CLASSIFICATION OF FAKE PROFILES FEATURES IN FACEBOOK USING K-NEAREST NEIGHBOUR (KNN), NEURAL NETWORK (NN) AND SUPPORT VECTOR MACHINE (SVM)

AHMAD NAZREN HAKIMI BIN AHMAD NASIR

MASTER OF SCIENCE
(COMPUTER SCIENCE)

UNIVERSITI PERTAHANAN NASIONAL MALAYSIA

2022

CLASSIFICATION OF FAKE PROFILES FEATURES IN FACEBOOK USING K-NEAREST NEIGHBOUR (KNN), NEURAL NETWORK (NN) AND SUPPORT VECTOR MACHINE (SVM)

UNIVERSITI PERTAHANAN NASIONAL
MALAYSIA

2022

CLASSIFICATION OF FAKE PROFILES FEATURES IN FACEBOOK USING K-NEAREST NEIGHBOUR (KNN), NEURAL NETWORK (NN) AND SUPPORT VECTOR MACHINE (SVM)

AHMAD NAZREN HAKIMI BIN AHMAD NASIR

Thesis submitted to the Centre for Graduate Studies, Universiti Pertahanan Nasional Malaysia, in fulfilment of the requirements for the Degree of Master of Science (Computer Science)

2022

ABSTRACT

Today, people rely heavily on Online Social Networks (OSN) which have piqued the interest of cyber criminals to carry out malicious acts. Coupled with the existence of illegal companies that make transactions with fake account services. To cater this fake account problem in OSN, this study focuses on identifying the most widely used fake Facebook accounts in OSN. It is included for their behaviour and features of fake account. This research methodology begins with data collection, identification of training and classifier functions, and finally validation and verification. The first process is to collect information about real and fake Facebook accounts. The second process is to use Facebook user feed data to understand user profile activity and identify the full set of features that play an important role in differentiating fake users from real Facebook users. Finally, we use these functions and identify the most important classifiers based on machine learning, which is mapping the identification of a total of 3 classifiers, namely K-nearest neighbour (KNN), support vector machine (SVM), and neural network (NN). The findings have revealed that the series of result shown that prediction the fake profile with good value of Classifying Accuracy (CA) which is KNN is 92%, NN is 94% and SVM is 95%. Same goes to Area Under Curve (AUC) which is KNN is 97%, NN is 98% and SVM is 98%. Ultimately, this finding will provide a new endeavour for countermeasure and protection of OSN users.

ABSTRAK

Hari ini, orang ramai sangat bergantung pada media sosial yang telah menarik minat penjenayah siber untuk melakukan perbuatan berniat jahat. Ditambah pula dengan kewujudan entiti yang melakukan transaksi dengan perkhidmatan akaun palsu. Bagi menangani masalah akaun palsu dalam media sosial ini, kajian ini memfokuskan kepada mengenal pasti akaun Facebook palsu yang paling banyak digunakan dalam media sosial. Ia termasuklah dengan tingkah laku dan ciri akaun palsu mereka. Metodologi penyelidikan ini bermula dengan pengumpulan data, pengenalpastian latihan dan fungsi pengelas, dan akhirnya pengesahan kepada akaun palsu tersebut. Proses pertama adalah untuk mengumpul maklumat tentang akaun Facebook sebenar dan palsu. Proses kedua ialah menggunakan data pengguna Facebook untuk memahami aktiviti profil pengguna dan mengenal pasti set lengkap ciri yang memainkan peranan penting dalam membezakan pengguna palsu daripada pengguna Facebook sebenar. Akhir sekali, kami menggunakan fungsi ini dan mengenal pasti pengelas terpenting berdasarkan pembelajaran mesin, iaitu memetakan pengenalpastian sejumlah 3 pengelas iaitu K-Nerest Neighbor (KNN), Support Vector Machine (SVM), dan Neural Network (NN). Penemuan telah mendedahkan bahawa keputusan menunjukkan bahawa ramalan profil palsu dengan nilai baik Klasifikasi Ketepatan (CA) iaitu KNN ialah 92%, NN ialah 94% dan SVM ialah 95%. Begitu juga dengan Area Under Curve (AUC) iaitu KNN ialah 97%, NN ialah 98% dan SVM ialah 98%. Akhirnya, penemuan ini akan menyediakan satu usaha baru untuk tindakan balas dan perlindungan pengguna media sosial.

ACKNOWLEDGEMENTS

First and foremost, I would like to acknowledge and give my warmest thanks to all my supervisors, Prof Madya Ts. Dr. Suzaimah bte Ramli, Dr. Muslihah binti Wook and Pn. Norulzahrah binti Mohd Zainudin who made this work possible. Their guidance and advice carried me through all the stages of writing my project. Thank You for your kindness.

I would also like to give special thanks to my lovely wife, Pn Fatimah Soliha binti Nawawi@Hassan and my childrens for their continuous support and understanding when undertaking my research and writing my thesis. Your prayer for me was what sustained me this far.

Finally, I would like to thank God, for letting me through all the difficulties. I have experienced your guidance day by day. You are the one who let me finish my study. I will keep on trusting you for my future. ALHAMDULILLAH

APPROVAL

The Examination Committee has met on **21 October 2021** to conduct the final examination of **Ahmad Nazren Hakimi bin Ahmad Nasir** on his degree thesis entitled **Classification of Fake Profiles Features in Facebook using K-Nearest Neighbour (KNN), Neural Network (NN) and Support Vector Machine (SVM).**

The committee recommends that the student be awarded the of Master of Science (Computer Science).

Members of the Examination Committee were as follows.

Prof Madya Dr. Syahaneim binti Marzukhi
Faculty of Defence Science and Technology
Universiti Pertahanan Nasional Malaysia
(Chairman)

Dr Nor Asiakin binti Hasbullah
Faculty of Defence Science and Technology
Universiti Pertahanan Nasional Malaysia
(Internal Examiner)

Ir. Ts. Dr. Shahrani binti Shahbudin
School of Electrical Engineering
Universiti Teknologi MARA
(External Examiner)

APPROVAL

This thesis was submitted to the Senate of Universiti Pertahanan Nasional Malaysia and has been accepted as fulfilment of the requirements for the degree of **Master of Science** (Computer Science). The members of the Supervisory Committee were as follows.

Prof. Madya. Ts. Dr. Suzaimah bte Ramli
Faculty of Defence Science and Technology
Universiti Pertahanan Nasional Malaysia
(Main Supervisor)

Dr. Muslihah binti Wook
Faculty of Defence Science and Technology
Universiti Pertahanan Nasional Malaysia
(Co-Supervisor)

Pn. Norulzahrah binti Mohd Zainudin
Faculty of Defence Science and Technology
Universiti Pertahanan Nasional Malaysia
(Co-Supervisor)

UNIVERSITI PERTAHANAN NASIONAL MALAYSIA

DECLARATION OF THESIS

Student's full name	: Ahmad Nazren Hakimi bin Ahmad Nasir
Date of birth	: 2 January 1990
Title	: Classification of Fake Profiles Features in Facebook using K-Nearest Neighbour (KNN), Neural Network (NN) and Support Vector Machine (SVM)
Academic session	: 2019/2021

I hereby declare that the work in this thesis is my own except for quotations and summaries which have been duly acknowledged.

I further declare that this thesis is classified as:

□ **CONFIDENTIAL** (Contains confidential information under the official Secret Act 1972)*

□ **RESTRICTED** (Contains restricted information as specified by the organisation where research was done)*

□ **OPEN ACCESS** I agree that my thesis to be published as online open access (full text)

I acknowledge that Universiti Pertahanan Nasional Malaysia reserves the right as follows.

1. The thesis is the property of Universiti Pertahanan Nasional Malaysia.
2. The library of Universiti Pertahanan Nasional Malaysia has the right to make copies for the purpose of research only.
3. The library has the right to make copies of the thesis for academic exchange.

______________________	______________________
Signature	**Signature of Supervisor/Dean of CGS/ Chief Librarian
Click here to enter text.	Click here to enter text.
IC/Passport No.	**Name of Supervisor/Dean of CGS/ Chief Librarian
Date:	Date:

*If the thesis is CONFIDENTAL OR RESTRICTED, please attach the letter from the organisation with period and reasons for confidentiality and restriction.
** Witness

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Introduction

The development of the Internet, Web 2.0, and communications technology offers users the opportunity to interact actively through various wired and wireless Internet-connected applications. Various applications are being developed today that allow users to communicate, access, share and distribute with other users around the world. The advancement of the internet and communication technology in Malaysia has a major impact on people's lives today (Ojo et al., 2019). Communication technology, for example, offers opportunities for individuals and organizations to increase efficiency in carrying out daily tasks, increase productivity and competitiveness in areas such as politics and business.

The Internet is one of the daily necessities in everyone's life. Easy internet access is available everywhere. In addition, through the use of smartphones, people now always get current information or news that is just at their fingertips. Undeniable, this internet access facility also opens up opportunities to use widespread social media among internet users. Online Social

Networks (OSN) are the current applications for internet users to do their day-to-day activities such as substance sharing, news browsing, posting messages, item audits and talking about occasions, and so on. In the meantime, different kinds of spammers are also drawn in the direction of these OSN.

There is no denying that today's society is more likely to use social media to discuss topical issues and to express its views on those issues (Abdullah et al., 2021). Today's popular platforms such as Facebook, Twitter, WhatsApp, Instagram and others are the main social media that are widely used by the public (Alshuaibi et al., 2018). This is combined with modern technology and the use of smartphones, which makes it easier for people to obtain and exchange information quickly and quickly. These digital criminals, including sexual stalkers, online fraudsters, campaigners, catfish, social bots and so on, aim to establish a trust system using different methods, by making counterfeit profiles to spread their substance and do tricks.

From the point of view of OSN crime expert, counterfeit profiles influence the system's general notoriety despite the loss of transmission capacity. In order to find out about these malicious clients, an enormous amount of work and increasingly refined robotic techniques are needed. An effort is made to extant a few classifications of highlights that have been utilized to prepare classifiers to distinguish a phonetic profile. Distinctive information slithering methodologies have been distinguished alongside some current information hotspots for fake profile discovery.

Today's social web, however, is not limited to human beings alone. In fact, online people and their social interactions can be programmed and fully automated. As (Zhang et al., 2018) stated, 'digitization drives notification; the use of technology in the field of human activity enables the creation of software to act in the place of humans.' Over the past decade, OSN such as Twitter, LinkedIn, and especially Facebook, has grown rapidly in size and influence. In 2018, Facebook had more than two billion active users. Such sites not only have a significant impact on social media but also on education, employment, industry, etc. Communication and information are easier than ever. However, there are many issues with privacy, cyberbullying, social engineering, and online impersonation.

A fake account can be described as an account that does not represent a real person or organization. This should not be confused with a clone whose identity is owned by one person but is misinterpreted as a malicious act by another. Facebook's total user base in 2017 consisted of fake or duplicate accounts (User Profile API, 2020). However, that number will fluctuate greatly as many new ones are generated every day and Facebook is taking steps to improve it. Fake accounts may still be very elusive for Facebook's security measures known as the Facebook Immune System (FIS) (Facebook Business, 2017). Tracking fake accounts remains a problem for Facebook research and social media security.

The FIS is the security infrastructure that Facebook uses to detect spam and other cyber scams. FIS works with intelligent software to detect suspicious links and behaviour patterns on social networking sites. The software is controlled by a group of security experts, but you can also study and take action on your own. While Facebook statistics show that the system as a whole is very effective, scammers are constantly looking for ways to bypass this security tactic and bring spam, scams, and malware to Facebook users. Since Facebook's personal pages can contain a large amount of personal information, the security of this very popular social networking site has always been an issue. Some of the security scams that have emerged on Facebook (Wang et al., 2020) include:

a. Like jacking, where scammers share interesting images or videos via "Likes." This content may include attempts to obtain personally identifiable information through surveys or to encourage users to download malware.
b. Social bots, which impersonating real Facebook users and other user’s friends to obtain personal information.
c. Infiltration of user feeds to distribute graphic images or other graphic images to user friends.

While Facebook continues to work to upgrade its security and prevent fraud, users can protect themselves by only “befriending” people they know, avoiding clicks on offers or sensational contacts and never agreeing to download files, provide personal information or paste code to their sailors.

1.2 Research Background

Social media with dynamic web features offers space - especially for users who want to share various personal information and daily activities with family members and friends. This advantage facilitates social media users to establish relationships, make friends and build networks online. Such thing opens up an opportunity for anyone to create a virtual network of relationships with each other’s. On social media, users are able to communicate and meet on a regular basis virtual with a new friend known in a fairly large social network, or being a part of a social network on the Internet.

A frequent example is an individual's name. The second example is an identification card that includes the individual's name, birth date and place of birth, nationality, meticulously captured fingerprints, as well as a securely stored and a photo of the individual. A third example is a private and open key that is securely associated with a Public Key Infrastructure. As a rule, character ought to be one of a kind as in each distinguishing object should just allude to at generally one individual. A similar individual may in any case have a few characters, similar to an international Identity Document (ID) and a couple of keys above, or then again, a social security number.

The genuine character is confirmed by social media expertise (Calbalhin, 2018). A cutting-edge international ID is a run of the mill case of this. Experts ensure that the picture, fingerprints, name, birthdate and so forth have a place with a similar individual, for example ensure the item connection. At a social media site, a client is normally distinguished by a profile. It normally contains an image and name, conceivably a location and birth date. The locales don't, notwithstanding, thoroughly watch that the individual with the personality insinuated in the profile truly made and controls the profile.

In the event that this isn't the situation, someone is utilizing another person's identity. This is called false personality. One can likewise make profiles that can utilize openly fabricated names and other data that can't be connected to any genuine individual in any nation. For this situation the character is known as a faked personality. Such a profile can contain an image of a genuine individual, picked for example arbitrarily from the Internet (David, 2016).

False characters assume an imperative job in progress held on dangers for example, facilitated, enduring, complex endeavours at bargaining focuses in legislative, non-administrative, and business associations. False characters are likewise frequently associated with different noxious exercises, as spamming, falsely expanding the quantity of clients in an application to advance it, and so forth (Van et al., 2018).

This thesis only focusing on Facebook social media because it is the most social media are used in Malaysia. For the target audience are focusing on student in public university and National Defence University of Malaysia (NDUM) are being chose because the student came from varies of family and culture.

1.3 Problem Statement

Social systems administration has end up an outstanding diversion inside the web at present, drawing in countless clients, burning through billions of minutes on such administrations. OSN administrations assortment from social associations-based stages like Facebook or Twitter to understanding dispersal driven phases reminiscent of Twitter or Google Buzz, to social media brands that send display frames like a Flicker. On the other hand, increasing security considerations and ensuring OSN privatization is still the most critical constraint and the most important task (Vishwanath et al., 2018).

When surfing OSN, people share extensive amounts of their private activities. With our personal information entirely or partially exposed to the general public, we make excellent targets for several types of attacks, the most serious of which may be recognised proof burglary (Ratna et al., 2016). Wholesale fraud occurs when each individual uses character abilities for personal reasons. Amid the prior years, online distinguishing proof robbery has been an essential issue thinking of it as influenced a huge number of individuals around the world (Swe & Myo, 2018).

Casualties of distinguishing proof robbery may endure remarkable sorts of punishments; for outline, they lose time or money, are sent to correctional institutions, destroy their open image or damage their relationships with partners, friends, and family. At present, most by far of OSN does never again confirms conventional users' obligations and has entirely defenceless privatizes and wellbeing arrangements (Jia et al., 2017). Actually, most OSN applications default their settings to insignificant privatises; and subsequently, OSN turned into a best stage for misrepresentation and misuse (Rathore et al., 2017).

OSN contributions have encouraged data fraud and impersonation assaults for genuine in the same class as gullible aggressors. To compound the situation, users were required to outfit right comprehension to set up a record in Social Networking sites. Simple observing of what clients share on-line would prompt cataclysmic misfortunes, not to mention, if such bills had been hacked. OSN have attracted researchers to mine and analyse large amounts of their data, investigate and scrutinize user activities as well as identify their irregular behaviours, and detect suspicious activity. Researchers sought to use practical methods to identify fake OSN profiles on OSN to evaluate various attribute categories such as blog-based attributes, information -based attributes, and attributes (Gao, P et al., 2015).

The use of fake news, hate speech, sensation, polarization, etc. was observed on Facebook. This trend has highlighted the need for new techniques to detect and prevent this behaviour. It is very appropriate to create a fake profile today (Londhe et al., 2015). Therefore, it is necessary to study the characteristics of fake OSN accounts for social networking sites that connect people who have the same interest on social media. You can learn a lot about how people react and what their needs are by analysing their relationship to one another. Social media accounts are a serious and growing problem that leads cybercriminals to engage in malicious activities. (Khaled et al., 2018).

The user must create his or her profile as an OSN member based on information such as name, age, gender, photo, date of birth, email address, interests, etc. (Agarwala et al., 2018). The motive behind creating fake accounts is to slander other people's profiles, trade fake news, post offensive messages like pictures, spread pornography, terrorist ads. Huge amount of data is generated online from social networks like Facebook, Twitter, Instagram, LinkedIn and others. Fake user accounts in online communities are a treasure trove for potential adversaries who are currently distributing fake product reviews, antivirus programs, spam, and paid troll election campaigns. on social networking sites (Tiwari, 2017).

Compared to the year 2019, there are 2.2 billion direct users, 1.7 billion Facebook customers use their mobile phones. Twitter is a social microblogging community with 332 million direct users, registering 11 hundred Tweets every second. LinkedIn is an expert network for technical media with four hundred million subscribers worldwide. Instagram and Snapchat have 380 million subscribers (Simsek & Yilma, 2018). Social media is an important function for us, 45% of the world population spends at least one hour a day on social media, news, photos, tweets, enjoying and social networking.

Profile data in online networks will likewise be static or dynamic. The subtleties that can be given to individual guidance during the profiling season are known as static information. There is also a place as a small print explained with a framework guide in the system called dynamic learning. Static learning incorporates statistic components of an individual and his or her advantages and dynamic information incorporates individual runtime propensities and territory in the system. By far most of momentum look into relies upon static and dynamic information. Anyway, this isn't significant to bunches of the social networks, where handiest some of static profiles are seen and dynamic profiles as a rule are not evident to the individual system.

The issues including social systems administration like protection, on-line tormenting, abuse, and trolling and numerous others. False profiles are the profiles which are not explicit and people with false certifications. The fake Facebook profiles all the more regularly are enjoyed malignant and unfortunate exercises, making issues the social network clients (Walt & Elof, 2018). People make counterfeit profiles for social designing, online pantomime to malign a man or lady, advancing and crusading for a character or a horde of people. Facebook has its security framework for users in the individual commissioning of spam and phishing.

The FIF has now not been prepared to monitor counterfeit profiles made on Facebook through clients to a greater degree. However, little study has been done to explore the features of fake account in OSN for counterfeit profiles. Undoubtedly social websites have made people's lives better, but there are some unavoidable and serious problems associated with them such as personal and professional abuse information, social engineering, online bullying and online impersonation (Akyon & Esat Kalfaoglu, 2019). The existence of fake profiles in networking is one of the main concerns for both OSN service providers and their users (Savyan & Bhanu, 2018) .

A forged profile symbolizes the identity (profile) of the person claiming to be someone who is not them. According to Facebook, if someone uses a Facebook account other than their primary account it is fake. Fake accounts are usually created to engage in various illegal, misleading, malicious, or discriminatory activities on the network, posing a threat to the network as well as its users. The motive behind a fake profile usually varies with the type of network for which it was created for (Kumari & Rathore, 2018). This article aims mainly to examine the reasons that encourage users to create fake identities on social networks. However, the goal of creating a fake identity depends largely on the type of online social network being targeted. In this way, newspapers categorize various genres of social networking sites and list the reasons for the existence of fake accounts on their networks and how they damage and exploit network facilities.

Since the computer revolution three decades ago, artificial intelligence has become a necessity for human lives. As part of this, machine learning and the presented methodologies are employed to solve real-world issues in place of humans by using their enhanced classification, optimization, and prediction skills. Artificial intelligence, although techniques are proposed to handle a variety of problems, each strategy may perform better in certain problem areas and datasets. Numerous studies have been done and have yielded conflicting results (Rathore et al., 2018). Numerous machine learning approaches are applicable for predicting and analysing classification data including Backpropagation Learning, Radial Basis Function Neural Networks, k-Nearest Neighbour and Support Vector Machine (Al-rousan, 2019). However, most of machine learning method that been used by other are restricted used for specific data only. Such as online social media data for respected country only.

1.4 Research Questions

In this study, three research questions (RQ) to be answered to achieve the outlined research objective (RO). They are;

a. RQ1: How fake account activities can be monitor in OSN?
b. RQ2: How can we investigate and distinguish these fake account identities in OSN?
c. RQ3: How can we validate whether the account is fake or not?

1.5 Research Objectives

Specifically, the research objectives (RO) are proposed to:

a. To analyse the behaviour of the fake account in OSN.
b. To identify differences between normal account, fake account by combining Fake account behavioural and digital signature features.
c. To validate the features using KNN, NN and SVM classification.

Indicates correlation between RQ, RO, Expected Outcome (EO), and this study hypothesis