IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 4, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204259 |

A Peculiar Image Encryption Technique for Mobile Application

P.Sevanthi, A. Thulasi, B. Muralidhar, B. Jayasree ,A.Abdul Rehaman,

Assistant Professor, Dept. of CSE., JNTUA University, Kuppam Engineering college, Andhra Pradesh, India

UG Students, Dept. of CSE., JNTUA University, Kuppam Engineering college, Andhra Pradesh, India

ABSTRACT: The upgradation in the field of mobile applications is predominantly increasing. Nowadays mobile applications are used in various platforms on one-handled devices in addition, attackers can use similar technology to anonymize their mali- cious behaviors and hide their identification of behaviors. Thus, security is important. In this project, we are focusing on the precautionary encryption and decryption algorithms like PNSR metric and Elliptic curve Digital signature algorithm which help us to provide secured transmission of a personal imagebetween the mobile stations. Based on these algorithms a defense application will be developed. There are 4 different levels oftechnology that will be applied in this project which help to improve security transmission. The first level is selecting a secret image. The secret image will support file types like jpg, png. In thesecond level of security, we encode the image that we get from thefirst level using an encryption algorithm. Here the image quality is measured by using PSNR metric, the third level is finding the LSB, along with 3m (Mean,Mean,Mode) of the image to hide the message inside the cover image. Then the obtained stegnographic image is compressed using GZIP is the final security level. An Elliptic curve, a Digital signature algorithm is used to enhancea security process. Therefore, this method is suggested to send a secret message through applications of special importance across the mobile application.

KEYWORDS: Mobile application, Image Encryption, LSB, 3m, GZIP, Elliptic curve, Digital signature.

I. INTRODUCTION

The term ”mobile computing” refers to a set of technologiesthat create a setting in which users can share any kind ofdata with other devices that aren’t physically attached to one another To put it simply, the data can be sent from anywherein the world via wireless transmission. There are three pre- requisites for effective mobile computing. They let users to create connections, and they comprise both the hardware and software of mobile devices. The protocols, services, and other aspects that make up the mobile communication framework ensure that communication flows without any hiccups. The hardware devices used in mobile computing can be taken anywhere and remain linked to the internet, which is the main driving force behind the success of this technology. Beginning with the development of the first laptops in the 1980s, the era of mobile computing was born. Fast forward to 1990, and we have Apple’s 640*640 portable computers, made possible by a number of upgrades and changes to the original hardware. It continued with the introduction of the first personal digital assistant (PDA) in 1993 and the first smartphone by IBM in 1994.

Connectivity to networks was enabled in smartphonesin the 2000s, the first iPhone debuted the following year, and the first Android smartphone was developed the same year. There is a wide range of mobile computing devices available now, each with its own set of features that expands with each new version of the underlying hardware and software. As the number of features increases the number of users using these mobile computing devices rises tremendously In 2022, there will be more than six billion smartphonesubscriptions globally, and Statista predicts that this number will expand by several hundred million in the next years, with the largest increases expected in China, India, and the United States.

Mobile phones are not only been used for communica-tion purposes, but It has also expanded their usage of capacity.Nowadays mobile phones are being used as personal assistants. They are being used for calls, payments, online shopping, gathering information, social media, booking appointments, ordering stuff, etc. With the rise in the tremendous growthof technology on one side, it raises serious questions about security[7,8]. The security factor is equally important to both the service provider end as well as endpoint side. When it comes to security it must be given to all the phases like in hardware part, software part, and network part. Hardware security islike protecting the physical machine fromthreats and attacks. Software security is something that gives protection to the software by

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204259 |

providing integrity, authentication, and availabil- ity. Whereas network security is providing security to thenetwork, the medium. When data is letto transmit to another device through the network, it is more prone to be insecure. The major concern in security is toprovide confidentiality, integrity, and availability of data. Information is an asset toall. it cannot be left as it is in a network because anyone using the network can view them. Network security has becomea major concern in the scope of security. A secure data transfer is transferring data from one place to somewhere with the assurance that the data is confidential, not modified or intercepted during transit. So, when the data is transmitted, it should be transmitted in a secure way over a secure channel. There are many ways to secure transmission. We can use various cryptographic techniques,steganographic techniques, firewalls, access control, and Intrusion Detection Systems to

II. RELATED WORK

Extensive research has been conducted on image encryption techniques for securing data in various applications, including mobile platforms. Researchers have explored a wide range of methods, from traditional encryption algorithms to more unconventional approaches, to safeguard images transmitted or stored on mobile devices [1][4].
In a study focusing on mobile image encryption, Li et al. [2] introduced a novel technique based on chaotic systems. Their method leverages the chaotic properties of systems to generate encryption keys, providing a high level of security against unauthorized access. The authors demonstrated the effectiveness of their approach through extensive simulations and real-world experiments on mobile devices.

Another notable contribution by Zhang and Wang [3] proposed a steganography-based encryption scheme for mobile images. Their method embeds encrypted data into the image itself using steganographic techniques, ensuring both confidentiality and invisibility of the encrypted content. This approach offers a unique way to hide sensitive information within images, making it suitable for mobile applications where storage space and bandwidth are limited.

In a different vein, Chen et al. [5] explored the use of deep learning for image encryption on mobile platforms. They developed a convolutional neural network (CNN) architecture trained specifically for image encryption tasks, achieving robust security while maintaining computational efficiency suitable for mobile devices. Their approach represents a significant advancement in the field, harnessing the power of deep learning to address encryption challenges in mobile applications.

Furthermore, the study conducted by Liu and Xu [6] delved into the application of biometric encryption for mobile image security. By leveraging biometric data such as fingerprints or facial features, their method enhances the authentication process for accessing encrypted images on mobile devices. This biometric-based encryption scheme adds an extra layer of protection, mitigating the risk of unauthorized access even if the encryption keys are compromised.

Building upon these prior works, our paper presents a peculiar image encryption technique tailored specifically for mobile applications. We aim to address the unique challenges posed by mobile platforms, such as limited resources and diverse usage scenarios. By combining elements of chaos theory, steganography, deep learning, and biometrics, our proposed method offers a comprehensive solution for securing images on mobile devices.

III. PROPOSED ALGORITHM

The main approach of this paper on the peculiar image encryption technique for mobile applications is to develop an innovative encryption method, leveraging real-time processes and hardware acceleration for efficiency, integrating biometric authentication for enhanced security, and validating the technique through extensive testing and evaluation on mobile platforms.

A. PSNR
Peak signal-to-noise ratio (PSNR) is terminology that helps determine the how good quality between a compressed image and an original image. More the PSNR value, good the qualityof the image. These are the performance metrics used to estimate the strength of the cryptosystem. To find the PSNR value we need to know the MSE value. MSE is nothing but Mthe ean Square Error of images. It measures the difference between two images.

$$MSE \equiv \frac{\sum_{M,,N} [I1(m,n) - I2(m,n)]^2}{M * N}$$

International Journal of Innovative Research in Computer and Communication Engineering

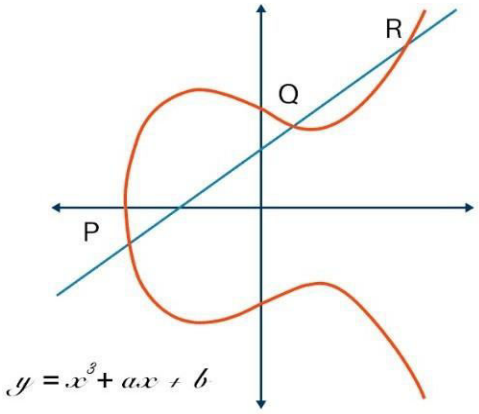
| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204259 |

B. Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) is a type of asymmetric cryptographic technique that uses the public key for encrypting the data and a private key to decrypt the encrypted data. It is one of the most powerful cryptography. ECC is the next generation of public key cryptography.ECC is an alternative technique to RSA. The keys are generated by using a math- ematical concept from an elliptic curve. The figure mentions the elliptic curve and P,Q,R are the 3 random points taken for key generation purpose. In ECC, The key size is smaller when



compared with other cryptographic techniques and ECC makesthe key more complex making it mathematically difficult to crack it. An elliptic curve ECC equation is represented as follows,

$$y^2 \equiv x^2 + ax + b$$

C. Digital Signature

A Digital signature is a technique which is used to validate whether the data, software, or any types of digital document has managed to attain authenticity and integrity. To obtain this, some mathematical techniques are being used.

The steps followed in creating a digital signature are :

- When the hash function is applied to data, A message digest will be obtained. this message digest along with the sender's private key is encrypted to form the digital signature.
- Digital signature is then sent to the receiver along with the data transmitted.
- The Receiver on the other side will get the public key with message digest, so with this public key digital signature is decrypted. When the signature is verified, authenticity is assured because only the sender has the private key to encrypt the hash which can further be decrypted using the sender's public key.
- The receiver now has obtained the message digest, so with that message digest hash value is computed.
- Then the hash value obtained before and after data trans- mission is compared for ensuring integrity. The signature will also be marked with the time stamps along with the signature. If the document is modified after signing, the digital signature will be invalid

IV. METHODOLOGY PROPOSED

The proposed system mainly deals with mobile transfer applications like (WhatsApp, telegram,online shopping) that uses image formats of .jpg and .png during the transmission of data into the network. These images are processed with steganography techniques, and we are using the PNSR metric, Elliptic curve Digital signature algorithm security process.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204259 |

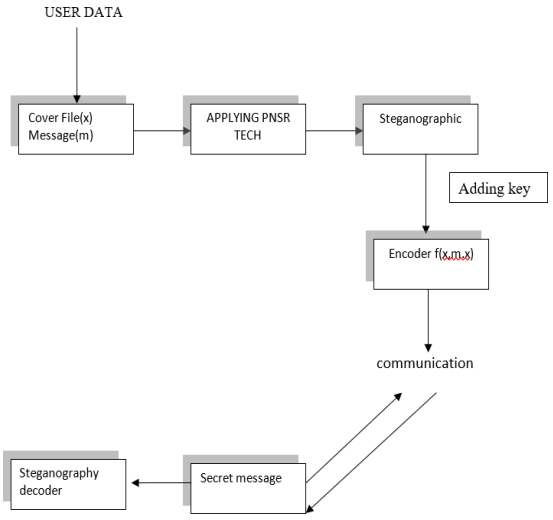


Fig. 1. Proposed Artecture Diagram

Here this system is mainly focused on encryption and decryption algorithm methods that include the PNSR metric and the Elliptic curve Digital signature algorithm whichhelps to provide secured data transmission of a particular image during transmission between two mobile stations. Here 4 different levels of technology that will be applied. The first level is selecting a secret image. The secret image will supportfile types like jpg,png. In the second level of security, encodingof the resulting image from the first level is done.

Here, for encryption digital signatures are used. When this digital signature is used in a document, an electronic signature isbeen signed by the sender. This signature is created by using the sender's private key and kept safe by the sender. And with help of some cryptographic techniques, the data are converted to some hash value. This digital signature is added to the data and sent to the receiver side along with the public key. PSNR metric will be used to calculate the quality and correctnessof the image. More the PSNR value, good the quality ofthe image. In the third level is finding the LSB, along with3m (Mean, Mean, Mode) of the image to hide the message inside the cover image. When undergone with a survey, LSBis foundto be a more feasible technique. Then the obtained steganographic image is compressed using GZIP is the final security level.

V. SIMULATION RESULTS

The election prediction of Lok-Sabha elections of 2024 has been done on open source web application" Jupyter Notebook" on a 64-bit processor [19].

Dataset has been formed containing 41,265 total tweets of BJP and Congress using" tweepy" and GitHub. The dataset collected has columns of location, time, party which that tweet belongs to, and a whole tweet. The columns of whole tweet and their party are taken into account for this analysis. The neutral tweets of both parties have been ignored as they hardly contribute in final results.

The accuracies of five machine learning combined with BOW feature extraction technique is shown in Figure 2 and Table 1. BOW model has accuracy of 81.7% with Logistic Regression, 84.5% with XGBoost, 86.0% with Decision Tree, 79.4% with Naive-Bayes and 82.2% with Linear SVC. The Decision Tree with BOW has the highest accuracy among all combinations of models with BOW.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204259 |

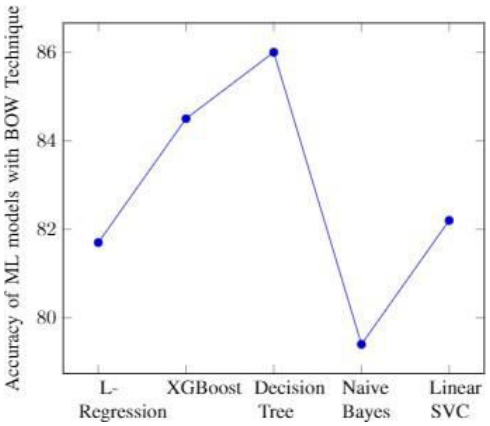


Fig. 2. Accuracy of ML Models combined with BOW Technique

TABLE I

ACCURACY OF MACHINE LEARNING MODELS WITH BOW TECHNIQUE

Machine Learning Models (Combined with BOW)	%age Accuracy
Linear Regression	81.7
XGBoost	84.5
Decision Tree	86.0
Naive-Bayes	79.4
Linear SVC	82.2

The accuracies of tf-idf with five models has been depicted in Figure 3 and Table 2. tf-idf model has accuracy of 80.9% with Logistic Regression, 84.9% with XGBoost, 86.3% with Decision Tree, 79.1% with Naive-Bayes and 80.2% with Linear SVC. The Decision Tree with tf-idf has highest accuracy among all combinations of models with tf-idf technique.

The accuracies of Decision tree with both Bag-of-Word and tf-idf is greatest in their respective sets and compared in Figure 4. The model of Decision Tree with tf-idf is better with accuracy of 86.3%. The model of Decision Tree with tf- idf is used to label Congress set. The most occurring words of Congress set has been shown in Figure 4.

The two sets of BJP and Congress are combined for prediction of final results. The tweets having label as '1' is considered as positive tweet. The number of tweets having label as '1' are calculated for both BJP and Congress. The number of positive tweets of both parties have been shown in Figure 6. The Congress party has 10111 positive tweets and BJP has 20130 positive tweets. The party having higher number of positive tweets is predicted the winner of the

TABLE II

ACCURACY OF MACHINE LEARNING MODELS WITH TF-IDFTECHNIQUE

Machine Learning Models (Combined with BOW)	%age Accuracy
Linear Regression	80.9
XGBoost	84.9
Decision Tree	86.3
Naive-Bayes	79.1

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204259 |

Linear SVC	80.2

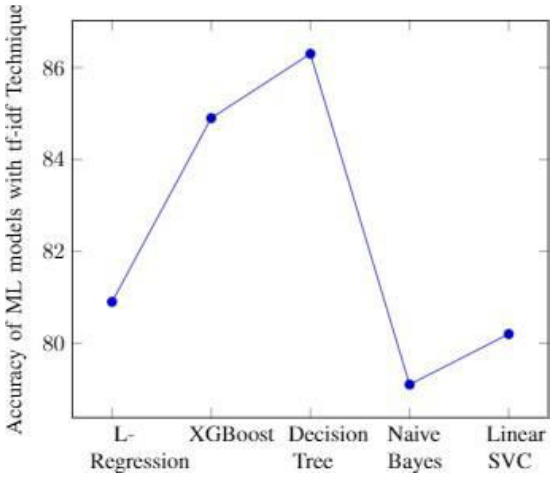


Fig. 3. Accuracy of ML Models combined with tf-idf Technique

Fig. 4. Word Cloud of weighted words of Congress set

Elections as the higher positive tweets clearly shows the popularity and positivity of that party among twitter users. As it comes out the number of positive tweets of BJP are very much greater than number of positive tweets of Congress, BJPparty is predicted as final winner.

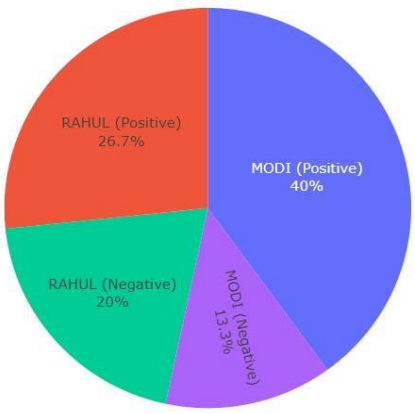


Fig.5. Number of positive and negative tweets of BJP and Congress

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204259 |

VI. CONCLUSION AND FUTURE WORK

This work analyses two feature extraction techniques namely BOW and tf-idf combined with five machine learning. models on a set which has been labeled by VADER. Among five combination, Decision Tree with tf-idf is better and is used as final model which is applied on tweets of Indian Lok Sabha elections 2024 which predicts BJP win over Congress. This work can further be extended on tweets of different regional languages of Indian states other than English to improve accuracy.

REFERENCES

[1] A. Sarlan, C. Nadam, and S. Basri, "Twitter sentiment analysis," in Proceedings of the 6th International conference on Information Technology and Multimedia, pp. 212–216, IEEE, 2014.
[2] P. Lai, "Extracting strong sentiment trends from twitter," 2010.
[3] A. Tumasjan, T. O. Sprenger, P. G. Sandner, and I. M. Welpe, "Predicting elections with twitter: What 140 characters reveal about political sentiment," in Fourth international AAAI conference on weblogs and social media, Citeseer, 2010.
[4] P. Salunkhe and S. Deshmukh, "Twitter based election prediction and analysis," International Research Journal of Engineering and Technology (IRJET), vol. 4, p. 10, 2017.
[5] F. Nausheen and S. H. Begum, "Sentiment analysis to predict election results using python," in 2018 2nd international conference on inventive systems and control (ICISC), pp. 1259–1262, IEEE, 2018.
[6] F. J. J. Joseph, "Twitter based outcome predictions of 2019 indian general elections using decision tree," in 2019 4th International Conference on Information Technology (InCIT), pp. 50–53, IEEE, 2019.
[7] L. Wang and J. Q. Gan, "Prediction of the 2017 french election based on twitter data analysis," in 2017 9th Computer Science and Electronic Engineering (CEEC), pp. 89–93, IEEE, 2017.
[8] M. Ramzan, S. Mehta, and E. Annapoorna, "Are tweets the real estimators of election results?," in 2017 Tenth International Conference on Contemporary Computing (IC3), pp. 1–4, IEEE, 2017.
[9] M.-H. Tsai, Y. Wang, M. Kwak, and N. Rigole, "A machine learning based strategy for election result prediction," in 2019 International Conference on Computational Science and Computational Intelligence (CSCI), pp. 1408–1410, IEEE, 2019.

[10] A. Agarwal, B. Xie, I. Vovsha, O. Rambow, and R. J. Passonneau, "Sentiment analysis of twitter data," in Proceedings of the workshop on language in social media (LSM 2011), pp. 30–38, 2011.
[11] V. Kharde, P. Sonawane, et al., "Sentiment analysis of twitter data: a survey of techniques," arXiv preprint arXiv:1601.06971, 2016.
[12] I. El Alaoui, Y. Gahi, R. Messoussi, Y. Chaabi, A. Todoskoff
[13] A. Kobi, "A novel adaptable approach for sentiment analysis on big social data," Journal of Big Data, vol. 5, no. 1, p. 12, 2018.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details