Vol. 15, No. 1, April 2026 • ISSN 2302-9609 (Print), 2746-4024 (Online)

L'Geneus: The Journal Language Generations of Intellectual Society

journal homepage: www.iocscience.org/ejournal/index.php/geneus

A Forensic Linguistic Investigation of Deceptive Communication in WhatsApp-Based Fraud

Adnan Fatir[1], Dikri Mudzaffar[2], Wadi Jazlan[3]

[1,2,3] Department of Informatics, Universitas Islam Indonesia, Yogyakarta, Indonesia
Jalan Kaliurang Km. 14,5, Yogyakarta, Umbulmartani, Ngemplak, Kabupaten Sleman, Daerah Istimewa Yogyakarta 55584, Indonesia

ARTICLEINFO

Article history:

Received: 26/02/2026
Revised: 27/03/2026
Accepted: 25/04/2026
Available online: 30/04/2026

Keywords:

Forensic Linguistics;
WhatsApp Fraud;
Deceptive Communication;
Cybercrime;
Digital Discourse Analysis.

ABSTRACT

The increasing use of digital communication platforms, particularly WhatsApp, has been accompanied by a growing number of online fraud cases that exploit messaging applications as a medium for deception and manipulation. As fraudsters increasingly rely on language to establish credibility, influence victims, and conceal fraudulent intentions, forensic linguistics has become a valuable approach for examining linguistic evidence within digital communication. This study aims to analyze the linguistic patterns and communicative strategies employed in WhatsApp chat-based fraud in order to identify indicators of deceptive communication. The research adopts a qualitative forensic linguistic approach using WhatsApp fraud chat transcripts collected from victim reports, archived scam conversations, and publicly available fraud documentation as the primary data source. The data were analyzed through lexical, syntactic, pragmatic, and discourse analysis to examine how language is strategically used by fraudsters. The findings reveal that fraudulent conversations are characterized by recurring lexical features such as urgency-related vocabulary, authority claims, security-related terminology, and reward-based expressions. Syntactically, fraudsters frequently employ imperative and interrogative structures to direct victim behavior and obtain sensitive information. Pragmatic analysis indicates the extensive use of directive, assertive, and commissive speech acts, as well as implicatures and persuasive strategies designed to create trust and encourage compliance. At the discourse level, fraudulent interactions typically follow structured stages involving introduction, trust-building, information gathering, persuasion, and execution, often supported by narrative manipulation and false identity construction. The study concludes that WhatsApp-based fraud exhibits identifiable linguistic characteristics that function as indicators of deception and criminal intent. These findings demonstrate the significant role of forensic linguistic analysis in detecting fraudulent communication, supporting digital forensic investigations, and contributing to cybercrime prevention efforts through increased public awareness and the development of language-based fraud detection systems.

1. Introduction

The rapid advancement of information and communication technology has significantly transformed the way people interact in modern society. The widespread availability of smartphones and internet access has facilitated the emergence of various digital communication platforms that enable individuals to exchange information instantly regardless of geographical boundaries(Castells et al., 2009). Among these platforms, WhatsApp has become one of the most popular messaging applications worldwide due to its ease of use, accessibility, and diverse communication features. Individuals, businesses, educational

institutions, and government agencies increasingly rely on WhatsApp for daily communication, making it an essential component of contemporary digital interaction.

Despite the numerous benefits offered by digital communication technologies, their widespread adoption has also created new opportunities for criminal activities in cyberspace(Smith, 2018). One of the most prevalent forms of cybercrime today is online fraud conducted through messaging applications. Fraudsters frequently exploit WhatsApp as a medium for carrying out deceptive schemes aimed at obtaining money, personal information, banking credentials, or other valuable assets from unsuspecting victims. Such fraudulent activities may involve impersonation of family members, company representatives, customer service officers, government officials, or financial institutions. As digital communication becomes increasingly integrated into everyday life, the frequency and sophistication of WhatsApp-based fraud continue to rise, posing significant challenges for both law enforcement agencies and the general public.

The success of many online fraud schemes depends not only on technological manipulation but also on the strategic use of language. Language serves as a powerful tool through which fraudsters construct credibility, establish trust, and influence the behavior of their targets(Anafo & Ngula, 2020). Through carefully crafted messages, perpetrators often create a sense of urgency, fear, authority, or opportunity that encourages victims to respond without critically evaluating the information provided. For example, fraudulent messages may claim that a bank account has been suspended, that a prize has been won, or that immediate verification is required to prevent financial loss. Such messages are designed to trigger emotional reactions that reduce skepticism and increase compliance. Consequently, understanding the linguistic mechanisms underlying fraudulent communication is essential for identifying how deception is achieved in digital environments.

The study of language in criminal and legal contexts is the primary concern of forensic linguistics. As an interdisciplinary field that combines linguistics and law, forensic linguistics examines language as evidence in investigations and judicial proceedings. The discipline has contributed significantly to areas such as authorship attribution, speaker identification, discourse analysis, and deception detection. In the context of cybercrime, forensic linguistic analysis provides valuable insights into how linguistic patterns can reveal the intentions, strategies, and identities of offenders. By examining lexical choices, grammatical structures, pragmatic functions, and discourse organization, researchers can uncover linguistic indicators that distinguish fraudulent communication from legitimate interaction.

WhatsApp fraud conversations provide a particularly valuable source of linguistic evidence because they contain authentic examples of interaction between perpetrators and victims(Leukfeldt & Roks, 2021). These conversations often reveal recurring communicative patterns, including persuasive language, repeated requests, strategic politeness, emotional appeals, and false claims of authority. The analysis of such linguistic features can contribute to a deeper understanding of how fraudsters manipulate language to achieve their objectives. Furthermore, identifying recurring linguistic markers may assist investigators in recognizing fraud schemes, tracing offender behavior, and developing more effective prevention strategies.

Research concerning forensic linguistics, digital fraud, deceptive communication, and cybercrime discourse has developed significantly over the last decade. One of the earlier studies relevant to deception detection was conducted by Wenlin Yao, Zeyu Dai, Ruihong Huang, and James Caverlee (2017). Their research explored online deception detection using real-world datasets and investigated linguistic characteristics that distinguish deceptive communication from truthful messages. The study demonstrated that deceptive texts often exhibit identifiable writing patterns, including variations in lexical complexity and persuasive language use. Their findings highlighted the importance of linguistic features as indicators of deceptive intent in digital communication environments.

Published by Institute of Computer Science (IOCS) | www.iocscience.org | www.iocspublisher.org

In a related study, Merylin Monaro, Chiara Galante, Riccardo Spolaor, Qian Qian Li, Luciano Gamberini, Mauro Conti, and Giuseppe Sartori (2018) examined deception detection through keyboard dynamics and written responses. Their research revealed that deceptive communication often leaves measurable behavioral and linguistic traces during text production. Although the study focused primarily on identity verification, it reinforced the broader forensic linguistic assumption that deceptive behavior can be identified through patterns embedded within textual communication.

Also in 2018, Ángel Hernández-Castañeda, Hiram Calvo, and Omar Juárez Gambino investigated the role of linguistic polarity in deception detection. Their study analyzed semantic and lexical features within deceptive texts and found that linguistic characteristics remain important indicators for identifying fraudulent or misleading communication. The research contributed to the growing body of literature emphasizing the role of language analysis in detecting deception in digital environments.

Another important contribution was provided by Roger McHaney, Joey F. George, and Manjul Gupta (2018), who examined textual cues in asynchronous online communication. Their study explored how embedded linguistic and nonverbal textual signals influence deception detection. The findings suggested that deceptive communication can be identified through strategic textual constructions and communicative cues, which are frequently present in online messaging environments. This research is particularly relevant to WhatsApp-based fraud because such scams often rely on carefully designed textual interactions to manipulate victims.

As digital communication platforms became increasingly associated with criminal activities, research began to focus more directly on messaging applications. Dennis Wijnberg and Nhien-An Le-Khac (2021) investigated forensic approaches to WhatsApp communication analysis. Their study addressed challenges faced by law enforcement agencies in accessing and analyzing WhatsApp communications used in criminal activities. The researchers emphasized the growing significance of WhatsApp as a platform frequently exploited for both legitimate and criminal purposes and highlighted the importance of digital forensic techniques for extracting communication evidence.

In the context of online fraud, Jeong Young Ho and Ha Hyung Joon (2022) conducted a study on messenger phishing crimes and their evolving patterns. By examining numerous cases of messaging-based fraud, the researchers identified common tactics used by perpetrators, including impersonation strategies and trust-building techniques. Their findings demonstrated that fraudulent interactions often depend heavily on linguistic manipulation and social engineering strategies designed to exploit victims' emotions and trust.

Similarly, Nam So Won, Lee Hak Sun, and Lee Sang Jin (2022) analyzed messenger-phishing cases to identify emerging fraud patterns and response strategies. Their study revealed that fraudsters frequently impersonate acquaintances and exploit interpersonal relationships through carefully constructed messages. The research provided valuable insights into how language is used strategically to establish credibility and deceive victims within digital messaging environments.

Research specifically addressing communication fraud on WhatsApp was conducted by Wahyuddin, Lutfiah Firdausiah Ersa, Gusti Aningsih, Taufik Hidayat, and Alem Febri Sonni (2023). Their study analyzed communication networks involved in online fraud through WhatsApp Messenger. The researchers highlighted how fraudulent actors utilize WhatsApp's communication structure to disseminate deceptive messages and conduct scams. Although the study focused primarily on communication networks rather than linguistic analysis, it underscored the growing role of WhatsApp in facilitating online fraud schemes.

Previous studies on cybercrime have primarily focused on technological vulnerabilities, cybersecurity measures, and victim behavior(Sabillon et al., 2016). While these studies have

provided important insights into the nature of online fraud, relatively limited attention has been given to the linguistic dimensions of fraudulent communication, particularly within messaging applications such as WhatsApp. Given that language is central to the execution of many fraud schemes, there is a need for further research that examines the specific linguistic strategies employed by perpetrators in digital interactions. Such research can enhance theoretical understanding within forensic linguistics while also generating practical applications for fraud detection and cybercrime prevention.

In addition, the growing reliance on digital evidence in criminal investigations has increased the importance of linguistic analysis as a forensic tool. Law enforcement agencies increasingly encounter cases in which chat messages, text conversations, and digital communications serve as critical pieces of evidence(Dodge et al., 2019). Understanding how linguistic evidence can be systematically analyzed to identify deceptive intentions and communicative patterns is therefore essential for modern forensic practice. Through the examination of WhatsApp-based fraud conversations, forensic linguistics offers a valuable framework for investigating the relationship between language, deception, and criminal behavior in digital environments.

Based on these considerations, this study seeks to analyze the linguistic characteristics of WhatsApp chat-based fraud from a forensic linguistic perspective. By examining the language patterns, persuasive strategies, and deceptive communication techniques employed by fraudsters, the study aims to contribute to the development of forensic linguistic knowledge and provide practical insights that may support cybercrime investigations and public awareness efforts. Ultimately, the research highlights the crucial role of language as both a tool of deception and a source of evidence in understanding and combating online fraud in the digital age.

2. Method

This study employs a qualitative research design within the framework of forensic linguistics(Clarke & Kredens, 2018). Specifically, the research adopts a qualitative forensic linguistic approach combined with qualitative content analysis to investigate linguistic patterns found in WhatsApp chat-based fraud. A qualitative approach is considered appropriate because the primary objective of the study is to understand and interpret the meanings, communicative functions, and linguistic strategies embedded in fraudulent conversations rather than to measure variables statistically. Since fraud communication often involves complex linguistic phenomena such as persuasion, deception, manipulation, and contextual meaning, qualitative analysis enables an in-depth examination of how language is strategically used by fraudsters to influence victims.

Qualitative forensic linguistic analysis focuses on language as evidence and seeks to identify linguistic features that may reveal communicative intentions, deceptive practices, and patterns of criminal behavior(Shuy, 2005). Through this approach, the study examines how lexical choices, grammatical structures, speech acts, and discourse organization contribute to the construction of fraudulent messages. Furthermore, qualitative content analysis allows the researcher to systematically categorize and interpret recurring themes and linguistic characteristics found within the collected chat data. By integrating these approaches, the study aims to provide a comprehensive understanding of the linguistic mechanisms underlying WhatsApp-based fraud.

The primary data for this study consist of WhatsApp chat conversations associated with fraudulent activities(Trisnasenjaya & Riadi, 2019). The data are obtained from several sources to ensure a diverse and representative sample of fraud communication. These sources include screenshots of WhatsApp fraud chats shared by victims, archived scam conversations collected from public awareness campaigns and cybersecurity forums, publicly available fraud reports

Published by Institute of Computer Science (IOCS) | www.iocscience.org | www.iocspublisher.org

published by governmental or cybersecurity organizations, and chat transcripts voluntarily submitted by victims of online fraud.

The selected data involve various forms of WhatsApp-based scams, including impersonation fraud, banking fraud, prize-winning scams, account verification scams, investment fraud, and social engineering attacks. These conversations provide authentic examples of interaction between fraudsters and victims, making them suitable for forensic linguistic examination. To protect privacy and maintain ethical standards, all personally identifiable information, including names, phone numbers, addresses, account details, and other sensitive information, is removed from the dataset prior to analysis.

The data collection process is conducted through several systematic stages(Rahi, 2017). First, WhatsApp chat transcripts related to fraudulent activities are collected from available sources, including victim reports, public databases, cybersecurity awareness websites, and archived scam documentation. Only conversations that clearly demonstrate fraudulent intent or deceptive communication are selected for analysis.

Second, the collected conversations are screened to ensure their relevance to the objectives of the study(Fritzen-Pedicini et al., 2019). Chats that do not contain sufficient linguistic content or lack evidence of fraud-related interaction are excluded from the dataset. The selected conversations are then categorized according to the type of fraud represented in the interaction.

Third, all personal and confidential information contained within the conversations is anonymized to ensure participant privacy and compliance with ethical research principles(Novak, 2014). Names, contact numbers, financial information, and any identifying details are replaced with neutral labels or pseudonyms.

Finally, the chat transcripts are organized into analytical units for systematic examination. Individual messages, message sequences, conversational exchanges, and interactional episodes are treated as units of analysis. This organization facilitates the identification of recurring linguistic patterns and communicative strategies across different fraud cases.

The data are analyzed using forensic linguistic analysis, which focuses on identifying linguistic features that characterize fraudulent communication(Humpherys et al., 2011). The analysis is conducted at four interrelated levels: lexical, syntactic, pragmatic, and discourse features.

The first level involves lexical analysis. This stage examines the vocabulary used by fraudsters, including word choice, repeated expressions, and fraud-related terminology(Chen, 2021). Particular attention is given to words that convey urgency, authority, trustworthiness, reward, fear, or financial gain. Recurrent lexical patterns are identified to determine how specific vocabulary contributes to deceptive communication.

The second level focuses on syntactic analysis. This analysis investigates sentence structures used within fraudulent messages, including declarative statements, imperative commands, interrogative forms, and other grammatical constructions(Anafo, 2017). The study examines how sentence patterns are employed to direct victim behavior, request information, or establish credibility. Imperative structures such as requests for immediate action and interrogative forms designed to extract information are analyzed as potential indicators of manipulation.

The third level involves pragmatic analysis. This stage explores how meaning is constructed beyond the literal content of messages. Speech act theory is applied to identify communicative functions such as requests, commands, promises, threats, warnings, and assertions(Kissine, 2013). Additionally, implicatures and indirect meanings are examined to understand how fraudsters convey persuasive intentions without explicitly stating them. The

Published by Institute of Computer Science (IOCS) | www.iocscience.org | www.iocspublisher.org

analysis also investigates various persuasion strategies used to influence victims' decisions and responses.

The fourth level consists of discourse analysis. At this stage, the overall organization and structure of conversations are examined. The analysis focuses on conversation sequencing, turn-taking patterns, topic development, and narrative construction. Particular attention is given to how fraudsters gradually build trust, establish authority, create urgency, and manipulate conversational flow to achieve their objectives. Narrative manipulation strategies, such as presenting fabricated scenarios or constructing false identities, are also analyzed to reveal broader discourse patterns associated with fraudulent communication.

Through the integration of lexical, syntactic, pragmatic, and discourse analyses, the study seeks to uncover the linguistic mechanisms that characterize WhatsApp-based fraud and contribute to its effectiveness.

To ensure the credibility and trustworthiness of the findings, several validation strategies are employed throughout the research process(Morse, 2015). First, data triangulation is conducted by collecting fraud conversations from multiple sources, including victim reports, public archives, and cybersecurity documentation. The use of diverse data sources enhances the reliability of the findings and reduces potential bias associated with a single dataset.

Second, peer review is utilized during the analytical process. Colleagues or researchers with expertise in linguistics, discourse analysis, or forensic studies are invited to review selected portions of the data and the resulting interpretations. This process helps ensure that the analysis remains objective and theoretically grounded.

Third, expert validation is conducted by consulting specialists in forensic linguistics, cybercrime studies, or digital communication. Their feedback assists in verifying the appropriateness of analytical procedures and the interpretation of linguistic evidence.

Finally, consistency checking is applied throughout the coding and analysis process. Linguistic categories, themes, and interpretations are reviewed repeatedly to ensure coherence and stability across the dataset(Eichstaedt et al., 2021). Any discrepancies identified during analysis are reexamined and resolved through systematic comparison of data segments. These procedures enhance the dependability, credibility, and confirmability of the research findings, thereby strengthening the overall quality of the study.

3. Results and Discussion

3.1 Results

One of the most prominent findings concerns the lexical characteristics of fraudulent messages. The analysis revealed frequent use of vocabulary associated with urgency, authority, security, and financial transactions. Words and phrases such as "urgent," "verification," "account blocked," "security code," "immediate action," "bank officer," and "official notification" appeared repeatedly across multiple fraud conversations. These lexical choices were not randomly selected but strategically employed to create a sense of importance and urgency. By emphasizing immediate consequences or limited opportunities, fraudsters attempted to reduce victims' ability to critically evaluate the information provided. The repeated occurrence of such vocabulary suggests that urgency-based lexical strategies constitute a fundamental component of fraudulent communication on WhatsApp.

In addition to urgency-related vocabulary, the analysis identified frequent use of terms associated with rewards and financial benefits(Wylie et al., 2014). Messages often contained references to prizes, lottery winnings, investment opportunities, cashback rewards, or unexpected financial gains. Such language was designed to stimulate positive emotional responses and increase the likelihood of victim engagement. The findings indicate that fraudsters exploit both fear and reward mechanisms through strategic lexical choices,

Published by Institute of Computer Science (IOCS) | www.iocscience.org | www.iocspublisher.org

demonstrating the dual role of language in creating psychological pressure and generating attraction.

The syntactic analysis revealed several distinctive sentence patterns within fraudulent conversations. Imperative structures were among the most common grammatical forms identified in the dataset. Messages frequently included commands such as "Click the link now," "Send the verification code," "Transfer the funds immediately," or "Confirm your account details." The use of imperatives reflects an attempt to direct victim behavior and establish conversational control. These commands often appeared alongside time-sensitive expressions, reinforcing the urgency conveyed through lexical choices.

Interrogative structures were also frequently employed, particularly during the information-gathering stage of fraudulent interactions(Meissner et al., 2014). Fraudsters used questions to obtain personal information, banking details, account credentials, or verification codes. In many cases, these questions appeared conversational and polite, reducing suspicion while gradually extracting sensitive information from victims. Declarative statements, meanwhile, were commonly used to present fabricated facts or false claims of authority. Messages asserting that an account had been compromised, a payment was pending, or a prize had been awarded were often formulated as definitive statements, thereby increasing their perceived credibility.

Pragmatic analysis further revealed the sophisticated communicative strategies employed by fraudsters(Carter, 2015). Speech act analysis demonstrated that fraudulent conversations frequently combined multiple communicative functions within a single interaction. Directive speech acts were particularly common, as perpetrators repeatedly instructed victims to perform specific actions such as clicking links, sharing personal information, or transferring money. These directives were often accompanied by commissive speech acts, including promises of rewards, guarantees of account recovery, or assurances of financial benefits. The combination of commands and promises created a persuasive environment in which victims were encouraged to comply with fraudulent requests.

The analysis also identified numerous instances of assertive speech acts in which fraudsters presented false information as factual. Perpetrators frequently claimed to represent banks, government institutions, telecommunications providers, or customer service departments. Such assertions were intended to establish authority and legitimacy within the interaction. In many conversations, the use of institutional language and professional terminology reinforced the impression that the sender represented a trustworthy organization. This finding highlights the role of language in constructing false identities and manipulating perceptions of credibility.

Another important pragmatic finding concerns the use of implicatures and indirect persuasion strategies. Rather than explicitly demanding sensitive information, fraudsters often implied potential negative consequences if victims failed to comply(Albrecht et al., 2016). For example, messages suggesting that an account would be suspended or that access would be permanently restricted created implicit threats without directly stating them. These indirect communicative strategies allowed perpetrators to exert pressure while maintaining an appearance of legitimacy. Such findings support the argument that fraudulent communication relies heavily on pragmatic manipulation and contextual interpretation.

The discourse analysis revealed recurring structural patterns across fraudulent conversations. Most interactions followed a relatively consistent sequence consisting of introduction, trust-building, information gathering, persuasion, and request execution stages. During the introduction stage, fraudsters established initial contact by presenting themselves as representatives of legitimate organizations or trusted individuals. This was followed by trust-building strategies involving polite language, professional terminology, and references to institutional authority.

Published by Institute of Computer Science (IOCS) | www.iocscience.org | www.iocspublisher.org

The information-gathering stage involved a series of questions designed to obtain personal details or verify account information(Buie & Yeske, 2015). Once rapport had been established, fraudsters introduced persuasive elements aimed at encouraging compliance. These elements often included warnings, incentives, or claims of urgency. Finally, the request execution stage involved direct instructions requiring victims to disclose confidential information, transfer money, or perform actions beneficial to the perpetrator.

A particularly significant discourse feature identified in the dataset was narrative manipulation. Fraudsters frequently constructed detailed narratives designed to make their claims appear plausible and convincing. These narratives often involved fabricated scenarios such as account security breaches, prize winnings, family emergencies, business transactions, or technical problems requiring immediate attention. The construction of coherent and emotionally engaging narratives enabled perpetrators to maintain victim engagement and reduce skepticism. Such findings demonstrate that successful fraud communication depends not only on individual linguistic features but also on the strategic organization of discourse over the course of the interaction.

The findings of this study support previous research in forensic linguistics and deception detection, which suggests that deceptive communication exhibits identifiable linguistic characteristics. The recurring use of urgency-related vocabulary, imperative structures, authority claims, persuasive speech acts, and structured narratives indicates that fraudulent communication is highly systematic rather than random. These linguistic patterns function collectively to create trust, establish credibility, generate emotional responses, and motivate victim compliance.

From a forensic linguistic perspective, the identified features represent valuable indicators that may assist investigators in recognizing fraudulent communication and understanding offender behavior. Lexical patterns, grammatical structures, speech acts, and discourse organization can serve as forms of linguistic evidence that contribute to the identification of deceptive intent and communicative strategies. Furthermore, these findings suggest that linguistic analysis may complement technological and digital forensic approaches in the investigation of cybercrime.

3.2 Discussion

The findings of this study demonstrate that WhatsApp-based fraud is fundamentally a linguistic phenomenon in which language functions as a strategic tool for deception, persuasion, and manipulation. The identified lexical, syntactic, pragmatic, and discourse features reveal that fraudulent communication is systematically designed to influence victims' perceptions and behaviors. These findings can be interpreted through the perspectives of forensic linguistics theory, deception theory, digital discourse analysis, and previous cybercrime research.

From the perspective of forensic linguistics, the results support the argument that language can serve as valuable evidence in criminal investigations(Coulthard et al., 2016). Forensic linguists such as Malcolm Coulthard and John Olsson have emphasized that linguistic patterns often reveal information about communicative intentions, authorship characteristics, and deceptive practices. The recurring use of urgency-related vocabulary, authority claims, repeated sentence structures, and persuasive discourse strategies identified in this study demonstrates that fraudsters employ recognizable linguistic patterns rather than random language choices. These patterns may function as linguistic markers that assist investigators in identifying fraudulent communication and understanding offender behavior. The findings therefore reinforce the forensic linguistic principle that language is not merely a medium of communication but also a source of evidence capable of revealing criminal intent and communicative strategy.

Published by Institute of Computer Science (IOCS) | www.iocscience.org | www.iocspublisher.org

The findings also align closely with deception theory, which suggests that deceptive communication is often characterized by deliberate linguistic manipulation aimed at influencing recipients' beliefs and actions. The frequent use of false authority claims, fabricated narratives, implicit threats, and promises of rewards reflects common deception strategies identified in previous research(Bailey, 2019). Fraudsters strategically construct messages that create credibility while simultaneously reducing opportunities for critical evaluation. The use of urgency-related expressions such as requests for immediate action is particularly significant because it exploits cognitive and emotional vulnerabilities that may impair rational decision-making. These findings support the view that deception is not solely achieved through false information but also through the strategic organization of language designed to shape interpretation and behavior.

Another important finding concerns the role of persuasive communication in fraudulent interactions. The analysis revealed that fraudsters frequently combine directive speech acts with commissive and assertive speech acts to increase the effectiveness of their deception(Hua et al., 2017). This pattern is consistent with theories of persuasive communication, which argue that successful persuasion often involves a combination of authority, trust-building, emotional appeal, and behavioral guidance. By presenting themselves as representatives of legitimate institutions and offering solutions to fabricated problems, fraudsters create communicative contexts in which compliance appears reasonable and beneficial. Consequently, language becomes a mechanism through which trust is artificially constructed and exploited for criminal purposes.

The findings can also be interpreted through the framework of digital discourse analysis. Unlike face-to-face interactions, WhatsApp communication occurs within a computer-mediated environment where textual messages serve as the primary medium of interaction. In such contexts, participants rely heavily on linguistic cues to establish credibility, interpret intentions, and negotiate meaning. The discourse patterns identified in this study demonstrate that fraudsters effectively adapt their communication strategies to the characteristics of digital interaction. The use of concise messages, sequential questioning, professional terminology, and carefully structured narratives reflects an awareness of how digital conversations function. Furthermore, the staged organization of fraudulent conversations from introduction and trust-building to persuasion and execution illustrates how discourse is strategically managed over time to achieve specific communicative goals.

The discourse structures identified in the present study also highlight the interactive nature of online deception. Fraudulent communication was found to involve a gradual process of relationship construction rather than a single deceptive message. This finding supports digital discourse perspectives that view communication as a dynamic process in which meaning emerges through interaction(Jones et al., 2015). Fraudsters continuously adjust their language in response to victim reactions, creating adaptive discourse patterns that maximize the likelihood of compliance. Such observations suggest that successful online fraud depends not only on individual deceptive statements but also on the broader organization of interactional sequences.

The results are further supported by previous cybercrime studies that have examined phishing, online scams, and messaging-based fraud. Earlier research has consistently reported that cybercriminals rely heavily on social engineering techniques that exploit psychological and emotional factors. Similar to previous findings, this study identified the use of fear appeals, urgency cues, authority claims, and reward-based incentives as central components of fraudulent communication. The recurrence of these strategies across different forms of cybercrime suggests that linguistic manipulation remains one of the most effective tools available to fraudsters. The findings therefore confirm that cybercrime is not solely a technological problem but also a communicative and linguistic phenomenon.

Published by Institute of Computer Science (IOCS) | www.iocscience.org | www.iocspublisher.org

Moreover, previous studies on phishing and online scam communication have demonstrated that fraudsters often construct messages designed to mimic legitimate institutional communication. The present study extends these findings by showing how such imitation occurs at multiple linguistic levels, including vocabulary selection, grammatical structures, speech acts, and discourse organization(Pickering & Garrod, 2013). Fraudsters not only imitate the language of trusted organizations but also reproduce interactional patterns that create an appearance of authenticity. This observation reinforces the importance of forensic linguistic analysis in distinguishing genuine communication from deceptive discourse.

The study also contributes to the growing body of research on cybercrime by highlighting the role of linguistic evidence in fraud detection and prevention. While many cybercrime investigations focus primarily on technical indicators such as IP addresses, device records, and digital traces, the findings suggest that language itself contains valuable information about offender strategies and intentions. Linguistic indicators identified in fraudulent WhatsApp conversations may therefore complement existing digital forensic approaches and enhance investigative effectiveness. Furthermore, public awareness campaigns may benefit from incorporating linguistic indicators into educational materials designed to help individuals recognize and avoid online fraud.

4. Conclusion

This study examined the linguistic characteristics of WhatsApp chat-based fraud through a forensic linguistic framework and found that fraudulent conversations exhibit distinctive lexical, syntactic, pragmatic, and discourse features that function as tools of deception and manipulation. The analysis revealed that fraudsters strategically employ urgency-related vocabulary, authority claims, emotional appeals, reward-based incentives, imperative sentence structures, persuasive speech acts, and carefully organized discourse patterns to establish credibility, gain victims' trust, and encourage compliance. These findings demonstrate that language plays a central role in the success of online fraud and that recurring linguistic markers can serve as valuable indicators of deceptive communication. The study has important implications for both theory and practice. From a theoretical perspective, it contributes to the fields of forensic linguistics, deception studies, and digital discourse analysis by highlighting how language operates as evidence of criminal intent in online environments. From a practical perspective, the findings suggest that forensic linguistic analysis can support cybercrime investigations, assist law enforcement agencies in identifying fraudulent communication, and contribute to the development of linguistic markers for fraud detection systems. Furthermore, public awareness and digital literacy programs can utilize these findings to educate users about common linguistic strategies employed by fraudsters and help individuals recognize potential scams. Nevertheless, this study is limited to WhatsApp-based fraud conversations and a specific dataset. Therefore, future research should compare fraudulent communication across different digital platforms such as Telegram, Facebook Messenger, Instagram, and email to identify similarities and differences in deceptive language use. Future studies may also employ larger multilingual datasets to explore cross-cultural variations in fraud discourse and enhance the generalizability of findings. In addition, advances in artificial intelligence and natural language processing offer opportunities for developing automated fraud detection systems that incorporate linguistic indicators identified through forensic linguistic analysis. Such efforts may contribute to more effective prevention, detection, and investigation of online fraud in increasingly complex digital communication environments.

5. References

Albrecht, C. C., Sanders, M. L., Holland, D. V, & Albrecht, C. (2016). The debilitating effects of fraud in organizations. In *Crime and Corruption in Organizations* (pp. 163–185). Routledge.

Published by Institute of Computer Science (IOCS) | www.iocscience.org | www.iocspublisher.org

Anafo, C. (2017). *The language of deception transitivity analysis of scam email messages*. University of Education Winneba.

Anafo, C., & Ngula, R. S. (2020). On the grammar of scam: transitivity, manipulation and deception in scam emails. *Word*, *66*(1), 16–39.

Bailey, F. G. (2019). *The prevalence of deceit*. Cornell University Press.

Buie, E., & Yeske, D. (2015). Gathering Information Necessary to Fulfill the Engagement. *CFP Board Financial Planning Competency Handbook*, 617–623.

Carter, E. (2015). The anatomy of written scam communications: An empirical analysis. *Crime, Media, Culture*, *11*(2), 89–103.

Castells, M., Fernandez-Ardevol, M., Qiu, J. L., & Sey, A. (2009). *Mobile communication and society: A global perspective*. Mit Press.

Chen, J. (2021). "You are in trouble!": A discursive psychological analysis of threatening language in Chinese cellphone fraud interactions. *International Journal for the Semiotics of Law-Revue Internationale de Sémiotique Juridique*, *34*(4), 1065–1092.

Clarke, I., & Kredens, K. (2018). 'I consider myself to be a service provider': Discursive identity construction of the forensic linguistic expert. *The International Journal of Speech, Language and the Law*, *25*(1), 79–107.

Coulthard, M., Johnson, A., & Wright, D. (2016). *An introduction to forensic linguistics: Language in evidence*. Routledge.

Dodge, A., Spencer, D., Ricciardelli, R., & Ballucci, D. (2019). "This isn't your father's police force": Digital evidence in sexual assault investigations. *Australian & New Zealand Journal of Criminology*, *52*(4), 499–515.

Eichstaedt, J. C., Kern, M. L., Yaden, D. B., Schwartz, H. A., Giorgi, S., Park, G., Hagan, C. A., Tobolsky, V. A., Smith, L. K., & Buffone, A. (2021). Closed-and open-vocabulary approaches to text analysis: A review, quantitative comparison, and recommendations. *Psychological Methods*, *26*(4), 398.

Fritzen-Pedicini, C., Bleasdale, S. C., Brosseau, L. M., Moritz, D., Sikka, M., Stiehl, E., Jones, R. M., & Program, C. D. C. P. E. (2019). Utilizing the focused conversation method in qualitative public health research: a team-based approach. *BMC Health Services Research*, *19*(1), 306.

Hua, T. K., Abdollahi-Guilani, M., & Zi, C. C. (2017). Linguistic Deception of Chinese Cyber Fraudsters. *3L: Southeast Asian Journal of English Language Studies*, *23*(4).

Humpherys, S. L., Moffitt, K. C., Burns, M. B., Burgoon, J. K., & Felix, W. F. (2011). Identification of fraudulent financial statements using linguistic credibility analysis. *Decision Support Systems*, *50*(3), 585–594.

Jones, R. H., Chik, A., & Hafner, C. A. (2015). Introduction: Discourse analysis and digital practices. In *Discourse and digital practices* (pp. 1–17). Routledge.

Kissine, M. (2013). *From utterances to speech acts*. Cambridge University Press.

Leukfeldt, E. R., & Roks, R. A. (2021). Cybercrimes on the streets of the Netherlands? An exploration of the intersection of cybercrimes and street crimes. *Deviant Behavior*, *42*(11), 1458–1469.

Meissner, C. A., Redlich, A. D., Michael, S. W., Evans, J. R., Camilletti, C. R., Bhatt, S., & Brandon, S. (2014). Accusatorial and information-gathering interrogation methods and their effects on true and false confessions: A meta-analytic review. *Journal of Experimental Criminology*, *10*(4), 459–486.

Morse, J. M. (2015). Critical analysis of strategies for determining rigor in qualitative inquiry. *Qualitative Health Research*, *25*(9), 1212–1222.

Novak, A. (2014). Anonymity, confidentiality, privacy, and identity: The ties that bind and break in communication research. *Review of Communication*, *14*(1), 36–48.

Pickering, M. J., & Garrod, S. (2013). An integrated theory of language production and comprehension. *Behavioral and Brain Sciences*, *36*(4), 329–347.

Rahi, S. (2017). Research design and methods: A systematic review of research paradigms, sampling issues and instruments development. *International Journal of Economics & Management Sciences*, *6*(2), 1–5.

Sabillon, R., Cano, J. J., & Serra-Ruiz, J. (2016). Cybercrime and cybercriminals: A comprehensive study. *International Journal of Computer Networks and Communications Security, 2016, 4 (6)*.

Shuy, R. W. (2005). *Creating language crimes: How law enforcement uses (and misuses) language*. Oxford University Press.

Smith, R. (2018). *Crime in the digital age: Controlling telecommunications and cyberspace illegalities*. Routledge.

Trisnasenjaya, H., & Riadi, I. (2019). Forensic analysis of Android-based WhatsApp messenger against fraud crime using The National Institute of Standard and Technology framework. *International Journal of Cyber-Security and Digital Forensics*, *8*(1), 89–98.

Wylie, K., Bell, A., Fitzgerald, G., Crilly, J., Toloo, S., Burke, J., & Williams, G. (2014). *The implications of activity based funding for emergency departments: a comprehensive literature review: statewide workforce and activity-based funding modelling in Queensland Emergency Departments Project (SWAMPED)*. Queensland University of Technology.

Published by Institute of Computer Science (IOCS) | www.iocscience.org | www.iocspublisher.org