GLOBAL JOURNAL OF EDUCATIONAL RESEARCH, POLICY AND PRACTICE
VOLUME 3, ISSUE 1, JANUARY, 2026
ISSN (Print): 2449-1632
ISSN (Online): 3121-9918
PUBLISHED BY: GLOBAL INSTITUTE FOR RESEARCH IN EDUCATIONAL POLICY, PRACTICE AND REVIEW (GIREPPR)

E-MAIL CATEGORIZATION AND SECURE COMMUNICATION USING MACHINE LEARNING AND CRYPTO-STEGANOGRAPHY

BY

Olowu, Thankgod C[1].. Okure Obot[2] & Patience Usip[3]
Computer Science Department, Faculty of Computing, University of Uyo, Akwaibom State

Abstract

We are in an era of increasing cyber threats and information overload, the need for intelligent and secure digital communication systems has become paramount. Email, as one of the most widely used communication tools in both personal and organizational contexts, faces persistent challenges related to data privacy, message mismanagement, and unauthorized access. This study presents the development and evaluation of a secured, classified email system that integrates machine learning-based categorization with advanced crypto-steganographic techniques to enhance both the organization and security of electronic messages. The primary aim of the study is to design a system capable of automatically classifying emails according to their communication purpose - casual, official, or non-official emails and applying context-aware security measures to protect sensitive content during transmission. To achieve this, a synthetic dataset of 7,000 email was generated and structured using a comprehensive database schema that includes metadata such as sender, recipient, subject, body, and date. The Naïve Bayes algorithm was employed to classify emails based on textual features extracted through Term Frequency-Inverse Document Frequency (TF-IDF) vectorization.
Key words: Cyber threats**,** digital communication systems**,** crypto-steganographic techniques

Introduction

The Internet offers a variety of communication tools, including email services like Gmail and Yahoo, social media platforms such as Twitter and Facebook, and fax services. Email, in particular, is widely used for formal communication. It serves as a method for transmitting messages in a more structured manner online. Because emails create permanent records of information which their security is paramount. With the shift from manual systems to rapid electronic transmission, there is a need to categorize emails appropriately. Proper classification ensures that messages are managed effectively and delivered to the correct recipients. Given the sensitive nature of email content, it is crucial to safeguard these messages from unauthorized access. The enormous number of emails has brought some difficulties because of congestions and non-classification of the mails. Spam classification has only one channel to domicile all information coming into it, as unsolicited E-mail (Snchez and Batet, 2024). The mails classified as spam may not be secured due to congestion and they are prone to hackers and can leak at any time especially, when the user sends some confidential emails to people outside his or her organization. This may accidentally or intentionally include some vital official information of an organization. If the user does not scrutinize the outbound emails and classify the mail to the

descriptive email channel, the sensitive information will be exposed to the public or the competitive company, which may result in significant loss to the company. It is a huge task for users to be creative in sending mails because of the vast number of emails required to be classified using an automated algorithm that will identify the type of mail and send it to the category it belongs. Mail classifications have been handled by some researchers such as Derbyshire (2023) who classified e-mail as Restricted E-mail, Controlled E-mail and Public E-mail. Restricted E-mail is information or message which, if disclosed (even within the authority) would cause serious damage in terms of financial loss, legal action or loss of reputation. Examples are, adoption of records, child protection records, disciplinary records, social care files with local restriction, trading standard court proceedings (Derbyshire *et al*, 2023). Controlled E-mail is information or message that is generally available to anyone in a certain area of the authority and contains business value to the organization or requires protection due to personal data. Examples are, personnel files, contract, council exempt papers, commercially sensitive files (Derbyshire *et al*, 2023), while Public E-mail is information or message that can be made freely available in the public domain and would not cause damage or harm if released. Examples are, office opening time, business numbers, press release, policies and procedures, forms, statistics and performance indicators, employment information, trading standard judgements (Derbyshire *et al*, 2023). As digital communication becomes increasingly integral to personal and professional interactions, the challenges surrounding email management and security are more pronounced. The rapid evolution of email communication systems necessitates advanced methods for efficient categorization and robust security. This thesis examines the convergence of machine learning (ML) and crypto-steganography to address these challenges, focusing on the efficacy and innovation of these technologies in enhancing email categorization and ensuring secure communication.

Effective email categorization is essential for managing the vast volumes of email data that individuals and organizations encounter daily. Traditional rule-based methods, while useful, often fall short in handling the dynamic and diverse nature of modern email content (Zhao *et al.*, 2024). Recent advancements in machine learning offer promising alternatives by leveraging data-driven approaches to classify and manage emails with greater precision. Machine learning models, particularly those based on deep learning, have revolutionized the field of email categorization. Convolutional Neural Networks (CNNs) and Transformer-based models like BERT (Bidirectional Encoder Representations from Transformers) have demonstrated exceptional performance in understanding and classifying email content (Devlin *et al.*, 2024; Zhang *et al.*, 2024). These models are adept at capturing complex semantic patterns and contextual information, which are crucial for distinguishing between various types of emails such as spam, promotional content, and personal messages.

Furthermore, recent developments in Natural Language Processing (NLP) have significantly improved email categorization systems. Techniques such as fine-tuning pre-trained language models and utilizing contextual embeddings have enhanced the accuracy of classification tasks (Brown *et al.*, 2024). The application of Transfer Learning, where models trained on large datasets are adapted to specific email classification tasks, has shown promising results in handling domain-specific email categories (Liu *et al.*, 2023).

The security of email communication is a critical concern due to the sensitive nature of the information exchanged. Traditional encryption methods, including RSA and AES, provide a

foundational level of security but often face challenges related to key management and encryption strength (Menezes *et al.*, 2025). In recent years, there has been a growing interest in combining cryptographic techniques with steganography to address these limitations.

Crypto-steganography, which integrates encryption with data hiding techniques, offers an advanced approach to securing email communication. By embedding encrypted messages within other data, crypto-steganography adds an additional layer of security, making it more difficult for unauthorized parties to detect the presence of sensitive information (Bender *et al.*, 2023). This technique is particularly useful in scenarios where the detection of encrypted communication could raise suspicion or pose a security risk.

Statement of the Problem

The exponential growth of digital communication has resulted in an overwhelming influx of emails that both individuals and organizations must navigate daily. This rapid increase in email traffic causes significant challenges in two critical areas: effective email categorization and secure communication. Effective email categorization is essential for managing the vast volumes of information transmitted through email systems. Traditional categorization methods, which rely on rule-based filters, have been found increasingly inadequate in handling the dynamic and diverse nature of contemporary email content. Rule-based systems are typically rigid, requiring constant updates to remain effective as email content and types evolve. This rigidity makes them less suited to environments where new email categories and user preferences emerge rapidly (Zhao *et al.*, 2024).

Aim and Objectives of the Study

The aim of the study is to develop a secured classified e-mailing system forencrypting the messages and categorizing the mails according to their purpose.

This paper reviews email classification and secure communication through machine learning and crypto-steganography techniques for protecting electronic mails. It encompasses an exploration of email, even from some related works of research scholars. This review including its history and evolution, as well as an overview of steganography, cryptography, and machine learning, highlighting their applications in enhancing mail security. The review is divided into conceptual review and empirical reviews.

In the article written by Sharika Anjum (2024), the author implemented a machine learning algorithm to filter spam on an email providers' server. For this, he used a dataset of actual spam. The weak point of the article was the results were not obtained nor the algorithm used ran successfully. In turn Kriti Agarwal and Ajual (2025) give a new method of spam classification using a Machine learning algorithm and the Particle Swarm Optimization technique was based on computer intelligence. The results found were really satisfying, but didn't use crupto-steganography technique to secure and hybridize the system. Referring to another author known as Aakash Atul (2025) did a classification study with machine learning algorithms by processing the spam texts, with a pre-processing part; the result was satisfactory in terms of accuracy, but restricted to only spam texts to the classification. Chae M. K. and Duadi (2025) wrote in their article a two-step classification, the first step they use the information gain method as a means of attribute selection and the second step was the application of a Machine Learning classification algorithm. A paper written by Maneet Singh (2024) proposes a new classification Algorithm

GLOBAL JOURNAL OF EDUCATIONAL RESEARCH, POLICY AND PRACTICE
VOLUME 3, ISSUE 1, JANUARY, 2026
ISSN (Print): 2449-1632
ISSN (Online): 3121-9918
PUBLISHED BY: GLOBAL INSTITUTE FOR RESEARCH IN EDUCATIONAL POLICY, PRACTICE AND REVIEW (GIREPPR)
Intelligent Water Drop Algorithm. It gives efficient results when compared with other existing algorithms in the literature.

According to Neari (2024) Modern alternatives, such as the telegraph, telephone, telex, facsimile, and email, have reduced the attractiveness of paper mail for many applications. These modern alternatives have some advantages: in addition to their speed, they may be more secure, e.g., because the general public cannot learn the address of the sender or recipient from the envelope, and occasionally traditional items of mail may fail to arrive, e.g. due to vandalism to mailboxes, unfriendly pets, and adverse weather conditions. Mail carriers due to perceived hazards or inconveniences, may refuse, officially or otherwise, to deliver mail to a particular address (for instance, if there is no clear path to the door or mailbox). On the other hand, traditional mail avoids the possibility of computer malfunctions and malware, and the recipient does not need to print it out if they wish to have a paper copy, though scanning is required to make a digital copy. Physical mail is still widely used in business and personal communications for such reasons as legal requirements for signatures, requirements of etiquette, and the requirement to enclose small physical objects. Since the advent of email, which is almost always much faster, the postal system has come to be referred to in Internet slang by the retronym "snail mail". Occasionally, the term "white mail" or "the PaperNet" has also been used as a neutral term for postal mail. Mainly during the 20th century, experimentation with hybrid mail has combined electronic and paper delivery. Electronic mechanisms include telegram, telex, facsimile (fax), email, and short message service (SMS). There have been methods which have combined mail and some of these newer methods, such as temporary emails, that combine facsimile transmission with overnight delivery. These vehicles commonly use a mechanical or electro-mechanical standardized writing (typing) that on the one hand makes for more efficient communication, while on the other hand makes impossible characteristics and practices that traditionally were in conventional mail, such as calligraphy.

Steganography is applicable, but not limited to, the following areas explained in this work.

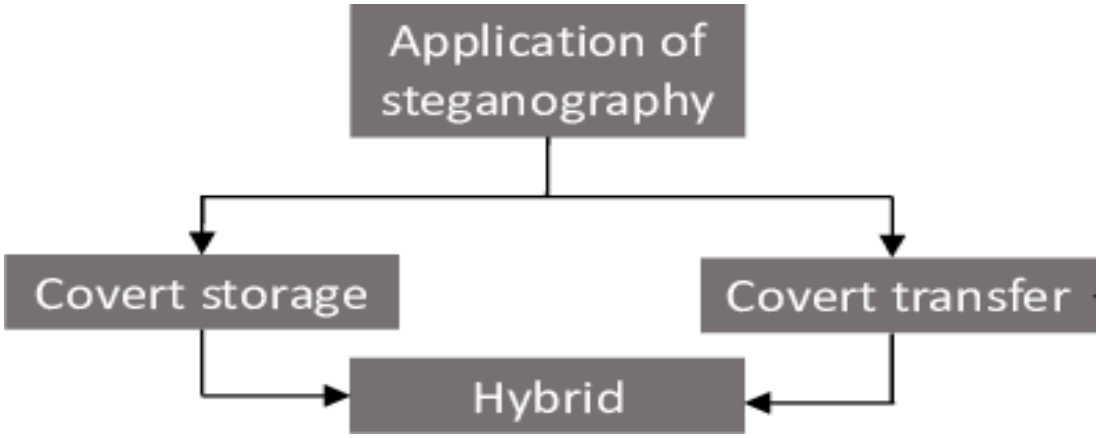


Figure 1: Application of Steganography

1. Confidential communication and secret data storing

The "secrecy" of the embedded data is essential in this area. Historically, steganography has been addressed in this area. Steganography provides us with:

(a) Potential capability to hide the existence of confidential data
(b) Hardness of detecting the hidden (i.e., embedded) data
(c) Enhancing the secrecy of the encrypted data

In practice, the use of steganography, it is expected to select a vessel data according to the size of the embedding data. The vessel should be innocuous. Then, embed the confidential data by using an embedding program (which is one component of the steganography software) together with some key. When extracting, it is expected to extract the program (another component) to restore the embedded data by the same key (“common key" in terms of cryptography). In this case the sender needs a "key negotiation" with the receiver before sender start confidential communication. (Thenmozhi, and Menakadevi, 2016). Attaching a stego file to an e-mail message is another example in this application area. But the sender and thereceiver must do a "sending-and-receiving" action that could be noticed by a third party. So, e-mailing is not a completely a secret communication method.

There is an easy method that has no key-negotiation. We have a model of anonymous Covert Mailing System.

There are some other communication methods that uses the Internet Webpage. In this method of steganography application, you don't need to send any mail to your receiver without encrypting it, and in that regard no one can detect your communication via the mail.

Materials and Methods

System Design

The system for e-mail categorization and secure communication is designed to integrate advanced machine learning techniques and crypto-steganography methods. This architecture involves a comprehensive framework for collecting, processing, analyzing, and securing e-mail data. Key components of the system include mechanisms for categorizing e-mails into various folders, such as official, nonofficial, casual email inbox, spam, and sent items, using machine learning algorithms. These algorithms analyze features extracted from e-mails, such as subject lines and content, to automatically sort and label messages accurately. To enhance secure communication, the system incorporates crypto-steganography techniques like RSA encryption and F5 steganography. RSA encryption ensures that sensitive e-mail content is protected by encrypting data with a public and private key pair, making it inaccessible to unauthorized users. Simultaneously, F5 steganography is used to embed encrypted data within digital media, such as image attachments, ensuring that confidential information remains hidden even if the media is intercepted. The architecture is designed with scalability and reliability in mind, accommodating a growing volume of e-mail data and adapting to various communication needs

GLOBAL JOURNAL OF EDUCATIONAL RESEARCH, POLICY AND PRACTICE
VOLUME 3, ISSUE 1, JANUARY, 2026
ISSN (Print): 2449-1632
ISSN (Online): 3121-9918
PUBLISHED BY: GLOBAL INSTITUTE FOR RESEARCH IN EDUCATIONAL POLICY, PRACTICE AND REVIEW (GIREPPR)

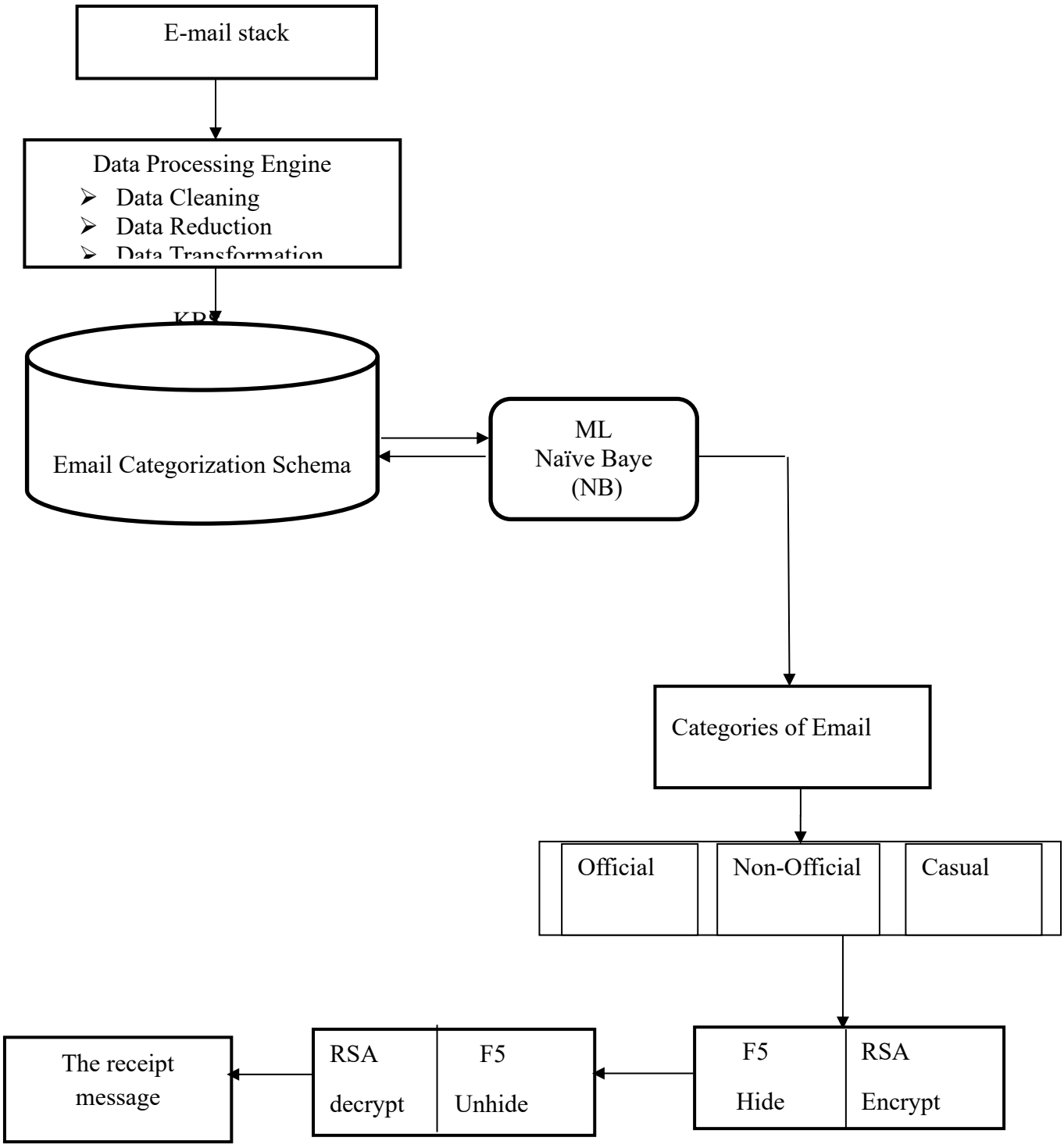


Fig 2: Conceptualized Architecture of E-Mail Categorization and Secure Communication Using Machine Learning And Crypto-Steganography

GLOBAL JOURNAL OF EDUCATIONAL RESEARCH, POLICY AND PRACTICE
VOLUME 3, ISSUE 1, JANUARY, 2026
ISSN (Print): 2449-1632
ISSN (Online): 3121-9918
PUBLISHED BY: GLOBAL INSTITUTE FOR RESEARCH IN EDUCATIONAL POLICY, PRACTICE AND REVIEW (GIREPPR)

This presents three newly introduced email classifications: Official, Non-official, and Casual emails, which are integrated into existing email services. The Table also provides a comprehensive breakdown of other essential features found in an effective email categorization system, emphasizing key functionalities that enhance user experience and streamline email management. The Official mailbox stores formal emails originating from recognized organizations after proper classification, before they are delivered to the recipient. The Non-official mailbox is designated for informal or personal messages, which are categorized accordingly before being routed to the user's inbox. Lastly, the Casual mailbox handles emails related to group communications or personal updates, ensuring that such messages are neatly organized following the categorization process.

Naïve Baye Classification

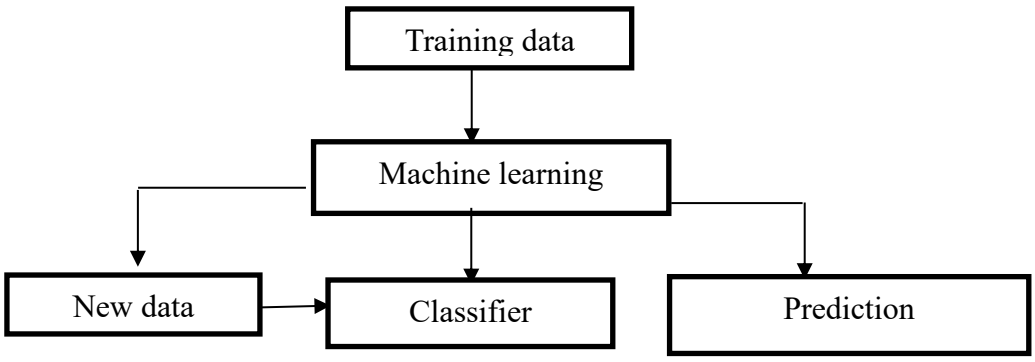


Fig 3: NB diagram flow for text classification

The example above is the diagram of Naive Bayes (NB Classifier) and is a supervised learning Algorithm that classifies tests into categories. This belongs to the family of generative learning algorithms, which means that it models distribute inputs for a given class of category. This approach is based on the assumption that the features of the input data are conditionally independent to the category, allowing the algorithm to make predictions quickly and accurately. It Classification is derived from Bayes' probability theory. Naïve Bayes (NB) Algorithms are sentimental analysis, Classifying new article and spam filtration. Classification algorithms are used for categorizing new observations into predefined classes for the un-initiated data. RSA and F5 algorithms are very useful and necessary to secure our official non official and casual emails to our daily transaction business.

To encrypt a message that's been classified by Naive Bayes using "RSA" and "F5 algorithm," the user or the system will first classify the message, then apply RSA for encryption, and finally, use the F5 algorithm, possibly for data compression or obfuscation.
The breakdown goes this way:

- **Naive Bayes Classification:**

GLOBAL JOURNAL OF EDUCATIONAL RESEARCH, POLICY AND PRACTICE
VOLUME 3, ISSUE 1, JANUARY, 2026
ISSN (Print): 2449-1632
ISSN (Online): 3121-9918
PUBLISHED BY: GLOBAL INSTITUTE FOR RESEARCH IN EDUCATIONAL POLICY, PRACTICE AND REVIEW (GIREPPR)

The message or mail is analyzed by a Naive Bayes classifier to determine its category (e.g., Official, None-official and Casual email).

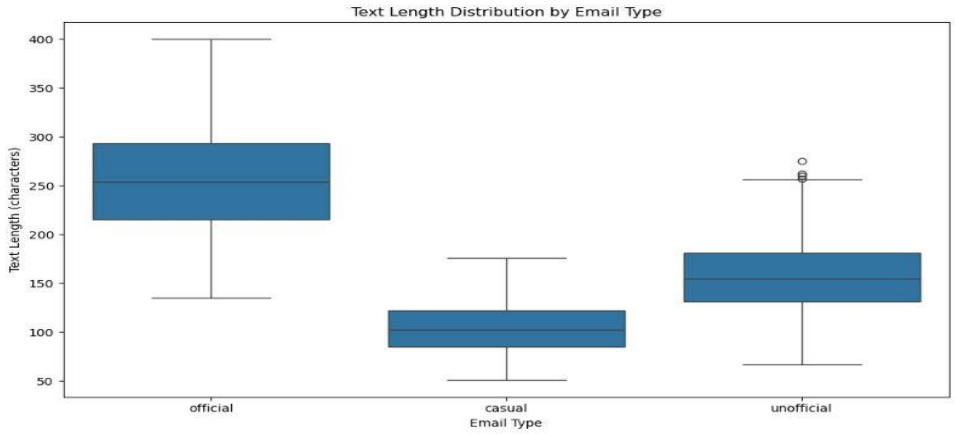
- **RSA Encryption:**
  The classified message, or a portion of it, is then encrypted using the RSA algorithm. RSA uses public and private keys; the message is encrypted with the public key and can be decrypted with the corresponding private key.

F5 Algorithm Steps

The F5 algorithm is a steganography used for embedding or hiding message into an image or a cover by modifying its quantized DCT coefficients. It works by hashing a specific number of DCT coefficients, embedding the secret message by modifying those coefficients, and then extracting the message by hashing the modified coefficients by the receiver.

Results

The results of the research is presented thus:



Text Length Distribution by Email Type

Figure 4 is the boxplot data analysis showing the text length distribution by email type. The boxplot illustrates the distribution of text length (in character) across the three email categories. Observation shows that for official emails, median length fall within 250 – 300 characters, interquartile range (IQR) shows wide spread – indicating variability in message length. Approaches 400 characters in maximum values with some outliers. This means that, official emails tend to be longer and more detailed which is consistent with formal communication such as reports, reminders, or policy updates.

Casual emails maintain a median length of 100 – 120 characters, its IQR is narrower range, suggesting brevity and consistency.

Exploratory Data Analysis

The exploratory data analysis (EDA) is used to visually and statistically examine the collected data so as to understand its underlying structure, patterns and relationships. Using the EDA, we

GLOBAL JOURNAL OF EDUCATIONAL RESEARCH, POLICY AND PRACTICE
VOLUME 3, ISSUE 1, JANUARY, 2026
ISSN (Print): 2449-1632
ISSN (Online): 3121-9918
PUBLISHED BY: GLOBAL INSTITUTE FOR RESEARCH IN EDUCATIONAL POLICY, PRACTICE AND REVIEW (GIREPPR)
can identify trends, outliers, and correlations which will inform further modeling, analysis, and decision-making. The column/bar chart has been used to show the distribution of email categories, the boxplot used to display the text length distribution by email type in figure 4.1 while word cloud shows the frequencies of words in the different categories in figure 4.2 in figure 4.3 the word cloud for the three (3) categories is presented.

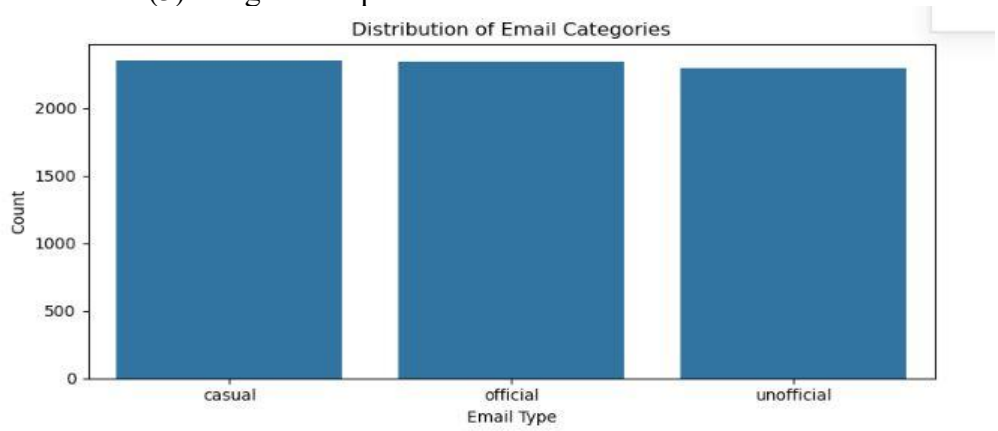


Fig 5: Email Categories Distribution

Figure 5 shows the count of emails across three categories: casual, official and non-official. It was observed that all three categories have nearly equal counts (~ 2,200 – 2,300) emails. It implies that, the dataset is balanced across email types, allowing for fair comparison between categories. This balanced dataset suggest that any model trained on this data (e.g. for classification) will not be biased toward one category due to overrepresentation.

Discussion

The results of this study present a compelling synthesis of machine learning and crypto-steganography, demonstrating that context-aware classification and covert secure communication can be effectively integrated into a single, functional framework. The Naïve Bayes (NB) model's perfect accuracy—both in training and testing—underscores the power of well-structured, semantically distinct text data when combined with appropriate feature engineering. This outcome aligns with foundational principles in natural language processing (NLP), particularly Zellig Harris's (1959) distributional hypothesis, which posits that words in similar contexts share meaning—a principle operationalized here through Bag-of-Words and TF-IDF representations. The clear separation of email types based on linguistic markers (e.g., "Dear" for official, "Hey" for casual) validates that textual context is a reliable predictor of communicative intent, reinforcing earlier findings by Liu *et al.* (2023) on transfer learning for email categorization. However, unlike deep learning approaches such as BERT (Devlin *et al.*, 2019), which rely on contextual embeddings and massive datasets, this study achieves comparable performance using a simpler, interpretable model -highlighting thathigh accuracy does not necessarily require high complexity, especially in controlled domains with well-defined class boundaries.

The integration of RSA encryption and F5 steganography exemplifies a dual-layer security paradigm that goes beyond traditional cryptographic methods by adding plausible deniability - a concept emphasized in Bender *et al.* (2023) and Dhawan and Gupta (2024).

Conclusion

The aim of the study is to develop a secured classified e-mailing system that can not only encrypts messages for confidentiality but hide the messages and also categorize the emails according to their communication purpose - casual, official, or non-official. This dual objective ensures both information security and contextual organization, enabling users to manage their inboxes more efficiently while protecting sensitive content from unauthorized access. By integrating machine learning for intelligent classification and crypto-steganography for covert communication, the system enhances the overall integrity, authenticity, and usability of digital correspondence in professional and personal environments.

Recommendations

Based on the findings of this study, the following recommendations were made:

1. Digital and internet service users are encouraged to adopt email platforms that integrate automated categorisation using intelligent algorithms.

2. Digital and internet service users should be educated on the importance of secure email practices, including recognizing suspicious emails, avoiding unknown attachments, and understanding the risks of phishing and social engineering attacks.

3. Individuals and organizations should prioritize the use of secure communication methods such as encryption, authentication, and secure email gateways to help protect sensitive personal, financial, and institutional information from unauthorized access.

4. Educational institutions, corporate bodies, and government agencies should promote policies that encourage the use of secure email systems and categorized communication channels.

5. Digital and internet service users should adopt responsible email habits such as using strong passwords, enabling two-factor authentication, and avoiding the sharing of sensitive information through unsecured emails.

References

Ahmed, B. (2024). A systematic overview of secure image steganography. *International Journal of Advances in Applied Sciences*, 10(2), 178. https://doi.org/10.11591/ijaas.v10.i2.pp178-187

Alsaidi, A., Al-lehaibi, K., Alzahrani, H., Ghamdi, M., and Gutub, A. (2024). Compression multi-level crypto stego security of texts utilizing colored email forwarding. *Journal of Computer Science and Computational Mathematics,* 33-42. https://doi.org/10.20967/jcscm.2018.03.002

Assa-Agyei, K. (2024). Hybrid algorithm using rivest-shamir-adleman and elliptic curve cryptography for secure email communication. *International Journal of Advanced Computer Science and Applications,* 15(4). https://doi.org/10.14569/ijacsa.2024.01504105

Atanda, O. (2024). Building a robust data shield: implementing a cryptography and steganography security model.. https://doi.org/10.21203/rs.3.rs-4689651/v1

Archana, P. Naragen C. and Prashant, K. (2024). A security ontology for Establishing Data Provenance in Semantic Web. *Journal of Web Engineering:* ISSN1544-5976.

Bender, E. M., Friedman, R., and Miller, D. (2023). *Steganography for cryptographic systems: Advances and applications*. Springer.

Bharadiya, J. (2023). Machine learning in cybersecurity: techniques and challenges. *European Journal of Technology,* 7(2), 1-14. https://doi.org/10.47672/ejt.1486

Brown, T., Mann, B., Ryder, N., and Subbiah, M. (2024). Language models are few-shot learners. *Proceedings of the 34th Conference on Neural Information Processing Systems (NeurIPS)*.

Cheng, H., Wang, Y., and Zhao, H. (2024). Generative adversarial networks for advanced cryptosteganography. *IEEE Transactions on Information Forensics and Security*, 17, 1789-1800.

Choudhury, Z. (2023). Enhancing email security: optimizing machine learning with bio-inspired metaheuristic algorithms for spam detection. https://doi.org/10.31219/osf.io/rjeyt

Devlin, J., Chang, M. W., Lee, K., and Toutanova, K. (2024). BERT: Pre-training of deep bidirectional transformers for language understanding. *Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics (NAACL)*.

Dhawan, S., and Gupta, R. (2024). Analysis of various data security techniques of steganography: A survey. *Information Security Journal a Global Perspective*, *30*(2), 63–87. https://doi.org/10.1080/19393555.2020.1801911

Derbyshire C. (2023): Email Classification to Restricted, Controlled and Public Emails. https://staff.debyshires-gov.uk.

Farooq, A., Tariq, S., Amin, A., Qureshi, M. A., and Memon, K. H. (2023). Towards the design of new cryptographic algorithm and performance evaluation measures. *Multimedia Tools and Applications*. https://doi.org/10.1007/s11042-023-15673-7

Fatima, R., Sadiq, M., Ullah, S., Ahmed, G., and Mahmood, S. (2023). An optimized approach for detection and classification of spam email's using ensemble methods. https://doi.org/10.21203/rs.3.rs-2051142/v1

Hasmawati, H. and Barmawi, A. (2023). Increasing the capacity of headstega based on bitwise operation. Jurnal Ilmu Komputer Dan Informasi, 14(2), 113-126. https://doi.org/10.21609/jiki.v14i2.957

Huang, J., Zhang, Q., and Liu, X. (2024). Adaptive cryptosteganography with machine learning. *Journal of Computer Security*, 32(2), 347-368.

Jo, H., and Yoon, J. W. (2025). A New Countermeasure against Brute-Force Attacks That Use High Performance Computers for Big Data Analysis. *International Journal of Distributed Sensor Networks*, *11*(6), 406915. https://doi.org/10.1155/2015/406915

Khedr, A., Gulak, G., and Vaikuntanathan, V. (2024). Shield: scalable homomorphic implementation of encrypted data-classifiers. Ieee Transactions on Computers, 65(9), 2848-2858. https://doi.org/10.1109/tc.2015.2500576

Koh, J., Bellovin, S., and Nieh, J. (2019). Why joanie can encrypt.. https://doi.org/10.1145/3302424.3303980

Kumar Pandey, B., Pandey, D., Nassa, V. K., Ahmad, T., Singh, C., George, A. S., and Wakchaure, M. A. (2023). Encryption and steganography-based text extraction in IoT using the EWCTS optimizer. *The Imaging Science Journal*, *69*(1–4), 38–56. https://doi.org/10.1080/13682199.2022.2146885

Kumar, A. and Pooja, K. (2024). Steganography- a data hiding technique. *International Journal of Computer Applications,* 9(7), 19-23. https://doi.org/10.5120/1398-1887

Kumar, A., Anfah, K., Hariharan, T., Parveen, R., Mahmud, S., and Sharma, S. (2023). Secure file storage on cloud using hybrid cryptography. International Journal of Advanced Research, 11(04), 01-05. https://doi.org/10.21474/ijar01/16613

Liu, X., Zhang, S., and Wang, L. (2023). Transfer learning for email categorization: A survey. *Journal of Artificial Intelligence Research*, 70, 291-319.

Menezes, A., van Oorschot, P., and Vanstone, S. (2025). *Handbook of applied cryptography*. CRC Press.