Jurnal Multidisiplin Indonesia (JOUMI)
Volume 4 Nomor 3 September 2026
E-ISSN : 2986-7541; P-ISSN : 2986-7533, Hal. 461-475
DOI: https://doi.org/10.62007/joumi.v4i3.1027
Tersedia: https://ejournal.alhafiindonesia.co.id/index.php/JOUMI

Analysis of Digital Content in The GEBER PK Program in Improving Digital Security Literacy Related to Deepfake AI

Warda Zahra[1*], Rahma Santhi Zianida[2]
[1-2]Communication Science Study Program, Bina Darma University, Indonesia
[*]*Corresponding Author: wardazahraa08@gmail.com*

Abstract. The rapid advancement of artificial intelligence has given rise to deepfake technology, which can realistically replicate a person's face and voice and has been misused as a means of digital fraud in Indonesia. One preventive effort is the Gerakan Bersama *Edukasi Pelindungan Konsumen* (GEBER PK) program, disseminated by financial institutions through social media. This study aims to examine the meaning contained in GEBER PK public service content related to digital security literacy on deepfake AI-based fraud. This research uses a qualitative approach with a semiotic analysis method. The research objects are a public service video uploaded on Bank Mandiri's official TikTok account and a public service poster uploaded on Bank BNI's official Instagram account in 2025. The video was analyzed using Roland Barthes' semiotic theory through denotation, connotation, and myth, while the poster was analyzed using Ferdinand de Saussure's semiotic theory through the relationship between signifier and signified. The results show that the Bank Mandiri video constructs meaning through four stages: trust formation through a fake identity, exploitation of trust and emotions, the impact of fraud, and the importance of vigilance and personal data protection. The Bank BNI poster conveys a similar message through five slides, emphasizing threat recognition, verification, and vigilance. Both contents emphasize digital security literacy through identity verification and personal data protection to address deepfake AI-based fraud.

Keywords: Deepfake AI; Digital Content; Digital Security Literacy; GEBER PK; Semiotics.

1. INTRODUCTION

The development of artificial intelligence (AI) has given rise to deepfake technology, an audio and video manipulation technique capable of realistically replicating a person's face and voice. Despite its benefits, deepfake's ability to produce content that resembles real conditions poses a challenge to the credibility of information in digital spaces, as the public increasingly struggles to distinguish authentic information from fabricated content. Muhammad Azka et al. (2025) explain that deepfake technology can produce highly realistic content manipulation with high visual and audio accuracy, contributing to the increased spread of misinformation and declining public trust.

The misuse of deepfake technology has occurred in Indonesia and has been used as a mode of digital fraud, including cases of manipulating the face and voice of public figures to offer cash prizes and direct victims to continue communication through private messages as part of a fraud scheme. This condition is in line with the findings of Boediman (2025), who explains that deepfake technology significantly blurs the boundary between truth and fiction, erodes media credibility, and is exploited to spread misinformation and manipulate public perception.

Naskah Masuk: 06 Juli 2026; Revisi: 09 Agustus 2026; Diterima: 07 September 2026; Terbit: 19 September 2026

Facing this threat, strengthening digital security literacy is important so that the public can recognize the characteristics of manipulative content, verify the information they receive, and safeguard the confidentiality of personal data. Aveny et al. (2023) affirm that digital literacy plays an important role in helping the public understand, filter, and evaluate information received through digital media, while Dhahir et al. (2024) emphasize the urgency of improving the public's ability to identify content that is potentially the result of AI engineering. Mutmainnah et al. (2024) also conclude that deepening digital literacy is a primary preventive measure against deepfake misuse.

Digital security literacy is not only related to the ability to recognize manipulated content, but also to the ability to use digital platforms safely and responsibly. Ratri & Aviyanti, (2025) explain that digital literacy is important in enabling users to find, evaluate, use, share, and create information responsibly when using social media platforms. This perspective is relevant to the threat of deepfake because users need to critically evaluate digital information before accepting or sharing it. Therefore, strengthening digital security literacy can support users in developing more careful and critical practices when interacting with AI-generated content.

The challenge becomes more complex because deepfake content can be presented in forms that appear authentic and convincing. Fahrudin & Rahman, (2025) argue that media literacy is an important strategy for preventing the spread of deepfake-based disinformation because users need not only technical skills to recognize manipulation, but also contextual awareness, ethical understanding, and the motivation to verify information. This supports the view that digital security literacy should include practical verification behavior when users encounter suspicious visual or audiovisual content on social media.

The need for such literacy is also influenced by the increasing presence of AI-generated media in everyday digital environments. Lao et al. (2025) show that encounters with deepfake content require media and information literacy practices that enable users to understand, respond to, and navigate AI-generated media. Their findings indicate that understanding how deepfakes are created and their potential social impact is an important part of media and information literacy. In this context, educational communication about deepfake risks can contribute to strengthening users' awareness before they respond to suspicious digital content.

One such educational effort is realized through the *Gerakan Bersama Edukasi Pelindungan Konsumen* (Joint Movement for Consumer Protection Education, GEBER PK) program, initiated by Bank Indonesia together with the Financial Services Authority (OJK), ministries, and the financial services industry to improve consumer literacy and protection

(Bank Indonesia, 2024). In its implementation, various banking institutions publish GEBER PK educational content through social media according to the characteristics of each platform.

Social media has become an important communication channel for institutions to disseminate public information because of its ability to distribute messages quickly and reach users through digital interaction. Razak & Sumanti, (2023) explain that social media can function as a communication medium for organizations in disseminating information to the public. In the context of GEBER PK, the use of social media allows consumer protection messages to be delivered through formats that are adapted to the characteristics of each platform. Zinaida & Anggraini, (2022) note that Instagram provides an effective channel for delivering promotional and informational messages to a broad audience, which helps explain why banking institutions increasingly rely on visual social media platforms to disseminate the GEBER PK Program's educational content. This study focuses on one public service video on the official TikTok account of Bank Mandiri (@bankmandiri) and one poster on the official Instagram account of Bank BNI (@bni46) in 2025, both of which raise the issue of AI deepfake-based fraud but are presented through different media characteristics: the video utilizes visual, audio, dialogue, and moving narrative elements, while the poster relies on a combination of static visual elements and text in a carousel format.

Previous research on deepfake generally focuses on the impact of technology misuse and the importance of digital literacy in facing this threat, such as studies on the representation of deepfake videos on social media as a form of disinformation and studies on the relationship between digital literacy and the ability to identify deepfake videos. However, research that specifically examines how educational messages about the threat of AI deepfake are represented through public service advertisements on TikTok and Instagram using a semiotic approach is still relatively limited. Based on the above description, this study aims to determine how meaning regarding digital security literacy related to the threat of AI deepfake is represented in GEBER PK Program content on Bank Mandiri's TikTok and Bank BNI's Instagram in 2025.

2. RESEARCH METHOD

This study uses a qualitative approach with a semiotic analysis method to understand and interpret the meaning constructed through communication messages in the GEBER PK Program's public service advertisements. The video on Bank Mandiri's TikTok account was analyzed using Roland Barthes' semiotic theory through three levels of meaning, namely denotation, connotation, and myth, while the poster on Bank BNI's Instagram account was

analyzed using Ferdinand de Saussure's semiotic theory through the relationship between the signifier and the signified. The use of these two approaches was adapted to the characteristics of each medium: the video is dynamic and narrative, while the poster is static and presented in a carousel format.

The object of this study is the GEBER PK Program's public service advertisement content published through the official TikTok account of Bank Mandiri and the official Instagram account of Bank BNI in 2025, containing educational messages about the mode of face and voice forgery in video call activities as well as educational posters aimed at obtaining victims' personal data and funds. This study does not involve respondents, interviews, or questionnaires, because the research data consists of media texts contained in the public service advertisement content, so the research focus is directed at interpreting the signs and meanings constructed in the media as a form of public communication.

Data collection techniques were carried out through observation and digital documentation. Observation was carried out by directly and repeatedly observing the communication elements in the content, such as signs, symbols, verbal messages, visual elements, and audio elements. Documentation was carried out by collecting video recordings, screenshots, text, and visual elements as analysis material. Data analysis was carried out in three stages: (1) identifying communication elements in the form of visual, verbal, and audio elements in the content; (2) interpreting the signs that had been identified through the levels of denotation, connotation, and myth in the video, as well as the signifier-signified relationship in the poster; and (3) interpreting the results of the analysis descriptively to understand how messages about vigilance against AI deepfake-based fraud are constructed through the GEBER PK public service advertisements.

3. RESULTS AND DISCUSSION

The objects analyzed in this study consist of a Digital Content video on the official TikTok account of Bank Mandiri (@bankmandiri) and a Digital Content poster on the official Instagram account of Bank BNI (@bni46), both published in 2025 as part of the implementation of the GEBER PK Program. Both contents raise the same theme, namely vigilance against fraud modes that utilize AI deepfake technology through the use of faces and voices made to resemble other people to build victims' trust, before being directed to provide personal data or transfer funds.

Analysis of the GEBER PK Public Service Video on Bank Mandiri's TikTok

Analysis of this video was carried out by dividing the footage based on the storyline, namely the opening, core, climax, and closing sections, then interpreted using Roland Barthes' semiotic theory through three levels of meaning: denotation, connotation, and myth.

Building Trust through a Fake Identity in the Opening Scene (00:00–00:06)



Figure 1. Opening Scene.

Source: TikTok @bankmandiri, 2025.

Table 1. Semiotic Analysis of the Initial Video Call Scene Based on Denotation, Connotation, and Myth.

Denotation	Connolation	Myth
The scene shows the initial moment of contact between the victim and the perpetrator through a video call, with the victim's initial enthusiastic and happy expression.	Represents how emotional closeness and admiration for a public figure (parasocial relationship) is exploited as a gap for trust. Deepfake technology can convincingly imitate faces and voices, thereby blurring the ability of visual senses to distinguish genuine from fake identities.	Challenges the common myth that "seeing is believing," while simultaneously forming a new myth that facial recognition alone is no longer sufficient to confirm someone's true identity in the digital era.

The scene in the 00:00 to 00:06 range shows that the victim's trust is built through a fake identity presented convincingly from the very first seconds of the video, so the victim accepts the communication without immediately questioning its authenticity. This spontaneous reaction indicates that the identity verification process that should have been carried out was instead skipped due to the strong sense of familiarity constructed by deepfake technology, while also confirming that the first six seconds of this video are already enough to break down a person's initial vigilance if not accompanied by a critical attitude toward the identity presented.

Exploitation of the Victim's Trust and Emotions in the Core Scene (00:13–00:35)

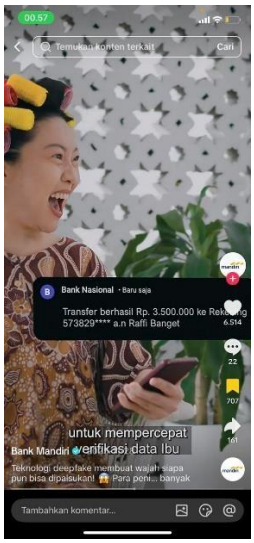


Figure 2. Core Scene.

Source: TikTok @bankmandiri, 2025.

Table 2. Semiotic Analysis of the Victim's Personal Data Submission and Fund Transfer Scene Based on Denotation, Connotation, and Myth

Denotation	Connotation	Myth
The scene shows the process of the victim providing personal data and transferring funds on the instructions of the perpetrator and a party claiming to be his assistant.	Shows the exploitation of hope for sudden fortune. The layered authority structure involving the perpetrator and the party claiming to be an assistant creates an illusion of procedural legitimacy that weakens the victim's vigilance.	Reflects the myth of unexpected fortune that persists in society, namely the belief that financial luck can come instantly without effort, which is exploited by the perpetrator to lower the victim's critical attitude.

The Impact of the Fraud and the Victim's Awareness in the Climax Scene (00:41–00:55)



Figure 3. Climax Scene

Source: TikTok @bankmandiri, 2025

Table 3. Semiotic Analysis of the Victim's Realization of Fraud Scene Based on Denotation, Connotation, and Myth.

Denotation	Connotation	Myth
The scene shows the moment the victim becomes aware of the fraud they have experienced, marked by a change in facial expression and the insertion of a warning text.	The regret shown signifies the consequences of misplaced trust. Audiovisual anomalies are positioned as markers that distinguish genuine content from fabricated content.	Forms the myth that regret comes too late, affirming the importance of prevention over regret, while also constructing digital vigilance as a form of civic responsibility in the digital era.

In the 00:41 to 00:55 range, the victim begins to realize the fraud after suffering losses, marked by a change in facial expression from previously happy to sad and disappointed within seconds. The video also inserts educational text reminding viewers to pay attention to anomalies in the audio or video movements as an indication of engineered content, so this section serves a dual function: showing the impact of the fraud while also teaching how to recognize the same signs of anomaly.

Vigilance and Data Protection in the Closing Scene (00:56–01:00)



Figure 4. Closing Scene.

Source: TikTok @bankmandiri, 2025.

Table 4. Semiotic Analysis of the Closing Campaign Message Based on Denotation, Connotation, and Myth.

Denotation	Connotation	Myth
The scene shows a closing message in the form of the campaign tagline "Jaga Datamu, Lindungi Danamu" ("Protect Your Data, Protect Your Funds") and the official identity of the GEBER PK Program.	The juxtaposition of the words "data" and "dana" (funds) implies that personal data security is closely related to financial security. The appearance of the official logo signifies the institutional legitimacy and credibility of the message.	Forms the myth that vigilant, data-literate digital citizens are protected citizens, while positioning banking institutions and government programs as parties that play a role in protecting the public from digital threats.

In the last two seconds of the video, the closing scene emphasizes the importance of vigilance in protecting personal data and financial information through a concise yet firm tagline, which implicitly summarizes the entire storyline of the video, from the personal data requested by the perpetrator to the funds successfully obtained through the fraud. The appearance of the official GEBER PK Program logo strengthens the legitimacy of the message as part of an official educational program supported by banking institutions.

Based on these four sections, the GEBER PK public service video on Bank Mandiri's TikTok conveys the message of AI deepfake fraud in stages: the victim is shown to easily trust a figure considered a public figure, that trust is exploited by the perpetrator to obtain personal data and funds, the victim's condition changes after realizing they have been deceived, and in the final part the video directs the public to be more careful and protect their personal and financial data. At the denotative level, the video shows a series of events between the victim and the perpetrator; at the connotative level, facial and vocal resemblance is used to build trust while the offer of a grant is used to influence the victim's emotions; and at the mythical level, an idea is formed that something that looks convincing does not necessarily reflect the actual state of affairs in digital communication.

Analysis of the GEBER PK Public Service Poster on Bank BNI's Instagram

Analysis of this poster was carried out by identifying each slide as a unit of analysis, then interpreted using Ferdinand de Saussure's semiotic theory through the relationship between the signifier and the signified, following the presentation flow on Bank BNI's Instagram account.

Initial Fraud Mode (Slide 1)

Table 5. Initial Fraud Mode.

Object Of Analysis	Signifier	Signified
	The display of "Unknown Number" on the mobile phone screen, a hand gesture holding the phone as if answering a call, an orange color on the call-to-action button	The "Unknown Number" display functions as an early warning sign of an unclear caller identity, which should trigger vigilance before the call is answered. The hand gesture places the audience in the position of a subject directly experiencing the situation, making the message feel more personal, while the orange color on the button functions as a marker of urgency as

	well as Bank BNI's institutional visual identity.

Source: Instagram @bni46, 2025.

The first slide builds a message of vigilance through the depiction of a call from an unknown number, becoming the initial stage to introduce the audience to a situation that needs to be scrutinized before accepting or trusting a call.

The Threat of Facial Manipulation (Slide 2)

Table 6. Threat of Manipulation and Face.

Object Of Analysis	Signifier	Signified
	A hooded, faceless figure, a devil emoji, a suspicious emoji, sound wave lines emanating from the figure.	The hooded, faceless figure represents an anonymous and unidentifiable threat. The devil emoji signifies malicious intent behind the action, while the suspicious emoji represents the vigilant reaction that the audience should have. The sound wave lines serve as a marker of the audio manipulation process by deepfake technology that undermines the authenticity of information received by the sense of hearing.

Source: Instagram @bni46, 2025

After the initial depiction of a situation to be wary of, the second slide clarifies the form of the threat through a figure concealing their identity and the presence of voice manipulation.

Identity Disguise to Build Trust (Slide 3)

Table 7. Identity Disguise to Build Trust.

Object Of Analysis	Signifier	Signified
	A plain white mask with no distinguishing features, a gesture of lifting the mask to cover the face, a blue color on the speech bubble.	The plain white mask represents the lack of a fixed identity of a face that can be forged into anyone, affirming that deepfake technology can imitate the face of anyone the victim recognizes and trusts. The gesture of lifting the mask reinforces the impression that a true identity is hidden behind a false one, while the blue color of the speech bubble signifies the calm and rational attitude recommended in carrying out verification.

Source: Instagram @bni46, 2025.

The third slide shows a form of identity disguise through the mask symbol, reinforcing the message that a person's face can be manipulated to resemble someone else.

Verification Steps and Prohibition on Sharing Data (Slide 4)

Table 8. Verification Steps and Prohibition on Sharing Data.

Object Of Analysis	Signifier	Signified
	An arrangement of icons on sequentially ordered capsule cards, with the fifth card highlighted with a full orange background.	The arrangement of icons on the capsule cards functions as a practical and systematic guide for the audience to verify indications of fraud, ranging from vigilance toward sudden gifts to the mismatch between mouth movements and voice. The highlighting of the fifth card through a full orange color, different from the other four cards with a white background, signifies the highest level of urgency related to the prohibition on sharing personal data such as card numbers and ATM PINs.

Source: Instagram @bni46, 2025.

The fourth slide provides information on the steps that can be taken to recognize and avoid AI deepfake-based fraud through a systematic verification guide.

Call for Vigilance (Slide 5)

Table 9. Call for Vigilance.

Object Of Analysis	Signifier	Signified
	A smiling expression, a gesture pointing upward, a speech bubble containing an invitation to comment.	The smiling expression and the upward-pointing gesture give a friendly and reassuring impression, positioning the bank as a trustworthy messenger, different from the threatening impression built in the second slide. The invitation to comment signifies an effort to build the audience's active engagement in the educational process, while also

	expanding the discussion regarding other modes of fraud.

Source: Instagram @bni46, 2025.

As the final part, the fifth slide directs the audience to participate in interacting and sharing information about other modes of fraud, showing that the message conveyed is not only informative but also encourages the audience's active engagement.

Based on the analysis of the five slides, the GEBER PK poster on Bank BNI's Instagram constructs a message about AI deepfake fraud through a series of complementary signs: the message begins with a situation of a call from an unknown number, followed by a depiction of a perpetrator concealing their identity and manipulating their face and voice, then provides verification steps and a prohibition on sharing data, before finally inviting the audience to remain vigilant. In Ferdinand de Saussure's theory, the relationship between the signifier and the signified is seen when the visual form displayed provides a certain meaning, such as "Unknown Number," which indicates the caller's unknown identity, the mask, which indicates the disguise of identity, and the verification card, which indicates the action that needs to be taken to confirm the truth of information. The arrangement of the five slides develops the message from the introduction of the problem toward actions that can be taken, so the poster does not stop at conveying information about the dangers of deepfake, but also provides practical guidance in dealing with suspicious digital communication.

Discussion

Based on the results of the semiotic analysis of both contents, this study found that the GEBER PK Program's public service advertisements, both on Bank Mandiri's TikTok video and Bank BNI's Instagram poster, consistently construct meaning about the importance of digital security literacy in facing the threat of AI deepfake-based fraud. Both contents raise the issue of identity manipulation through this technology, although presented with different media characteristics: Bank Mandiri's video conveys the message through an audiovisual narrative flow that develops from the formation of trust to the need for prevention, while Bank BNI's poster arranges the message directly and gradually through a series of slides, starting from the introduction of the threat to verification steps.

This finding is supported by Ariwibowo et al. (2026), who explain that deepfake technology can produce highly realistic synthetic audiovisual content by replicating a person's face, voice, and expressions in detail. The high level of realism can make manipulated content appear convincing and create difficulties in determining the authenticity of digital information.

This condition is reflected in the GEBER PK content, which emphasizes the importance of recognizing potential manipulation and verifying information before trusting the identity presented in digital communication.

Both contents provide knowledge that helps the public recognize and face the risk of digital fraud. Messages about the characteristics of facial and voice manipulation provide an initial understanding of how the deepfake mode works, while messages about identity verification, vigilance toward information, and personal data protection provide direction on concrete actions that need to be taken. This is in line with the view of Aveny et al. (2023) that digital literacy plays an important role in helping the public understand, filter, and evaluate information received through digital media, so that digital security literacy in both contents is not merely related to technical knowledge, but also to attitudes and concrete actions in maintaining self-security in digital spaces.

This finding is further supported by Pratama et al. (2023), who found that digital literacy is significantly related to an individual's ability to prevent the spread of false information. Individuals with stronger digital literacy tend to be better able to search for information, evaluate content, and verify the truth of information obtained through digital media. This is reflected in the GEBER PK content through messages that encourage users to verify information and evaluate suspicious digital communication before accepting it as true.

This finding is in line with Boediman (2025), who explains that advances in deepfake technology present a distinct challenge in distinguishing genuine information from engineered results, because the technology's ability to manipulate faces and voices makes content appear convincing. This condition is reflected in the GEBER PK content through the depiction of a fake identity and symbols indicating manipulation, so that the public is directed not to make facial and vocal resemblance the sole benchmark for the authenticity of a person's identity. In addition, the finding on the importance of the ability to recognize and assess manipulative content is also in line with Dhahir et al. (2024), who emphasize the urgency of improving the public's ability to identify content resulting from AI engineering.

The findings are also relevant to Nurkholisah et al. (2025), who highlight that the development and misuse of deepfake technology create new challenges in addressing cybercrime and increase digital vulnerability. In the context of the GEBER PK content, this vulnerability is addressed through educational messages that encourage users to verify information, recognize suspicious digital communication, and avoid immediately trusting identities presented through manipulated media. Therefore, the content functions not only as

an explanation of the deepfake threat but also as an educational effort to reduce the potential risks of digital fraud.

4. CONCLUSION

Based on the results of the semiotic analysis of the GEBER PK public service video on Bank Mandiri's TikTok and the poster on Bank BNI's Instagram in 2025, this study concludes that the meaning contained in both contents relates to four main points: the formation of trust through a fake identity, the exploitation of the victim's trust and emotional condition, the impact arising after the fraud occurs, and the importance of vigilance and personal data protection. These four points are reinforced through the message on Bank BNI's poster regarding the introduction of identity manipulation, information verification, and data protection.

Bank Mandiri's video constructs this message through an audiovisual narrative flow based on Roland Barthes' semiotic theory at the levels of denotation, connotation, and myth, while Bank BNI's poster arranges the message gradually through a series of slides based on the signifier-signified relationship in Ferdinand de Saussure's semiotic theory. This difference in presentation characteristics shows that digital security literacy messages can be constructed through various forms of signs, adapted to the characteristics of each social media platform used.

It can thus be concluded that the meaning contained in the GEBER PK public service advertisements on Bank Mandiri's TikTok and Bank BNI's Instagram affirms the importance of digital security literacy as a form of public defense against digital identity and information that has the potential to be manipulated. The public not only needs to recognize the existence of AI deepfake fraud modes, but also needs to carry out verification and maintain the confidentiality of personal data and financial information, in line with the main objective of the GEBER PK Program in improving consumer literacy and protection in digital spaces.

REFERENCES

Ariwibowo, T., Ismaidar, I., Rahman, M. S. A., Nurdana, S. A., & Waruwu, P. R. (2026). Analisis hukum pidana terhadap penyebaran deepfake berbasis artificial intelligence (AI) dalam perspektif pembaruan hukum pidana di Indonesia. *YUSTISI, 13*(2). https://doi.org/10.32832/yustisi.v13i2.23887

Aveny, A. K. M., Trio Mahendra, Y., & Saputra, D. (2023). Literasi digital sebagai upaya menangkal hoax di lingkungan masyarakat Indonesia. *Jurnal Tonggak Pendidikan Dasar: Jurnal Kajian Teori dan Hasil Pendidikan Dasar, 2*(1), 36–48. https://doi.org/10.22437/jtpd.v2i1.22866

Azka, M. D. A., Aulia, N. F., Ananda, F., & Putra, P. (2025). Pengaruh deepfake terhadap kepercayaan publik pada informasi visual di media sosial. *Kajian Administrasi Publik dan Ilmu Komunikasi, 2*(2), 286–301. https://doi.org/10.62383/kajian.v2i2.401

Bank Indonesia. (2024, March 27). *Regulator dan industri kompak gencarkan edukasi pelindungan konsumen* [Press release]. https://www.bi.go.id/id/publikasi/ruang-media/news%20release/Pages/sp_266324.aspx

Boediman, E. P. (2025). Exploring the impact of deepfake technology on public trust and media manipulation: A scoping review. *Jurnal Komunikasi, 19*(2), 313–334. https://doi.org/10.20885/komunikasi.vol19.iss2.art8

Dhahir, D. F., Kenda, N., Dirgahayu, D., Syarifuddin, S., Djaffar, R., Widihastuti, R., Rustam, M., & Pala, R. (2024). The relationship of digital literacy, exposure to AI-generated deepfake videos, and the ability to identify deepfakes in Generation X. *Jurnal Pekommas, 9*(2), 357–368. https://doi.org/10.56873/jpkm.v9i2.5873

Fahrudin, A., & Rahman, A. (2025). Peran literasi media sebagai strategi pencegahan penyebaran disinformasi berbasis deepfake. *JIKA (Jurnal Ilmu Komunikasi Andalan), 8*(2), 121–133. https://doi.org/10.31949/jika.v8i2.15470

Lao, Y., Hirvonen, N., & Larsson, S. (2025). Everyday encounters with deepfakes: Young people's media and information literacy practices with AI-generated media. *Journal of Documentation, 81*(7), 216–235. https://doi.org/10.1108/JD-01-2025-0007

Mutmainnah, A., Suhandi, A. M., & Herlambang, Y. T. (2024). Problematika teknologi deepfake sebagai masa depan hoax yang semakin meningkat: Solusi strategis ditinjau dari literasi digital. *UPGRADE: Jurnal Pendidikan Teknologi Informasi, 1*(2), 67–72. https://doi.org/10.30812/upgrade.v1i2.3702

Nurkholisah, S., Rismana, D., Nugroho, A. E., Munjiyah, A., & Ayunisa, Q. (2025). Deepfake sebagai bentuk kejahatan siber baru: Tantangan kriminalisasi dalam hukum pidana Indonesia. *Jurnal USM Law Review, 8*(3), 2421–2445. https://doi.org/10.26623/julr.v8i3.13060

Pratama, F. R., Komariah, N., & Rodiah, S. (2023). Hubungan antara kemampuan literasi digital dengan pencegahan berita hoaks di kalangan mahasiswa. *Informatio: Journal of Library and Information Science, 2*(3), 165–184. https://doi.org/10.24198/inf.v2i3.43792

Ratri, S. Y., & Aviyanti, L. (2025). Unlocking digital literacy in Indonesia: Insights from the use of social media platforms. *Jurnal Prima Edukasia, 13*(1), 191–200. https://doi.org/10.21831/jpe.v13i1.83433

Razak, A., & Sumanti, S. T. (2023). Penggunaan media sosial sebagai media komunikasi dalam penyebaran informasi pada Dinas Kominfo Kota Medan. *Communication & Social Media, 3*(1), 1–6. https://doi.org/10.57251/csm.v3i1.939

Zinaida, R. S., & Anggraini, R. (2022). Strategi advertising dan sales promotion Yhoophii Shop Palembang di Instagram. *Jurnal Audiens, 3*(3), 149–158. https://doi.org/10.18196/jas.v3i3.14197