International Journal of Engineering and Management Research
e-ISSN: 2250-0758 | p-ISSN: 2394-6962
https://ijemr.vandanapublications.com

Peer Reviewed & Refereed Journal
Volume-13, Issue-3 (June 2023)
https://doi.org/10.31033/ijemr.13.3.41

Automatic Detection of Fake Profiles in Online Social Network using Soft Computing

Faisal Farooqui[1] and Muhammed Usman Khan[2]
[1]PG Student, Department of Computer Science & Engineering, Integral University, Lucknow, INDIA
[2]Assistant Professor, Department of Computer Science & Engineering, Integral University, Lucknow, INDIA

[1]Corresponding Author: faisalfarooqui007@gmail.com

Received: 30-05-2023 Revised: 15-06-2023 Accepted: 30-06-2023

ABSTRACT

The proliferation of social media platforms and online communities has led to an increase in the creation and utilization of fake profiles for various deceptive purposes. Detecting these fake profiles is crucial to maintaining the integrity, security, and trustworthiness of online platforms. This abstract provides an overview of the techniques and challenges involved in automatically detecting fake profiles.

The detection of fake profiles poses a significant challenge due to the ever-evolving strategies employed by malicious actors. However, researchers and platform developers have devised several techniques to tackle this problem. Profile completeness analysis examines the information provided by users, such as profile pictures, connections, and consistency of details. Sparse or inconsistent data may raise suspicions of a fake profile. Image analysis involves reverse image searching and analyzing metadata to identify instances of profile picture misuse or manipulation.

Linguistic analysis focuses on analyzing the language used in profile descriptions, posts, and comments. Patterns such as poor grammar, spelling mistakes, or generic content may indicate automated or fraudulent account activity. Social network analysis studies the network structure and connections between accounts, identifying clusters of suspicious profiles with similar connections. Behavioral analysis techniques aim to identify abnormal or bot-like behavior exhibited by fake profiles, such as excessive friend requests, repetitive posting patterns, or spamming.

Machine learning models have emerged as powerful tools for fake profile detection. These models are trained on historical data, learning patterns and features associated with fake profiles. They can then classify new profiles based on these learned characteristics. CAPTCHA or verification tests provide an additional layer of security by deterring automated bot account creation.

Despite the progress made, detecting fake profiles remains a challenge. Adversarial actors continuously adapt their strategies, making it difficult to stay ahead. The privacy concerns and ethical implications surrounding the collection and analysis of user data also present challenges. Additionally, false positives and negatives are common in automated detection, requiring continuous refinement and improvement of detection techniques.

***Keywords*—** Image Analysis, Linguistic Analysis, Social Network Analysis, Behavioral Analysis

I. INTRODUCTION

Detecting fake profiles can be challenging, but there are several techniques and strategies that can help identify suspicious or fake accounts. While no method is foolproof, combining multiple approaches can improve the accuracy of the detection process. Here are some common techniques used to automatically detect fake profiles:

Profile Completeness: Fake profiles often have incomplete or sparse information. They may lack profile pictures, have limited connections or interactions, or provide inconsistent details[1,2].

Image Analysis: Reverse image search can help identify fake profile pictures by checking if the same image appears elsewhere on the internet. Additionally, analyzing image metadata, such as file properties or manipulation traces, can provide clues about image authenticity[3,4].

Linguistic Analysis: Analyzing the language used in profile descriptions, posts, and comments can reveal patterns indicative of fake profiles. Poor grammar, spelling mistakes, excessive repetition, or generic content may suggest automated or fraudulent account activity[5,6].
Social Network Analysis: Examining the network structure and connections between accounts can help identify clusters of fake profiles. If multiple accounts have similar or identical connections, it could indicate a network of fake profiles created for deceptive purposes[7,8].

Behavioral Analysis: Fake profiles often exhibit suspicious behavior such as excessive friend requests, repetitive posting patterns, or spamming. Analyzing user activity, such as posting frequency, timing, or engagement patterns, can help identify abnormal or bot-like behaviour.
Machine Learning Models: Using machine learning algorithms, it is possible to train models to detect fake profiles based on historical data. These models can learn

Peer Reviewed & Refereed Journal
Volume-13, Issue-3 (June 2023)
https://doi.org/10.31033/ijemr.13.3.41

patterns and features associated with fake profiles and then classify new profiles accordingly[9,10,11].

CAPTCHA or Verification Tests: Implementing CAPTCHA or other verification mechanisms can help deter automated bot account creation. While they may not catch all fake profiles, they can add an extra layer of protection.

User Reporting: Encouraging users to report suspicious profiles can help identify fake accounts. Incorporating reporting features and reviewing user complaints can aid in the detection process.

It's important to note that no single method is 100% accurate, and combining multiple techniques is generally more effective. Additionally, social media platforms and online communities often employ their own algorithms and strategies to detect and mitigate fake profiles[12].

Method	Number of images in the training set	Success rate	Reference
Principal Component Analysis	400	79.65%	[3]
Principal Component Analysis + Relevant Component Analysis	400	92.34%	[3]
	170	tanh function 69.40%	[4]
Independent Component Analysis	40	Gauss function 81.35%	[4]
Hidden Markov Model	200	84%	[5]
Active Shape Model	100	78.12-92.05%	[7],[8]
Wavelet Transform	100	80-91%	[9]
Support Vector Machines	-	85-92.1%	[10],[11]
Neural Networks	-	93.7%	[12]
Eigenfaces Method	70	92-100%	[13]

II. METHODOLOGY

Face Detection Authentication

Combining classifier is also a very nice strategy to improve performance of classifier. Adaboost combines number of weak classifiers to improve the performance of single weak classifier. Bagging stands for bootstrap aggregation. It averages over the predictions of all models. Most often bagging improves the performance of final classifier model. In bagging, different classifiers are trained on different datasets which randomly sampled from given data. Except for this random variations, the different classifiers effectively be the same. Boosting is major idea that come into pattern recognition over last fifteen years. In Adaboost, we assign weights to the point in the dataset which can be normalized so that they sum to one. Support vector machine is considered as one of the best classifier having great performance both in genomic to text data. The popularity for SVM was gained during 1990s and can be applied to complex data types beyond feature vectors (e.g., graphs and relational data sequences) by designing kernel functions for such data. HAAR features are also used extracting features which uses HAAR filters. HAAR features are sensitive to directionality of patterns. Local binary pattern are used for detecting edges and one of the very popular technique and used in wide range of applications. LBP is efficient for texture classification. It codifies local pattern in which in which central pixels has some threshold and is compared with neighboring pixels. The Local binary pattern histograms have different subareas at that point, linked into a spatially improved part histogram and is characterized as:

$$Hij = xy\ (Fi\ (x\ ,\ y) = i\ )I\ ((x\ ,\ y)$$

where I = 0, …, L−1; j = 0, …, N −1.

The different separated element histogram portrays the nearby surface and datasets of facial features.

LBP computation. SVM classifier is been utilized with HOG highlights for face identification. Hoard enormously outflanks wavelets what's more, level of smoothing

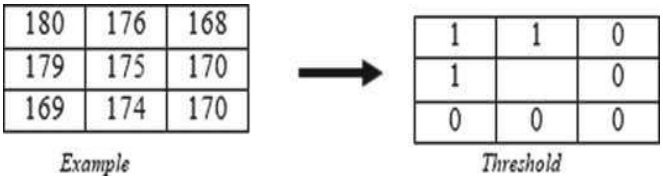

Figure 1: Pattern

prior to computing slopes harms, results underlines a significant part of the accessible data is from unexpected edges at fine scales that obscuring this for diminishing the affect-ability to spatial position is an error. Angles ought to be determined at the best accessible scale in the current pyramid layer and solid nearby differentiation standardization is fundamental for acceptable outcomes (Figs. 1 and 2).

Though SVM are planned to settle an old style two class issue which returns a parallel worth, the class of the object. To prepare our SVM calculation, we plan the

Peer Reviewed & Refereed Journal
Volume-13, Issue-3 (June 2023)
https://doi.org/10.31033/ijemr.13.3.41

Figure 2: Face detection. *Source* Internet

Face Recognition Authentication

Eigenfaces considered as 2D face acknowledgment issue, and countenances will be generally upstanding and front facing. That is the reason three dimensional data about the face isn't needed that lessens intricacy by a huge piece. It converts the face pictures into a bunch of premise capacities which basically are the head parts of the face pictures looks for headings in which it is more productive to address the information. This is mostly valuable for decline the computational exertion (Fig. 3).

Direct discriminant examination is principally utilized here to decrease the number of elements to a more sensible number previously acknowledgment since face is addressed by an enormous number of pixel esteems. Every one of the new aspects is a straight mix of pixel esteems, which structure a format. The direct blends acquired utilizing Fisher's straight discriminant are called Fisher faces. LBP is an request set of double examinations of pixel forces between the middle pixel and its eight encompassing pixels.

LBP(xa, ya) = oS(im − ia)2n
n

Gabor channels can take advantage of striking visual properties such as spatial restriction, direction selectivity, and spatial recurrence qualities. Thinking about

Dataset	Detection		
	Adaboost		SVM
	Haar	LBP	HOG
[1]	99.28%	95.32%	92.58%
[2]	98.56%	98.99%	94.30%
[3]	98.41%	69.93%	87.79%
[4]	96.96%	94.16%	90.98%
[5]	90.75%	88.91%	89.59%
Mean	**96.79%**	**89.46%**	**91.04%**

Figure 3: Face detection results summary

Data Set	Sub-Division	Images	Resolution	Individuals	Image/Individual
A	Face 94	3078	180*200	153	~20
	Face 95	1440	180*200	72	20
	Face 96	3016	196*196	152	~20
	Grimace	360	180*200	18	20
B	Pain Expressions	599	720*576	23	26

Figure 4: Face Recognition results summary

III. PRIOR APPROACH

Naive Bayes Classification

In Bayesian classification there is a hypothesis that the given data belongs to a par- ticular class. Then calculatethe probability for the hypothesis of being true. This is among the most practical approaches for certain types ofproblems. The approach requires only one scan of the whole data.

The Bayes theorem is

$$P(A/B) = \frac{P(B/A)P(A)}{P(B)}$$

Where P(A) refers to the probability that event A will occurs .

P(A/B) stands for the probability that event A will happen, given that event B has already happened. The Naive

Bayes classifier exploits the Bayes's rule and assumes independence of attributes.

It assigns an instance S_k with attribute values (A1=V1 ,A2=V2 , … . . , Am=Vm) with maximum Prob (Ci / (V1 ,V2,….Vi)) for all i.

For example the probability of assigning to class Ci and Cj is calculated for an instance Skbelonging to Ci Likelihood of Sk belonging to Ci

$$\text{Prob}\left(\frac{c_i}{v_1, v_2, \cdots v_m}\right) = \frac{P\left((v_1, \ldots v_m)/c_i\right) \cdot P(c_i)}{P(v_1 \ldots \ldots vm)}$$

Likelihood of Sk belonging to Cj

Peer Reviewed & Refereed Journal
Volume-13, Issue-3 (June 2023)
https://doi.org/10.31033/ijemr.13.3.41

$$\text{Prob}\left(\frac{c_j}{v_1, v_2, \cdots v_m}\right) = \frac{P\left((v_1, \ldots v_m)/c_j\right) \cdot P(\text{cj})}{P(v_1 \ldots \ldots vm)}$$

Therefore, when comparing Prob $\left(\frac{c_i}{v_1, v_2, \cdots v_m}\right)$ and Prob $\left(\frac{c_j}{v_1, v_2, \cdots v_m}\right)$

Only need to compute $P\left((v_1, v_2 \ldots \cdot v_m)/c_i\right)\cdot P(c_i)$ and $P[(v_1, v_2 \ldots v_m)/(c_i)] \cdot P(c_j)$

Under the assumption of independent attributes,
Furthermore,

$$P\ C\ i = \frac{\text{no training sample belong to } C_i}{\text{total No of training sample}}$$

IV. OUR APPROACH

Identifying Fake profile on social media with the help of Facial Recognition Technology

While registering the profile on social media, the user will have to scan their face in addition to providing their ID and password. This scanned facial image will then be stored in the database and will be used in future to verify the authenticity of user. The technology collects a set of unique biometric data of each person associated with their face and facial expression to identify, verify and/or authenticate a person. Unlike other identification solutions such as passwords, verification by email, or fingerprint identification, Biometric facial recognition uses unique mathematical and dynamic patterns that works as a face scanner and makes this system one of the safest and most effective ones.

User level Approach to determine if the user's profile is fake or genuine

Creating a single mathematical equation to determine the authenticity of a user's profile is a complex task since it requires considering multiple factors and data points. However, you can develop a scoring mechanism that combines various features and assigns a score indicating the likelihood of a profile being fake or genuine. Here's an example of how you can formulate such an equation:

Let's denote the user's profile as P and the features extracted from the profile as F = {f1, f2, ...,fn}. Each feature represents a characteristic or attribute of the profile that can be indicative of its authenticity. The values of these features can be normalized between 0 and 1 for simplicity[23,24]:

- Assign weights to each feature: W = {w1, w2, ...,wn}, where each weight represents the importance or significance of a feature in determining the profile's authenticity. The weights can be assigned based on domain knowledge or learned from the training data.
- Calculate the normalized score for each feature: S = {s1, s2, ...,sn}, where sj = f j * w j.
- Calculate the overall profile score, denoted as Score(P), by combining the individual feature scores. One approach is to use a weighted sum
    - Score(P) = Σ(sj) / Σ(wj) for j = 1 to n.
- Here, the numerator represents the sum of all feature scores, and the denominator represents the sum of their corresponding weights. The division ensures that the score is normalized within the range of 0 to 1.
    - Interpretation: Set a threshold value, T, which acts as a decision boundary. If Score(P) > T, the profile is classified as genuine; otherwise, it is classified as fake.
    - Determining the optimal weights and threshold value typically requires training the model using labeled data and applying techniques such as machine learning or statistical analysis. By adjusting these parameters based on the training data and evaluating the model's performance, you can refine the equation to achieve better accuracy in differentiating between fake and genuine profiles.

1. At the time of signing up to a social media platform, the user will have to fill all the personal information as well as scan their face for biometric purposes. Providing facial biometric will be mandatory for creating a profile on the platform.
2. Once the profile is created the user will try to login to the account using their credentials. Ask the user for authentication using facial recognition:
    - If the person accepts, verify the user with facial recognition technology.
    - If the person denies, allow them to login only for a specific number of times (say 5 times)
3. While the user has logged in and is using the platform, show "Verification of User Identity with Facial Recognition" modal occasionally to the user for authentication purposes.
    - If the person accepts, verify the user with facial recognition technology.

Peer Reviewed & Refereed Journal
Volume-13, Issue-3 (June 2023)
https://doi.org/10.31033/ijemr.13.3.41

- If the person denies, allow them to login only for a specific number of times (say 5 times)

4. If the user has logged in for the specific number of times (5 times) and tries to log in for the 6th time without providing facial recognition, generate an alert for the user to notify them that they have exhausted the maximum number of attempts without facial authentication. Provide an option to continue using their profile only after facial authentication is done.
5. If there has been no action taken on the alert generated, the system will block the user profile temporarily. To unblock the account the user will have to mandatorily provide facial recognition authentication.
6. If the user does not authenticate the blocked account using facial recognition, the account will stay blocked for a specific number of days, after which it will be permanently deleted[28].

Figure 1.6: Facial reorganization while login process

System level approach to determine if the user's profile is fake or genuine

1. At the time of user registration, store user facial biometric details mandatorily in the system.
2. In the database, each user will have a unique identification ID and a parent ID. They both will have the same values initially when the user profile is created.
3. A job will run daily at a specific time which will find all the user IDs with same Facial_Encrypted_Identity_Value (facial biometric data)
4. In case of multiple profiles, the profile with the oldest date will become parent profile. In the database, the parent ID value for all the other child profiles will be updated to reflect the newly identified parent. The system will generate alert notification to all the profile users to make them aware of the situation.
5. The system will generate alert notification to the parent profile asking them to start using facial authentication. This alert will be generated for a specific number of times (say 5 times). All other child profiles will be temporarily blocked.
6. If there has been no action taken on the alert generated, the system will block the parent user profile temporarily. To unblock the account the user will have to mandatorily provide facial recognition authentication.
7. For child profiles provide an option CONCERN TO DETACH (with Facial Authentication check the child profile can detach itself from Parent profile and become independent)
8. After the job execution if a profile entry in database has same value for Unique identification ID and parent ID, the profile is considered as independent.
9. If the parent user does not authenticate the blocked account using facial recognition, the account will stay blocked for a specific number of days, after which it will be permanently deleted.

The system proposed is a real-time system. It takes enter photo through a net camera continuously till the application logges off.. The captured photo are then cropped via the Face Detection module and saves only the facial in formation in JPEG structure of 100x100 matrix size. This is a colored image matrix having three layers. The layers are for red, green, and blue colour in the image.The snap shots are saved in a sequence of their incidence time. That is, the face which is detected first is saved first in the database and then ext is saved at the next location in database. The identify of the face photo is simply the numbers with extension.jpg. These numbers are the sequence wide variety generated at the time of capturing. There are two factors for having filename as the range name. First is that it clearly suggests the sequence of the character they have come in-front of the camera. And these cond factor is, at the time of training the structures equentially takes the training dataset of face images. It's very easy to create database of egienface the use of this approach as any for loop is succesful to increase the sequence wide variety till the end of file. While if the filename is something, say text, then this would have been challenging to do. After growing the database the machine is trained itself via calculating the face space. This is carried out by way of the use of the principal component evaluation algorithm accompanied through linear discriminant evaluation algorithm. These two algorithms are explained above. They minimize the dimension of the facespace. These faces tempo keeps on altering after each change made to the TRAININGDATABASE. The photograph which is detected with the aid of the internet camera are saved in anotherfile/folder known as

Peer Reviewed & Refereed Journal
Volume-13, Issue-3 (June 2023)
https://doi.org/10.31033/ijemr.13.3.41

TESTDATABASE, they are additionally in number.jpg format, e.g. 1.jpg, 194.jpg.number.jpgformat,e.g.1.jpg,194.jpg.

Figure 5: Images used in the system

In the database, there are five hundred samples, five photographs of every student in one-of-a-kind positions with different emotions. The face picture used in this system is of100 x a hundred each. The pics in the TEST DATABASE are used to check the system's accuracy and to recognize the face from our database.Facerecognitionratetotallydependuponthedatabase andthesizeoftheimageused.Also dimension of the picture determines the accuracy price of the system. In this paper, we studied and analyzed the facial facets and extraction the usage of fast PCA and LDA. Here, the assessment between PCA and LDA really exhibit this.

PCA < LDA:

- The training dataset is large.
- The variety of training is ample (using a gallery).
- The number of elements is giant (dimension).

PCA > LDAL:

- The training dataset is small.
- The range of training lessons is now not enough (using a gallery).
- The quantity of aspects is small (dimension).

There are number of output of the proposed device is shown beneath one through one. In Figure 6, the preliminary window that appliers will seem to be like. In Figure 7, the face detection is shown and in Figure 8, the face recognition module is shown.

Figure 6: The system application GUI's opening screen

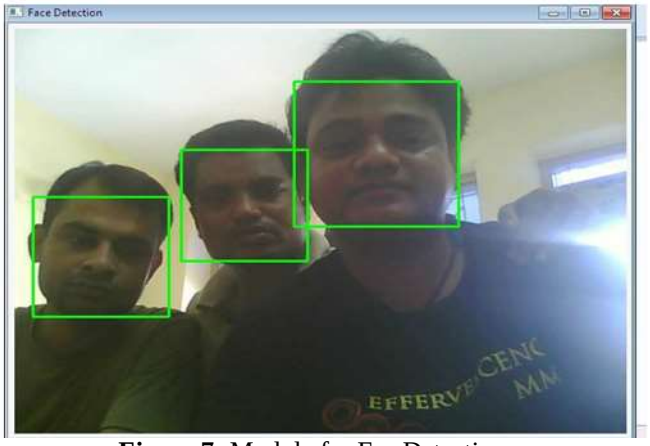

Figure 7: Module for Fac Detection

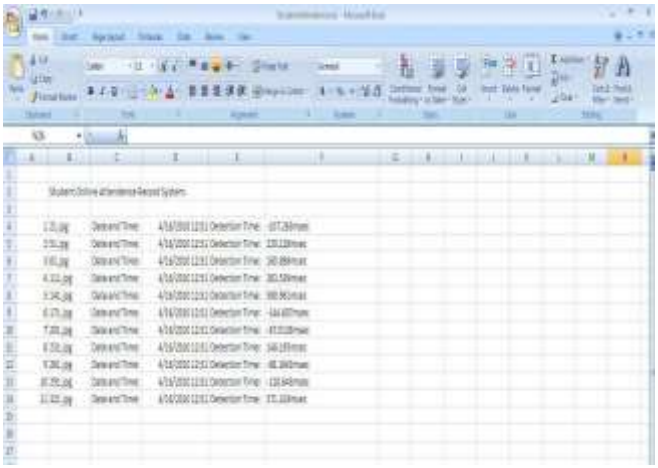

Table 5.2.3: Instant face recognition for at ten dance System file

Figure 8: Face recognition module

Peer Reviewed & Refereed Journal
Volume-13, Issue-3 (June 2023)
https://doi.org/10.31033/ijemr.13.3.41

V. CONCLUSION

Automatic detection of fake profiles is a critical area of research and development. By combining various techniques, such as profile completeness analysis, image analysis, linguistic analysis, social network analysis, behavioral analysis, machine learning models, and verification tests, platforms can enhance their ability to identify and mitigate the impact of fake profiles. Continued research, collaboration, and adaptation to emerging trends are vital to combating the persistent problem of fake profiles in the digital landscape.

This paper discussed about difference between face recognition and detection. Face detection is done by using Adaboost. Face detection is detecting one or many faces insteal images or sequence of video images. Eigen face is image-based detection which involves the extraction of eigen applying Principal Component analysis, faces which reduces the dimensionality of input spaces. One of the problem with eigen faces is that it does not minimize intra class variance. Fisher's Linear Discriminant is classifier is optimal classifier compared to PCA which reduces intra class variance. Machine learning algorithm also provides method to train classifier for detection and recognition of faces using unique measurement of faces and match that data with the known faces in a database. Kernel method and SVM are some of the machine learning algorithm (Fig.4).

REFERENCES

[1] Kumar, N. & Reddy, R. N. (2012). *Automatic detection of fake profiles in online social networks* (Doctoral dissertation).

[2] Kulkarni, S. M., Dhamdhere, V. & Young, M. (2018). Automatic detection of fake profiles in online social networks. *Open Access International Journal of Science and Engineering*, *3*(1), 70-73.

[3] Sahoo, S. R. & Gupta, B. B. (2021). Multiple features based approach for automatic fake news detection on social networks using deep learning. *Applied Soft Computing*, *100*, 106983

[4] Srivastava, S., Haroon, M. & Bajaj, A. (2013, September). Web document information extraction using class attribute approach. In: *4th International Conference on Computer and Communication Technology (ICCCT)*, pp. 17-22.

[5] Khan, W. & Haroon, M. (2022). An efficient framework for anomaly detection in attributed social networks. *International Journal of Information Technology*, *14*(6), 3069-3076.

[6] Khan, W. & Haroon, M. (2022). An unsupervised deep learning ensemble model for anomaly detection in static attributed social networks. *International Journal of Cognitive Computing in Engineering*, *3*, 153-160.

[7] Zare, M., Khasteh, S. H. & Ghafouri, S. (2020). Automatic ICA detection in online social networks with PageRank. *Peer-to-Peer Networking and Applications*, *13*, 1297-1311.

[8] Khan, W. & Haroon, M. (2022). An unsupervised deep learning ensemble model for anomaly detection in static attributed social networks. *International Journal of Cognitive Computing in Engineering*, *3*, 153-160.

[9] Sansonetti, G., Gasparetti, F., D'aniello, G. & Micarelli, A. (2020). Unreliable users detection in social media: Deep learning techniques for automatic detection. *IEEE Access*, *8*, 213154-213167.

[10] Khan, W. (2021). An exhaustive review on state-of-the-art techniques for anomaly detection on attributed networks. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(10), 6707-6722.

[11] Siddiqui, Z. A. & Haroon, M. (2023). Research on significant factors affecting adoption of blockchain technology for enterprise distributed applications based on integrated MCDM FCEM-MULTIMOORA-FG method. *Engineering Applications of Artificial Intelligence*, *118*, 105699.

[12] Husain, M. S. (2020). A review of information security from consumer's perspective especially in online transactions. *International Journal of Engineering and Management Research*, *10*.

[13] Khan, A. M., Ahmad, S. & Haroon, M. (2015, April). A comparative study of trends in security in cloud computing. In: *Fifth International Conference on Communication Systems and Network Technologies*, pp. 586-590.

[14] Ala'M, A. Z., Faris, H., Alqatawna, J. F. & Hassonah, M. A. (2018). Evolving support vector machines using whale optimization algorithm for spam profiles detection on online social networks in different lingual contexts. *Knowledge-Based Systems*, *153*, 91-104.

[15] Khan, N. & Haroon, M. (2022). Comparative study of various crowd detection and classification methods for safety control system. *Available at: SSRN 4146666*.

[16] Siddiqui, Z. A. & Haroon, M. (2022). Application of artificial intelligence and machine learning in blockchain technology. In *Artificial Intelligence and Machine Learning for EDGE Computing*, pp. 169-185. Academic Press.

Peer Reviewed & Refereed Journal
Volume-13, Issue-3 (June 2023)
https://doi.org/10.31033/ijemr.13.3.41

[17] Haroon, M., Tripathi, M. M. & Ahmad, F. (2020). Application of machine learning in forensic science. In: *Critical Concepts, Standards, and Techniques in Cyber Forensics*, pp. 228-239. IGI Global.

[18] Shu, K., Wang, S. & Liu, H. (2018, April). Understanding user profiles on social media for fake news detection. In: *IEEE Conference on Multimedia Information Processing and Retrieval (MIPR)*, pp. 430-435.

[19] Khan, W., Haroon, M., Khan, A. N., Hasan, M. K., Khan, A., Mokhtar, U. A. & Islam, S. (2022). DVAEGMM: Dual Variational Auto encoder with gaussian mixture model for anomaly detection on attributed networks. *IEEE Access*, *10*, 91160-91176.

[20] Tripathi, M. M., Haroon, M., Khan, Z. & Husain, M. S. (2022). Security in digital healthcare system. *Pervasive Healthcare: A Compendium of Critical Factors for Success*, 217-231.

[21] Shakeel, N., Haroon, M. & Ahmad, F. (2021). A study of wsn and analysis of packet drop during transmission. *International Journal of Innovative Research in Computer Science & Technology (IJIRCST)*.

[22] Khan, N. & Haroon, M. (2023). A personalized tour recommender in python using decision tree. *International Journal of Engineering and Management Research*, *13*(3), 168-174.

[23] Khan, W. & Haroon, M. (2022). A pilot study and survey on methods for anomaly detection in online social networks. In: *Human-Centric Smart Computing: Proceedings of ICHCSC*, pp. 119-128. Singapore: Springer Nature Singapore.

[24] Yamak, Z., Saunier, J. & Vercouter, L. (2018). SocksCatch: Automatic detection and grouping of sockpuppets in social media. *Knowledge-Based Systems*, *149*, 124-142.

[25] Tripathi, M. M., Haroon, M. & Ahmad, F. (2022). A survey on multimedia technology and internet of things. *Multimedia Technologies in the Internet of Things Environment*, *2*, 69-87..

[26] Haroon, M., Misra, D. K., Husain, M., Tripathi, M. M. & Khan, A. (2023). Security issues in the internet of things for the development of smart cities. In: *Advances in Cyberology and the Advent of the Next-Gen Information Revolution*, pp. 123-137. IGI Global.

[27] Haroon, M., Tripathi, M. M., Ahmad, T. & Afsaruddin. (2022). Improving the healthcare and public health critical infrastructure by soft computing: An overview. *Pervasive Healthcare: A Compendium of Critical Factors for Success*, 59-71.

[28] Bailer, W., Thallinger, G., Backfried, G. & Thomas-Aniola, D. (2021, May). Challenges for automatic detection of fake news related to migration. In: *IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA)*, pp. 133-138.