

# **TIEVS - FAKE CAR IMAGES ANALYZATION SYSTEM**

2021-195

Project Proposal Report

S.K.A.K.I Madhushani – IT18082548

Supervisor – Ms. Manori Gamage

Co-Supervisor – Ms. Suriyaa Kumari

B.Sc. (Hons) Degree in Information Technology Specializing in  
Information Technology

Department of Information Technology

Sri Lanka Institute of Information Technology  
Sri Lanka

March 2021

# **TIEVS - FAKE CAR IMAGES ANALYZATION SYSTEM**

2021-195

Project Proposal Report

S.K.A.K.I Madhushani – IT18082548

Supervisor – Ms. Manori Gamage

Co-Supervisor – Ms. Suriyaa Kumari

B.Sc. (Hons) Degree in Information Technology Specializing in  
Information Technology


Department of Information Technology

Sri Lanka Institute of Information Technology  
Sri Lanka

March 2021

## DECLARATION

I declare that this is my work, and this proposal does not incorporate without acknowledgment any material previously submitted for a degree or diploma in any other university or institute of higher learning. To the best of my knowledge and belief, it does not contain any material previously published or written by another person except where the acknowledgment is made in the text.

| Name                  | Student ID | Signature   |
|-----------------------|------------|---|
| Madhushani S.K.A.K.I. | IT18082548 |  |

The supervisor/s should certify the proposal report with the following declaration.

The above candidate is carrying out research for the undergraduate  
Dissertation under my supervision.

Signature of the supervisor:

Date:

## ABSTRACT

This proposal is prominently focused on implementing analysis on conflicting fake image systems, targeting the items being on sale within our 'Tievs' online classified advertising platform, specifically on Cars. Nowadays, the public does not utilize tangible information sources such as newspapers, magazines, booklets, Leaflets, etc. With the development of advanced technology, these advertisements could reach a higher range of target audiences through online classified advertisement platforms, much more easily and securely. without needing to travel personally for long distances and exchanging money with other people, just to apply for or to receive the advertisement post(s), no need to waste our time and safety. Hence it has become the goal of our 'Tievs' online web application to provide such facilities, all the while enhancing them to outsmart other products with similar intentions. Most classified advertising products currently in use do not prioritize detecting and preventing fake advertisement images or characteristic details from being submitted, let alone inspect them internally and inform the respected users who are in the process of submitting the advertisement. Even more, many implemented online classified advertising systems, simply do not exhibit rich user interfaces for smooth functionality or promote quality user experience and user-friendliness, in consonance with the latest trending technologies. Supply the solution to this through the 'Tievs' online advertisement platform, In the event, a customer is in the process of filling out the necessary details and attaching relevant images to their advertisement on our 'Tievs' online classified advertisement platform, the system will internally examine for fake, inappropriate, misleading, mismatching images within. If detected, the system will swiftly prompt the customer before the advertisement is submitted, that an inaccurate image is being attached, so that the customer can take the corrective measures and eliminate the problematic scenario, regardless of it being done accidentally or deliberately.

Key Words – Analyzation of fake images, Image Processing Algorithm, Images, Surf Algorithm, Machine learning

## Table of content

|   |     |
|---|-----|
| Declaration .....                             | i   |
| Abstract.....                                 | ii  |
| Table of Content.....                         | iv  |
| List of Figures.....                          | v   |
| List of Tables.....                           | vi  |
| List of Abbreviations.....                    | vii |
| 1 Introduction.....                           | 1   |
| 1.1 Background.....                           | 1   |
| 2.2 Literature Survey .....                   | 4   |
| 3.3 Research Gap .....                        | 5   |
| 4.4 Research Problem.....                     | 7   |
| 2 Objectives.....                             | 9   |
| 1.1 Main Objective.....                       | 9   |
| 2.2 Specific Objectives.....                  | 9   |
| 3 Methodology.....                            | 10  |
| 3.1 Research Methodology.....                 | 10  |
| 3.2 System Overview.....                      | 11  |
| 3.3 Software Development Life Cycle .....     | 12  |
| 1.1 Project Requirements.....                 | 13  |
| 3.1.1 Functional requirements .....           | 13  |
| 3.1.2 Non-functional requirements .....       | 14  |
| 2.2 Gantt Chart.....                          | 15  |
| 4 Description of Personal and Facilities..... | 16  |
| 5 Budget and Budget Justification.....        | 17  |

|                     |    |
|---------------------|----|
| Reference List..... | 18 |
|---------------------|----|

## LIST OF FIGURES

|   |      |
|---|------|
|   | Page |
| Figure 1.1 – Classification of image forgery detection.....                 | 2    |
| Figure 1.2 –Testing image of SURF algorithm.....                            | 3    |
| Figure 1.3 – Fake car ad.....   | 3    |
| Figure 1.4 – The structure of the proposed common fake feature network..... | 14   |
| Figure 1.2.2 - Fake Car images ad in Craigslist.....                        | 15   |
| Figure 3.2 – Research Methodology.....                                      | 16   |
| Figure 3.1 – System Overview Diagram.....                                   | 17   |
| Figure 3.3 – Agile methodology.....   | 20   |
| Figure 5.1 - Gantt Chart.....   | 20   |

## LIST OF TABLES

|   | Page |
|---|------|
| Table 1.1 – Comparison of previous researches ..... | 6    |
| Table 5.1 – Budget.....                             | 16   |

## LIST OF ABBREVIATIONS

| Abbreviation | Description                   |
|--------------|-------------------------------|
| SURF         | Speeded Up Robust Features    |
| CBIR         | content-based image retrieval |
| UI           | User Interface                |



# 1. INTRODUCTION

## 1.1 Background & Literature Survey

Smart online advertising platforms have been growing globally to extract life amidst the busy schedule. Nowadays people are using technology to rework their community in positive ways. That's called a “smart community”. With information technology developments, the usage of online classified advertising portals has been growing immensely, throughout recent years due to many factors such as the higher availability than traditional classified deliverances (magazines, booklets, newspaper, leaflets tend to get inaccessible during a lockdown) [1], ease of use, pandemic problems, economical, less consummation of precious time out of people’s busy schedules and having access to a wider range of customers and sellers. Some of the examples are Craigslist, Carewale, CarDheko, ikman.lk etc. Most people understand the potential of data technology and form successful alliances to figure together to use technology to form residents’ lives easier, healthier, and more productive. Therefore, all people using these online platforms for daily life activities will make their work easier. There, advertisers upload different images for the applications, set different prices, and make purchases. Here different advertisers upload different images. but the average person should be able to identify whether they are fake or irrelevant. Or they may be fooled into buying the product.

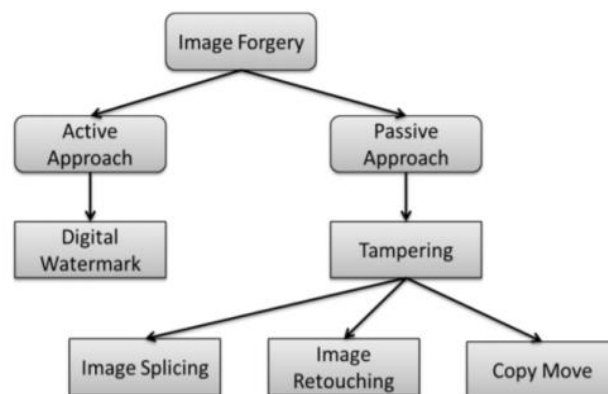
People cannot detect photo forgeries. Therefore, when uploading fake images with image size, price tag, logo tags to the site an advertiser accidentally or deliberately, damages the user's view of the ad as well as the advertising firm. Considering that the fake/irrelevant images are not recognizable, this 'Tives' application works to provide a solution to that shortcoming.

Images are more user-friendly to human eyes than content. For instance, most people focus on the content of the image while watching the ads regardless of the context since images can talk and tell the story [2]. However, in the digital era manipulating images is not easy to detect and prevent. The main problem happens when conflicting images have spread the web without any control. People tend to believe that each picture they see is

real without considering the likelihood that those images could be tempered, faked, or control. All mentioned issues arise the need for further research in this field.

Fraudulent image detection has been investigated for many years. generally, fake image detection investigates different characteristics of images and attempts to seek out traces to research. As mentioned above, most of the normal fraudulent detection techniques are often categorized into three classes, copy-move detection, splicing detection, and image retouching detection.

A study conducted by Yuanfang Guo et al: introduced a technique to detect the classes of fake images. Using these techniques, they researched how to detect fake or colorized images. By Adding images with some colorized or conflicting to the application of the ad by some advertisers, customers can not identify it as colorized or not.[1] Consequently, the customer is more probably to be misled by this. Our ‘Tives’ application overcomes these by considering the following techniques and adapting the System accordingly.



*Figure1- Classification of image forgery detection*

### **1.1.1. Copy-move detection**

Copy-move detection relies on identifying duplicated regions during a tampered image. Intuitively, these techniques tend to hunt an appropriate feature during a particular domain, such the detection are often performed via searching the foremost similar two units (such as patches). Different methods usually exploit different features.

### **1.1.2. Splicing Detection**

In most cases, splicing detection detects manipulated regions that originate from various source images. Unlike copy-move detection, these methods detect tampered regions using a variety of traces (features), which normally expose differences between tampered and untampered regions. Splicing detection is currently divided into four categories based on their mechanisms: compression-based methods, camera-based methods, physics-based methods, and geometry-based methods.

### **1.1.3. Image Retouching Detection**

In most cases, image retouching detection assumes that the original images have been restored or updated. for example, considers the similarities, distances, and number of equal pixels among different blocks to discern in painted pictures.

Feng Qi et al: In the study, It provides an efficient algorithm based on SURF. The research offers an effective SURF-based algorithm (Speeded Up Robust Features). In order to find and accurately describe digital images, the procedure uses the SURF algorithm, firstly, the SURF feature detector when extracting images and matching feature points in the image. The character description of the individual feature point vector will then be calculated using the DAISY algorithm rather than the SURF algorithm. The fake matching points are discarded with the RANSAC algorithm in the

process of matching functional points. Finally, it will calculate the space geometrical transformation parameters between two images according to the remainder of the match point and thus complete the matching procedure.[8]



Figure 1. Feature Points of the DoH Test Image

*Figure 1- Testing image of SURF algorithm*

Classified car advertisement, an advertiser adds some funny bone car images with a trademark of the modern automotive industry to the platform to scam the customer. The picture below is an example for that.



*Figure 1.2- Add hilarious Fake Car Ads*

## 1.2. Research Gap

Even though It is perspicuous that some researchers have attempted to implement an outstanding model that is capable of detecting and prevention fake images with a decent accuracy level, still much more undiscovered innovative methodologies are yet to be realized.

The most common way of analyzing fake/irrelevant images is predicting whether fake or not for a section of text by doing a classification task. Moreover, former researchers were dependent on the use of some techniques for the detecting and preventing process. For example, Khaled A. N. Rashed et al [5] used the content-based image retrieval (CBIR) technique to detect fake images. And they used Web 2.0, Community and Collaborative Activities to analyze fake images. They created a system able to identify the fake images and image content, as well as the system, need to be able to manage user's interaction. They believe that content-based image retrieval (CBIR) techniques and harnessing collective intelligence is the appropriate solution for this problem.

Chih-Chung Hsu et al: One of the most advanced CNN image identification car models is a dense block, a critical component of DenseNet. However, the monitored learning strategy is educated while the proposed CFF pair learning strategy refers to a semi-monitored learning strategy improved by them. A two-streamed network to enable CFF-learning feedback in a pair way is the proposed CFFN. The traditional CNNs, which are one-stroke, cannot obtain the pairing relevant information on the other hand, which means that the traditional CNNs cannot easily learn the common characteristics. In the CFFN suggested, any advanced CNN network, like ResNet Xception or DenseNet , may have been part of the backbone network. The performance of fake picture recognition will also be enhanced when the backbone network is trained to have the best feature representation capability. To that end, DenseNet is chosen by the proposed CFFN as a backbone network.[13]

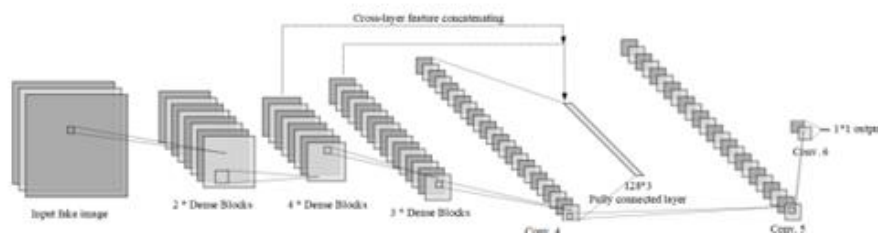


Figure1.2. 1. The structure of the proposed common fake feature network.

Table 1.1 below depicts in tabular form, the summarization of the above explanation.

| <b>Research</b>                      | <b>Addressing<br/>the cold start<br/>problem</b> | <b>Combination<br/>of different<br/>algorithm</b> | <b>Detection<br/>fake<br/>image</b> | <b>Prevention<br/>fake<br/>image</b> |
|--------------------------------------|--|---|-------------------------------------|--------------------------------------|
| Research A                           | ✗  | ✓   | ✗                                   | ✗                                    |
| Research B                           | ✗  | ✓   | ✓                                   | ✗                                    |
| Research C                           | ✓  | ✗   | ✓                                   | ✗                                    |
| Proposed<br>Recommendation<br>System | ✓  | ✓   | ✓                                   | ✓                                    |

*Table 1.1 – Comparison of previous researches.*

### 1.3 Research Problem

User-friendly classified advertising platforms that provide the price predictions for selling products are obscure. In addition, from the applications' developers and owner's point of view, they have to implement strict program logic to identify or prevent fraudulent advertisements being posted (fake images/ irrelevant descriptions) accidentally or deliberately by users of the system, through verification and validation processes internally. This will require inspecting posts separately and meticulously, even after the ad being posted to the customers and if so, customers will view those fraud ads and lose confidence in using the platform for their needs, enabling loss of application reputation as well.

Most classified advertising products currently in use do not prioritize detecting and preventing fake advertisement images or characteristic details from being submitted, let alone inspect them internally and inform the respected users who are in the process of submitting the advertisement. Even more, many implemented online classified advertising systems, simply do not exhibit rich user interfaces for smooth functionality or promote quality user experience and user-friendliness, in consonance with the latest trending technologies.



*Figure 1.2.2 – Fake Car images ad in Craigslist*

While it is obvious that many parties have already introduced online classified advertisement platforms in recent years, a highly improved application with a comprehensive machine-learning technology and Image processing algorithm has yet to be implemented to reinforce key functions in order to effectively meet customer requirements.

Furthermore, since Internet growth, these online ads have become the main part of the advertising market. And also, the internet advertising sites have a lot of advertising every day (Eg: eBay, Craigslist). Although advertisers had a high impact on the popularity of the online advertising sector. Therefore, it is a critical issue at present to proactively identify, identify or avoid fake images about the content of advertising. The widespread accessibility of the web attracts undesirable online scammers who pose as true sellers by posting fake ads with conflicting images a view to defrauding wishful buyers. Scammers can steal millions of dollars from unsuspecting users and threaten the reputation and utility of online ad services.

In order to unintentionally or purposefully recognize and avoid advertising with counterfeit images (false images/irrelevant descriptions) from being posted by users of the system, applications' developers and proprietors can enforce rigorous programming logic by verifying and validating internally. This requires the inspection of posts, even after the ad is placed on the customers, individually and thoroughly, and if so, consumers view these fraud ads and will lose confidence in the platform's use, thereby allowing users to lose their credibility for their application [2]. Currently, most classified advertising goods do not prioritize the detection and prevention of false images, let alone internally inspect them and advise the valued customers in the process of advertising. And also, many online classified advertisements, there simply are no extensive user interfaces in line with the latest modern technology to promote quality user experience and user-friendliness.

Recent approaches to image processing involve the instances of both fake pictures by user label or not. To enable an algorithm to learn how to categorize ads. I decided that I use image processing to choose cases that are likely falsified images in order to overcome the implied problem.



## **2. OBJECTIVES**

### **1.2 Main Objectives**

- A systematic and rich user-friendly smart solution to allow stakeholder advertising to be published efficiently and accurately without problems, as well as offering an optimized, interactive system search facility, to look and find items to buy seamlessly and productively in accordance with specific customers' requirements. (Will aim at one classified type of car, for example)
- The aim of this study is to implement a fake picture sensing system using an image processing algorithm to prevent an advertiser or persons with deceptive intentions from making the advertisement fake by themselves before submitting an advertisement for an item of a particular type (such as Cars) during the year.
- When the advertiser submits their advertisement into the system, is inspected by the images system it contains. If the advertiser added the fake images, the system will prompt the cautious message to the advertiser asking it to identify and remove this fake image.

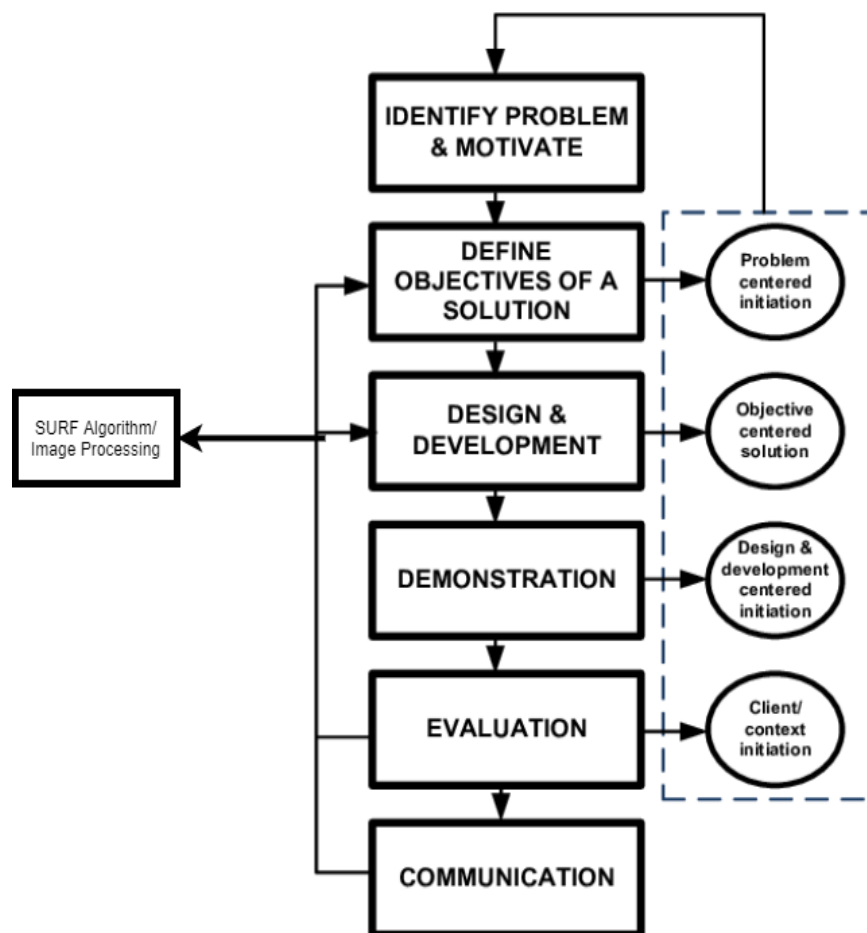
### **2.1 Specific Objective**

- successful utilize of JPEG features algorithm, for image forgery detection.
- Proactively identifying and preventing fraudulent/ conflicting images, from being posted in the application.
- Identifying if the advertiser input ill-matched/ conflicting images into the application and prompts them cautious messages if they repeatedly attempt to input such irrelevant images.

### 3. Methodology

#### 3.1 Research Methodology

This industry will highlight how development is managed and carried out. A short conversation on the feasibility study is also included. As this is the implementation of a research project Agile development strategy is used to execute the system module by module



*Figure 3.2 – Research Methodology*

### 3.2 System Overview

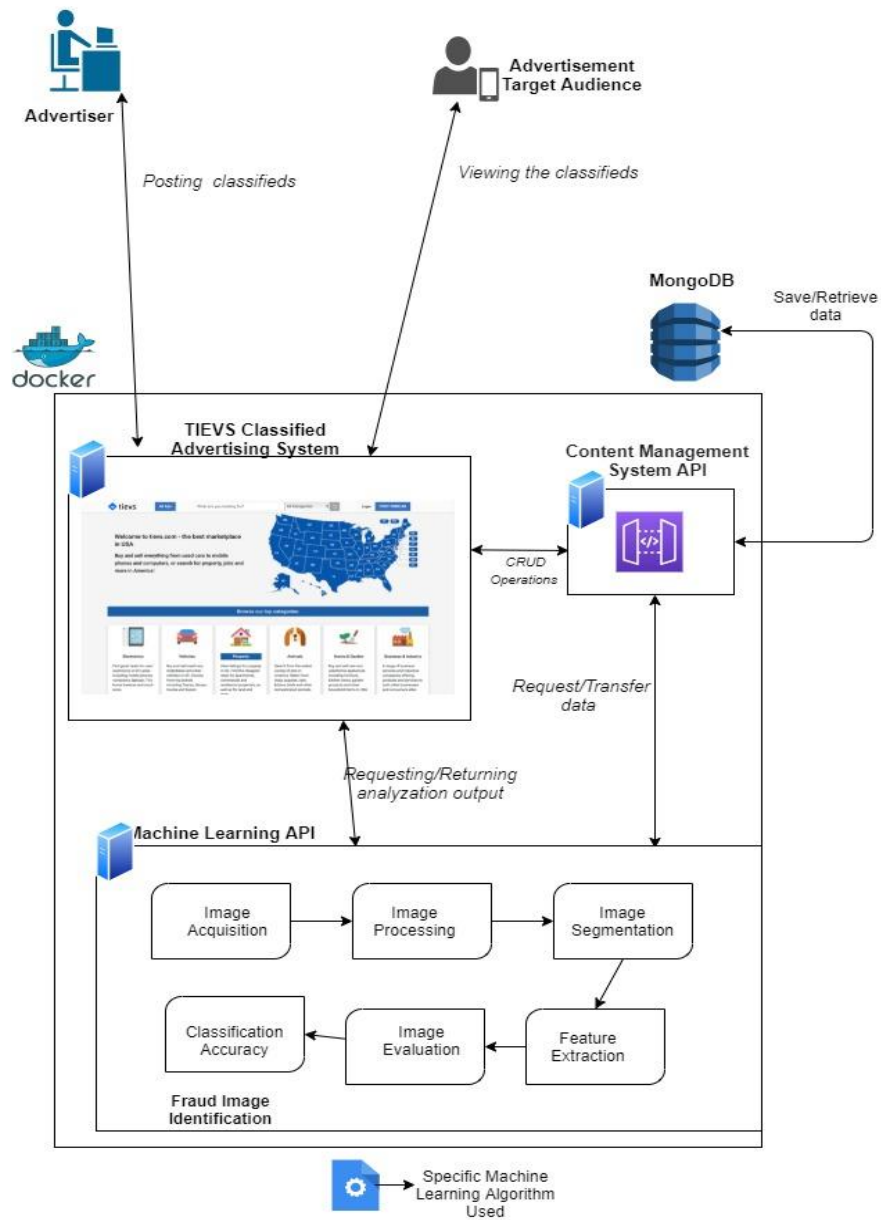


Figure 3.3- System Overview Diagram

### 3.3 Software development Life Cycle

An agile methodology is considered for the life cycle development of software. Furthermore, the Scrum methodology is primarily covered within the enormous Agile framework. Scrum is the lightweight framework that enables people, teams, and institutions to gain value for complex challenges by means of agile strategies. Product backlog creation, sprint planning and backlog creation, daily scrum conference, sprint retrospect, and sprint review are the incessant but iterative essential steps taken in a scrum strategy. The same methods will be pursued successfully for this proposed system. When you resume, it's safe to say. the same methods are successfully followed for this proposed system. It is safe to say that many unanticipated events will occur while research is carried out, particularly because some of the desired areas should be first analyzed. The existing and developed strategy will not be pursued the same way in this situation, because changes will have to be made when dealing with the impediments to the study process. In this way, agile methodology is important to make the implementation process easier and more consistent. Agile can provide research with increased control, improved efficiency, higher quality, satisfied customers, and greater return on investment according to Figure 3.1 below.

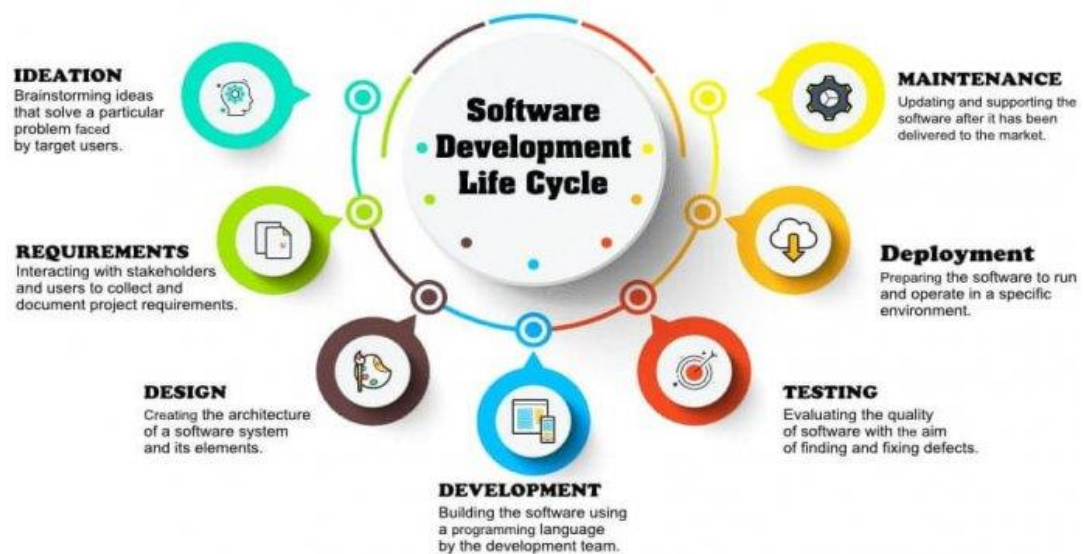


Figure 3.3 – Figure Agile Methodology

## **3.4 Project Requirements**

### **3.4.1 Functional requirements**

- Successful customer navigation to the application
- The proper visual interface of advertising process elements should be implemented for a convenient representation of the different features of a car.
- Integration between the Machine learning API and the fake image analysis system.
- Proactively identify and prompt a warning message before submitting the advertisement.

### **3.4.2 Non-functional requirements**

- Accuracy
- Scalability
- Adaptability
- Efficiency
- Ease of use
- Maintainability
- Reliability

### 3.5 GANTT CHART

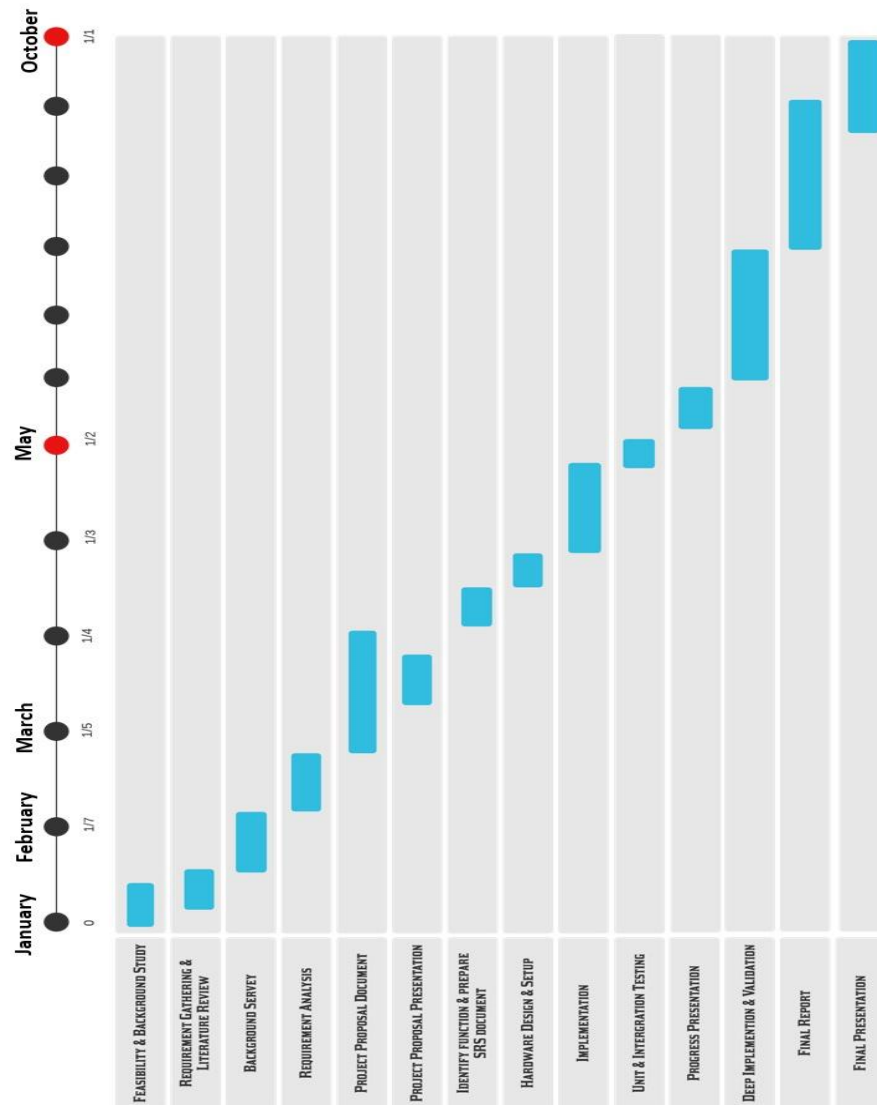


Figure 5-1 Gantt Chart

## **4. Description of Personal and Facilities**

### **Detection and prevention of fake images**

- Detection of fake, ill-matched, conflicting, or unsuitable images within the advertisement form, and displaying cautious warnings, using image processing techniques.
- Fake or irrelevant images must be identified before a user post an advert containing one, rather than examining for such images after it has been submitted if it's essential to handle future conflicts.
- Through training all competent image processing algorithm models with predefined image data, which targets a specific item range, (Ex: Vehicles) and identifying the most optimal image processing algorithm model that, additionally, supports 'Tievs' requirements, the application will be able to successfully inspect whether there are any fake/inappropriate images, that are going to be uploaded with the advertisement form by the customers.
- Build and developed algorithm Client side Serve side Components for test and extraction for an item from advertisement from prior to posting.
- Integration with developed algorithm and visualize the cautious message for the advertiser in form of suggestion.

## 5 BUDGET AND BUDGET JUSTIFICATION

| Component                                 | Amount (USD) | Amount (LKR) |
|---|--------------|--------------|
| 1GB Memory – 1vCPU Droplet (Frontend)     | 60           | 12000        |
| 2GB Memory – 1vCPU Droplet (Backend & DB) | 120          | 24000        |
| .com Domain Name                          | 12           | 2400         |
| <b>Total</b>                              | <b>192</b>   | <b>38400</b> |

*Table 6.1- Budget*



## REFERENCE LIST

- [1] Y. Guo, X. Cao, W. Zhang, and R. Wang, "Fake colorized image detection," *IEEE trans. inf. forensics secur.*, vol. 13, no. 8, pp. 1932–1944, 2018.
- [2] B. Liu, C.-M. Pun, and X.-C. Yuan, "Digital image forgery detection using JPEG features and local noise discrepancies," *ScientificWorldJournal*, vol. 2014, p. 230425, 2014.
- [3] J. Frank, T. Eisenhofer, L. Schönherr, A. Fischer, D. Kolossa, and T. Holz, "Leveraging frequency analysis for deep fake image recognition," *arXiv [cs.CV]*, pp. 3247–3258, 2020.
- [4] *Researchgate.net*. [Online]. Available: [https://www.researchgate.net/publication/259950220\\_Blind\\_Fake\\_Image\\_detection](https://www.researchgate.net/publication/259950220_Blind_Fake_Image_detection). [Accessed: 23-Mar-2021].
- [5] *Researchgate.net*. [Online]. Available: [https://www.researchgate.net/publication/342088036\\_Exposing\\_Fake\\_Images\\_With\\_Forensic\\_Similarity\\_Graphs/citations](https://www.researchgate.net/publication/342088036_Exposing_Fake_Images_With_Forensic_Similarity_Graphs/citations). [Accessed: 23-Mar-2021].
- [6] M. Laliberte, "The 9 biggest scams to avoid when buying a car on Craigslist," *Business Insider*, 25-Apr-2019.
- [7] B. Zitová and J. Flusser, "Image registration methods: a survey," *Image Vis. Comput.*, vol. 21, no. 11, pp. 977–1000, 2003.
- [8] J. Xingteng, W. Xuan, and D. Zhe, "Image matching method based on improved SURF algorithm," in *2015 IEEE International Conference on Computer and Communications (ICCC)*, 2015, pp. 142–145.
- [9] "45 fake car ads from craigslist," *Cockeyed.com*. [Online]. Available: [https://cockeyed.com/citizen/accord/100\\_postings/45\\_fakes.php](https://cockeyed.com/citizen/accord/100_postings/45_fakes.php). [Accessed: 23-Mar-2021].
- [1] A. Kunbaz, S. Saghir, M. Arar, and E. B. Sonmez, "Fake image detection using DCT and local binary pattern," in *2019 Ninth International Conference on Image Processing Theory, Tools and Applications (IPTA)*, 2019, pp. 1–6.
- [1] "Home," *Govmu.org*. [Online]. Available: <https://nlta.govmu.org/Pages/default.aspx>. [Accessed: 23-Mar-2021].
- [1] C.-C. Hsu, Y.-X. Zhuang, and C.-Y. Lee, "Deep fake image detection based on pairwise learning," *Appl. Sci. (Basel)*, vol. 10, no. 1, p. 370, 2020.
- [1] M. Ahmed, "False image injection prevention using iChain," *Appl. Sci. (Basel)*, vol. 9, no. 20, p. 4328, 2019.

