*IJFL (International Journal of Forensic Linguistic)*

Vol. 5, No. 1, 2025, Page 18-22

*P-ISSN: XXXX-XXXX*
*E-ISSN: XXXX-XXXX*

# Linguistic Features in Online Scam Texts: A Case Study on Fake Lottery Schemes

**Ferni Saefatu**

*Universitas Warmadewa*

fernisaefatu14@gmail.com

Published: 31/05/2025

**How to cite (in APA style):**
Saefatu, F. (2025). Linguistic Features in Online Scam Texts: A Case Study on Fake Lottery Schemes. *IJFL (International Journal of Forensic Linguistic)*, 5(1), 18-22. Doi: http://dx.doi.org/xxxxxxjr.xx.xxx.Page

**Abstract-** Online fraud in the form of fake lottery schemes is a type of cybercrime that relies on the power of language to persuade, direct, and manipulate victims. This study aims to identify and analyze the distinctive linguistic features found in scam texts delivered via short messages (SMS and WhatsApp). The method employed is a descriptive qualitative approach using content analysis within the framework of forensic linguistics. The data were collected from ten fraudulent messages circulating in the community during the period of January to May 2025. The results show that scam texts typically use hyperbolic diction, imperative sentences, visual symbols such as capitalization and exclamation marks, and include the names of official institutions to create a sense of legitimacy. These linguistic strategies reveal a systematic pattern used by perpetrators to influence the emotions and reasoning of their targets. These findings are expected to enhance public linguistic literacy and support the development of text-based fraud detection systems.

**Keywords:** Forensic Linguistics, Online Fraud, Fake Lottery, Short Messages, Linguistic Analysis.

## I. INTRODUCTION

The development of digital communication technology has provided many conveniences for society; however, it has also opened up opportunities for cybercrimes, one of which is fraud conducted via text messages (SMS), WhatsApp, and social media platforms. One of the most common types of fraud found in Indonesia is fake lottery scams that claim to be from large companies, government institutions, or telecommunication service providers. This type of scam typically targets the public by promising large prizes and directing message recipients to contact a specific number, fill in personal information, or transfer a certain amount of money. This phenomenon is not only a legal and cybersecurity issue but is also of linguistic interest, particularly within the field of forensic linguistics.

Forensic linguistics, as a branch of applied linguistics, studies the use of language within legal and criminal contexts. According to Coulthard and Johnson (2007), forensic linguistics involves the application of linguistic analysis to investigate texts related to criminal acts. In the context of online fraud, language is not merely a tool for communication, but also a means to construct illusions, instill false trust, and manipulate recipients into acting according to the perpetrator's intentions. Therefore, analyzing the linguistic features of scam messages is essential as part of efforts to prevent fraud and understand the linguistic strategies employed by perpetrators.

Fake lottery scams tend to display distinctive linguistic patterns that can be identified. Olsson (2008) explains that fraudulent texts often contain persuasive, imperative, and manipulative language. The language is deliberately crafted to create a sense of urgency, artificial credibility, and emotional pressure on the reader. These features include the use of words such as "CONGRATULATIONS," "WINNER," "IMMEDIATELY," as well as references to well-known institutions like "TELKOMSEL," "BANK INDONESIA," or "MINISTRY" to create a false sense of legitimacy. Additionally, excessive use of punctuation, capitalization, and brief imperative sentences are also common characteristics.

According to Gibbons (2003), language in criminal contexts is often manipulated to conceal the speaker's true intentions. In fraud cases, the perpetrator uses language as a form of hidden power, operating psychologically rather than overtly. This is supported by Shuy (1998), who argues that linguistic analysis can uncover the hidden strategies used in criminal texts, including word choices that are persuasive, enticing, or intimidating.

Meanwhile, Eades (2010) emphasizes the importance of cultural and social context in understanding language use in legal processes. In developing countries like Indonesia, the public's vulnerability to fraud is often influenced by disparities in linguistic knowledge and a high level of trust in authority figures. Perpetrators exploit this by creating the illusion of official institutions in their scam texts.

Research into the linguistic aspects of scam messages is relevant not only in the field of linguistics but also in information security, law, and digital literacy. According to Solan and Tiersma (2005), understanding the structure and function of language in legal contexts can help uncover motives, identify perpetrators, and determine the purpose of communication. In the Indonesian context, where digital literacy is uneven, people often fall victim to scams due to a lack of awareness of suspicious language patterns. Therefore, this study is expected to contribute to raising public linguistic awareness while also strengthening interdisciplinary collaboration between linguistics and law enforcement.

Another opinion is offered by McMenamin (2002), who states that each individual has a unique linguistic pattern that can be identified in written texts. Thus, linguistic analysis of scam messages can also be used to identify potential perpetrators through their linguistic fingerprints. Meanwhile, Grant (2013) asserts that understanding the stylistic features of criminal language can assist in developing automatic detection technologies, such as chatbots or message-filtering systems.

Previous research has examined various forms of language crimes in forensic contexts, but specific studies on online fraud involving fake lottery schemes remain limited, especially in the Indonesian setting. Some earlier studies, such as Taufiq (2022), have shown that scam messages tend to exhibit linguistic patterns that can be systematically mapped. However, studies that deeply integrate forensic linguistic approaches focusing on word choice, sentence structure, and language style in fake lottery texts are still rarely found. Therefore, this research is necessary in order to describe and understand how language is used as a tool for deception in the digital context.

Based on the background above, this study aims to identify and analyze the distinctive linguistic features found in online scam texts using the fake lottery method. The main focus of this research is on word choice (diction), sentence structure, and language style used by perpetrators to persuade and manipulate victims. The results of this study are expected to contribute not only to the advancement of forensic linguistics but also serve as a practical reference for public education and the development of language-based fraud detection systems in the future.

## II. METHODS

This study employs a descriptive qualitative approach with an analysis based on forensic linguistics. The primary focus of the research is to identify the linguistic features used in online scam texts, particularly those involving fake lottery schemes. The data sources consist of ten samples of scam messages obtained from documented short messages (SMS and WhatsApp) that have circulated among the public and been shared on social media between January and May 2025. The data were purposively selected based on specific criteria, namely texts containing elements of manipulation, calls to contact a specific number, and references to prizes or cash rewards.

Data analysis was conducted using content analysis techniques, focusing on linguistic elements such as word choice (diction), sentence structure, punctuation, use of capitalization, and persuasive language style. This analytical technique aligns with Krippendorff's (2004) view that content analysis is highly relevant in examining patterns of written communication with specific purposes, including in the context of text-based criminal activity. The analysis was carried out manually by recording and categorizing recurring linguistic features found in the texts.

According to Yin (2016), a qualitative approach enables researchers to gain an in-depth understanding of phenomena within complex social and cultural contexts, such as the use of language in digital fraud. This study also applies the principle of data triangulation to ensure the validity of the findings, by comparing data from various sources (different messages) and observing the consistency of linguistic patterns used by the scammers. In the analytical process, this research refers to the forensic linguistic framework as outlined by Grant and MacLeod (2016), which emphasizes the importance of identifying linguistic strategies used to deceive, manipulate, or mislead the message recipients. By employing this approach, the study aims to reveal language patterns that are not only linguistically distinctive but also significant from psychological and criminological perspectives.

## III. RESULT AND DISCUSSION

### Linguistic Patterns in Fraudulent Messages

The analysis of ten online scam messages using the fake lottery scheme reveals consistent and strategic linguistic patterns aimed at persuading and manipulating victims. These messages are crafted with specific linguistic strategies designed to influence the recipient's emotions, perceptions, and actions. The language used in such scams is far from neutral; rather, it serves as a persuasive and manipulative tool, carefully constructed to create false trust and urgency. Generally, the language is emotional and persuasive, with short, direct, and often imperative sentence structures.

Firstly, in terms of word choice, the use of words such as "CONGRATULATIONS," "YOU WIN," "DIRECT PRIZE," and "TRANSFER IMMEDIATELY" is intended to simultaneously evoke excitement and urgency. These words are typically written in capital letters and often accompanied by exclamation marks—for example: "CONGRATULATIONS!!! YOU HAVE WON 100 MILLION FROM TELKOMSEL!" According to Olsson (2008), word selection in fraudulent texts is done strategically to create shock value and psychological pressure, prompting victims to act quickly in accordance with the scammer's instructions. These words play a key role in building false expectations and creating the illusion of sudden luck, ultimately weakening the reader's critical thinking.

In addition, some messages contain legal- or administrative-sounding phrases such as "OFFICIAL," "REGISTERED WITH THE MINISTRY OF FINANCE," or "LISTED IN BANK INDONESIA." The purpose of these phrases is to construct a sense of legitimacy and authority, as though the message originates from a government institution. This tactic strengthens the illusion that the prize is real and must be claimed immediately. In forensic linguistics, this strategy is referred to as institutional impersonation, where authority is mimicked to psychologically suppress the victim's doubts.

Secondly, the sentence structure in these messages is dominated by commands and direct instructions. Sentences such as "CONTACT THIS NUMBER IMMEDIATELY," "TRANSFER REGISTRATION FEE," and "SEND YOUR DATA NOW" demonstrate subtle coercion. Shuy (1998) notes that imperative sentences in criminal contexts are often used to control the target's behavior through linguistic pressure masked by everyday language. These instructions are designed to suppress the victim's thinking time, induce fear or anxiety, and create pressure to comply without seeking advice or thinking critically.

Thirdly, the use of symbols and punctuation marks is a striking feature. Many messages contain repeated exclamation marks, full-sentence capitalization, and references to official institutions, such as "BANK INDONESIA," "MINISTRY OF FINANCE," or "TELKOMSEL HEADQUARTERS." Gibbons (2003) affirms that language criminals frequently use institutional attributes as fake legitimacy tools to convince victims that the messages are genuine and trustworthy. Visual elements like logos, capital letters, and

paragraph layouts resembling official announcements further reinforce the linguistically-based fraud strategy.

Moreover, there is a noticeable pattern of repetition in writing style and structure, indicating that scammers employ pre-designed templates or text formats proven to be effective. This suggests a level of professionalism in crafting such fraudulent messages. Some messages even adopt promotional language, such as "HURRY! TODAY ONLY!" or "DON'T MISS YOUR CHANCE TO WIN!" resembling advertising strategies. These techniques not only entice but also manipulate the recipient's emotional decision-making.

**Message Format and Manipulation Strategies**

Further data categorization reveals that eight out of ten messages include fake links or WhatsApp numbers that recipients are urged to contact immediately. The message format is crafted to resemble official announcements, complete with document numbers, announcement dates, and legal terms like "official," "legal," or "valid." This writing style is intentionally manipulated to create a formal and convincing appearance. In some cases, scammers even include fake digital signatures, fabricated registration numbers, and names of employees or institutions to enhance the message's legitimacy. This demonstrates that the scammers exploit not only language but also visual forms and administrative structures to deceive victims. McMenamin (2002) states that criminal language style can be identified through recurring patterns and the use of consistent linguistic and non-linguistic elements. It is not uncommon for scammers to imitate the style of official decrees, even adding fake letterheads or digital stamps to establish seemingly authentic credibility.

Some messages also use time-pressure language, such as "IMMEDIATELY," "LIMITED," or "TODAY ONLY." These terms create the illusion that the recipient must act quickly, leaving little time for reflection—a common technique in persuasive communication aimed at reducing rationalization space. This strategy is known as linguistic urgency, often used in advertising and promotion. However, in the context of fraud, it becomes manipulative. Emphasizing limited time is intended to suppress cognitive resistance and accelerate impulsive decision-making.

In other messages, emotional manipulation strategies are employed, such as claiming that the recipient is the only lucky winner or warning that the prize will be forfeited if not claimed promptly. This combines loss aversion with the euphoria of winning—an emotional pairing that can effectively disable rational thinking.

**Implications and Recommendations**

The findings underscore the importance of linguistic education and digital literacy for the public, so that individuals can recognize the linguistic patterns used in cybercrime. A lack of awareness regarding the characteristics of scam messages leads many people to fall victim and suffer financial loss. Therefore, linguistic literacy is urgently needed in the digital era, especially for lower-education groups who are most vulnerable to such crimes.

Institutions such as the Ministry of Communication and Information (Kominfo), telecommunication service providers, and educational institutions should collaborate to run public campaigns highlighting language-based fraud schemes. These campaigns could take the form of online seminars, educational infographics, and interactive digital simulations that teach people how to identify suspicious messages. Furthermore, fake messages can also be used as datasets to train AI models in text-based fraud detection.

This research can also benefit law enforcement agencies and digital service providers in designing automated detection systems based on linguistic patterns, as suggested by Grant and MacLeod (2016). By recognizing specific patterns, digital security systems can better filter and flag potentially fraudulent messages. This opens opportunities for the development of Natural Language Processing (NLP)-based scanning software to detect manipulative linguistic features in messages. In the future, such technologies could be integrated into messaging platforms to automatically warn users when they receive messages with scam characteristics.

In addition, these findings can contribute to the field of education, particularly in language and digital communication instruction. Content on linguistic fraud can be incorporated into school and university curricula as part of critical literacy and 21st-century skills development. This education is

not only academically beneficial but also equips learners with essential life skills to navigate the risks of communication in the digital age.

## IV. CONCLUSION

Thus, it can be concluded that language in online scam messages is not just a communication tool, but a psychological weapon used strategically to direct, trick and control the victim's behavior. The linguistic patterns used are not coincidental, but designed with a clear purpose to influence the recipient's thoughts and emotions. Language becomes a key tool in the creation of a false reality that subtly but effectively manipulates the target's consciousness. Forensic linguistic analysis contributes significantly to uncovering the structure and intent behind criminal messages, and provides a foundation for more effective technological interventions and public education. This understanding needs to be continuously developed and disseminated through inter-sectoral cooperation so that people are more vigilant and capable of facing the challenges of digital communication in this modern era. This research also opens up further opportunities to develop a linguistic classification framework for other types of online fraud, such as phishing, investment fraud, and digital extortion. Thus, digital consumer protection efforts can be further strengthened through an interdisciplinary approach involving linguistics, technology and law in an integrated manner. This interdisciplinary synergy will strengthen collective efforts in building an adaptive, educative and sustainable digital security system.

## REFERENCES

Coulthard, M., & Johnson, A. (2007). An Introduction to Forensic Linguistics: Language in Evidence. Routledge.

Eades, D. (2010). Sociolinguistics and the Legal Process. Multilingual Matters.

Gibbons, J. (2003). Forensic Linguistics: An Introduction to Language in the Justice System. Blackwell Publishing.

Grant, T. (2013). Identifying People through Language: Forensic Linguistics in Practice. Palgrave Macmillan.

Krippendorff, K. (2004). Content Analysis: An Introduction to Its Methodology (2nd ed.). Thousand Oaks, CA: Sage Publications.

McMenamin, G. R. (2002). Forensic Linguistics: Advances in Forensic Stylistics. CRC Press.

Olsson, J. (2008). Forensic Linguistics. Continuum.

Shuy, R. W. (1998). The Language of Confession, Interrogation, and Deception. Sage Publications.

Solan, L. M., & Tiersma, P. M. (2005). Speaking of Crime: The Language of Criminal Justice. University of Chicago Press.

Taufiq, M. (2022). “Strategi Bahasa dalam Penipuan Melalui Media Sosial: Studi Linguistik Forensik.” Jurnal Bahasa dan Hukum, 8(2), 110–123.

Yin, R. K. (2016). Qualitative Research from Start to Finish (2nd ed.). New York: The Guilford Press.