Indonesian Journal of Advanced Research (IJAR)
Vol. 4, No. 8, 2025: 1815-1828

Artificial Intelligence Deepfake Against Cybercrime Threats

Faqih Azhar[1*], Sulaimah[2], Khaerudin Imawan[3], Abdul Jalil Hermawan[4]
Faculty of Social and Political Sciences, University of Swadaya Gunung Jati
Corresponding Author: Faqih Azhar, faqih.azhar41@gmail.com

A R T I C L E I N F O

Keywords: Artificial Intelligence, Deepfake, Cybercrime.

Received: 5, July
Revised: 19, July
Accepted: 20, August

A B S T R A C T

This research aims to determine the practice of artificial intelligence in deepfake applications against cybercrime threats. Current technological developments have given rise to communication media using artificial intelligence technology in deepfake applications. The deepfake application can change a person's visual and audio using a deep learning system and is widely used by the public and business actors. However, this technology often leads to cybercrime such as fraud and identity theft. This study uses a descriptive qualitative method with data collection through literature review and analysis descriptively. The findings answer problems related to fraud and identity theft, focusing on the East Java Governor case, and emphasize the need for preventive measures by the public and government to avoid misuse of deepfake applications.

DOI prefix: https://doi.org/10.55927/ijar.v4i8.15119
ISSN-E: 2986-0768
https://journal.formosapublisher.org/index.php/ijar

INTRODUCTION

Today's technological developments create benefits for users, especially for the community. Technology is usually used to interact or communicate with people, as well as for business transactions that require the help of technology.(Yoga, 2019) The emergence of technology makes it easier for people to live their daily lives. However, this convenience brings serious problems to society because technology is misused with the aim of harming others, one of which is the threat of fraud and identity theft. (Zamroni, 2017)

The misuse of technology has a negative impact on society, where the crime is through a network or computer system called cybercrime. This crime has characteristics that are different from other crimes in terms of victims, perpetrators, crime scenes and causes of the case, so it requires regulation and handling outside of applicable regulations. Factors that cause cybercrime include negligence in the use of computers, security that is not properly maintained and the ease of unlimited internet access. (Lazarus et al., 2022)

Cybercrime is related to the threat of fraud over the internet and the theft of identity or personal data. In addition to using the help of computer systems and internet networks, these crimes can also use new technology that is currently being developed, namely Artificial Intelligence technology (hereinafter referred to as AI). This technology is considered an artificial intelligence that was created to help make people's lives easier in various fields.(Ubaidillah et al., 2022) However, today, AI technology is misused by individuals who harm the public and are irresponsible by creating fake videos using deepfake applications.

A deepfake application is an application that is used using artificial intelligence from deep learning and AI technology. This application originated from a combination of the word deep learning with the word fake which is interpreted as a technology to create fake multimedia content. Deepfake applications were created from 2017, where the application became the center of attention all over the world.(Walczyna & Piotrowski, 2023) Initially, deepfake applications were used to replace the faces of actors in movies and were considered temporary entertainment. However, as the times develop, deepfake applications are considered a serious threat to state security and become detrimental to society. (Muqsith & Pratomo, 2021)

The technology of deepfake applications is used to spoof images, conversational sounds and videos with very real results. An example of a deepfake application that is usually used is Animate Anyone from Alibaba Group. The app can make the images in the photo into a moving video or turn them into an animation. In addition, animate anyone can also change someone's face, manipulate sounds, and can take someone's face and paste it onto someone else's face. The use of deepfake applications is a place to establish communication in a virtual community which is a form of cyber culture. In this virtual community, a person will be free to express themselves to others in daily life. However, the sophistication resulting from this application can be a time bomb for society, where deepfake applications can be misused to spread false information to others and can steal the identity of others.(Kasita, 2022)

This will raise a question about the use of AI technology in deepfake applications against fraud and identity theft in Indonesia. Based on this description, the researcher is interested in dismantling the practice of using artificial intelligence technology, especially deepfakes against the threat of cybercrime, especially in the case of the Fraud of the Governor of East Java, Khofifah. This paper aims to analyze and find out the correct use of AI technology to avoid cybercrime in the abuse of deepfakes. This writing is also expected to not only provide benefits for the author, but also to make a real contribution to the government and society, especially in dealing with cybercrime threats, as well as providing education and insight for readers about AI technology in deepfake applications to cybercrime threats.

LITERATURE REVIEW

Research materials related to artificial intelligence: deepfakes against cybercrime threats that will be a reference and comparison with this research are:

a. Research by Itsna Hidayatul Khuna on "Deepfake, a new challenge for netizens" from Promedia Journal: Public Relations and Communication Media Volume 5, Number 2 of 2019. The method used in the research is qualitative descriptive using literature sources from article writing. This study explains that deepfake applications are a challenge, which can cause widespread hatred, become a political and propaganda tool so that netizens are required to have good emotional intelligence when using the internet. (Hidayatul Khusna Sri Pangestuti, 2019)
b. Research from Intan Leliana, et. al regarding "Ethics in the Deepfake Era: How to Maintain Communication Integrity" from the BSI Repository Journal Volume 1, Number 1 of 2024. The method used in the study is qualitative descriptive using literature methods from journals and books. This study explains that the use of artificial intelligence technology in deepfake applications if associated with cyber culture will affect integrity in communication ethics. The use of deepfake applications is very influential in a person's communication so that in its use, caution must be exercised so that there is no misuse of other people's faces or voices. (Leliana et al., 2024)
c. Research from Najwa Ramadhina, et.al on "Dynamics of Change in Human Communication in the Era of Artificial Intelligence Technology" from the Journal of Communicator Sphere, Volume 3, Number 2 of 2023. The methods used in the study are literature review with the internet and document based research which is a reference for data. This research discusses the development of artificial intelligence technology that has a significant effect on human communication, where humans are faced with new challenges with the role of artificial intelligence technology as a link, so that in this case it requires effective collaboration between artificial intelligence and humans.(Ramadhina et al., 2023)
d. Research from Pramana, et.al on "Adapting to Technological Changes: Artificial Intelligence and the Evolution of Interpersonal Communication" from the Scientific Journal of Social Dynamics Volume

7, Number 2, Year 2023. The method used in this study is qualitative descriptive by reviewing the literature with Elsevier and Google Scholar databases, printed books and other sources. This study discusses the evolution of interpersonal communication as part of adaptation to changes in communication technology using artificial intelligence or artificial intelligence. Unlike previous technology that has a role as a communication channel, this artificial intelligence can shift the role of communicators in human interpersonal communication. (Pramana et al., 2023)

e. Research from Moh. Rusnoto Susanto on "Cybercultures and Social Change: A Pragmatic Review of the Phenomenon of Cybercultures" from the Journal of Deconstruction Volume 9, Number 1 of 2023. The method used in the study is a phenomenological approach method that becomes a pragmatic study analysis knife to unravel the results of reflection on social changes that are critically reviewed on the phenomenon of cybercultures. This research produces a pragmatic study through contextual reflection through postcolonial studies and social change, as well as the relationship of social change through studies in the form of paradigmatic reflection of Baudrillard's simulacra theory and Gadamer's hermeneutic view of social change triggered by the phenomenon of cybercutres. (Moh. Rusnoto Susanto, 2022)

The majority of earlier research on deepfake technology and cybercrime has focused on ethical issues, detection methods, or the political ramifications on a worldwide scale. However, there is still a dearth of study specifically addressing the misuse of deepfakes in Indonesia, especially when it comes to public authorities, and is examined utilising simulacra theory and cyber culture. By examining the Khofifah Indar Parawansa fraud case, this study fills the knowledge vacuum by offering a contextual understanding of how deepfake-driven hyperreality affects local communities' fraud, identity theft, and public trust.

METHODOLOGY

The research method used in this study is qualitative descriptive which is a method of depicting social problems that are happening in society, one of which is the use of AI technology in deepfake applications that are misused so that cybercrime threats occur, such as cases of fraud and identity theft in the community in Indonesia. This study tries to explain existing data and sources regarding the conditions and situations for the use of artificial intelligence technology in deepfake applications that create cases of fraud and identity theft in the people in Indonesia. Data collection in research uses literature studies which is a collection technique that uses tracing on the data and sources to be researched.(Sugiyono, 2019) This will produce data sources in the form of books, journals, articles, news and several other scientific research. After all the data has been collected, the researcher analyzes using a descriptive method by describing the facts that have been obtained from the data and sources to be further analyzed so as to produce a discussion formulation in the research. (Fadli, 2021) The

analytical knife used in this study, namely the Simulacra theory (simulacrum) explained by Jean Baudrillard, states that where reality exists is pseudo-reality and artificial reality (hyper-reality). This theory explains that engineering in the media of technology creates a single condition, where everything is considered more real than reality. Humans cannot distinguish between falsehood and truth, which is how AI technology works in creating artificial media that cannot distinguish truth and falsehood. The AI technology applied in deepfake applications has benefits for commercial and other interests, but it also poses a serious threat to the personal data of the people who are being misused.

RESEARCH RESULTS AND DISCUSSION

Working Process of Artificial Intelligence Technology

AI technology that continues to develop has a significant impact on information exchange and communication methods that have created a new trend in obtaining more efficient and effective information. Gunkel said that AI technology in the field of communication was created as a way for humans to exchange information.(Nurkholis & Ikasari, 2023) The function of AI technology as a communicator between interlocutors through robot technology is created to communicate verbally and non-verbally with ordinary humans. In addition to facilitating communication, AI technology also automates and optimizes communication through audio visuals that can change according to the voice that is communicating. (Malatji & Tolah, 2024)

Perkembangan teknologi secara cepat di berbagai macam bidang ilmu dapat memudahkan masyarakat berkomunikasi, dimana hal tersebut didukung dengan kelahiran teknologi baru, yaitu Artificial Intelligence (AI). Teknologi ini diciptakan oleh Alan Turing yang merupakan ilmuwan asal Inggris yang membuat tes gagasan dalam memastikan kecerdasan alat tersebut sehingga hasil penelitiannya dinamakan Turing test. Selanjutnya teknologi AI ditunjukan pada acara Dartmouth Conference tahun 1956 kepada Professor John McCarthy yang berasal dari Massachusetts Institute of Technology (Mobarakeh, 2023). The designation is intended so that artificial intelligence can resemble and identify the thinking of normal humans so that machines can be created that can imitate real humans.

AI technology that continues to develop has a significant impact on information exchange and communication methods that have created a new trend in obtaining more efficient and effective information. Gunkel said that AI technology in the field of communication was created as a way for humans to exchange information.(Nurkholis & Ikasari, 2023) The function of AI technology as a communicator between interlocutors through robot technology is created to communicate verbally and non-verbally with ordinary humans. In addition to facilitating communication, AI technology also automates and optimizes communication through audio visuals that can change according to the voice that is communicating. (Malatji & Tolah, 2024)

AI technology has penetrated into several applications used by humans every day, including:

a. Social media that uses the help of AI technology, such as Facebook, Instagram and X (Twitter). The help of AI technology can help humans to find the content or information needed through words or images searched on social media.
b. Google's search engine features have used the help of AI technology to get the most appropriate and relevant search results to the information needed.
c. The ChatGPT application, which appeared at the end of 2022, has helped humans to search for useful references and information.
d. Deepfake applications that can turn a person's visuals and audio into someone else in the form of photos and videos. This application has many mock applications that are used for free, such as deepswap, basedlabs, Vidnoz, Pixble, swapface and other applications.

Changes Before and After Using Artificial Intelligence (AI) Technology

Before using AI technology, people communicated by phone without looking at the visual form and images, and when searching for information, there were limitations that could only be found in physical or printed sources. Unlike after using AI technology, people can find out the audio and visuals of their interlocutors when communicating online through streams, video calls and online meetings, and can search for various kinds of information with search engine features.

The use of AI technology as a communication tool is currently widely used in global marketing strategies in a country, one of which is in the field of Korean Pop (Kpop) music. The emergence of AI technology is motivated by public interest in Kpop music and supported by the excellence of human resources in creating AI technology innovations for the music industry. One example of the use of AI technology in the Kpop music industry is online concerts, streaming and fansigning, through video calls between artists and their fans. This is done by SM Entertainment, which is the largest Kpop agency in South Korea that already uses the concept of AI technology in the marketing of its artists' music. In addition to being used for marketing Kpop artists, an information and technology company in South Korea, Pulse9 Entertainment, has created the development of AI technology that created a virtual girl group called Eternity. (Fadilla et al., 2023)

AI technology is also useful for helping humans in various other fields besides communication, where there are changes before and after using AI technology, including:

a. Health

Before the advent of AI technology, treatment and diagnosis were carried out on the basis of doctors' medical experience and knowledge. Unlike after the advent of AI technology, diagnoses can be strengthened by the analysis of big data from various sources.

a. Education

Before the advent of AI technology, teaching methods used traditional approaches, where teachers provided subject matter and students learned by

listening to or reading textbooks. Unlike AI technology, teaching methods use online platforms, and other digital resources.

b. Scientific Research Fields

Before the advent of AI technology, data analysis was often done manually by researchers, so it often required a lot of time and effort. It is different after the existence of AI technology, where research becomes more efficient supported by research models, such as machine learning and deep learning.

c. Transportation Field

Before AI technology, vehicles did not have a navigation system to find the right route and did not have the ability to communicate with each other. Unlike after the existence of AI technology, vehicles already have a connected GPS system to allow for more efficient route planning, and have a connected system that can communicate with each other so that it adapts to the surrounding infrastructure and as a prevention of collisions.

Potential for Deepfake Applications for Cyber Crime in the East Java Governor Fraud Case

Deepfakes are a type of artificial intelligence that uses a deep learning method with the Generative Adversarial Network (GAN) algorithm. This technology is used to create photos, videos, and audio that are similar to reality. Deepfake technology has a mechanism by collecting data that is spread across the internet. The data is then generated by adjusting the conditions requested by the user, whether it is adjusting facial expressions, voice intonation, or facial expressions. (Jufri & Putra, 2021)

Technological advances in the current era of modernization and globalization require people to continue to adapt to the use of technology that makes it easier for people to communicate and access any information. The development of technology brings social changes to society, where technology creates innovative and logical advances for humans that make people's behavior more instant with all the convenience provided by technology. This technological advancement does not rule out the potential for cases of fraud and theft of people's personal data.(Yusuf & Ar Rosyid, 2023) Over time, the number of technology users is increasing, so it requires protection of people's personal data. In such cases, legal regulations are needed that can protect people's personal data, especially in cases of fraud and identity theft in Indonesia. This aims to protect the privacy of the community and not interfere with people's private lives. (Anggen Suari & Sarjana, 2023)

Deepfake applications are a combination of AI technology products with deep learning technology products which are techniques for detecting and recognizing human faces through images and audio visuals. In addition, the capabilities of deepfake applications are also applied in the creation of video and audio visuals that are made to look real even though the original shape of their faces and voices is fake.

The use of deepfake applications is not only used in the music industry, but can be used as a means of communication and business transactions.(Haeruddin et al., 2023) But over time, the use of deepfake

applications can also be abused by a person. Based on the view of cyber culture regarding the use of artificial intelligence technology in deepfake applications, it is a very worrying problem of cyberspace in the current era of technological development because the results of deepfake applications are similar to the real ones and cannot distinguish between what is real and which is the result of deepfake applications.(Uchendu et al., 2021)

The exploitation of the abuse of deepfake applications in AI practice was experienced by one of the officials in Indonesia. With the development of Artificial Intelligence, especially deepfakes that are increasingly rapid in society, of course, not a few cybercrime individuals have emerged. One of them is the deepfake fraud case of the Governor of East Java, Khofifah Indar Parawansa.

Figure 1. Source: kominfo.jatimprov.go.id/berita.

According to a KOMINFO report, these fraudsters manipulated using Artificial Intelligence deepfake technology to imitate Governor Khofifah's face. East Java Police Chief, Inspector General of Police Nanang Avianto, said that the three perpetrators were arrested when they received a report of fraud using a video of East Java Governor Khofifah Indar Parawansa using Artificial Intelligence technology selling cheap motorcycles to the public on social media. The video contains a face and voice that is very similar to Governor Khofifah, selling cheap motorbikes for 500 thousand rupiah to the public. As if it is a special subsidy program from the Governor of East Java for East Java residents, without an on-site payment process (COD) and complete official documents.

The video of the Khofifah deepfake manipulation fraud was uploaded by the perpetrators to a number of TikTok social media @khofiggh759, @khofiljatim, @khofiaamlxh, and several other accounts. As long as the perpetrators carry out the action, they all have different roles. One perpetrator made a video using deepfake AI technology and also created a bank account, another perpetrator uploaded a video on social media, and the last perpetrator became the admin of the Whatsapp application. When the victims of the deepfake video are tempted by the offer of cheap motorcycles, they will contact the Whatsapp number listed by the perpetrators on TikTok accounts claiming to be Governor Khofifah.

Figure 2. Source: kominfo.jatimprov.go.id/berita.

This deepfake scam lasted for three months. The perpetrators received profits of 86 million rupiah from the victims who came from four different provinces. Starting from East Java Province, West Java, Central Java, to North Maluku Province. The fraud case adds to the public's concern about the improper use of technology. (Mustofa et al., 2023)

Cases of fraud and identity theft cause a lot of losses to society, so it is necessary to analyze from the perspective of cyber culture regarding AI technology in Deepfake Applications against the threat of fraud and identity theft. (Mustofa et al., 2023)

Current technological developments have given rise to technology in the form of artificial intelligence applied by deepfake applications used as a medium of communication between parties in various countries by changing a person's visuals, audio, and video. The use of deepfake applications has also been applied in filters on social media applications, such as Instagram, Snapchat and Tiktok. (’Uyun & Hakim, 2020) In its current use, it is entertaining and positive for everyone, but in the long term it will cause abuse in the use of artificial intelligence technology in the deepfake application which has the potential to harm individuals or groups of people.

The threat of cybercrime in the form of fraud and identity theft using artificial intelligence technology in deepfake applications is an illustration of the hyperreality stated by Jean Baudrilard in the Simulacra Theory. The Simulacra theory explains that engineering in the medium of technology will create a single condition, where everything is considered more real than reality. The results of artificial intelligence technology in deepfake applications create falsehoods that are considered more true than the truth so that humans cannot distinguish between real and fake. In the case of East Java Governor Khofifah's deepfake, the fraud victims believed the AI-generated video with a face and voice that was very similar to Khofifah's. Then without cross-checking further information, they followed the instructions of the scammers to transfer some money because the pseudo-reality video was difficult to distinguish from the real reality.

The use of artificial intelligence technology in deepfake applications is worth watching out for because the application is widely accessible to the public

so that ordinary users can use it by collecting photos that will be used as objects and one video to attach the face object. The use of this technology can cause problems and losses for some parties. (Malik et al., 2022) If a deepfake application is used in the political field as in the case of Governor Khofifah's deepfake which was discussed earlier, this will be something dangerous because it will be easier to lead the opinion of political figures by adjusting the voice, face and lips of the figure without the permission of the figure concerned. Apart from politics, the use of deepfake applications using photos or videos of other objects without permission will cause other problems so that deepfake applications must be considered by everyone. Artificial intelligence technology in deepfake applications will give rise to other criminal acts, one of which is fraud and identity theft. (Rana et al., 2022)

The act of fraud and identity theft using artificial intelligence technology in deepfake applications affects the security of cyber space in the community, where people feel unsafe in communicating or conveying information through social media applications that have deepfake applications.(Seow et al., 2022) The impact of these actions causes the cyber culture that develops in society to create a sense of worry and fear for the public, if information belonging to the public is misused by irresponsible deepfake application users and individuals who will launch fraudulent crimes using information data belonging to the public. (Patel et al., 2023)

The Correct Use of AI Technology to Avoid Cybercrime in Deepfake Abuse

Media and cyberspace have led to the growth of cultural renewal that gives rise to cyber culture . Cyber culture is considered a value that originates from interaction between parties which in its application is related to the media. This value will be recognized directly and indirectly which will then be implemented in the interaction between the parties. The characteristics of cyber culture will have an effect on life related to cyber space or called cyberspace in the community environment.(Prasad Adhikary, 2020) In the study of cyber culture, the internet is a simple communication medium when compared to direct face-to-face communication media. This is due to the development of the generation that has used applications to convey messages in the form of emoticons or writings so that it is useful to convey understanding or information between the two parties. (Purwanto & Nuha, 2020)

The presence of deepfake applications requires a holistic approach to the use of artificial intelligence technology, where the approach is in the form of providing overall support, both in mental, physical, social, spiritual and emotional well-being. This aims to enable the public to recognize, overcome and understand problems that arise through deepfake applications, as well as maintain the integrity of communication to avoid manipulative and incorrect information (Leliana et al., 2024). In maintaining integrity in communication ethics, the government, the community and institutions must work together to improve communication standards, especially in the use of social media.

Cases of fraud and theft of personal data due to the use of deepfake applications require improvements in the form of actions to improve the cyber culture of the community towards the correct use of artificial intelligence

technology . These actions can be in the form of notifications about false information and checking reliable sources so that the results of communication through deepfake applications can be known for the truth and specific explanations. In addition, technology-related institutions and the government are obliged to adopt provisions that can limit the use of deepfake applications incorrectly, where these provisions are in accordance with public freedom of speech and the protection of people's personal data.

The application of artificial intelligence (AI) technology according to simulacra theory is a representation of natural relationships in various elements of human life and is also the beginning of the era of the industrial revolution. Simulacra theory is a theory of space where the mechanism of simulating human life takes place. If the use of AI technology has a negative impact on human life, then there has been a shift in the mechanism of representation of simulacra theory that was born as a consequence of the development of information technology science. Since the existence of AI technology, human life has changed where it has become easier for humans to find information, communicate with others, find new insights and lifestyles. This creates a habit in human life every day. In this condition, humans have been trapped and trapped in a new reality space that is considered real, when in fact it is included in a pseudo-reality, all fake and full of engineering. The pseudo-reality in question is the antithesis space of a kind of deconstruction. (Moh. Rusnoto Susanto, 2022)

The entire reality of human life in various fields has in fact been constructed through some pre-made models. The development of AI technology not only extends the human body or life system, but can reproduce nostalgia, reality and the human past. The reality created by AI technology has taken over the real reality and has become a new reference model for the community. These symptoms will be directly proportional to technological developments and the entry of the latest era of life of the world's people in the flow of cybercultures.

CONCLUSIONS AND RECOMMENDATIONS

There are various restrictions on this study. First of all, it only uses secondary data and literature reviews, which could not be up to date with the latest advancements in deepfake technology or law enforcement procedures. Second, because the study only looks at one instance, its conclusions might not apply to all cybercrime cases in Indonesia that involve deepfakes. Third, the analysis focusses on simulacra theory and cyber culture rather than technological detection techniques or comprehensive legal frameworks, which can be studied in more detail in further research.

Conclusions related to artificial intelligence deepfakes against the threat of cybercrime, as follows:

1. AI technology that continues to develop has a significant impact on information exchange and communication methods that have created a new trend in obtaining more efficient and effective information.
2. Before using AI technology, people communicated by phone without looking at the visual form and images, and when searching for information, there were limitations that could only be found in physical or

printed sources. Unlike after using AI technology, people can know the audio and visuals of their interlocutors when communicating online through streams, video calls and online meetings, and can search for various kinds of information with search engine features.

3. Deepfake applications are a combination of AI technology products with deep learning technology products which are techniques for detecting and recognizing human faces through images and audio visuals. The use of deepfake applications is abused both in the music industry, politics and other fields, where the abuse is indicated by acts of fraud and identity theft of a person's personal data.
4. If the use of AI technology has a negative impact on human life, then there has been a shift in the mechanism of representation of simulacra theory that was born as a consequence of the development of information technology science. Since the existence of AI technology, human life has changed where it has become easier for humans to find information, communicate with others, find new insights and lifestyles. This creates a habit in human life every day.

The presence of deepfake applications requires a holistic approach to the use of artificial intelligence technology, where the approach is in the form of providing overall support, both in mental, physical, social, spiritual and emotional well-being. This aims to enable the public to recognize, overcome and understand problems that arise through deepfake applications, as well as maintain the integrity of communication to avoid manipulative and incorrect information.

ADVANCED RESEARCH

Based on the above conclusions, further study is needed to explore comprehensive strategies for mitigating the negative impacts of deepfake technology within the broader scope of cybercrime. Future research could examine the development of advanced detection systems, legal and ethical frameworks, and public awareness initiatives that emphasize digital literacy. In particular, studies should focus on how deepfake misuse affects individual privacy, trust in digital communication, and societal security, while also exploring multidisciplinary approaches combining technological, psychological, and legal perspectives to foster resilience against AI driven manipulation.

REFERENCES

'Uyun, Z. Q., & Hakim, L. (2020). CYBER CULTURE OF SOCIAL MEDIA: IDENTITY AS TRASH OF INFORMATION. *ORASI: Jurnal Dakwah Dan Komunikasi*, *11*(1). https://doi.org/10.24235/orasi.v11i1.6264

Anggen Suari, K. R., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *6*(1). https://doi.org/10.38043/jah.v6i1.4484

Dinas Komunikasi dan Informatika Provinsi Jawa Timur. (2025, April 28). Polda Jatim ungkap kasus penipuan deepfake AI kepala daerah, pelaku kantongi keuntungan hingga Rp87 juta. *Kominfo Jatim*.

https://kominfo.jatimprov.go.id/berita/polda-jatim-ungkap-kasus-penipuan-deepfake-ai-kepala-daerah-pelaku-kantongi-keuntungan-hingga-rp87-juta

Fadilla, A. N., Ramadhani, P. M., & Handriyotopo, H. (2023). Problematika Penggunaan AI (Artificial Intellegence) di Bidang Ilustrasi : AI VS Artist. *CITRAWIRA : Journal of Advertising and Visual Communication*, *4*. https://doi.org/10.33153/citrawira.v4i1.4741

Fadli, M. R. (2021). Memahami desain metode penelitian kualitatif. *HUMANIKA*, *21*(1). https://doi.org/10.21831/hum.v21i1.38075

Haeruddin, H., Herman, H., & Hendri, P. P. (2023). Pengembangan Aplikasi Emoticon Recognition dan Facial Recognition menggunakan Algoritma Local Binary Pattern Histogram (LBPH) dan Convolutional Neural Network (CNN). *Jurnal Teknologi Terpadu*, *9*(1). https://doi.org/10.54914/jtt.v9i1.613

Hidayatul Khusna Sri Pangestuti, I. (2019). Deepfake, Tantangan Baru Untuk Netizen Deepfake, a New Challenge for Netizen. *AGUSTUS 1945 JAKARTA 1 PROMEDIA*, *2*.

Jufri, M. A. A., & Putra, A. K. (2021). Aspek Hukum Internasional Dalam Pemanfaatan Deepfake Technology Terhadap Perlindungan Data Pribadi. *Uti Possidetis: Journal of International Law*, *2*(1). https://doi.org/10.22437/up.v2i1.11093

Kasita, I. D. (2022). Deepfake Pornografi: Tren Kekerasan Gender Berbasis Online (KGBO) Di Era Pandemi Covid-19. *Jurnal Wanita Dan Keluarga*, *3*(1). https://doi.org/10.22146/jwk.5202

Lazarus, S., Button, M., & Kapend, R. (2022). Exploring the value of feminist theory in understanding digital crimes: Gender and cybercrime types. *Howard Journal of Crime and Justice*, *61*(3). https://doi.org/10.1111/hojo.12485

Leliana, I., Irhamdhika, G., Haikal, A., Septian, R., & Kusnadi, E. (2024). ETIKA DALAM ERA DEEPFAKE: BAGAIMANA MENJAGA INTEGRITAS KOMUNIKASI. *Jurnal Visi Komunikasi*, *22*(02). https://doi.org/10.22441/visikom.v22i02.24229

Malatji, M., & Tolah, A. (2024). Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI. *AI and Ethics*. https://doi.org/10.1007/s43681-024-00427-4

Malik, A., Kuribayashi, M., Abdullahi, S. M., & Khan, A. N. (2022). DeepFake Detection for Human Face Images and Videos: A Survey. In *IEEE Access* (Vol. 10). https://doi.org/10.1109/ACCESS.2022.3151186

Mobarakeh, B. I. (2023). Systems and method for medical platform employing artificial intellegence and wearable devices. *US Patent App. 17/821,101*.

Moh. Rusnoto Susanto. (2022). Cybercultures dan Perubahan Sosial: Sebuah Tinjauan Pragmatis Terhadap Fenomena Cybercultures. *Dekonstruksi*, *9*(01). https://doi.org/10.54154/dekonstruksi.v9i01.126

Muqsith, M. A., & Pratomo, R. R. (2021). The Development of Fake News in the Post-Truth Age. *SALAM: Jurnal Sosial Dan Budaya Syar-I*, *8*(5).

https://doi.org/10.15408/sjsbs.v8i5.22395
Mustofa, Z., Arifatuzzahro, A., Nazira, A., Wahyuni, R. D., & Mukminin, A. (2023). PENGARUH PENERAPAN ARTIFICIAL INTELLEGENCE PADA KEHIDUPAN MASYARAKAT DI INDONESIA. *Lisyabab : Jurnal Studi Islam Dan Sosial*, *4*(1). https://doi.org/10.58326/jurnallisyabab.v4i1.184
Nurkholis, A., & Ikasari, I. H. (2023). Peran Artificial Intellegence dalam Sistem Informasi Manajemen. *Jurnal Artificial Inteligent Dan Sistem Penunjang Keputusan*, *01*(01).
Patel, Y., Tanwar, S., Gupta, R., Bhattacharya, P., Davidson, I. E., Nyameko, R., Aluvala, S., & Vimal, V. (2023). Deepfake Generation and Detection: Case Study and Challenges. *IEEE Access*, *11*. https://doi.org/10.1109/ACCESS.2023.3342107
Prasad Adhikary, D. R. (2020). DeLillos White Noise Postmodern Effects of Cyber Culture on Youths. *The International Journal of Social Sciences and Humanities Invention*, *7*(07). https://doi.org/10.18535/ijsshi/v7i07.02
Purwanto, H., & Nuha, A. A. (2020). Post Dakwah di Era Cyber Culture. *DAKWATUNA: Jurnal Dakwah Dan Komunikasi Islam*, *6*(2).
Ramadhina, N., Jason, F., Pratama, M. F., Raihan, L. A., Al Mufti, S., & Meranti, M. (2023). Dinamika Perubahan dalam Komunikasi Manusia di Era Teknologi Artificial Intelligence. *Communicator Sphere*, *3*(2). https://doi.org/10.55397/cps.v3i2.57
Rana, M. S., Nobi, M. N., Murali, B., & Sung, A. H. (2022). Deepfake Detection: A Systematic Literature Review. In *IEEE Access* (Vol. 10). https://doi.org/10.1109/ACCESS.2022.3154404
Seow, J. W., Lim, M. K., Phan, R. C. W., & Liu, J. K. (2022). A comprehensive overview of Deepfake: Generation, detection, datasets, and opportunities. *Neurocomputing*, *513*. https://doi.org/10.1016/j.neucom.2022.09.135
Sugiyono. (2019). *Metode Penelitian Kuantitatif* (Setiyawami (ed.); Edisi Ke 2). Alfabeta, cv.
Ubaidillah, Kurnia, A. D. N., & Octaviany, R. V. (2022). Kejahatan Cybercrime di Era 4.0. *Prosiding Seminar Nasional Ilmu Ilmu Sosial (SNIIS)*, *1*.
Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers and Security*, *109*. https://doi.org/10.1016/j.cose.2021.102387
Walczyna, T., & Piotrowski, Z. (2023). Quick Overview of Face Swap Deep Fakes. In *Applied Sciences (Switzerland)* (Vol. 13, Issue 11). https://doi.org/10.3390/app13116711
Yoga, S. (2019). Perubahan Sosial Budaya Masyarakat Indonesia Dan Perkembangan Teknologi Komunikasi. *Jurnal Al-Bayan*, *24*(1). https://doi.org/10.22373/albayan.v24i1.3175
Yusuf, M. B., & Ar Rosyid, H. (2023). Pengaruh Society 5.0 dalam Kehidupan Masyarakat. *Jurnal Inovasi Teknologi Dan Edukasi Teknik*, *3*(2). https://doi.org/10.17977/um068v3i22023p116-121
Zamroni, M. (2017). Perkembangan Teknologi Komunikasi Dan Dampaknya Terhadap Kehidupan. *Jurnal Pendidikan*, *X*(2).