International Journal for Modern Trends in Science and Technology, 8(10): 37-42, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0810008
Available online at: http://www.ijmtst.com/vol8issue10.html

Detection of Fake and Clone accounts in Social Media by Employing Machine Learning Techniques

Swaroopa Shastri | Reena Rathod

Department Of Computer Science(MCA), VTU CPGS Kalaburagi, Kalaburagi, Karnataka, India.

To Cite this Article
Swaroopa Shastri and Reena Rathod. Detection of Fake and Clone accounts in Social Media by Employing Machine Learning Techniques. International Journal for Modern Trends in Science and Technology 2022, 8(10), pp. 37-42. https://doi.org/10.46501/IJMTST0810008

Article Info
Received: 08 September 2022; Accepted: 29 September 2022; Published: 04 October 2022.

ABSTRACT

People with comparable interests or connections in the real world can communicate on an online social network (OSN). The security and privacy concerns around OSN are growing along with its popularity. Users of social networks are facing significant security issues due to fake and cloned profiles. Cloning of user profiles is a severe issue in which information about already existing users is taken to make fake profiles, that are utilized to harm the identity of the original profile owner. A fake profile is one that is created on social media under name of individual or business that doesn't actually existing in order to engage in malicious behavior. In this proposed work can identify fake and clone Twitter profiles. Random Forest, Decision Tree, and Logistic Regression techniques are utilised to detect Profile Clonin. The effectiveness of these strategies in identifying fake and clone profiles is compared. Precision of outcomes are associated between the results of different methodologies and the Random Forest algorithm gave the best accuracy.

KEYWORDS: *Clone, Fake, Random Forest,Decision Tree, and Logistic Regression techniques, Online Social Networks, OSN*

1. INTRODUCTION

Billion of users throughout the world use ONLINE Social Networks (OSN) like Twitter, Instagram, LinkedIn, Facebook, etc. to establish network connections. A new era of networking has been ushered in by social networks' simplicity and accessibility.

Users of OSN exchange a wide range of information on network, including images, videos, institution names, telephone numbers, mail addresses, residential addresses, family relationships, financial information, and employment information. If attackers get their hands on this information, the consequences are very bad. The majority of OSN consumers are ignorant of safety hazards that social networks pose and are therefore vulnerable to these assaults. If children are the victims, the risks are more serious. **Cloned profiles are created from data of existing users,that are being used to steal identities of those who hold them. The two forms of profile cloning are similar website & across site**. It's possible to build duplicate profile on another network by utilizing a user's login credentials from another networkPerson information obtained from one network and used to create a fake profile on some other platform in which user does not have an account is known as a phishing attack, this practise is known as cross-site profile cloning. As

social networks make it relatively easy to register in an effort to draw in more members, the number of fraudulent profiles being created is rising alarmingly. To contact a victim and engage in malicious activity, an attacker makes a false profile. Additionally to disseminate spam and false news.

The paper is set up as follows. In Section II, the literature review is described. In Section III, the suggested methodology is described. The findings are discussed in Section IV. Finally, Section V provides the paper's conclusion.

2. RELATED WORK

In today's social networks, fake and clone profiles pose a very real threat. Therefore, a detection technique is absolutely important to catch these con artists that exploit people's faith to collect personal data and fabricate false profiles. Many academics have researched this topic and suggested ways to spot these kinds of social network profiles. Following are some of these techniques discussed.

Sowmya P and Madhumita Chatterjee [1] established a similarity metric, and decision tree methods are utilised. In order to engage in malevolent behaviour and commit online social crimes, fake profiles are created. So, a detection technique that can successfully identify duplicated and false profiles in online social networks has been proposed.

A prototype has been proposed by Georgios Kontaxis, Iasonas Polakis, Sotiris Ioannidis, and Evangelos P Markatos [2] to determine whether or not users have been the target of a cloning attempt. Information from profile page is used to search OSN for other profiles that have a similarity to user profile. A similarity score is calculated by comparing the similarity of attribute values. Random Forest, Decision Tree and Logistic Regression are algorithms that may be used to identify both false & clone accounts in order to protect users' social life. A clone is a profile that has high degree of resemblance with original.

In their research, Brodka, Mateusz Sobas, and Henric Johnson[3] provide two new methods for detecting cloned profiles. Using a network of connections is one approach, while using similarity in attribute values between the original & cloned profiles is a another approach. A person who is unaware knowing his profile is already duplicated will become victim. Once the victim's name has been entered as the main key, a query search is used to find all profiles with names of victims in it. S is determined by comparing the victim's profile (Pv) with that of the possible clone (Pc). In this case, it's assumed that there is a clone of profile since S(Pc, Pv)>Threshold. Due to his knowledge including which account is his original, the user does manual verification.

Researchers Cresci S and Di Pietro R and Petrocchi M and Spognardi A, Tesconi M examined most relevant characteristics and regulations (presented by Academia and the Media) for identifying fake Twitter accounts in their study [4]. These rules and characteristics were used to train a variety of machine learning classifiers. Class A classifier was then built, which can differentiate between real and bogus accounts.

Ahmed El Azab, Amira M. Idrees, Mahmoud A. Mahmoud, and Hesham Hefny [5] has proposed a classification strategy to detect bogus Twitter accounts. From numerous research, they've pulled together several relevant characteristics for the identification process, refined it, & provided them certain weight in the first phase. Only seven of the 22 attributes that can reliably identify fake accounts were chosen after applying these parameters to classification methods. The classification method that produces the most accurate results is chosen after a comparison of the available strategies based on the obtained results.

A method has been presented by M.A.Devmane and N.K.Rana[6], and the many activities to be researched include updates, Wall posts and comments, by recent actions, etc. Based on the comparison of threshold levels of user-specific profile attribute values and network similarity analysis, malicious that steals users' identities is discovered. Creating an account, user operation, monitoring, searching recent activity, detecting cloned profiles, choosing a profile to be studied, and determining whether a profile is real or fake are some of the processes used in the research. Experiments are also used to assess the procedures, and the results unmistakably showed that, when compared to established techniques, the suggested algorithms are advantageous and efficient. With a large amount of profile data, it can be seen that the

approach utilised can locate the cloning profile with approximately 93.87% accuracy.

In order to discover the degree of similarity between the cloned profile and the genuine one on Facebook, Kiruthiga. S., Kola Sujatha. P, and Kannan[7] have presented a technique where clone attacks are recognised based on user action time period and users click pattern. The performance of the similarity between users is enhanced by Cosine similarity and Jaccard index.

A categorization approach for identifying bogus Twitter accounts has been put forth by Buket Erşahin, Ozlem Aktaş, Deniz Kilinç, and Ceyhun Akyol[8]. He used supervised discretization (EMD) on numerical features to preprocess our dataset, and he then examined the naive Bayes predictions.

3. PROPOSED METHODOLOGY

TheproposedarchitectureconsistsofmodulesforFakeProfiledetectionandCloneProfiledetection.Twitter profiles that are false are found using the fake detection module. Here, bogus profiles are discovered using methods that efficiently separate them from real profiles. One of the rules used to identify phoney accounts is that they typically lack a profile name and an image. They don't give any background information on the account. Because they don't want to reveal their location in tweets, the geo-enabled field will be set to false. They frequently tweet a lot, occasionally their profiles won't have tweeted at all, etc. When the rules are applied to the profile, a counter is incremented for each matching rule; if the counter value exceeds a set threshold, the profile is deemed to be phoney.

Utilizing similarity measures, profiles that are clones based on Attribute and Network similarity can be found. As input, the user profile is used. From the profile, user identifiable information is taken. The search is for profiles with characteristics that match the user's profile. If the similarity index exceeds the threshold, the profile is classified as a clone; otherwise, it is considered normal[1]

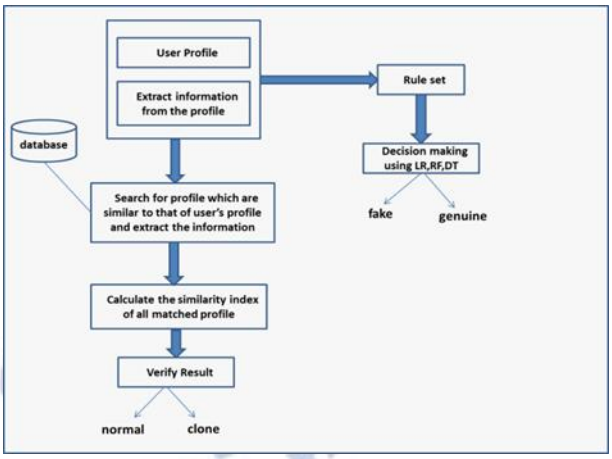

Fig.1.Architectureofproposedsystem.

Based on the similarity of attribute values between the profiles, attribute similarity is determined. The following characteristics are taken into account while calculating similarity: Name, ScreenName, Language, Location, and Time zone. Cosine similarity and Levenshtein distance are used to gauge how similar the qualities are to one another. Levenshtein distance is used to determine similarity between two sequences, and cosine similarity is used to determine similarity between words.

Cosinesimilarityformulaisgivenbyequation(1)

$$\mathbf{similarity}(\mathbf{A},\mathbf{B}) = \mathbf{cos}(\boldsymbol{\theta}) = \frac{\mathbf{A}\cdot\mathbf{B}}{\|\mathbf{A}\|\,\|\mathbf{B}\|} \qquad (1)$$

Where θ is angle between the vectors

A.B is dot product between A and B and calculate as

$$\mathbf{A}.\mathbf{B} = A^T B = \sum_{i=1}^{n} A_i B_i = A_1 B_1 + A_2 B_2 + \cdots \ldots + A_n B_n$$

$\|\mathbf{A}\|$ represents the the L2 norm or magnitude of the vector which is calculated as

$$\|\mathbf{A}\| = \sqrt{A_1^2 + A_1^2 + \cdots . + A_1^n}$$

When there are two non-zero vectors named Ai and Bi.

A cosine similarity of 1 exists between two vectors when they have the same orientation, 0 when they are at 90°, and -1 when they are diametrically opposing [1]. A similarity metric used to compare two sequences is the Levenshtein distance.

The Levenshtein distance between any two sequences is the least amount of insert, delete, or substitution operations necessary to transform one sequence into another. Equation describes the Levenshtein distance between two strings, a, and b, with lengths I and j, respectively (2)

$$lev_{a,b}(i,j) = \begin{cases} \max(i,j) & \text{if } \min(i,j) = 0 \\ \min \begin{cases} lev_{a,b}(i-1,j) + 1 \\ lev_{a,b}(i,j-1) + 1, \\ lev_{a,b}(i-1,j-1) + 1_{ai \neq bj} \end{cases} & \text{otherwise} \end{cases}$$

Network relationships are used to calculate network similarity[1]. The Followers ids parameter is used in this case to compare the profiles' network profiles. The list of accounts that the user is following is provided by followers ids. In order to prove that it is a genuine profile, the clone profile always tries to connect to the same group of people as its legitimate owner. Therefore, we can determine whether two profiles are similar or dissimilar in terms of network relationships by comparing the Followers ids of the two profiles.

The calculation of network similarity follows the equation (3)

Where NetSim - Network Similarity is concerned,
NetSim (Pv, Pc) = (|MFF vc|)/(|Fv|.|Fc| (3)
Pc - Profile of clone
Pv - Profile of victim
MFFcv - Set of Pv and PC's matching Followers ids
Fv - Set of Pv Follower IDs
Fc - Set of Pc Follower IDs

The profile is handled as a clone if the NetSim value is higher than the threshold, else it is processed normally[1]

In order to use classification methods, features are chosen. If an attribute does not depend on another property and improves the categorization process, it is chosen as a feature.

The dataset of profiles that have already been categorised as fake, real, or clone is required for the training purpose of the classification algorithms after attribute selection. The The process of dividing a data object into classes according to its associated qualities is known as classification. Decesion Tree, Random Forest, and Linear Regression are the categorization techniques used in this research. Classification uses a classifier.

Information gain and entropy are the splitting variables in C4.5. The attribute with the greatest information gain is chosen to make the decision, and the partitioned sub-trees are then cycled through again. The increase in information as demonstrated by equation (4)

Information(D) = -∑ (i=1)^n Pi log2 Pi (4)

where Pi is a symbol for probability.

To determine whether the Decision Tree technique is being utilised for classification, the Clone Porofile Detection Module is used. Based on the provided data, a decision tree is built. The property that divides the sample sets into subgroups most successfully is selected to go at each node of the tree.

The attribute with the greatest information gain is chosen to make the decision, and the partitioned sub-trees are then cycled through again. By creating a structure that resembles a tree, the Decesion Tree algorithm determines how similar the qualities are. The profile that is provided is compared to the profiles that are already stored in the database. The given profile is referred to as a clone if it matches one of the profiles in the database; otherwise, it is considered normal.

Random Forest is a flexible method that can do both regression and classification tasks. Different Decision Trees are produced on the subset of data. Additionally, it utilises the method based on all votes to integrate each tree prediction to obtain the overall tree prediction. It shares almost all of the same hyperparameters with bagging classifiers or decision trees. The best outcome will be used to forecast and identify dishonesty after creating many different types of trees. Each clasiifier result denotes a separate branch of the tree.

In machine learning, supervised learning methods like logistic regression are frequently used. A group of independent factors are used to predict the dependent variable's measure. When the dependent variable is categorical, the prediction is made using logistic regression. The probabilities that fall inside that range of numbers are provided by this algorithm. Answers can be True or False; there is no correct or wrong response. Various evaluation metrics are used to assess the system's performance.

Confusion matrix is a method for describing how well a classification system performs. You can use a confusion matrix to better understand what your classification model is doing correctly and what kinds of mistakes it is making. To identify the location of the error, the confusion matrix is used to depict all algorithm outputs.

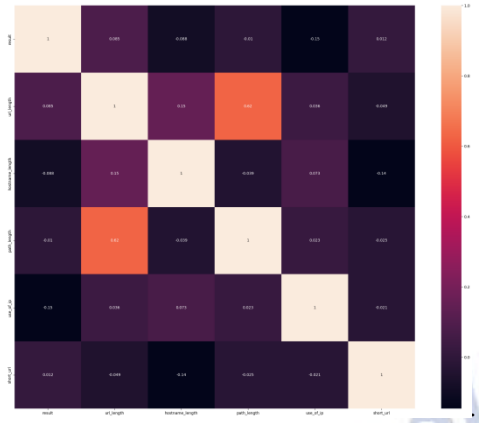

Fig2:confusion matrix

4. Result and Experiment

DatasetsUsed

The experiment's datasets were gathered via the Kaggle website. The URL is gathered A dataset called urldata.csv has 450175 records in it. It includes of Twitter datasets that are real, fake, and cloned. There are 76.80% of begin urls and 23.20 percent of malicious urls.

Data for training and testing are separated from the dataset.Classification algorithms are trained using training datasets, and the effectiveness of the algorithms is assessed using testing datasets. 80% of the data from the dataset was utilised to create a training data set, while 20% was used to create a testing data set.

24784 tweets in all were input into the system to help it detect fraudulent, clone, and profile accounts. As demonstrated in Fig. 3, the rule set was effective and successfully distinguished between real and phoney accounts with an accuracy of 96.12% by the random forest algorithm, 95.82% by decision tree, and 77.68% by logistic regression.

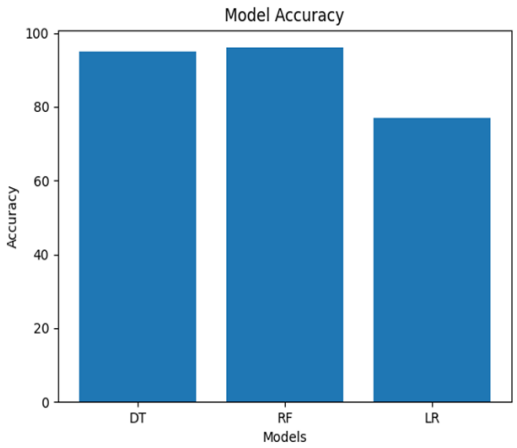

Fig 3:model accuracy comparison graph

Totalno.ofrecords	450175
No.ofgenuinerecords	1970
No. of fake records	345000
No.ofclonerecords	100000

Table:1

Models	Accuracy
Decision Tree	95.82%
Logistic Regression	77.68%
Random forest	96.12%

Table :2

The Result shows accuracy of all three algorithm. Soitcanbeconcludedthat clone detection using Decesion Tree and random forest gives better results as compared to that of using Logistic Regresion classification algorithm and random forest algorithm gave best accuracy.

5. Conclusion

Fake and clone profiles have become a major problem in online social networks. Occasionally, threats stemming from these profiles are heard in day-to-day living. As a result, a detection method that can find duplicate and duplicated Twitter profiles has been proposed. In order to identify between actual and phoney profiles, customary guidelines were used. Clone identification was carried out, and the effectiveness of Decision Tree, Logistic Regression, and Random Forest was evaluated. This study include tweets as well by utilising NLP methods .Decision tree, random forest, and logistic regression performed better than C4.5 in detecting the majority of the clones that were given into the algorithm And In this work, only profile characteristics of duplication detecting have been considered. To achieve high accuracy, more machine learning techniques might be applied.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Sowmya P and Madhumita Chatterjee ," Detection of Fake and ClonedProfiles in Online Social Networks", Proceedings 2019: Conference onTechnologiesforFutureCities(CTFC)

[2] Georgios Kontaxis, Iasonas Polakis, Sotiris Ioannidisand Evangelos P Markatos, "Detecting Social Network Profile Cloning", 2013

[3] Piotr Bródka, Mateusz Sobas and Henric Johnson, "Profile CloningDetection in Social Networks", 2014 European Network IntelligenceConference

[4] Stefano Cresci, Roberto DiPietro, Marinella Petrocchi, Angello Spognardi, Maurizio Tesconi,"Fame for sale: Efficient detection of fake Twitter followers", 2015 Elsevier'sjournal Decision Support Systems, Volume80

[5] Ahmed El Azab, Amira M Idrees, Mahmoud A Mahmoud, HeshamHefny,"FakeAccountDetectioninTwitterBasedonMinimumWeighted Feature set", World Academy of Science, Engineering andTechnology,InternationalJournalofComputerandInformationEngineeringVol:10, 2016

[6] M.A.Devmaneand N.K.Rana, "Detection and Prevention of Profile Cloningin Online Social Networks ", 2014 IEEE International Conferenceon Recent Advances and Innovations in Engineering

[7] Kiruthiga.S,KolaSujatha.PandKannan.A,"Detecting CloningAttackinSocialNetworksUsingClassificationandClusteringTechniques"2014InternationalConferenceonRecentTrendsinInformationTechnology

[8] Buket Erşahin, Ozlem Aktaş, Deniz Kilinç, Ceyhun Akyol, "Twitterfake account detection", 2017 International Conference on ComputerScienceand Engineering(UBMK)