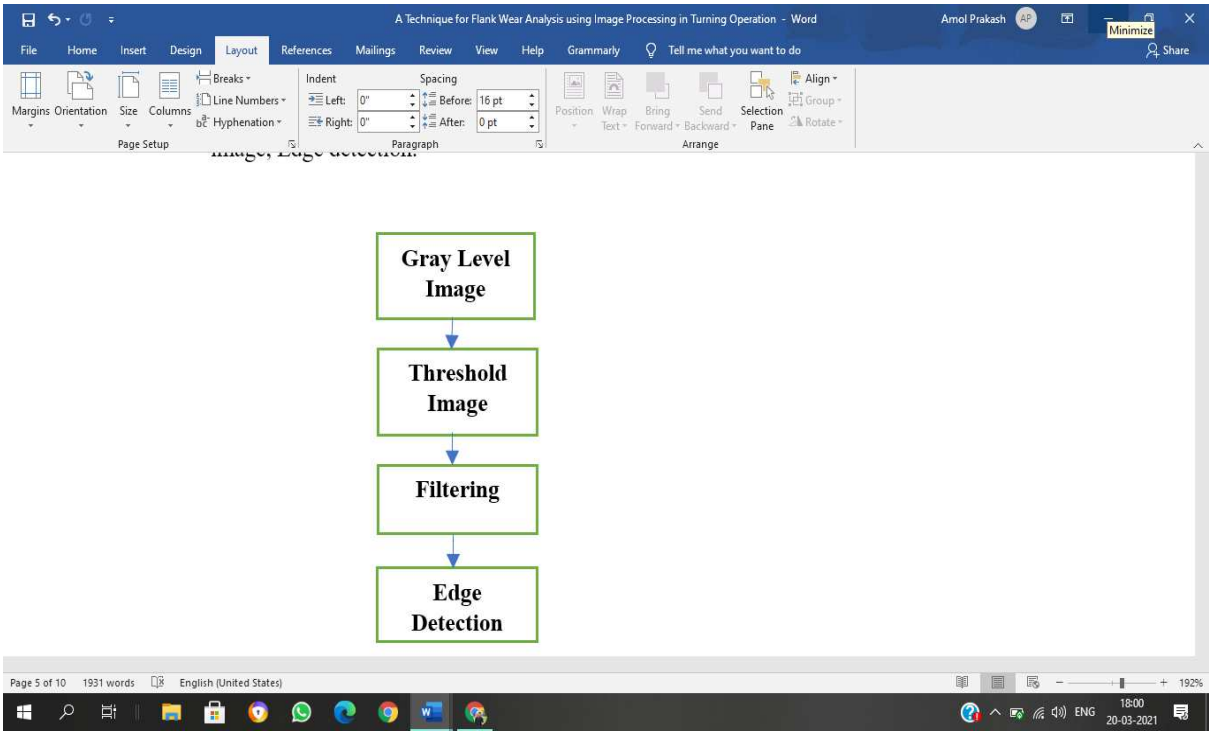


Fig. 4. Image processing Steps

Gray Scale Image. Generally, all the digital image processing methods or techniques involve the gray level transformation of the image this is because it operates directly on pixels. It includes 256 levels of Gray [8]. Figure 5 shows the gray level image of the carbide tool.

Fig. 5. Gray Level Transformation of Original image

Threshold image. The main aim of thresholding images is to declare a limit for pixel values in a gray scale. It is used to convert the gray level image to a binary image [9]. The gray level image of the tool is processed into threshold image shown in figure 6.

Fig. 6. Threshold imaging of Gray level image

Filtering of image. In image processing, filtering of the image is primarily used to suppress either the high frequencies in the image that means to smooth the image, or the low frequencies which is to enhance or distinguish the edges in the image [10]. Filtered image of the tool is shown in figure 7.

Fig. 7. Filtering of the image

Edge Detection. An edge can be defined as a set of associated pixels that form a boundary between two separate sections. There are three types of edges:

Horizontal edges

Vertical edges

Diagonal edges

Edge detection is used to observe any significant change in the features of an image in the gray level. This texture signifies the end of one section in the image and the beginning of another. It reduces the amount of data in an image and preserves the structural properties of an image [11]. The edges of the tool represented by white borders can be seen in the figure 8.

Fig. 8. Edge detection of the filtered image

2.4. Turning operation

Turning operation is done on conventional lathe machine PLD-6G. The configuration of the lathe machine is mentioned below:

Spindle Bore- 38 mm

Automatic Grade- Automatic

Layout- Horizontal

Brand/Make- Pathak

Power- 2 HP

The turning operation shown in figure 9 is done with work piece firstly as mild steel rod of 1-inch diameter and later as high carbon steel rod of 3-inch diameter. The spindle speed was 480m/min. The chuck was a four-jaw chuck. The depth of cut was given from 0.5 mm to 6.0 mm after every completion of feed of mm. Feed given for the operation was 87 mm The same parameters and values were given in the case of a high carbon steel rod.

Fig. 9. Fig. 9. High carbon steel rod while turning operation

2.5. Capturing of the image of the tool after machining

Figure 10 shows the wear on the flank face of the tool after machining.

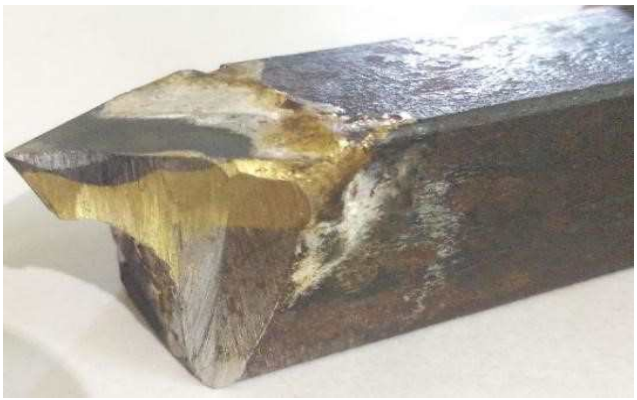


Fig. 10. Image of the tool after machining

2.6. Image processing of the image of the tool after machining

The same steps shown in the Figure 11 to 14 have been followed for image processing of the image of the tool after machining

Gray Scale Image

Fig. 11. Gray level image of the tool after machining

Threshold image

Fig. 12. Threshold image of the tool after machining

Filtering of image

Fig. 13. Filtering of the image of the tool after machining

Edge Detection

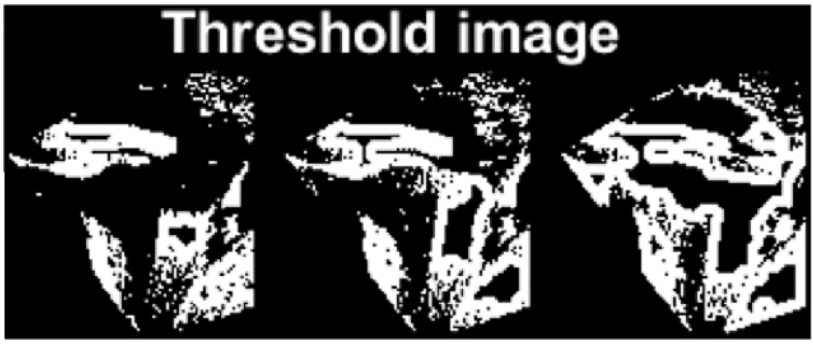


Fig. 14. Edge detection of the wear in the image of the tool after machining

2.7. Comparing the images of the tool i.e., before and after machining

In this section, a visual comparison is done based on two images. Figure 15 shows the edge detection of the image on the tool before machining and the edge detection of the image on the tool after machining.

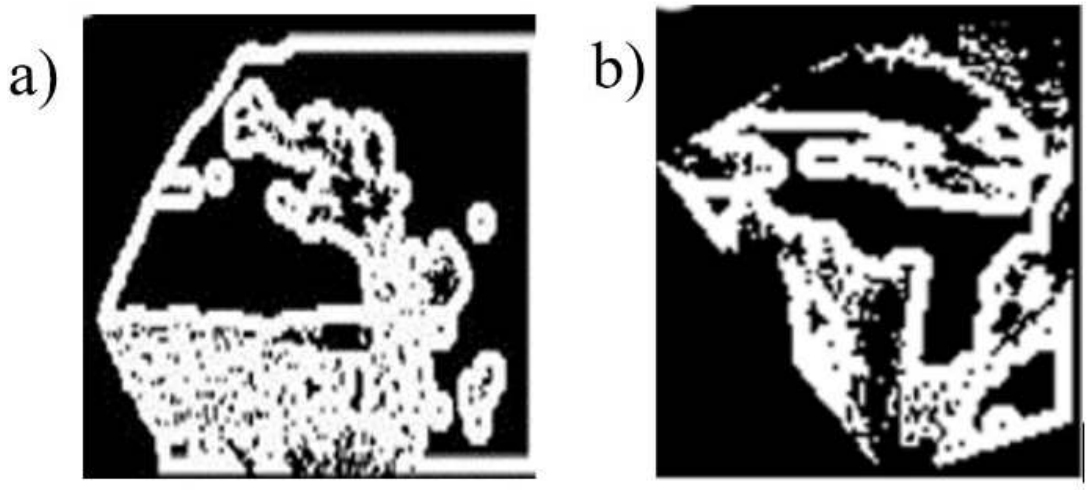


Fig. 15. Edge detection of the image of the tool before and after machining respectively

2.8. Analysis of the wear on the tool

In the section of comparison, it is visible that the image of the tool after machining has many irregular surfaces and curves on the flank face of the tool but there is no such irregular surface on the image of the tool before machining. By the geometrical analysis of both the images, it is clear that the flank face of the tool has some wear after machining continuously

3. Conclusion

The paper depicts a method employing digital image processing to directly analyze tool deterioration. The conducted experiment shows the effectiveness and simplicity of proposed method in accurately monitoring tool deterioration. Consequently , it can be applied in both type of small and large scale industries to optimize tool usage through direct in-cycle analysis of tool flank wear .

The focus of the proposed method are:

To detect both major and minor errors for cutting tools, and

To use it as a safeguarding machining process for stability.

References

1. M. Sortino, "Application of statistical filtering for optical detection of tool wear," International Journal of Machine Tools & Manufacture, vol. 43, pp. 493-497, 2003.
2. T. Pfeifer and L. Wiegers, "Reliable tool wear monitoring by optimized image and illumination control in machine vision," Measurement, - 218, 2000.
3. O. G. Moldovan, S. Dzitac, I. Moga, T. Vesselenyi and I. Dzitac, "Tool-Wear Analysis Using Image Processing of the Tool Flank," symmetry, vol. 9, p. 296, 2017.
4. S. Mehta, S. A. Rajput, Y. Mohata and M. B. Kiran, "Measurement and Analysis of Tool Wear Using Vision System," in IEEE 6th International Conference on Industrial Engineering and Applications, 2019
5. T. Kitagaw, K. Maekawa, T. Shirakashi and E. Usui, "Analytical prediction of flank wear of carbide tools in turning plain carbon steels (part 1) - characteristics equation of flank wear," Bulletin of the Japan Society of Precision Engineering, pp. 263 - 269, 1988.
6. A. Siddhpura and R. Paurobally, "A review of flank wear prediction methods for tool condition monitoring in a turning process," International Journal of Manufacturing Technology, vol. 65, pp. 371 393, 2013.
7. "Introduction to Selecting Turning Tools important decisions for the selection of cutting tools for standard turning operations," MachiningCloud, 2016.
8. Java T Point, "Gray Level Transformation," [Online]. Available: https://www.javatpoint.com/.
9. B. İşgör, "A Software Programmer," October 2020. [Online]. Available: https://asoftwareprogrammer.com/.
10. R. Fisher, S. Perkins, A. Walker, and E. Wolfart, "Digital Filters," University of Edinburgh, 2003. [Online]. Available: https://homepages.inf.ed.ac.uk.

A Survey on Phishing Website Detection

Ajay Kumar Gupta
Department of Computer Science & Engineering (AI)
IIMT College Of Engineering, Gr. Noida, U.P. India
ajayguptagorakhpur@gmail.com

Abstract

Phishing attack is an attempt to obtain confidential information or data, such as credit / debit card details, username, passwords, etc. by creating a fake website which is very much similar to genuine website. Because of visual similarity of website, users are not able to distinguish between a legitimate and phishing websites. Phishing attack often targets users to enter their personal information at a phishing website. Then that information is directly sent to attackers. In today‘s world most of the phishing attack takes place with the help of spoofed emails. The attacker first sends the email to victim which looks like it‘s come from genuine sender. The spoofed email contains the link to such phishing websites. When the victim clicks this link and enters the credentials/information, the information is directly passed on to the attackers. The attackers then misuse this information. Phishing attack is still among the top ten cyber attacks. Hence, the security experts are looking for a reliable and steady detection mechanism with high accuracy. This paper aims to compare all the phishing website detection techniques.

Keywords: Phishing Attack; Phishing Website; Machine Learning Algorithm; Social Engineering; Deep Learning Algorithms; Neural Network

1. Introduction

Phishing attack is an attempt to steal the confidential or personal information of user by creating a fake website which looks very similar to legitimate website and it‘s very hard for general user to differentiate it. Now-a-days phishing attack is the one of the easiest way to gain the confidential information such as bank details or password, etc. It is not difficult to make or clone the website which look as genuine website. Phishing attacks are becoming successful because of social engineering and lack of users knowledge or awareness. As per the Verizon‘s Data Breach Investigation Report (DBIR) 2020 [1], 22% of total breaches in year 2019 involved phishing. As per Phish labs trends and intelligence report [2] the phishing attacks grew by 40.9% and among these attacks almost 83.9% attack targets credentials of the users in the year 2018. It is very difficult to mitigate such attack but we can improve our defense mechanism by classifying such websites with high accuracy.

2. Related Work

Many researchers have analyzed the statistics of URL which are suspicious in many different ways. We review the previous works in the phishing website detection using statistics features of URL‘s. There are various categories of approaches for detecting phishing website attacks such as: (a) Blacklist or White-list based Detection [3], [4], (b) Phishing Website Detection based on Visual Similarity [5], (c) Heuristic Characteristics based Phishing Website Detection [6], (d)Machine Learning based Phishing Detection[7], [8], [9], [10].

The blacklist or white-list approaches works by maintaining the blacklist or white-list of the visited websites. This approach is mostly used by Google‘s safe browsing API and Firefox browser to detect phishing URL [11]. But the drawback for such approach is that, we are not able to maintain the list at real-time. Hence, it can‘t detect a zero hour phishing attacks.

After some more approaches, some researchers tried to detect phishing attacks by using visual similarities. Medvet et al proposed an approach which simply compare the websites using three visual parameters that plays an important role in detecting the phishing and legitimate web-pages. These features are image embedded in page, text and style of page and overall visual appearance of

the web-page [12]. The drawback for this approach is that if web-page is distorted then the mechanism is not able to detect it correctly.

Later, heuristic based detection evolves. Jin-Lee et al proposed an approach which extracts some heuristic features or characteristics from the web-page. These information is used to detect the phishing websites [13]. This approach is able to detect zero hour phishing attacks. Here, we can‘t guaranteed that the considered characteristics are always present in the attacks and therefore this method may detect genuine website as fake website.

To overcome all the drawbacks of previous approaches, machine learning algorithms are evolved. Machine learning techniques [14], [15], [16], [17] consist of so many algorithms. They uses the previous generated data for judgement making or predicting future data , the algorithm to make a decision or prediction on future data. Using such technique, the algorithm examines websites URL _s by analyzing extracted features . This technique enables accurate detection of phishing websites, incuding zero-hour phishing attacks . The drawback of this approach is that some algorithm‘s accuracy to detect is moderate while some algorithm take more time to train. Another disadvantage is that the dataset must be preprocessed before applying to any algorithm which is not possible in real-world. Hence, preprocessing the data is a hectic task for researchers in this approach.

3. Dataset

URL of legitimate and fake websites are collected to form the dataset. The dataset is named as ―Phishing Website Detection Dataset‖ [18] and is freely available on UCI repository website for download. Dataset consist of all together 10,000 URL‘s in which 5,000 URL‘s are legitimate and 5,000 URL‘s are phished websites. Every URL has 30 features associated with them and one class label. Class label is to show that the URL is legitimate or fake. Class label is _1‘ for _phishing website‘ and _0‘ for _legitimate website‘. All other features has values which are binary except the domain name.

4. Characteristic Extraction

Characteristics Extraction is the most prominent phase before applying any machine learning algorithm. Feature Extraction is considered as preprocessing step in Machine Learning. We implemented the python code for feature extractions using some standard libraries. Thirty properties are derived from the raw/ unprocessed datasets , and they are arranged in to three distinct categories .They are as follows:-

1. Address-Bar based Features
2. Domain based Features
3. HTML JavaScript based Feature
4. Abnormal based Features

Below are the fields that we considered for phishing website detection:

4.1Address Bar based Features

1. Using IP Address : If IP address is present in URL then the value is set to 1 else it is set to 0. Because most of the legitimate websites do not use any IP address in an URL. If you see any IP address in websites URL then that URL may be use to steal sensitive information of the users.

2. Long URL to Hide Suspicious Part: Most commonly used determined length of valid URLs is 54 because longer the URL length more difficult to remember for users. And if the URL is long then the URL may hide the doubtful part in the address bar. If URL surpass characters the feature value as assigned is 1otherwise it set to 0 .

3. URL Shortening Services ―TinyURL‖: Attackers commonly employ URL shortening services such as Tiny URLs and make them concise . The focus is to redirect users to phishing websites . If an attacker utilizes any Tiny URI services , such as bit.ly the feature is assigned a value of 1, otherwise it is set to 0.

4. URL‘s having ―@‖ Symbol: Value for this feature is 1 if @ symbol is presentin an URL else its value is 0. Attackers may add @ symbol in the URL which leads the browser to ignore everything before the ―@‖symbol and the real address which is present after ‖@‖ symbol opens up.

5. URL Redirection: If in URL address ―//‖ symbol is present then value for this feature is set to 1 else to 0. If ―//‖ is present more than once within the URL address then it means that the user will be redirected to another web-page.

6. The feature is marked as 1 when the domain name is separated by a dash (-) symbol, and 0 otherwise. Authentic URLs typically avoid using the dash symbol (-), but attackers may intentionally introduce it to the domain name to sow confusion, leading users to believe they are on a legitimate website. For instance, a valid website such as http://www.coepmis.com could be mimicked by an attacker with a deceptive counterpart like http://www.coep-mis.com, adding an element of confusion for unsuspecting users. Sub Domain and Multi Domains: The

domain may contain the sub domain in URL. For counting the sub domain in URL, we need to count the number of dots in URL.

7. HTTPS Protocol: If the developer uses the https protocol then the website is legitimate if the certificate is issued from the trusted domain.

8. HTTPS Domain: If HTTPS domain is registered for this URL path then the feature value is set to 1 else to 0. Attacker may mimic the ―HTTPS‖ domain to a fake URL in orde to trick users.

9. Domain Age: If domain age is very recent then the URL may be phished. Hence, we track domain age and we can set the value for this feature as 1 if domain age is long or 0 if domain age is short i.e. recently created domain.

10. Favicon: The graphical icon used for visual remembering of website is called as favicon. If the favicon is loaded from other domain then webpage may be considered as phishing website.

11. Using Non-Standard Ports: Every protocol which is used in working of any website has a preferred status i.e. either open or close port. If preferred status is closed for FTP protocol but actual status is open then that website may be a phishing website.

4.2 Domain Rooted Properties

1. Call URL: In this feature we analyze whether the external multimedia files such as images, tables or videos are embedded within a web-page shares the same domain or not.
2. Anchor Tag: We have to extract the source code of the web-page using web spiders to find the anchor tag used in that web-page. In HTML anchor tag is specified by ¡a¿ tag. If the anchor tag and web-page have different domain then the percentage is calculate to find the class of website.
3. Links in tags: We find the percentage of links in Meta, Script and Links tags which are from different domain.
4. Server Form Handler (SFH): The SFH is used to handle the forms submitted. If the domain of webpage and SFH is different than it may be a phishing website because the submitted information is used by external domain.
5. Attackers might utilize "mailto:" functions in the source code of a URL to forward user details, including cookies, to their individual or anonymous email. If these methods are detected, the traits is assigned a value of 1; otherwise, it is set to 0.

6. Abnormal Link: This feature is extracted using the WHOIS database. If the URL includes the host name then it is legitimate.

4.3 HTML JavaScript based Feature

1. Website Forwarding: This feature counts number of times a web-page is redirects to other web-page. This feature is important because phished websites redirects user from one web-page to other several times.
2. Status Bar Customization: Attacker may change the status of ―onMouse Over‖ event which makes changes on status bar using JavaScript.
3. Disabling Right Click: Many attackers disables the option to right click using JavaScript, so that users cannot download the source code of that web-page.
4. Using pop-up Window: No genuine website ask users to enter their information in a pop-up window. These pop-ups are only used for warning but attackers may use them for taking users information.
5. IFRAME: We need source code of the required URL to extract IF RAME feature. IFRAME tag in HTML is employed to integrate additional web content into an already existing webpage. Attackers may use ―IFRAME‖ tag to add webpage with full size on another web-page and make it phishing website. Hence, user is not able to identify that inserted web-page is not a part of website; they consider it as a part of main web-page and fill up the information.

4.4 Abnormal based Features

1. Domain Age: It is also an important feature to detect since most of the fake websites are live only for some short period. DNS Record: DNS is used to convert the domain name of website into IP address of website. If any website does not have DNS record then its value is set to 1 else its value is 0.
2. Website Rank: Website Rank feature measures how important the required website compared to other websites similar to that URL. We can say that the lesser the website rank the more important the website. We found that major phishing websites don‘t have significant website rank. The value of this feature is 1 if the website rank is greater than 10,000 else it‘s set to 0.
3. Page-Rank: Page-Rank measures how important the web-page is on the internet. The Page-Rank is directly proportional to importance of that web-page. Most phishing web-pages have no Page-Rank.
4. Google Index: This feature verify whether a web-page or URL is registered on Google index.

5. Number of Links Pointing To Page: It indicates how legitimate a website is, since most of the phishing website does not have any links pointing to that web-page.
6. Statistical Report Based Features: This feature refers to some statistical reports such as Top 10 domains, Top 25 IP which belongs to phishing websites.

5. Algorithms

Phishing Website Detection is a classification problem as we have to predict that the considered URL is fake i.e. 1 or legitimate i.e. 0. Hence, we implement all the classifier present in machine learning. We study all these classifiers in details.

5.1 Decision Tree Classifier

The Decision Tree Algorithm [19] stands out as one of the most widely embraced approaches in machine learning. Renowned for its simplicity in implementation and comprehension, this algorithm operates by choosing the optimal split among attributes for classification, serving as the root of the decision tree. This process iterates until a leaf node is reached. The resultant decision tree model becomes a valuable tool for predicting target values, with each internal node denoting an attribute and each leaf node signifying a class label or target value. The determination of nodes within the decision tree relies on process such as the Gini index and information gain

5.2 Random Forest Classifier

The Random Forest algorithm stands as a prime example of an ensemble learning approach, intricately rooted in the principles of the decision tree algorithm. This algorithm, documented as Random Forest [20], constructs a forest comprising various distinct decision trees.. The random forest algorithm uses the concept the collects the weak decision made by all trees to make a strong decision. Higher the number of decision trees for consideration higher will be the accuracy for classification.

Bootstrap method is used for creation of trees. Within the bootstrap technique, both traits and dataset samples are systematically chosen with replacement to construct individual trees. The Random Forest algorithm similarly relies on Gini index and information gain to determine optimal splits for each tree. This iterative process continues until the algorithm generates a specified number 'N' of decision trees. Every tree within the forest provides predictions for the goal value, and the algorithm subsequently tallies votes for each anticipated target. Ultimately, the Random Forest algorithm designates the most frequently voted predicted target value as the final prediction.

5.3 Support Vector Machine

The Support Vector Machine [21], commonly referred to as SVM, is a frequently employed machine learning algorithm for classification. In SVM, every data locations is represented as a point in an n-dimensional space, where a separating line—termed the 'hyper plane'—is constructed for classifying different classes. This algorithm identifies the nearest points, known as support vectors, and establishes a line connecting them, from which a perpendicular line is then drawn. The gap between support vectors and the hyper plane is termed the 'margin.'.

The primary objective of SVM is to maximize this margin, aiming for optimal classification of the dataset. Additionally, to transform lower-dimensional data into higher-dimensional data using SVM incorporates the kernel trick.

5.4 Multi-layer Perceptron

A multi-layer perceptron is also called as MLP. A multi-layer perceptron [22] is a subset of feed forward neural network. Multi-layer Perceptron commonly contains three layers which is mainly named as input, output and hidden layers. MLP uses multiple layers and non-linear activation functions. It‘s capable of distinguishing the data that is not linearly separable. In MLP, learning occurs in the perceptron by changing connection weights after each piece of data is processed, based on the amount of error in output compared to the predicted results.

5.5 XGBoost Classifier

XGBoost [23] is an acronym for eXtreme Gradient Boosting. XGBoost is an algorithm that has recently been dominating in machine learning techniques. XGBoost is an implementation of gradient boosted decision tree which helps to design the model which has higher speed as well as performance. It attempts to accurately predict a target variable by combining the estimates of a set of simpler and weaker models.

6. Implementation Steps

6.1 Importing the required libraries

Import the required libraries for data processing, performing operations, etc. The libraries such as Numpy library for matrix operations, Pandas library for dataset operations, Matplotlib and Seaborn

libraries for graphs plotting, etc. The most important library is SciKit Learn which is required for creating implementing machine learning algorithms very easily.

Data Pre-Processing

Most important step here is feature extraction that means consider the features which are relevant for our algorithm to train. Then check that is there any NaN, Null, missing value in the extracted dataset. If any of these values are present then fill that places with appropriate values. Then make features as input _X‘ and label or target as _Y‘.

6.2 Divide dataset

Divide the dataset in two parts i.e. train data and test data. I divide the train test data in 8:2 proportion. Hence, we consider only 80% of dataset for training and 20% of dataset for testing.

6.3 Train and Test Model

As phishing detection is a classification problem. I created the classifier models using the predefined method in sklearn library and train the created model by specifying some parameters. Then computing the accuracy on train and test datasets. We may improve the accuracy of the model by varying some default parameters of the models.

6.5Deploy Model

After training and testing the model, we save it for further use. This saved model later be used for deployment in real-time projects to classify the URL‘s correctly. This models may be used as an API for implementing them in projects.

7. Results

The model that we studied is evaluated using the accuracy as a metric. The formula for calculating accuracy for each model is as shown below:

Accuracy = (TP+TN)÷($TP + TN + FP + FN$)

Accuracy is one of the most intuitive performance measures. We can say that, the greater correctness is good for prototype. But it only holds when our dataset is symmetric that means values of false positive and false negative are almost similar or same. In our case the benchmark

dataset is almost symmetric. Hence, we use accuracy as a prime metric for evaluation. The ML model takes the selected features to detect the URL.

The scikit-learn tool serves as a means to incorporate various machine learning algorithms. The dataset is partitioned into training and testing sets in a specific ratio 80:20.Each of these classifiers are trained on training dataset and evaluated using test dataset. Performance of

Sr. No.	Model name	Train Accuracy	Test Accuracy
01	Decision Tree Classifier	81.30	81.30
02	Random Forest Classifier	81.80	82
03	Support Vector Machine	80	80.60
04	Multilayer Perceptron	83.60	84.20
05	XGBoost Classifier	86.70	86.20

Table 1. Detection Accuracy of Models

The models are evaluated by calculating accuracies of the models. The accuracies obtained are as shown in Table 1: From Table 1, we can say that XGBoost have highest train and test accuracy amongst all the models. The comparison of all these models based on test and train accuracies are clearly visible in the bar chart shown below:

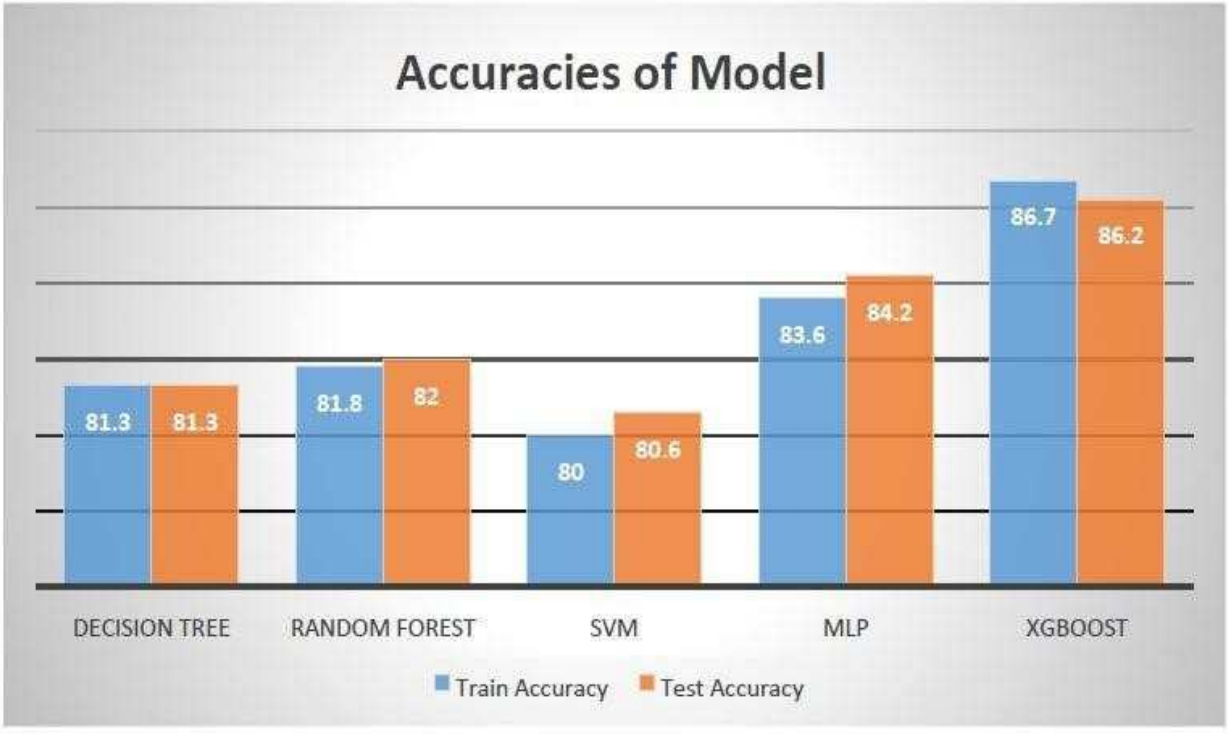


Fig.1. Comparison of implemented models

Fig 1 Depicts the identification correctness of all categorizer when train , test dataset is used and graph clearly shows that detection accuracy using XGBoost is maximum that other classifiers.

8. Conclusion

In this paper, we survey all the previous approaches of machine learning by implementing all the classifiers using the default parameters and predefined methods in sklearn library. We evaluated all the models using a benchmarked dataset containing 10,000 instances. Mainly this paper aims to compare all the models to know which model outperforms on the benchmark dataset. We also study every model in depth for understanding its advantages and disadvantages. The most important part of this survey paper is to how we can mitigate the disadvantages of the models which in turn helps to improve the accuracy for new models under research. From Table 1, we can say that the highest accuracy of almost 87% was achieved using XGBoost algorithm. From our overall study, we can say that XGBoost classifier is the best algorithm amongst all the studied model.

References

1. Verizon‘s 2020 Data Breach Investigations Report (DBIR), [online] Available at: https://enterprise.verizon.com/en-gb/resources/reports/dbir/
2. Phishlabs, ―2019 Phishing Trends and Intelligence Report: The Growing Social Engineering Threat‖ 2019, [online] Avail able at: https://www.phishlabs.com
3. P. Prakash, M. Kumar, R. R. Kompella and M. Gupta, ‖PhishNet: Predictive Blacklisting to Detect Phishing Attacks,‖ 2010 Proceedings IEEE INFOCOM, San Diego, CA, USA, 2010, pp. 1-5, doi: 10.1109/INFCOM.2010.5462216.
4. Amine Belabed, EsmaAmeur, and A. Chikh. A personalized whitelist approach forphishing webpage detection. 2012 Seventh International Conference on Availability, Reliability and Security, pages 249-254, 2012.
5. Masanori Hara, Akira Yamada, and Yutaka Miyake. Visual similarity-based phishingdetection without victim site information. pages 30 - 36, 05 2009.
6. Hoon, Lee Kim, Dong Lee, Jin. (2015). Heuristic based Approach for Phishing SiteDetection Using URL Features. 131-135.10.15224/978-1-63248-056-9-84.
7. Mohammed Alkawaz, Stephanie Steven, and Asif Iqbal Hajamydeen. Detectingphishing website using machine learning. pages 111114, 02 2020.
8. M. Khonji, Y. Iraqi, and A. Jones. Phishing detection: A literature survey. IEEECommunications Surveys Tutorials, 15(4):2091-2121, 2013.
9. Rishikesh Mahajan and Irfan Siddavatam. Phishing website detection using machinelearning algorithms. International Journal of Computer Applications, 181:45-47, 10 2018.
10. Saha, D. Sarma, R. J. Chakma, M. N. Alam, A. Sultana, and S. Hossain. Phishingattacks detection using deep learning approach. pages 1180-1185, 2020.
11. Google Developer‘s, Google Safe Browsing API‘s v4, [online] Available at: https: //developers.google.com/safe-browsing/v4

12. Medvet, Eric Kirda, EnginKruegel, Christopher. (2008). Visual-Similarity-BasedPhishing Detection. 10.1145/1460877.1460905.
13. KIM, DONG LEE, JIN. (2015). Heuristic based Approach for Phishing Site Detection Using URL Features. 131-135. 10.15224/978-1-63248-056-9-84.
14. VahidShahrivari, Mohammad Mahdi Darabi Mohammad Izadi, (2020). PhishingDetection Using Machine Learning Techniques, arXiv:2009.11116v1 [cs.CR] 20 Sep 2020
15. Preeti, Nandal R., Joshi K. (2021) Phishing URL Detection Using MachineLearning. In: Hura G., Singh A., Siong Hoe L. (eds) Advances in Communication and Computational Technology. Lecture Notes in Electrical Engineering, vol 668. Springer, Singapore. https://doi.org/10.1007/978-981-15-5341-7\ textunderscore42
16. A. Alswailem, B. Alabdullah, N. Alrumayh and A. Alsedrani, ‖Detecting PhishingWebsites Using Machine Learning,‖ 2019 2nd International Conference on Computer Applications Information Security (ICCAIS), Riyadh, Saudi Arabia, 2019, pp. 1-6, doi: 10.1109/CAIS.2019.8769571.
17. Arun Kulkarni and Leonard L. Brown III, ―Phishing Websites Detection using Machine Learning‖ International Journal of Advanced Computer Science and Applications(IJACSA), 10(7), 2019. http://dx.doi.org/10.14569/IJACSA.2019.0100702
18. Dua, D. and Graff, C. (2019). UCI Machine Learning Repository http://archive. ics.uci.edu/ml. Irvine, CA: University of California, School of Information and Computer Science.
19. Patel, Harsh Prajapati, Purvi. (2018). Study and Analysis of Decision Tree BasedClassification Algorithms. International Journal of Computer Sciences and Engineering. 6. 74-78. 10.26438/ijcse/v6i10.7478.
20. Breiman, L. Random Forests. Machine Learning 45,5–32(2001). https://doi.org/10.1023/A:1010933404324
21. Zhang Y. (2012) Support Vector Machine Classification Algorithm and Its Application. In: Liu C., Wang L., Yang A. (eds) Information Computing and Appli cations. ICICA 2012. Communications in Computer and Information Science, vol 308.Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-34041-3_27 22.
22. Marius, PopescuBalas, Valentina Perescu-Popescu, Liliana Mastorakis, Nikos. (2009). Multilayer perceptron and neural networks. WSEAS Transactions on Circuits and Systems. 8.
23. Chen, Tianqi, and Carlos Guestrin. ―XGBoost.‖ Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (2016): n. pag. Crossref. Web.

Comprehensive Review On CNN-based Malware Code Detection with Hybrid Optimization Algorithms

Prabhat Kumar Srivastava
Department of Computer Science & Engineering
IMS Engineering College Ghaziabad, U.P., India
sri_prab@rediffmail.com

Abstract

As daily use of the internet increases, the myriad malware attacks are increasing day by day which leads to purloin of crucial data of individual, company, or organization. Various malware detection systems or software are build and used, and are the first status must be established in order of importance or urgency for the prevention of the purloin of data. Traditional malware detection method uses feature selection and extraction (like in data mining, we have feature selection and extraction, which are different stages), which are time-consuming. Thus, keeping in view these vulnerabilities, many researchers used artificial intelligence paradigms i.e. machine learning (also used feature extraction and classification as different stages), deep learning for the improvement of the system. By going through various experiments done by many researchers. This paper demonstrates the malicious code detection based on deep learning algorithm i.e. CNN, with hybrid PSO-BAT optimization algorithm which increase the accuracy and help in attaining the better result.

Keywords: Malware detection, PSO-BAT optimization algorithm, CNN-algorithm.

1. Introduction

In later-days, the internet becomes the part of goods and daily necessities-product list, not even a single person in the world can do work without the use of the internet. Due to the regular increased use of the internet, people with spiteful intentions are getting the door open for performing the malicious act on the internet rather than in real life [1]. As we already know the definition of Malware word consist of two words ―mal‖ and ―ware‖, ‖ mal‖ means ―bad‖, ‖evil‖, and ―wrong‖ whereas ―ware‖ means ―intangible product or item manufactured‖, so malware is defined as the data or software which are designed to commit wrong or harm the other intentionally. So, malware generation increased exponentially with the increased use of the internet. Even smart phone is also targeted for malware attacks , because of the pervasiveness of smart phone and have a huge market share, using local-based services i.e. software services which use geographic information (regarding health, indoor object search, entertainment, work, personal life) to provide information to users apart from prevailing services such as SMS, Voice calls, multimedia services, etc. various stealth approaches such as encryption, code transformation generates known malware, which led to using of behaviour, anomaly and dynamic analysis based method which help in detecting unknown malware[2]. The most recent strain of ransom ware evades different static analysis methods, like signature-based approaches, through Distorting code, encrypting dynamically loaded code, and employing packing techniques serve as measures in the latest ransom ware to thwart various static analysis methods.. On the other hand, dynamic analysis remains resilient against these tactics. But still existing dynamic tools to these techniques are not able to scale to compare code fast and identify the origin of a new piece of malware in a time. Most of the detection malware software uses a signature-based malware classification techniques, which is used to recognize anonymous malware by comparing them to database of previously captured malware.

Whereas static and dynamic analysis also plays an important and different role which is differentiated as below:-

Static Analysis	Dynamic Analysis
a) Features are drawn from binary code of a program and then it is used to distinguish between malware and legitimate software.	a) It determines the runtime behavior of a program by determining the program while in running mode.
b) Advantages: Binary code contain very useful information about the malicious behavior of a program.	b) Analysis the runtime behavior of a program which is not obfuscated.
c) Disadvantages: Fails at different code obfuscation techniques used by the virus code and also at polymorphic and metmorphic malware.	c) Time consuming because stimulated environment is quite different from real environment. So malware behave in a different way on both these environment.

Table 1: Difference between static analysis and dynamic analysis

Dynamic analysis is a thing that contribute extra features to static analysis, as both are much deterrent to code obfuscations. And both techniques have their own pros and cons. P.V.Shijo, A.Salimhas proposed integrated static and dynamic determination of malicious program method[3].

Drawback of these method are, that it takes more time in feature selection. Hybrid analysis generate good result, so this detection techniques is constantly used in real time scenario.

2. Background

A malicious code attack is a day –to- day cyber-attack, where malicious software perform execution of unauthorized action on the casualty system. Its name was officially defined by Cohen in 1984, but its behavior come into notice since at least 1970.The two main methods such as static determination and dynamic determination where static determination uses various methods such as file fingerprinting, extraction of hard-coded strings, file format, AV scanning, packer detection disassembly etc. and dynamic analysis uses the difference between defined points and observing runtime behavior [5]. Most of the malware detection techniques are based on signature based detection which only detect known malware but unable to detect unknown, zero- day attack, obfuscated and mutated [4]. To overcome the drawback in signature-based detection technique, researchers have to turn to behavior based detection technique such as, capture malicious API calls throughout execution of the program. Behavior-based techniques gives more accuracy in results than signature-based techniques in detecting polymorphic malware whereas it is not able to detect many polymorphic viruses, known as packers[5].Heuristic based malware detection uses machine learning and data mining techniques to learn the behavior of features such as API call, CFG,N-gram,

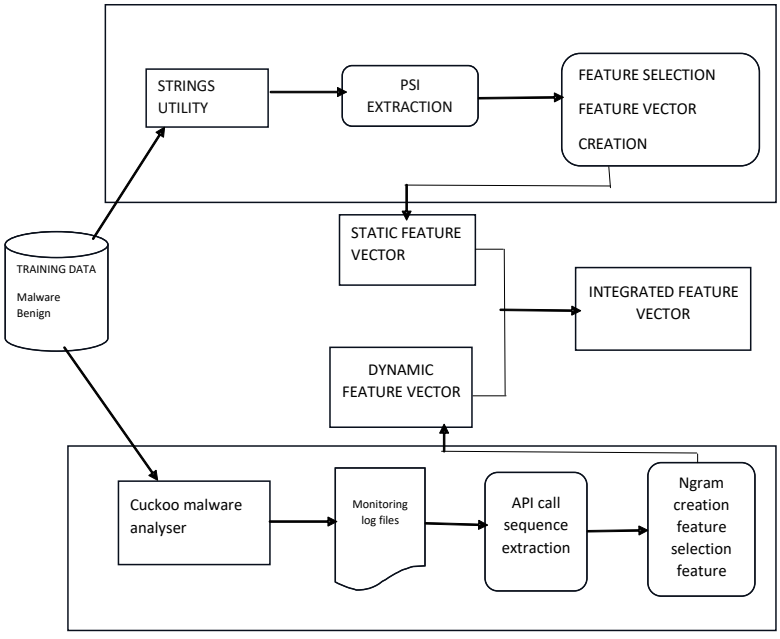


Figure1:Static and dynamic malicious program detection model[3]

opcode etc. The main disadvantage of this method is time complexity [6]. Model checking-based uses the concept of pushdown automata to model the program using SCTPL logic (stack computation tree predicate logic) is an advanced version of the branching- temporal logic CTL with variable, quantifier and predicates over stack. The drawback of this model is that its time complexity and space complexity is large [7].Then, next step is deep learning- based method which reduced the time complexity, android malware detection problem is common now a day‘s which uses large of space, by extracting android malware API sequence by cuckoo sandbox, these sequences are converted text based classification problem and using word2vec to text is converted into vectorization, then deep learning algorithm Bi- LSTM is used to classify the malware and benign, deep learning algorithm is used for large dataset [8]. As increase in use of internet increase data production is also increasing, which leads to the storage of data on the cloud due to which malicious code developer also get opportunities to access and deteriorate the information which is kept on the cloud [1].Mobile devices-based effective to detect both new and old generation malware, but can‘t detect complex malware. IoT- based uses both method static and dynamic but unable to detect complex malware. Malware detection methods are shown in figure 2.

The standard metrics are used to evaluate the performances of classifier such as accuracy, precision, recall and f1-score,these metrics are estimated based on true positive (TP),True negative(TN),False positive(FP),and false negative (FN)[9].

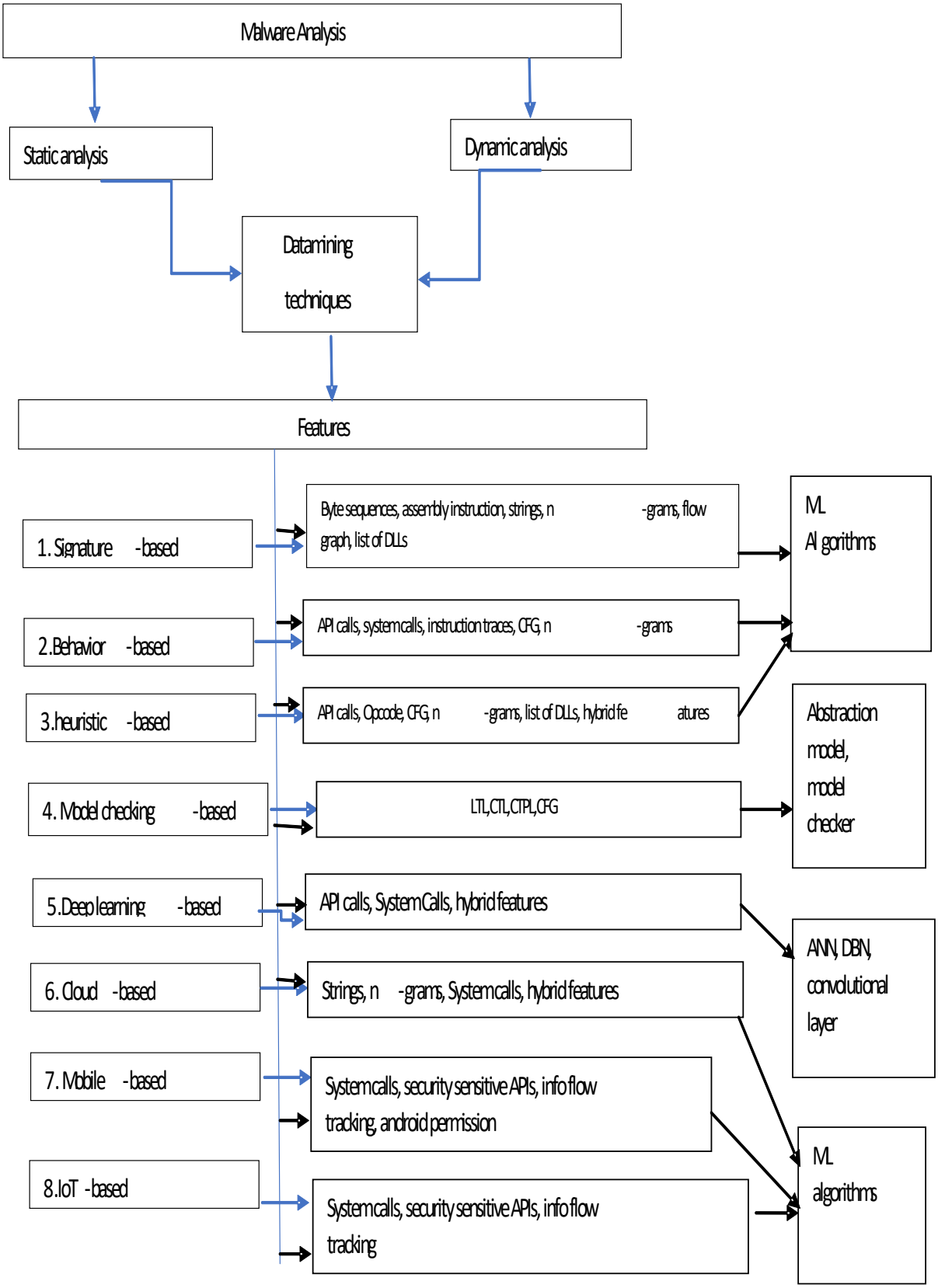


Figure 2: Malware detection method

True Positive: Rate of malicious code correctly classified by malware application

True Negative: Rate of benign classified by benign classifier.

False Positive: Rate of malware misclassified by malware application

False Negative: Rate of benign misclassified by benign classifier.

Depending upon above parameters advantages and disadvantages of detection are decided which help in determining the best approach for detection of malware. The advantage and disadvantages are shownin the table3.

3. OPTIMIZATION ALGORITHM

There are many features in the dataset which are redundant and irrelevant which leads to worsen the output of the learning algorithm then create an over fitting problem. These redundant features Detroit the accuracy and the computation time complexity of algorithm. The feature selection consist of many steps such as:

Malware detection Methods	Advantages	Disadvantages
Signature-based [10]	Less true positive, can detect only malware which belong to same family	Many false Positive
Behaviour-bases [11]	Many true positive, Can detect new malware	High false positive, difficult to group the behaviour as malicious and normal
Heuristic-based [12]	Gives more True positive because uses static and dynamic analysis	Moderate false positive because obfuscated by metamorphic techniques
Model checking-based [13]	Less true positive, can detect only malware which belong to same family	Many false positive, can't detect new malware
Deep learning-based [14]	More true positive, reduce feature space	Less false negative
Cloud based [15]	More true negative, because of bigger malware database and intensive computational resources	Less false negative, due to real-time monitoring
Mobile based [16]	More true positive, can detect new and old malware	False positive, Cannot detect complex malware
Iot based model [17]	More true positive, can detect new and old malware	False positive, can't detect complex malware

Table 3: Advantage and disadvantage of malware detection

1. Procedure Generation: subset of features is generated, then search strategy is applied to obtain the promising candidate feature subset.
2. Strategy of Evolution: In order to find the best feature subset out of candidate feature subset, we have to determine the goodness of the each feature.
3. Criterion for stopping: stopping criteria is always determined
4. Procedure validation: It is used for validation of subset of features

Feature selection provide following benefit such as:

It reduce training and resource usage time

It reduce storage requirement

It improve prediction performance

From the perspective of the gradient information the optimization methods are further classified as:-

1. First order optimization
2. Second order optimization
3. Heuristic derivative –free optimization

First order optimization is also called stochastic gradient method and its variant, it is also known as black box optimization. Its common algorithms are gradient descent, stochastic gradient descent, nesterov accelerated gradient descent, stochastic variances reduction gradient etc. and second Order optimization or higher order optimization converges at a faster speed, drawback of this method is operation and storage increases. As the output of a black-box or second order optimization that does not provide derivative information, the method in which objective function is defined by a deterministic black box which handles the different types of constraints removes the drawback of the first order and second order is known as heuristic derivative free optimization.[10].Earlier, due to incessant use of data mining techniques false positive rates are also incessant in the output which leads to the indispensable detection of malware, for the improvement

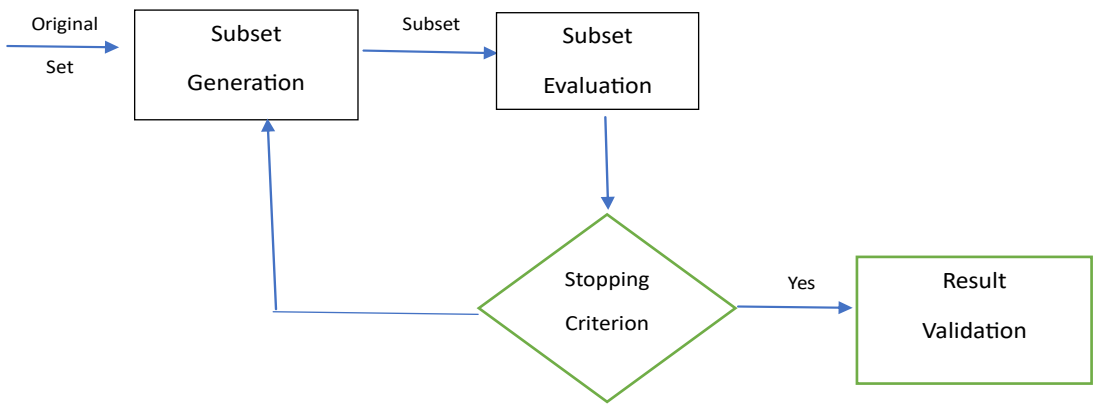


Figure 3: Feature selection steps [10]

of detection a introduce a novel model for discovering knowledge-based databases, enhancing Apriori association rule mining through the integration of particle swarm optimization (PSO) into the Apriori algorithm. Examples of optimization algorithms in the context of the traveling salesman problem are also provided. by Olawale surajudeen Adebayo et.al [19].

Statement: finding the shortest path

Solution: Optimization solution for travelling salesman problem

Decision variable: binary vector based on whether the trip exits or not.

Objective: Minimize the distance travelled.

Constraint: each stop on only two trips.

Conclusion in the form of workflow:

4. Related Work

In 2018,zhihuacui,feixue ,xingjuancaiet al Introduced an innovative technique employing a deep learning approach to identify malware variants, wherein malicious code is transformed into a gray scale image then CNN algorithm is used for identification and classification that automatically extract the features of the malware images and Utilizing a bat algorithm to tackle the data imbalance within diverse malware families.

Accuracy: 94.5%

Dataset: 9342 binary imageof25 malware families

Advantages: 1) detection speed of model is faster

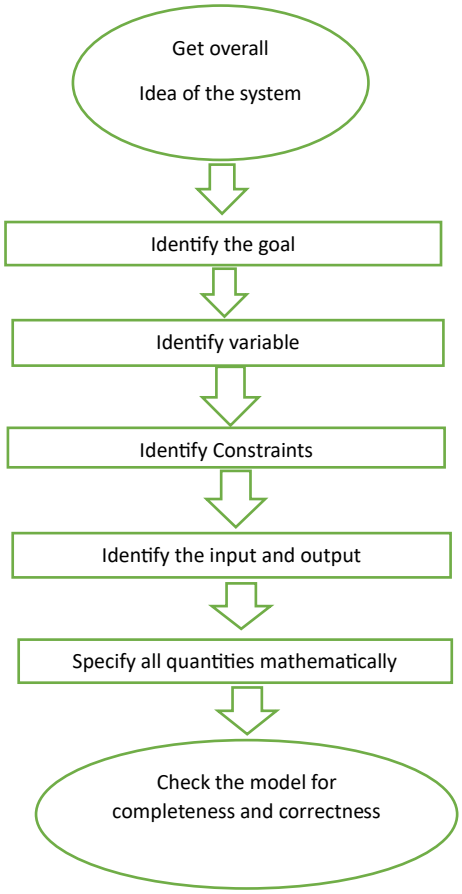


Figure 4: Steps in optimization modelling

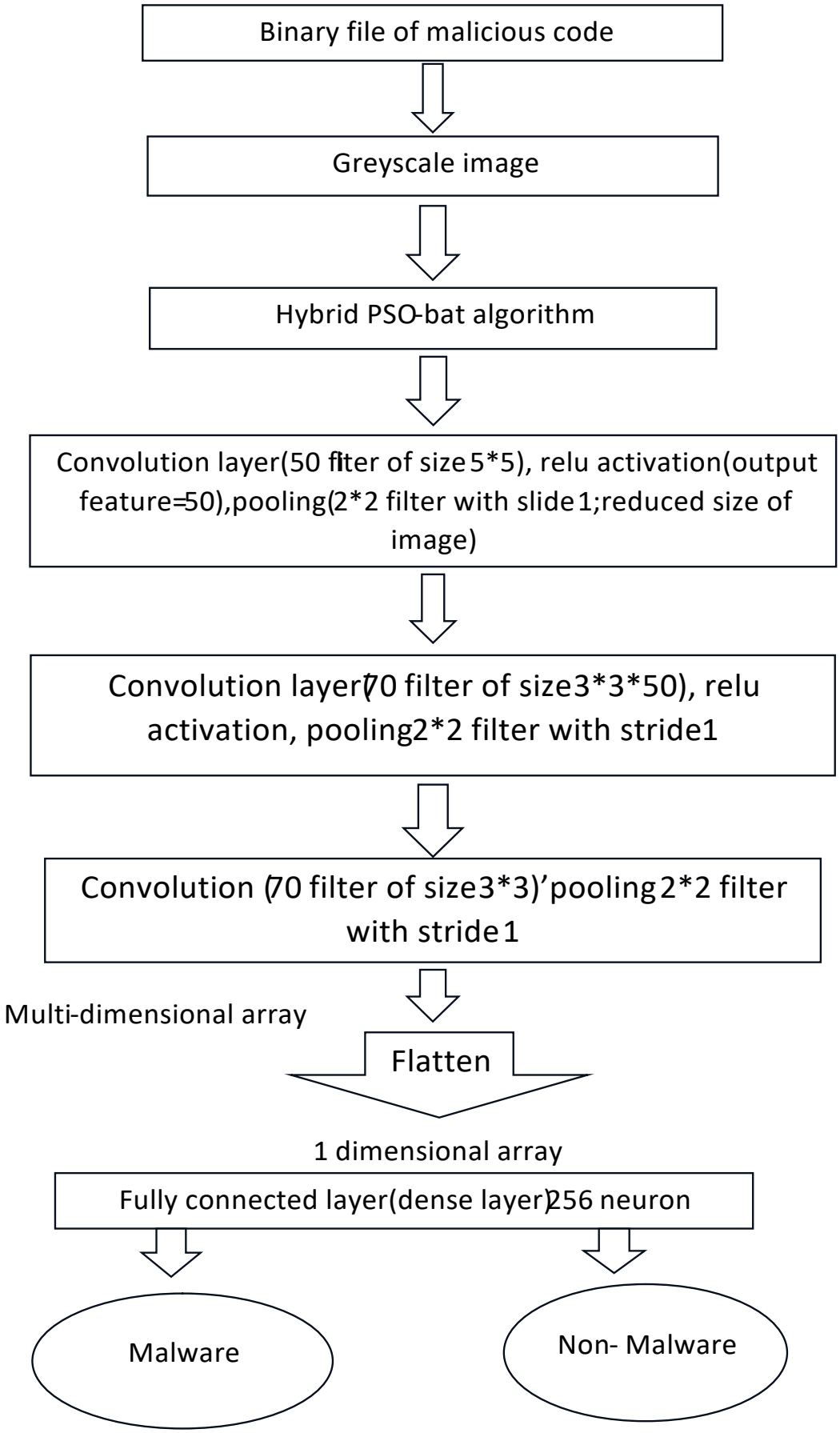


Figure 5: Malware detection with PSO-Bat optimization

2) Provide effective result for the data imbalance among different malicious families

Disadvantages: require all input images of fixed size which limit the model

Optimation algorithm: Bat algorithm

Improvement: 1) spp-net(spatial pyramid pooling layer) extract features at variable scale

2)Transforming the malicious code into colour images

In 2019,Pengzhang, bowen sun et.al proposed a novel malware detection method which remove the drawback of the previous method by enhancing traditional greyscale image into RGB image and then put the image into vgg-16, then used SPP- NET to remove the fixed size problem.

Accuracy: 95.5%

Dataset: 1000 windows platform PE malware Advantages: gives output in RGB form Disadvantage: time complexity increases

Improvement: optimization algorithms can be used for better feature selection [22] Meenu Ganesh,priyanka pednekaret.al proposed cnn-based learning model extract the pattern of malware detection rather than extracting signature

Dataset: 144 android permissions, where the activation of individual permission is represented by 0 and 1 (2500 android application, 200 malicious and 500 no-malicious)

Accuracy:93%

[23] Daniel Gibert,carlesmater et.al proposed a convolutional neural network for classification of malicious code which is represented by images and then developed Proposing a file-agnostic deep learning approach for effectively categorizing malware, wherein malicious software is grouped into similarities based on unique patterns obtained from visualizing them as images.

Dataset: malign dataset and Microsoft malware classification

[24] Xin-she yang had given a review and application about the bat algorithm that is efficient algorithm in three key points/features: frequency tuning, automatic zooming and parameter control.

Tien-szu pan proposed a hybrid particle swarm optimization with bat algorithm, in this several worst individuals of particles in PSO will be replaced with the best individual particle in bat algorithm after running some fixed iterations, and vice-versa i.eworst poorer individual of Bat algorithm will be replaced with the finest particle of PSO.

5. PROPOSED MODEL

To remove the drawback such as time complexity and space complexity ,by keeping the above parameter in the view we proposed a model which used hybrid PSO-Bat algorithm as optimization algorithm for better selection of features from binary dataset from 9,342 greyscale images of 25 malware families, the following flow work presents the proposed model:

6. CONCLUSION

This work, presented as thorough view of malware detecting utilizing deep learning on various platforms. This review paper uncover the various optimization techniques and its comparison and tries to cover the gap between the existing detection techniques and this novel technique. The review showed that how the existing optimization algorithms work with deep learning and machine learning approach, by keeping these optimization algorithm in the view we choose two optimization i.e PSO and Bat algorithm for best feature selection, then the optimized output is fed to the CNN algorithm which increase the accuracy rate by two to three percentage with the reduction of time complexity.

References

1. P. Faruki et al., "Android Security: A Survey of Issues, Malware Penetration, and Defenses," in IEEE Communications Surveys & Tutorials, vol. 17, no. 2, pp. 998-1022, Secondquarter 2015, doi: 10.1109/COMST.2014.2386139.
2. Ö. A. Aslanand R. Samet, "A Comprehensive Review on Malware Detection Approaches," in IEEE Access, vol. 8, pp. 6249-6271, 2020, doi: 10.1109/ACCESS.2019.2963724.
3. P.V. Shijo, A. Salim,"Integrated Static and Dynamic Analysis for Malware Detection,"Procedia Computer Science,Volume 46,2015,Pages 804-811,
4. S. Akcay, M. E. Kundegorski, C. G. Willcocks and T. P. Breckon, "Using Deep Convolutional Neural Network Architectures for Object Classification and Detection Within X-Ray Baggage Security Imagery," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 9, pp. 2203- 2215, Sept. 2018, doi:10.1109/TIFS.2018.2812196.
5. R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran and S. Venkatraman, "Robust Intelligent Malware Detection Using Deep Learning," in IEEE Access, vol. 7, pp. 46717-46738, 2019, doi: 10.1109/ACCESS.2019.2906934.
6. Souri,A.,Hosseini,R.Astate-of-the-artsurveyofmalwaredetection approaches using data mining techniques. Hum. Cent. Comput. Inf. Sci. 8, 3 (2018). https://doi.org/10.1186/s13673-018-0125-x
7. Feizollah, Ali &Anuar, Nor&Salleh, Rosli& Wahid, Ainuddin. (2015). A review on feature selection in mobile malware detection. Digital Investigation. 3.22–37.10.1016/j.diin.2015.02.001.
8. K. He and D. Kim, "Malware Detection with Malware Images using Deep Learning Techniques," 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering

(TrustCom/BigDataSE), Rotorua, New Zealand, 2019, pp. 95- 102, doi: 10.1109/TrustCom/BigDataSE.2019.00022.

9. Tiwari, S., Singh, B. & Kaur, M. An approach for feature selection using local searching and global optimization techniques. Neural Comput&Applic28, 2915–2930 (2017). https://doi.org/10.1007/s00521-017-2959- y
10. Nath H.V., MehtreB.M. (2014) Static Malware Analysis Using Machine Learning Methods. In: Martínez Pérez G., ThampiS.M., Ko R., Shu L. (eds) Recent Trends in Computer Networks and Distributed Systems Security. SNDS 2014. Communications in Computer and Information Science, vol 420. Springer, Berlin,Heidelberg.
11. Galal, Hisham. (2015). Behavior-based features model for malware detection. Journal of Computer Virology and Hacking Techniques. 12. 10.1007/s11416-015-0244-0.
12. P. Khodamoradi, M. Fazlali, F. Mardukhi and M. Nosrati, "Heuristic metamorphic malware detection based on statistics of assembly instructions using classification algorithms," 2015 18th CSI International Symposium on Computer Architecture and Digital Systems (CADS), Tehran, Iran, 2015, pp. 1-6, doi:10.1109/CADS.2015.7377792.
13. Song F., TouiliT. (2012) Efficient Malware Detection Using Model-Checking. In: Giannakopoulou D., Méry D. (eds) FM 2012: Formal Methods. FM 2012. Lecture Notes in Computer Science, vol 7436. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-32759-9_34

Blockchain and IOT Based Secure Future City Architecture

Dinesh Singh
Department of Computer Application,
Technical Education & Research Institute, Ghazipur, Uttar Pradesh, India-233001
singhdinesh8888@gmail.com

Abstract

Internet of Things (IOT) is the most significant revolutionary technology of this time. Because of the large volume and centralized architecture of IOT networks, privacy and security remain a major concern. On the other hand block chain based methods provide decentralized protection and privacy. IOT and smart city technology developers can now create different forms of unified communications, data applications and solutions. This article analyzes the Internet of Things protection technologies by incorporating block chain IOT applications. To address both cryptographic security and privacy concerns, the proposed IOT-based smart city architecture uses BC technologies. Furthermore, BC has a very low overhead on the IOT network. The new system is a block chain based fully distributed access management framework for IOT. This article discusses the similarities and differences between block chain and IOT technologies, as well as a general reference framework that can be used to build a variety of block chain based community IOT applications.

Keywords: Machine Learning, Smart Healthcare, Smart Home, Wireless Sensor Networks, Smart City.

1. Introduction

Internet of Things is the developmental innovation that has filled in ubiquity in science and designing applications to tackle difficulties without the requirement for human impedance. IOT has brought the digital and physical worlds closer together by giving objects cognitive sense so that they can better help us. The Internet of Things (IOT) has been integrated into a variety of industries to provide a more cognitive framework for providing personalized applications to consumers and improving their overall experience.

Inventing a feature or a new application with characteristics similar to block chain, which would reduce power consumption and processing time, may be a future research recommendation for block chain and IOT. Other potential projects include determining the most cost-effective approach to use block chain based safety clarifications and developing a mechanism to ensure the safety and secrecy of applications in Block chain.

The decentralization offered by block chain and decentralized ledger technologies allows IOT and smart city application developers to use this technology, especially in multi-stakeholder deployments. Actual IOT implementations are becoming more complex, relying on software and hardware technology that is shared and operated by a variety of organizations and stakeholders. To allow IOT system owners and application developers to collaborate with third-party IOT service and data providers in multi-stakeholder implementations, trust, protection, and privacy must be guaranteed. As a result, future IOT apps and implementations will focus on a variety of third-party platforms for connectivity, processing, storage, and computing, while also receiving a financial reward for exchanging their data with other device developers.

Table 1 summarizes some recent literature analyses and studies. First, we discuss the basics of block chain's layout and terms. We present the latest research developments in each of the associated with future city, as well as promising smart block chain applications in these sectors.

We introduce a new framework for handling IOT devices in this paper. The architecture connects geographically dispersed sensor networks to a decentralized access control scheme. The solution is built on block chain technologies, and it enforces access control policies.

Since we have presented a comprehensive overview of IOT and block chain, as well as the need to combine all of these innovations, the above description of the contributions of this paper compared to other literature can be illustrated.

Own approach distinguishes itself from others by employing a distinctive structures that avoids integrating block chain technologies into IOT devices .This improves our solution's usability in a wide range of IOT situations with minimal functionality.

Year	Ref.	Technology Approach	Focus
2018	[1]	Block chain	Issues and suggestions for building block chain based IoT applications
2018	[2]	Block chain and Bit coin	Current Bit coin confidentiality concerns and privacy-related risks to Bit coin users, as well as an examination of current privacy-preserving solutions
2018	[3]	Block chain and IOT	IoT encryption and privacy technologies focused on block chain
2019	[4]	Block chain and AI	Compile a list of new block chain technologies, platforms, and protocols aimed specifically at the AI sector.
2019	[5]	Block chain and Automobile	Analyzes the huge promise of block chain technology in the automobile industry, focusing on its security capabilities.
2019	[6]	Block chain	Applicability of block chain in smart cities

Table 1. Recent literature analyses.

2. Background

In this part, we initiate some challenges in IOT and block chain integrated IOT technology.

2.1. Challenges in IOT

The Internet's growing availability has increased global knowledge sharing. Knowledge about our planet and climate may be collected at a far higher granularity using a network of inexpensive sensors and interconnected stuff. IOT not only saves time and resources, but it also achieves automation, which is the most important factor in today's technology environment, where all operations can be completed without human intervention while improving service quality. The software portion of IOT assists in data processing and decision-making, while a user interface allows users to communicate with the system. IOT systems are just the technology that links everything in an IOT environment, allowing for connectivity, data flow, device management, encryption, authentication, and application features. The research group is paying attention to IOT privacy and security. IOT Systems solutions use a centralized brokered networking system, in which all data is stored in a single location, such as a cloud server. To address these issues, Block chain is one of the

most popular technologies that incorporates all of these features into its architecture and can thus be used to secure IOT networks. The network architecture is shown in Fig. 1

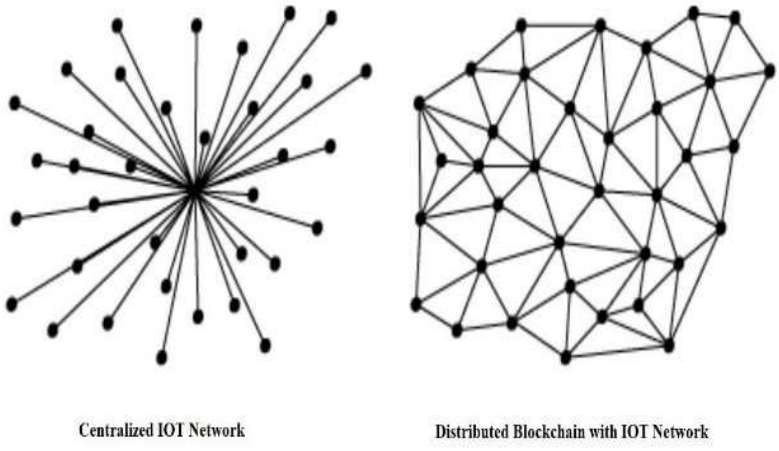


Figure 1. Network in block chain integrated IOT technology

2.2. Block chain integrated IOT Technology

Block chain is a ledger based technology that can be used in a variety of applications. It was first adopted in 2008 as the foundation for the crypto currency Bit coin. Over the years, several block chain applications have been created to execute situations other than crypto currencies. BC enables IOT systems to coordinate the processing of transactions between devices.

The BC's main objective is to liberate people from the confidence we are now obliged to place in intermediaries who govern and "manage" a large portion of citizens' lives. Several methods, as well as security and cryptographic functions, have been used to accomplish this goal. The block chain functions as a decentralized database system built on agreement instruction, enabling the shifting of standards among components. BC would improve the privacy and dependability of IOT systems by making them more robust. Everyone can transact on the BC since it is a network without controllers and organizations rely solely on the quality of the cryptographic algorithms that govern the operation. A permissioned BC restricts the actors who can engage in the system state consensus. Anyone can join the network, engage in the block verification process to reach a consensus, and build smart contracts using permissionless BC. The BC's decentralization is what makes it secure and distributed; however, it enables any central entity to be eliminated. Although, when combined with IOT, blockchain technology has the potential to overcome IOT's privacy and reliability concerns.

3. Analyzing the territory of (BC) applications

The part will focus on some of the majority common block chain application attributes in future cities, identified by the compositions as shown in figure 2. These block chain applications are described below

3.1. Smart Healthcare

A block chain-enabled healthcare infrastructure, according to Kundu et al. maintains the accuracy and interoperability of medical health data, enhances the consistency of insurance claim adjudication, and provides high-quality patient-centric facilities [7]. The number of medical data shared between healthcare providers and insurance companies has increased dramatically in recent years [8]. This insurance industry has aided in the creation of data-driven healthcare models [9]. Healthcare services operate with substantial quantity of individual data, necessitating rigorous security and control access , ensuring a high level of protection and authorized entry [10]. Block chain technology addresses concerns related to safeguarding data, ensuring privacy, and establishing liability in the realm of intelligent healthcare. It assists in consolidating and securing clinical data, capitalizing on health information for scientific objectives, and easing the way in and transfer of patient medical logs. [11]. This progress empowers physicians to quickly retrieve medical records, potentially detecting early indications of serious illnesses and preserving lives. As the unfortunate incidents around COVID-19 have shown, this is particularly critical in places of high population density. Block chain's collaboration features will also help streamline healthcare operations, monitor COVID-19 patients, and reduce hospital overcrowding. BC technology contains the capacity to be immensely helpful in ensuring trustworthy and accurate data, allowing big-data innovations to reach their maximum potential and develop innovative solutions focused on healthcare data. This is possible because smart cities will use technologies to modernise their healthcare infrastructure and develop more agile delivery networks.

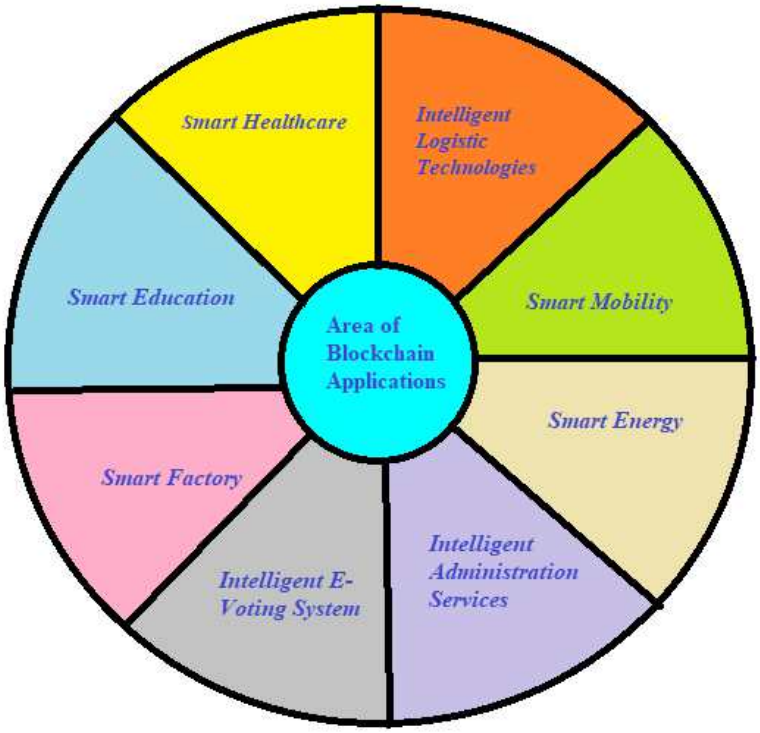


Figure 2. Area of block chain applications

3.2. Intelligent Logistic Technologies

Smart factories highlight the production aspect and will be discussed in a later segment, are also deeply intertwined with smart logistics [12]. The scope of logistics and supply-chain operations has expanded over time, encompassing various practices and fields of complex value chains [13]. Most supply chains, according to Christopher and Holweg [14], lack versatility and the potential to easily respond to evolving demand and environmental circumstances. It will make coordination and knowledge sharing between the various parties involved in logistics processes easier [13]. A highly observable supply chain is a good way to reduce knowledge asymmetry, uncertainties, and organizational inefficiencies in smart cities [15]. As per Aggarwal et al. Block chain is an important method for document synchronization, faster customs clearance, approvals, and processing time reduction in the logistics industry [15]. Block chain helps smart city growth by improving the efficiency of supply chains and the quality and traceability of goods during their manufacturing and usage cycles. Similarly, block chain technology enables smart city residents to monitor and trace the origins of their goods and services, increasing customer loyalty and confidence [16].

3.3. Smart Mobility

Smart mobility increases the accessibility and affordability of new and environmentally friendly transportation services. Smart mobility, according to Chun and Lee [17], will contribute to a more inclusive and safer future public transit system, thanks to smart technology. Smart mobility necessitates the implementation of cost-effective, environmentally friendly, and sustainable public transportation. City planners incorporating blockchain aim to create a streamlined transit network, enabling individuals to directly access and pay for solutions. The effectiveness of public equivalents passage can be enhanced through block chain-based smart mobility systems. Additionally, these systems provide flexibility in insurance rates based on driver activity and enhance accessibility to car-sharing programs [18]. Residents in smart cities stand to gain easier access to public transit, reduced travel times, and heightened safety through the implementation of block chain technologies.. Smart vehicles can keep track of their records, communicate with home automation, and conduct secure banking transactions using crypto currencies, such as automatic charging time payment [18]. Public transit services and private mobility providers can use block chain technologies to minimize emissions, lower costs, boost sales, and improve customer loyalty.

3.4. Smart Energy

The core objective of implementing smart energy is to assure the utilization of renewable, cost-effective, and efficient energy sources. If the demand for smart energy increases, block chain technology has the potential to enhance the resilience of the entire energy market. Block chain enables individuals and consumers to monitor their real-time energy consumption and distribution. It also plays a pivotal role in advancing clean energy goals by improving green energy trading and providing a secure platform for individuals to market their surplus green energy.

In return, this backs governments in providing incentives such as discounts and tax reductions to renewable energy providers. Furthermore, block chain enables more efficient control of energy exchange requirements for households and businesses, diminishing response times and improving transaction security. [19]. As highlighted by Park et al., the incorporation of block chain-based energy labels in contractual transactions can directly connect various energy sources. [20]. According to a recent report by Aggarwal et al., block chain proves beneficial in managing electricity transition and storage in the smart grid, bringing greater transparency to energy transactions [21].

3.5. Intelligent Administration Services

Incorporating block chain technologies into public service networks has the ability to broaden the reach of public service systems [22]. The technological facets of technology will ensure greater privacy and protection, boosting smart citizens' trust and promoting their involvement and engagement in public services. França et al. [23] recommend that block chain be used to enhance solid waste collection in small Brazilian municipalities. Marsal-Llacuna [24] performed a related analysis to investigate the potential of blockchain as a decentralized and bottom-up distribution system for urban governance. Block chain has the potential to be an effective platform for advancing civic agendas, enhancing compatibility, and maintaining the benefits of public service delivery. The implementation of technology in government could lower the barriers to smart people using its electronic services. Block chain technology enables smart cities' public governance to be more efficient and transparent, and it has the ability to boost community interest in government. Block chain has the potential to allow the government to provide people with more customized services while still increasing transparency.

3.6. Intelligent E-Voting System

The value of governments' ability to have ease, transparency, and transparency in democratic elections is shown by an increasing body of scholarly studies on e-voting. Many countries have recognized a pressing need for governments to go digitally and introduce e-voting in elections. The strong security capabilities of block chain, as well as its ability to efficiently store votes and increase election transparency, are core advantages of the system in e-voting processes. COVID-19 has shown that in periods during pandemics, public access to secure e-voting processes can be vital to preserving both public health and democratic processes. Li et al. suggest that block chain-based e-voting technologies can boost voting performance in terms of time and expense [22]. Since smart people will exercise their right to vote independently of their geographical position, block chain helps smart-city administrations to save money when building election infrastructure. Block chain technology allows the democratic process to be more open and avoids efforts to exploit voting records, which increases voter participation. Block chain technologies can help residents of smart

cities engage and trust in public decision-making processes. In smart cities, block chain technology will allow e-voting, which enhances efficiency, lowers costs, and guarantees a fair and inclusive voting process.

3.7. Smart Factory

Cyber attacks, industrial espionage, and faulty production data will all be made worse by working in smart factories. Any IOT system and machinery used in smart factories will benefit from block chain's decentralised administration, governance, and tracking. Several plants, for example, continue to suffer sudden breakdowns, workflow delays, and planned and unscheduled repairs. The ability to process large volumes of data, according to Wildemann and Hojak [25], is critical to the success of smart factories. According to Mistry et al. [26], block chain may assist manufacturing applications in running more effectively and rapidly over insecure networks, as well as allow faster data delivery and stable industrial automation. Factory workers may focus on controlling production processes thanks to block chain, which simplifies automated workflows and service distribution across industrial IoT devices. The use of block chain technologies in conjunction with smart-factory equipment allows for more automated and autonomous manufacturing processes. By establishing safe and stable production processes, block chain technology will serve as the foundation for smart factories in smart cities. Automated workflows would benefit from smart factories focused on blockchain technologies, resulting in improved efficiency and effectiveness of operations.

3.8. Smart Home

Smart homes represent the increasing introduction and incorporation of a range of emerging innovations into home networks for the purpose of improving the quality of life. According to Apthorpe et al. the widespread use of IoT systems in smart homes raises privacy threats [27]. Smart homes have benefited immensely from Internet of Things (IoT) technology and Internet appliances. According to Edwards and Grinter smart home manufacturers face a range of obstacles in the implementation of smart-home applications, including a lack of customer knowledge and device accountability [28]. According to Ferdous et al. blockchain can help with confidence and traceability in smart homes [29]. Blockchain has the power to address the issue of smart-home entity interoperability. Park et al. emphasize the importance of blockchain in fostering smart home connectivity, improving automated energy sharing operations in smart homes, and encouraging more efficient practises within smart homes and inside smart cities [30]. People in smart cities reside in smart homes and utilize blockchain technologies to secure their safety and data sovereignty. By allowing interoperable networks to connect and share data, blockchain technology aids the construction of smart homes.

3.9. Smart Education

In terms of local growth and convergence between academic institutions and smart cities, the quality and feasibility of smart cities are based on education and the quality of schools. According to Zhou and Hu the protection of academic information systems is a crucial factor that limits the efficiency of information systems and has a significant impact on resource management and conversion [31]. The smartness of its people, their ability to learn and obtain higher education degrees [32], and their readiness to embrace emerging technology are all essential characteristics of a smart community. For managing large volumes of educational records, block chain technology offers a highly secure design [33]. Higher education frameworks can be transformed into long-term learning networks using block chain technology [34]. The adoption of a decentralized and stable university management framework is often seen as crucial to enhancing educational resource usage. Block chain technology eases questions about security problems present in the educational system by building a data-secure ecosystem inside smart cities. Although several jurisdictions have adopted laws and regulations for the governance and management of educational data, they struggle to resolve security issues about the illegal storage and use of students' sensitive data [35]. Higher standards of data protection would help students because they would be able to make more educated educational choices because block chain avoids malicious attacks and data leakage [36]. Smart education is facilitated by block chain technology, which offers a forum for the safe and permanent documentation of personal accomplishments.

4. Blockchain integrated IOT technology architecture

The architecture described in this paper is new. A copy of the block chain must be present on each node in a block chain network. In a decentralized access management scheme, access control information is processed and transmitted using block chain technologies.

A single smart contract determines all of the activities permitted in the access control system as part of the solution. We go over the various components of the architecture in greater depth. Figure 3 depicts the data flow architecture of our system. The architecture can be broken down into its parts.

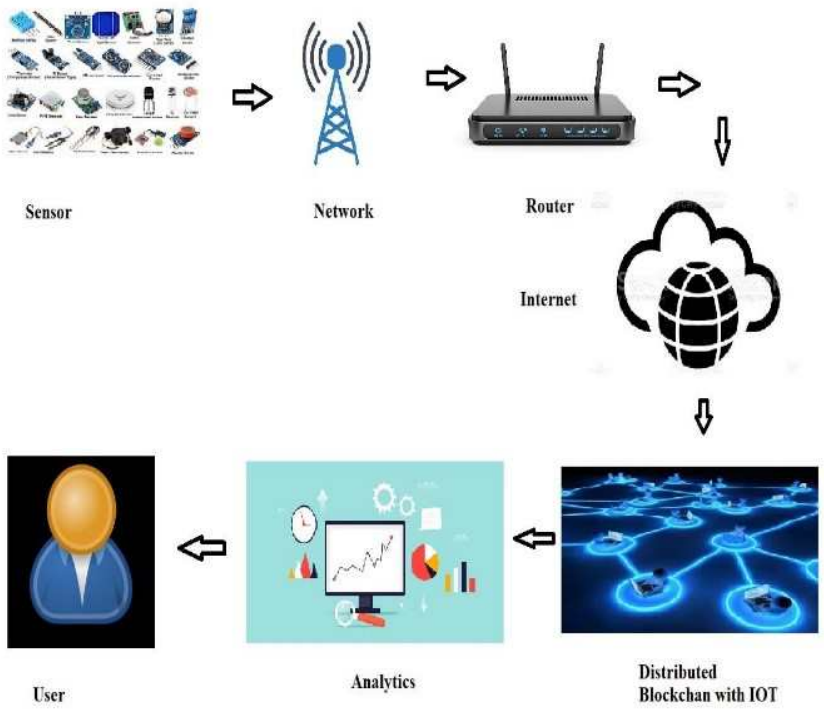


Figure 3. Data flow architecture in Block chain integrated IOT architecture

4.1. Wireless Sensor Networks

Wireless Sensor Networks allows for connectivity in low-power and low-light applications. The computing power, memory, and/or energy availability of IOT devices in the wireless sensor network are constrained. One of the criteria of our architecture is that all devices in the block chain network must be uniquely identified worldwide. Using existing IOT cryptographic technologies, each device's public key would be generated automatically. Public key generators may be a viable solution to the problem of generating large, unique random numbers. As a result, implementing encryption connections would ensure that unique identifiers are maintained.

4.2. Managers

In our system, managers are referred to as "lightweight nodes." Constrained devices will become managers in the system without being hampered by their hardware constraints. Our method does not require a constant connection to the block chain network. IOT devices must be certified under the supervision of a manager. Every registered IOT device in the system must be assigned to at least one registered manager. Managers should create particular access control permissions for IoT devices that have been registered under their control.

4.3. Agent Node

The smart contract is deployed by a specific block chain node in the architecture. During the lifespan of the access control system, the smart contract is owned by the agent node. The agent node is a block chain node in our system that is responsible for deploying the system's only smart contract. All

nodes in the block chain network must be aware of the smart contract's address in order to communicate with it.

4.4. Smart Contract

This smart contract may be one and will never be removed from the system. Once a transaction has triggered an operation, the miners can keep the transaction's information internationally available. All of the access management system's activities are specified in the smart contract, which is caused by block chain transactions. Managers are the only institutions with the authority to communicate with the smart contract.

4.5. Block chain Network

We selected a private block chain because all of the prototype's components are more dimensioned, allowing us to evaluate the system with more confidence. A relevant block chain node in the architecture deploys the smart contract. The block chain interface should be used by nodes to store and access the access control policies of individual devices on a global scale. By accepting transactions and maintaining copies of the block chain, miners in the network help keep the network secure and stable.

4.6. Management Hubs

Management hub nodes are not allowed to be restricted to gadgets. Such devices must have high performance features in order to serve as many simultaneous requests from IoT devices as possible. To be a component of the block chain network entails maintaining a local copy of the block chain as well as keeping track of network transactions. A management hub node can be linked to multiple sensor networks, and multiple management hub nodes can be linked to the same block chain node. Once an IOT device is introduced to the system, the manager node of that device must inform the respective management hub node of the device's credentials and also the device's location of the management hub node.

The block chain with IOT application's architecture must be capable of handling the network's massive traffic while also ensuring data security and being resistant to threats and attacks. Lightweight, scalability, openness, mobility, accessibility, concurrency, and other features make it ideal for access control.

Challenge	Description
Scalability	This may result in centralization. The technology behind crypto currencies like Bit coin will be unveiled if it were centralized.
Storage facility	When compared to the ledger-based block chain technology, the storage

limitations	capacity necessary for sensors and actuators in the IoT ecosystem is very low.
Lack of workforce	When this technology is combined with the idea of IoT, the skilled force on this technology is highly limited.
Processing time	When these computing capacities vary, the time needed to perform encryption varies, resulting in processing time variations.
Differences in computing power	Because IOT systems are varied and linked over a large network, adding block chain technology to the mix makes things even more complicated.
Energy Efficiency	The supplier of power-based coercive equipment with batteries traditionally benefits BIOT endpoints. As a result, energy efficiency was critical for allowing long-term node placement.
Privacy	The anonymity was not accomplished because entire transactions were shared, allowing third parties to examine and classify these transactions and infer the identities of the participants.
Security	The key to maintaining secrecy for a personal user is flawless management of his or her own unique keys, so what the attacker wants to do with the public key is steal something from him or her or impersonate someone.
Adaptability	Application Programming Interfaces (APIs) can be as user-friendly as possible to make the work of block chain programmers simpler.

Table 2. Challenges in Block chain integrated IOT technology.

5. Discussion and Future Research

As a basis for new investigations, we summarize and coordinate previous research results. Most notably, each sector can be used as a springboard for more in-depth investigation. Though we consider our approach to be thorough at this time, new research fields could appear in the future. Our approach should not be regarded as a blueprint for determining the limits of current study, but rather as encouragement for other researchers to select one of the topics. The challenges in block chain integrated IOT technology are shown in Table. 2.

This is especially true when it comes to the scalability solutions that such architectures can offer. Including AI capability in data analytics could help smart cities reap the benefits of block chain technologies in fields like health care, administration, energy generation. The literature we reviewed focuses on block chain as a smart city engine, with little attention paid to the possible negative consequences of its implementation. With the use of block chain technology, new attack vectors and security compromises could emerge.

6. Conclusion

One of the solutions for resolving the concerns and problems of IOT has been listed as block chain technology. Block chain and IOT promise to achieve explosive growth in all areas of human society. The comprehensive characteristics of block chain and IOT promise to solve the majority of issues that companies are facing, particularly when adopting new and untested marketing strategies. The block chain and distributed ledger technologies have the ability to solve the privacy, scalability, trust, security problems that IOT and smart city applications encounter. While completed, the study will shed light on topics such as the contributions of these two innovations, as well as the problems that people and enterprises will face when transitioning business models, among other things. In this paper, the various IOT applications that can be combined with block chain technologies are discussed. This paper would provide a fundamental understanding of the need for block chain in the Internet of Things. It also explains the relationship between IOT and Block chain, as well as the motivation for their integration. This article presents a reference dataflow architecture for block chain based IOT applications, highlighting the key communication channels required to connect the IOT layer to the block chain layer. The benefits of combining IOT and Block chain have also been explored in order to entice researchers to participate and study more in this field.

Acknowledgement

This work did not obtain any particular grants from public, private or non-profit funding organizations.

References

1. T. M. Fernández-Caramés and P. Fraga-Lamas, ―A Review on the Use of Blockchain for the Internet of Things,‖ *IEEE Access*, vol. 6. Institute of Electrical and Electronics Engineers Inc., pp. 32979–33001, May 30, 2018, doi: 10.1109/ACCESS.2018.2842685.
2. M. Conti, K. E. Sandeep, C. Lal, and S. Ruj, ―A survey on security and privacy issues of bitcoin,‖ *IEEE Commun. Surv. Tutorials*, vol. 20, no. 4, pp. 3416–3452, Oct. 2018, doi: 10.1109/COMST.2018.2842460.
3. M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, ―Blockchain technologies for the internet of things: Research issues and challenges,‖ *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2188–2204, Apr. 2019, doi: 10.1109/JIOT.2018.2882794.
4. K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, ―Blockchain for AI: Review and open research challenges,‖ *IEEE Access*, vol. 7, pp. 10127–10149, 2019, doi: 10.1109/ACCESS.2018.2890507.

5. P. Fraga-Lamas and T. M. Fernández-Caramés, ―A Review on Blockchain Technologies for an Advanced and Cyber-Resilient Automotive Industry,‖ *IEEE Access*, vol. 7, pp. 17578–17598, 2019, doi: 10.1109/ACCESS.2019.2895302.
6. J. Xie *et al.*, ―A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges,‖ *IEEE Commun. Surv. Tutorials*, vol. 21, no. 3, pp. 2794–2830, Jul. 2019, doi: 10.1109/COMST.2019.2899617.
7. Kundu, D. Blockchain and trust in a smart city. Environ. Urban. ASIA 2019, 10, 31–43.
8. Demirkan, H. A smart healthcare systems framework. IT Prof. 2013, 15, 38–45.
9. Hu, Y.; Bai, G. A systematic literature review of cloud computing in eHealth. Health Inform. Int. J. 2014, 3, 11–20.
10. Muhammed, T.; Mehmood, R.; Albeshri, A.; Katib, I. UbeHealth: A personalized ubiquitous cloud and edge-enabled networked healthcare system for smart cities. IEEE Access 2018, 6, 32258–32285.
11. Sinclair, S. Spanish Researchers Working to Curb Coronavirus Spread with Blockchain App.Available online:https://in.finance.yahoo.com/news/spanish-researchers-working-curb-coronavirus-140007260.html (accessed on 26 June 2020).
12. Allam, Z.; Dhunny, Z.A. On big data, artificial intelligence and smart cities. Cities 2019, 89, 80–91.
13. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A decentralized privacy-preserving healthcare blockchain for IoT. Sensors 2019, 19, 326.
14. 8.Christopher, M.; Holweg, M. ―Supply Chain 2.0‖: Managing supply chains in the era of turbulence. Int. J. Phys. Distrib. Logist. Manag. 2011, 41, 63–82.
15. Aggarwal, S.; Chaudhary, R.; Aujla, G.S.; Kumar, N.; Choo, K.-K.R.; Zomaya, A.Y. Blockchain for smart communities: Applications, challenges and opportunities. J. Netw. Comput. Appl. 2019, 144, 13–48.
16. Ferdous, M.S.; Biswas, K.; Chowdhury, M.J.M.; Chowdhury, N.; Muthukkumarasamy, V. Chapter two—Integrated platforms for blockchain enablement. In Advances in Computers; Kim, S., Deka, G.C., Zhang, P., Eds.; Role of Blockchain Technology in IoT Applications; Academic Press: Cambridge, MA, USA, 2019; Volume 115, pp. 41–72.
17. Chun, B.-T.; Lee, S.-H. Review on ITS in Smart City. Adv. Sci. Technol. Lett. 2015, 98, 52–54.
18. Li, J.; Greenwood, D.; Kassem, M. Blockchain in the built environment and construction industry: Asystematic review, conceptual models and practical use cases. Autom. Constr. 2019, 102, 288–307.
19. Chaudhary, R.; Jindal, A.; Aujla, G.S.; Aggarwal, S.; Kumar, N.; Choo, K.-K.R. BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system. Comput. Secur. 2019, 85, 288–299.

20. Park, L.W.; Lee, S.; Chang, H. A sustainable home energy prosumer-chain methodology with energy tags over the blockchain. Sustainability 2018, 10, 658.
21. Aggarwal, S.; Chaudhary, R.; Aujla, G.S.; Kumar, N.; Choo, K.-K.R.; Zomaya, A.Y. Blockchain for smart communities: Applications, challenges and opportunities. J. Netw. Comput. Appl. 2019, 144, 13–48.
22. Li, J.; Greenwood, D.; Kassem, M. Blockchain in the built environment and construction industry: Asystematic review, conceptual models and practical use cases. Autom. Constr. 2019, 102, 288–307.
23. França, A.S.L.; Amato Neto, J.; Gonçalves, R.F.; Almeida, C.M.V.B. Proposing the use of blockchain to improve the solid waste management in small municipalities. J. Clean. Prod. 2020, 244, 118529.
24. Marsal-Llacuna, M.-L. Future living framework: Is blockchain the next enabling network? Technol. Forecast. Soc. Change 2018, 128, 226 234.
25. Wildemann, H.; Hojak, F. Main Di_erences and Commonalities Between the Aircraft and the AutomotiveIndustry. In Supply Chain Integration Challenges in Commercial Aerospace: A Comprehensive Perspective on the Aviation Value Chain; R ichter, K., Walther, J., Eds.; Springer International Publishing: Cham, Switzerland, 2017; pp. 119–138, ISBN 978-3-319-46155-7.
26. Mistry, I.; Tanwar, S.; Tyagi, S.; Kumar, N. Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges. Mech. Syst. Signal Process. 2020, 135, 106382.
27. Apthorpe, N.; Reisman, D.; Feamster, N. A smart home is no castle: Privacy vulnerabilities of encrypted IoT tra_c. arXiv2017, arXiv:1705.06805.
28. Edwards, W.K.; Grinter, R.E. At home with ubiquitous computing: Seven challenges. In Ubicomp 2001:Ubiquitous Computing; Abowd, G.D., Brumitt, B., Shafer, S., Eds.; Springer: Berlin/Heidelberg, Germany, 2001;pp. 256–272.
29. Ferdous, M.S.; Biswas, K.; Chowdhury, M.J.M.; Chowdhury, N.; Muthukkumarasamy, V. Chapter two—Integrated platforms for blockchain enablement. In Advances in Computers; Kim, S., Deka, G.C., Zhang, P., Eds.; Role of Blockchain Technology in IoT Applications; Academic Press: Cambridge, MA, USA, 2019; Volume 115, pp. 41 –72.
30. Park, L.W.; Lee, S.; Chang, H. A sustainable home energy prosumer-chain methodology with energy tags over the blockchain. Sustainability 2018, 10, 658.
31. Zhou, Z.; Hu, C. Research on the risk identification of academic information system based on the comprehensive weighting method. Inf. Sci. 2017, 8, 29.
32. Ortiz-Fournier, L.V.; Márquez, E.; Flores, F.R.; Rivera-Vázquez, J.C.; Colon, P.A. Integrating educational institutions to produce intellectual capital for sustainability in Caguas, Puerto Rico. Knowl. Manag. Res. Pract. 2017, 8, 203–215.

33. Fernandez-Carames, T.M.; Fraga-Lamas, P. Towards next generation teaching, learning, and context-aware applications for higher education: A review on blockchain, IoT, fog and edge computing enabled smart campuses and universities. Appl. Sci. 2019, 9, 4479.
34. Aamir, M.; Qureshi, R.; Khan, F.A.; Huzaifa, M. Blockchain based academic records verification in smart cities. Wirel. Pers. Commun. 2020, 113, 1397–1406.
35. Filvà, D.A.; García-Peñalvo, F.J.; Forment, M.A.; Escudero, D.F.; Casañ, M.J. Privacy and identity management in Learning Analytics processes with Blockchain. In Proceedings of the Sixth International Conference on Technological Ecosystems for Enhancing Multiculturality, Salamanca, Spain, 24–26 October 2018; Association for Computing Machinery: Salamanca, Spain, 2018; pp. 997–1003.
36. Ismail, L.; Materwala, H. A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions. Symmetry 2019, 11, 1198.

Image Fusion Techniques based on Optimization Algorithms: A Review

Ashish Dixit
Assistant Professor (CSE)
Ajay Kumar Garg Engineering College Ghaziabad.
ashishdixit1984@gmail.com

Abstract

In image processing applications, image fusion techniques gain popularity because they combine the most appropriate features of different source images in order to generate a single image that contains more information and is more beneficial. In this paper, initially, we have studied the analysed the conventional spatial and transform domain image fusion techniques. These techniques face numerous challenges, and to overcome them, optimization algorithms are deployed. These algorithms search for the optimal solution for the image fusion technique based on the objective function. Therefore, the main focus of this paper is to study and analyse the optimization algorithms based on various factors.

Keywords: Image Fusion, PSO(particle swarm optimization), YSGA(Yellow Saddle Goatfish Algorithm)..

1. Introduction

Image fusion is a technique in which two or more data sets of a related observation are combined to produce a composite result that possesses the salient characteristic of each component. Image Fusion [1] is a process of combining multi sensory, multi temporal and/or multi view images into a single high quality image. The fused image contains more spatial, temporal and spectral Information than any of the input images, thereby increasing the utility application of the image. It is a process of integrating all relevant information of the individual images while rejecting all redundant information. The main requirement of this process is that it should preserve all significant features of the input images, while ensuring that no artifacts are introduced into the fused image The images to be fused together may be acquired through different sensors or at different times or may have different spatial and spectral characteristics. It is a process which retains the most desirable information of each individual image. In the literature, images are processed in the spatial and frequency domains [6]. The image pixels are directly processed in the spatial domain. On the other side, image pixels are transformed into frequency domain. After that, frequency domain coefficients are fused and inverse transform is taken to obtain final fused image in the output. However, spatial domain produces spatial distortion in the fused images [6]. Therefore, frequency domain is more preferred in the image fusion methods. However, it faces shift invariance issue [7]. To overcome this issue, we have explored various optimization algorithms. These algorithms are deployed for determine the optimal weight values of coefficients that used for fusion purposes. The most preferred optimization algorithms are bat algorithm [8], genetic algorithm (GA) [9-10], particle swarm optimization (PSO) [11], grasshopper optimization (GO) [12], grey wolf optimization (GWO) [13] and hybrid combination of optimization algorithms. The exploration and exploitation rate defines how optimization algorithm superior over others. However, hybridization increases the algorithm complexity in terms of computational time. Therefore, we have explored other optimization algorithms that provide better exploration and exploitation rate. We have found in the literature, Yellow Saddle Goatfish (YSG) algorithm [14]. This algor ithm is based on the hunting behaviour of yellow saddle goatfish to capture prey. Today, image fusion is being used in a wide range of applications, such as, in remote sensing, in medical imaging, in robotics, in micro-scopic imaging, in analysis of images from satellite, in military, in surveillance and in computer vision.

2. Different Image Fusion Techniques

Image fusion techniques can be categorized into three categories [5]. These are Pixel level algorithms (Low level Image Fusion): Pixel based algorithms considers correspondence between

pixels in the input images. In this method, information regarding each pixel obtained from a group of pixels in input images. Pixel level algorithms work either in spatial domain or in the transform domain. The pixels value is directly manipulated in spatial domain. In the transform domain, image is first transferred into frequency domain using Fourier Transform. All fusion operations are performed in frequency domain. The inverse Fourier transform finally gives the fused image.

Feature level algorithms (Mid level Image Fusion):

Feature based algorithms divides the images into regions and fuses the regions based on salient features such as edges, textures etc. These algorithms are less sensitive to noise introduced at signal level.

Decision level algorithms (High level Image Fusion):

Decision level based algorithms combine image descriptions for fusion. In formation extracted from input images are combined according to decision rules resulting in common interpretation.

3. Literature Review

In this section, we have studied and analyzed the existing image fusion methods are designed in the literature.

AsanIhsan Abas, Nurdan Akhan Baykan [8], Image capturing equipment have a narrow field of view. In other words, a single photograph may capture a variety of sharply focused objects at various distances from one other. Multiple objects may be captured in one picture by merging data from 2 or more separate photographs, which is what is meant by the term "image fusion." As an alternative to the usual MST Transform, Bat Algorithm (BA) multi-focus image fusion is provided in this study to address the limitations of the standard convolution. The first step is to conduct a particular MST (Laplacian Pyramid or Curvelet Transform) on the two source pictures to get their low-pass and high-pass regions. Optimization techniques were then employed to discover the best weights for coefficients in low-pass regions to increase the fusion picture's accuracy, and lastly, the fused multi-focus picture is recreated using the Inverse MST. Image fusion algorithms' performance is evaluated utilizing reference and non-reference assessment metrics in the experimental evidence.

S. Kavitha and K.K. Thyagharajan [9], It is the goal of this research project to develop an algorithm for the fusion of multimodal medical (brain) images and to increase their quality in terms of information (informational content), contrast (edge contrast), and edge quality, even without loss of information or false information. Additionally, the source picture that adds the most detail to the merged image should be easy to locate, ideally with a less amount of search space. For optimum parameter estimation and fusion, wavelet and genetic algorithm (GA) are used in conjunction. An algorithm is used to breakdown the source pictures using wavelet (DWT/UDWT) and extract the

genetic functions from each area. No matter how big or small a picture becomes, the number of attributes stays the same. The appropriate weight value for each source picture is determined using the genetic function, and the fusion procedure is then completed. A feature recovered after decomposition eliminates unpredictability in the selection of the beginning population when MSE is employed as a fitness criterion. Also, the UDWT, DWT, DWT-GA, and UDWT-GA fusion pictures are assessed using subjective and objective criteria for each of the fusion approaches (QI, IE, MI, PSNR, RMSE, SF)

Huang,B.,Yang[15],2020hasbeendiscussedanoverviewofmultimodalmedical image fusion methods. In this paper Author compare image fusion from three aspects, based on spatial domain, transform domain, and based on deep learning. In Spatial domain fusion produces spectral distortion of fused images, in transform domain-based fusion has the advantages of good structure and avoiding distortion, but also generates noise during the fusion processing. Deep learning has improved the effect of fusion, but also has some defects; like the framework of deep learning is single, the amount of data for training is small, consist of high, training of deep learning is time-consuming, which requires high requirements for computer hardware configuration. In this paper research hotspot is the fusion of two modes like fusion of MRI/CT,MRI/PET, and MRI/SPECT.

Ebenezer Daniel [13], Optimum Homomorphic Wavelet Fusion (OHWF) for multi-modal medical image fusion has been proposed in this study. Here, the benefits of both the homomorphic filter and the wavelet transform are combined into a single picture frame for easy implementation. By merging anatomical and functional data utilizing multi-level decomposition, the suggested approach improves the quality of fusion. A series of images from the database were merged using MR-PET, MR-SPECT, MR T1-T2, and MR-CT modal fusion techniques that researchers developed in-house here. Hybrid Genetic-Grey Wolf Optimization is used to choose the best scale values (HG-GWO). HG-GWO uses a genetic algorithm to choose the random control parameters that are best for the experiment. This technique's MI, QAB/F STD, and Entropy metrics are compared to those of other fusion methods for the purposes of performance evaluation. Compared to other state-of-the-art enhancement techniques, their proposed method yields better results.

Shaik Shehanaz, Enenezer Daniel and Sivaji Satrasupalli [16], (2021) proposed an optimum weighted average fusion (OWAF) methods using PSO for multimodal medical image fusion to improve the performance of fusion. In this approach DWT method is used for decomposition of input multiple modalities in to various Sub groups. The resultant energy bands were weighted using optimum weights, attained using particle swarm optimization algorithm(PSO). This approach was tested over MRI-PET, MRI-SPECT and MRI-CT image fusion. The quantitative evaluation was performed using established fusion performance matrices such as structure similarity index measure

(SSIM) root mean square error, peak signal to noise ratio (PSNR), Entropy and mutual information. Robustness of OWAF is tested over Gaussian and speckle noise in all the input modalities. This approach significantly reduced the computational time than conventional GA approach. The limitation of these methods is used only normalized and registered image dataset, in future develop registration algorithm for the purpose of multi central applications. also use various new optimization algorithm to reduce computational time for image fusion.

Zaldívar, D., Morales, B., Rodriguez, A., Valdivia-G, A., Cuevas, E.andPérez-Cisneros, M. [17], 2018 developed, a hunting model of Yellow Saddle Goatfish. At some abstraction level, the approach can be characterized as a search strategy for optimization proposes. The algorithm contempt latest two distinct categories of search agents (fish): chasers and blockers. In each sub-population one fish assumes the role of chaser while the rest are considered blockers. Depending on the category, each element is undergone by a set of different evolutionary operations which emulate the different collaborative behaviours that represent in the natural hunting process. The fitness value represents the relative success that an element experiment during the hunting process. With the use of this biological model, the new search strategy improves the optimization results in terms of accuracy and convergence in comparison to other popular evolutionary techniques. The algorithm has been also tested over several engineering optimization problems and compared to the performance against its competitors. The experimental results demonstrate this technique is fast, accurate and robust.

4.Performance Evaluation Measure

Table 1 shows the performance metrics are used to evaluate the performance of the Image Fusion method.

Sr No.	Parameter	Equation
1.	Root Mean Square Error (RMSE): This parameter indicates the spectral quality. It is calculated by determining the difference between the reference and fused image.	$RMSE = \sqrt{\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(I_R(i,j)-I_F(i,j))^2}{MN}}$ (2) Where MN denotes the size of the image. I_R and I_F is the referenced and fused image.
2.	Peak-Signal-to-Noise-Ratio (PSNR): This parameter is maximum computed in the image fusion methods to calculate the overall quality of the fused image.	$PSNR = 10\log_{10}\frac{L^2}{MSE}$ (3) Where MSE denotes the mean square error and L denotes the number of grey levels in the image. In a grey scale image, its value is 255.

3.	Mutual Information (MI): This parameter measures the similarity between reference and fused images. The higher value of MI denotes the more details and textual information in it.	$MI = \sum_{i=1}^{M}\sum_{j=1}^{N} hI_R I_F(i,j) \times \log_2\left(\frac{hI_R I_F(i,j)}{hI_R(i,j)hI_F(i,j)}\right)$ (4) Where $hI_R I_F$denotes the joint grey level histogram of I_R and I_F.
4.	Structural Similarity Index Measure (SSIM): This parameter measures the structure similarity between reference and fused image. Its value varies in between -1 to 1. Value 1 shows that both images are similar and structural information is preserved.	$SSIM = \frac{(2\mu_{I_R}\mu_{I_F}+C_1)(2\sigma_{I_R I_F}+C_2)}{(\mu_{I_R}{}^2+\mu_{I_F}{}^2+C_1)(\mu_{I_R}{}^2+\mu_{I_F}{}^2+C_2)}$ (5) Where $\mu_{I_R}\mu_{I_F}$ denotes the mean intensity values of referenced and fused image. C_1C_2 are constant.
5.	Entropy: The average quantity of information in the fusion image can be represented by the size of information entropy.	$E = \sum_{i=1}^{L} p_i \log_2 p_i$ (6) p_i is the ratio of the number of pixels whose gray value is *i*to the total number of pixels in the image, and satisfies $\sum_{i=1}^{L} p_i$=1. The higher value of entropy represents the maximum information contained by image.

Table 1 Performance Metrics [18,19]

5.Conclusion&Future Work

It has been found by conducting a Literature view that each image fusion technique suffers from in consistency and high complexity. Also some traditional methods of image fusion like Simple Average, Minimum, Maximum etc. have limitations in fused image like image is not clear, blurring effects, block discontinuities, etc. Gray scale images are in focus in most of the existing work instead of color images. Multimodal medical image fusion research results are more significant but the problems existing in the fusion effect are only improved not fully solved, like color distortion and feature extraction problem. Weights overcome the above challenges, were used for coefficients selection. Primary weighted average fusion may not provide effective fused image due to affixed weight value for fusion, due to that optimum weight selection can enhance the performance by selecting the effective weights for multi-level decomposition components.

In the future, fuzzy logic is taken under consideration to remove multiple noises. In the future, multi-objective function is taken under consideration in the pre-processing method. We will explore meta heuristic algorithms which required minimum internal parameter value and quickly searches the optimal solution.

References

[1]ArdeshirGoshtasby, A. and Nikolov, S., 2007. Guest editorial: Image fusion: Advances in the state of the art. Information Fusion, 8(2), pp.114-118.

[2] Ma, J., Ma, Y. and Li, C., 2019. Infrared and visible image fusion methods and applications: A survey. Information Fusion, 45, pp.153-178.

[3] Du, J., Li, W., Lu, K. and Xiao, B., 2016. An overview of multi-modal medical image fusion. Neurocomputing, 215, pp.3-20.

[4] Rajagopal, M. and Venkatesan, A.M., 2016. Image fusion and navigation platforms for percutaneous image-guided interventions. Abdominal Radiology, 41(4), pp.620-628.

[5]Zhang, Y., 2008. Methods for image fusion quality assessment-a review, comparison and analysis. The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, 37(PART B7), pp.1101-1109..

[6] Tirupal, T., Mohan, B.C. and Kumar, S.S., 2021. Multimodal medical image fusion techniques–A review. Current Signal Transduction Therapy, 16(2), pp.142-163.

[7] Qayyum, H., Majid, M., Anwar, S.M. and Khan, B., 2017. Facial expression recognition using stationary wavelet transform features. Mathematical Problems in Engineering, 2017.

[8] Abas, A.I. and Baykan, N.A., 2021. Multi-Focus Image Fusion with Multi-Scale Transform Optimized by Metaheuristic Algorithms. Traitement du Signal, 38(2).

[9] Kavitha, S. and Thyagharajan, K.K., 2017. Efficient DWT-based fusion techniques using genetic algorithm for optimal parameter estimation. Soft Computing, 21(12), pp.3307-3316.

[10] Bhardwaj, J., Nayak, A. and Gambhir, D., 2021. Multimodal medical image fusion based on discrete wavelet transform and genetic algorithm. In International Conference on Innovative Computing and Communications (pp. 1047-1057). Springer, Singapore.

[11] Shehanaz, S., Daniel, E., Guntur, S.R. and Satrasupalli, S., 2021. Optimum weighted multimodal medical image fusion using particle swarm optimization. Optik, 231, p.166413.

[12] Dinh, P.H., 2021. A novel approach based on grasshopper optimization algorithm for medical image fusion. Expert Systems with Applications, 171, p.114576.

[13] Daniel, E., 2018. Optimum wavelet-based homomorphic medical image fusion using hybrid genetic–grey wolf optimization algorithm. IEEE Sensors Journal, 18(16), pp.6804-6811.

[14] Zaldívar, D., Morales, B., Rodríguez, A., Valdivia-G, A., Cuevas, E. and Pérez-Cisneros, M., 2018. A novel bio-inspired optimization model based on Yellow Saddle Goatfish behavior. Biosystems, 174, pp.1-21.

[15]Huang, B., Yang, F., Yin, M., Mo, X. and Zhong, C., 2020. A review of multimodal medical image fusion techniques. Computational and mathematical methods in medicine, 2020.

[16]Shehanaz, S., Daniel, E., Guntur, S.R. and Satrasupalli, S., 2021. Optimum weighted multimodal medical image fusion using particle swarm optimization. Optik, 231, p.166413.

[17]Zaldivar, D., Morales, B., Rodríguez, A., Valdivia-G, A., Cuevas, E. and Pérez-Cisneros, M., 2018. A novel bio-inspired optimization model based on Yellow Saddle Goatfish behavior. Biosystems, 174, pp.1-21.

[18] Hermessi, H., Mourali, O. and Zagrouba, E., 2021. Multimodal medical image fusion review: Theoretical background and recent advances. Signal Processing, 183, p.108036.

[19] An, F.P., Ma, X.M. and Bai, L., 2022. Image fusion algorithm based on unsupervised deep learning-optimized sparse representation. Biomedical Signal Processing and Control, 71, p.103140.Characteristic Extraction