International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 2, Mar-Apr-2026, ISSN (Online): 2395-566X

Instaguard: Fake Instagram Account Detection

Mrs. P.V. Javkar[1], Mr. Damodhar N Bulbule[2], Mr. Arya D Tapkir[3], Mr. Kaivalya R Bhadange[4], Mr. Devraj A Yadav[5]
[1]Project Guide SVCP, Pune
[2]Computer Technology Department

Abstract- Social media platforms have become a major part of daily communication, marketing, entertainment, and information sharing. Among them, Instagram is one of the most widely used platforms across the world. However, the rapid growth of Instagram has also led to the creation of a large number of fake accounts. These fake accounts are often used for scams, impersonation, phishing, spam promotion, fake giveaways, misinformation, and fraudulent advertisements. Detecting such accounts has become an important research problem in the field of cybersecurity and social media analysis. Traditional fake account detection systems mainly focus on profile-related information such as follower count, following count, number of posts, account age, and user activity. Although these features are useful, they may fail to detect accounts that hide suspicious content inside images. Many fake Instagram accounts include scam messages, promotional offers, fake links, or misleading text inside profile images, stories, and post images. Such hidden text cannot be effectively analyzed using normal text-based techniques alone. This paper proposes a method for detecting fake Instagram accounts using Optical Character Recognition (OCR). OCR is used to extract text from profile pictures, post images, and other visual content associated with an Instagram account. After text extraction, suspicious keywords, spam patterns, links, and unusual promotional phrases are analyzed. These OCR-based features are combined with profile-level features such as follower-following ratio, posting behavior, account age, username structure, and bio information. Based on these features, the account is classified as genuine or fake. The proposed approach improves the detection of fake accounts by analyzing both textual and visual content. This makes the system more effective in identifying hidden spam techniques used by fake profiles. The paper also discusses methodology, algorithm steps, feature extraction, preprocessing, system architecture, results, limitations, and future scope.

Keywords – Fake Instagram Account Detection, Optical Character Recognition (OCR), Social Media Security, Cybersecurity, Image Text Extractio.

I. INTRODUCTION

Social media has transformed the way people communicate, share information, promote businesses, and interact with communities. Instagram, in particular, has become one of the most popular platforms for sharing photos, videos, and stories. Millions of users actively use Instagram for personal communication, entertainment, influencer marketing, and business branding.

Despite its popularity, Instagram faces a major issue in the form of fake accounts. Fake accounts are profiles created with false identities or malicious intentions. These accounts may be used for various harmful activities such as:

- Sending spam messages
- Promoting fake products or services
- Impersonating celebrities or brands
- Running phishing attacks
- Spreading false information
- Increasing fake followers and engagement
- Conducting financial scams

Fake accounts reduce user trust and create security risks for individuals, businesses, and the platform itself. Detecting such accounts is difficult because fake profiles often imitate real users by using profile pictures, copied bios, and attractive posts. Some advanced fake accounts avoid detection by embedding suspicious content within images rather than writing it openly in captions or profile descriptions.

Optical Character Recognition (OCR) is a technology used to detect and extract text from images. By using OCR, it becomes possible to examine the hidden textual content present in images posted by Instagram accounts. This extracted text can reveal spam offers, scam messages, misleading claims, suspicious links, and repeated promotional patterns.

This project introduces an OCR-based fake Instagram account detection system. The system combines image-based text extraction with profile feature analysis. This combination improves the ability to identify suspicious accounts more accurately than traditional methods alone.

II. PROBLEM STATEMENT

The number of fake Instagram accounts has increased significantly with the growth of social media usage. These fake accounts create several problems, including online fraud, impersonation, misinformation, cyberbullying, and spam marketing. Existing fake account detection methods often rely on profile statistics, activity patterns, and textual information in captions or bios. However, such methods may fail when suspicious content is embedded inside images.

Fake account creators frequently place scam offers, promotional text, or external links inside images to avoid automatic text analysis. As a result, traditional systems that ignore image content may classify such accounts incorrectly.
Therefore, there is a need for a more advanced detection technique that can analyze both account profile information and textual content hidden inside images. OCR provides a useful solution to extract such hidden text and improve the performance of fake account detection systems.

III. OBJECTIVES

The main objective of this project is to detect fake Instagram accounts by using OCR (Optical Character Recognition) and profile-based analysis.

1. To study fake Instagram accounts The project aims to understand how fake accounts are created and how they affect social media platforms through spam, scams, and misleading activities.
2. To collect Instagram profile and image data
   The system collects important account information such as profile image, post images, bio, and other profile details for analysis.
3. To preprocess images for OCR The project uses image preprocessing techniques like resizing and grayscale conversion so that the text inside images can be extracted more clearly.
4. To extract text from images using OCR A main objective is to use OCR to read text from Instagram profile pictures and posts, especially when fake accounts hide suspicious content inside images.
5. To identify suspicious keywords and patterns
   The extracted text is analyzed to find spam words, fake offers, unusual links, and misleading phrases that are often found in fake accounts.
6. To analyze profile-based features The project also studies account-related details such as followers, following, posting behavior, and profile information to support fake account detection.
7. To classify the account as real or fake The final objective is to combine OCR text features and profile features, then apply a classification method to identify whether the Instagram account is genuine or fake.
8. To improve social media security This project helps in detecting suspicious accounts and supports safer use of Instagram by reducing spam and fake activities.

IV. WORKING OF PROJECT

The proposed system is designed to detect fake Instagram accounts by combining OCR-based text extraction with profile analysis.

Step 1: Input Instagram Data
The system first takes Instagram account details as input. This includes profile images, post images, and basic account information needed for analysis.

Step 2: Image Preprocessing
The collected images are preprocessed before OCR is applied. In this step, operations like resize and grayscale conversion are used to make the text clearer and easier to read.

Step 3: Apply OCR
After preprocessing, the images are given to an OCR engine such as Tesseract. The OCR engine reads the text present inside profile images and posts.

Step 4: Store Extracted Text
The text obtained from OCR is stored for further analysis. This helps the system examine all extracted words and phrases properly.

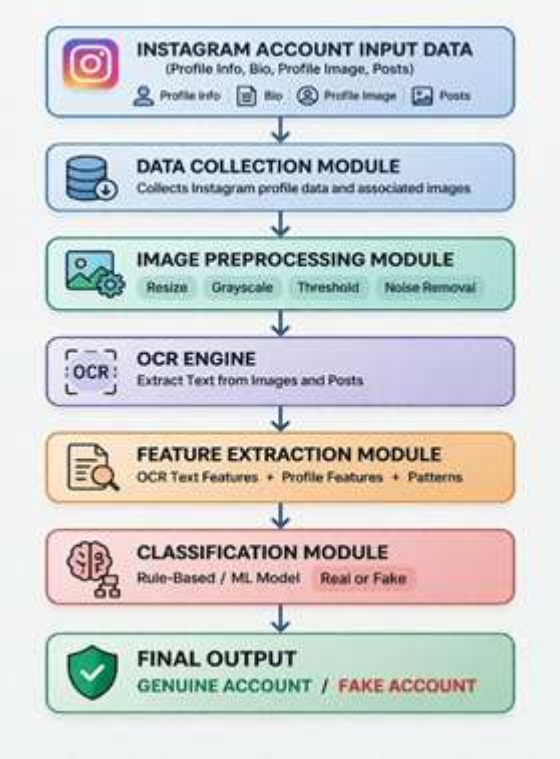
Step 5: Analyze Suspicious Keywords and Patterns
The extracted text is checked for suspicious content such as spam words, fake offers, unusual links, and misleading phrases. This step helps identify whether the account shows fake behavior.

Step 6: Extract Profile Features
The system also studies profile-related features such as account details and visible activity information. These features help support the OCR results in detecting fake accounts.

Step 7: Apply Classification Model
After collecting all features, the system applies a classification model. This model uses the OCR text and profile features to make the final decision.

Step 8: Final Classification
Finally, the account is classified as real or fake. The output helps in identifying suspicious Instagram accounts and improving social media security.

V. PROJECT WORKFLOW DIAGRAM



VI. FUTURE SCOPE

The proposed fake Instagram account detection system using OCR provides a useful method for identifying suspicious accounts by extracting text from images and analyzing profile details. However, this project can be improved further in many areas to make the system more accurate, faster, and more suitable for real-world social media security applications. The current paper mentions that future improvements may include machine learning integration, analysis of larger datasets, and real-time detection systems. These ideas can be expanded in a broader way as described below.

Integration with Advanced Machine Learning Models
In future, the system can be enhanced by using advanced machine learning algorithms for better classification of Instagram accounts. Instead of using only basic rule-based detection, models such as Decision Tree, Random Forest, Support Vector Machine, and Neural Networks can be trained using OCR text features and profile features. These models can learn complex fake account patterns and improve detection accuracy. This directly extends the paper's current idea of classifying accounts as real or fake using extracted features.

Use of Deep Learning Techniques
The project can also be expanded with deep learning methods. Deep learning can help in better image understanding, text pattern recognition, and fake profile classification. Convolutional Neural Networks can analyze profile images and post images more effectively, while advanced text models can study suspicious phrases extracted through OCR. This can make the system smarter and more reliable in detecting modern fake accounts.

Analysis of Larger and More Diverse Datasets
The current work can be improved by testing the system on a larger dataset of Instagram accounts. A larger dataset containing both genuine and fake profiles will help the model understand more types of spam behavior, image-based scams, and suspicious posting styles. It can also improve the general performance of the system and reduce classification errors. The paper already identifies larger dataset analysis as a future direction.

Real-Time Fake Account Detection
Another important future improvement is the development of a real-time fake account detection system. In such a system, newly created Instagram accounts or suspicious posts can be analyzed instantly. This would help detect malicious accounts at an early stage before they spread spam, scams, or false information. Real-time detection can be very useful for social media monitoring and moderation. The uploaded paper already notes real-time detection as part of future scope.

Improved OCR Accuracy
The quality of OCR plays a major role in the success of the project. In future, the system can use better OCR methods to improve text extraction from low-quality images, blurred pictures, stylized fonts, or colorful promotional images. More accurate OCR will help detect fake accounts that try to hide suspicious text in complex image designs.

Multilingual Text Detection
Many fake Instagram accounts may use different languages in their posts and profile images. The current project can be extended by adding multilingual OCR support. This would help the system detect suspicious text in multiple languages instead of only one language. Such an improvement would make the system more useful on global social media platforms where users post content in different regional and international languages.

Detection of Fake Accounts Through Stories and Reels
At present, the project mainly focuses on profile images and post images. In future, the same concept can be extended to Instagram stories, reels, and short videos. Many fake accounts use temporary stories or video overlays to promote scams and fake offers. By analyzing text present in video frames and story content, the system can become more powerful and cover a wider range of fake account activities.

Combining OCR with Behavioral Analysis
Future systems can combine OCR-based image analysis with deeper behavioral analysis. This means the system can study not only the text inside images but also user behavior such as posting frequency, repeated comments, engagement patterns, follow-unfollow activity, and interaction style. Combining both visual and behavioral data would create a stronger fake account detection framework.

Suspicious Link and URL Analysis
Another future improvement is automatic link analysis. Fake accounts often include suspicious links in images, bios, or posts. The system can be enhanced to detect shortened URLs, unsafe domains, phishing links, and repeated promotional websites. This will help the model better identify scam-related accounts and increase user safety.

Deployment as a Social Media Security Tool
The proposed model can also be developed into a practical software tool or dashboard for security monitoring. This tool can be used by social media administrators, researchers, businesses, or brand owners to identify suspicious Instagram accounts automatically. It can generate alerts, risk scores, and reports about fake account activities.

Brand Impersonation Detection
In future, the project can be extended to detect fake accounts that imitate celebrities, influencers, companies, and public figures. Many fake accounts copy profile images, usernames, and promotional content to mislead users. By comparing OCR text, profile structure, and account behavior, the system can help in detecting impersonation attempts more effectively.

Use in Other Social Media Platforms
Although this project is focused on Instagram, the same OCR-based method can be applied to other social media platforms such as Facebook, X, TikTok, and Telegram channels where fake accounts and scam promotions are also common. Expanding the model to other platforms can increase the usefulness of the research.

Better Accuracy Through Hybrid Models
In future, the system can use a hybrid approach where OCR, machine learning, profile analysis, and image pattern detection all work together. Such a hybrid system can reduce false positives and false negatives and provide more accurate fake account identification.

Automatic Warning and Reporting System
Another useful extension is to build an automatic warning system. Once an account is detected as suspicious, the system can alert users or administrators. It may also support automatic reporting of highly suspicious profiles for manual review. This can help reduce the spread of spam and fraud quickly.

Contribution to Safer Online Environments
Overall, the future development of this project can contribute to stronger cybersecurity and safer social media use. By improving accuracy, speed, scalability, and practical implementation, the system can become an effective solution for detecting malicious accounts and protecting users from fake activities.

VII. CONCLUSION

In this project, a method for detecting fake Instagram accounts using OCR (Optical Character Recognition) has been presented. The system focuses on extracting text from Instagram profile images and post images, then analyzing that text along with profile- based features to identify whether an account is genuine or fake. The uploaded paper already concludes that OCR can be used to improve fake account detection by analyzing image-based text content.

The project shows that fake Instagram accounts often hide suspicious information inside images, such as spam messages, fake promotional offers, misleading text, and unusual links. Traditional fake account detection methods mainly depend on account details like followers, following, and post count, but they may miss such hidden text. By using OCR, the system can extract these textual clues from images and make the detection process more effective.

Another important outcome of the project is that combining OCR-based text analysis with profile feature analysis gives better support for classification. Instead of depending on only one type of data, the system studies both image content and account details. This makes the model more useful for identifying suspicious profiles that appear normal at first look but contain scam-related content in their images.

Thus, the proposed system is helpful in improving social media security and reducing the risk caused by fake Instagram accounts. It can support users, researchers, and platforms in identifying malicious profiles more accurately. Overall, this project demonstrates that OCR is a valuable technique for fake account detection and can be further improved with advanced models, larger datasets, and real-time implementation in the future.

Acknowledgement
First and foremost, I would wish to record my gratitude and thanks to Mrs. P.V.Javkar our mentor, for her essential assistance, encouragement, and direction in successful completion of project. I express my thanks to Dr. (Mrs.) M.S.Jadhav (Principal), Prof. A.V.Kurkute (Head of Department, Computer Technology) and Mrs. P.V.Javkar (Project Coordinator) for their valuable guidance. I am also thankful to other teachers and non-teaching staff of Computer Technology Department and Library for their cooperation and help. Lastly, I need to extend my thanks to all those, who helped us directly or indirectly in completing this team project.

REFERENCES

1. Smith, R. "An Overview of the Tesseract OCR Engine." Proceedings of the International Conference on Document Analysis and Recognition, IEEE.
2. Stringhini, G., Kruegel, C., and Vigna, G. "Detecting Spammers on Social Networks." Proceedings of the Annual Computer Security Applications Conference.
3. Cresci, S., Di Pietro, R., Petrocchi, M., Spognardi, A., and Tesconi, M. "The Paradigm-Shift of Social Spambots: Evidence, Theories, and Tools for the Arms Race." International World Wide Web Conference / IEEE Internet Computing.
4. Viswanath, B., Bashir, M. A., Crovella, M., Guha, S., Gummadi, K., Krishnamurthy, B., and Mislove, A. "Towards Detecting Anomalous User Behavior in Online Social Networks."
5. OpenCV Documentation. "Image Processing Techniques for Preprocessing and Analysis."
6. Scikit-learn Documentation. "Machine Learning Models for Classification and Prediction."
7. Tesseract OCR Documentation. "Optical Character Recognition for Text Extraction from Images."
8. Instagram / Social Media Security related research articles on fake profiles, spam detection, and impersonation detection.