




DOI: 10.22363/2312-9220-2023-28-4-741-748
EDN: KOLCJF
UDC 070:004.738.5

Research article / Научная статья

Biometrics in online media: an anti-crisis paradigm shift

Sasha Shilina 

Paradigm Research, 86 Gorgasali St, Batumi, 6000, Georgia

 sasha@paradigmfund.io

Abstract. Online media is currently grappling with a crisis characterized by diminishing trust, the widespread dissemination of misinformation, and the alarming proliferation of fake news and experiences. The aim of the study – to delve into the challenges plaguing the digital media landscape and to propose the adoption of biometric technology as a potential solution. Biometrics, as a cutting-edge technology, encompasses the intricate process of quantifying and statistically assessing the unique physical and behavioral characteristics that distinguish individuals from one another. Its multifaceted potential extends far beyond mere identification. It is established that biometrics excels in the vital realms of identity verification, content authentication, and countering malicious activities like bots and Sybil attacks. Furthermore, it is applicable for tailoring personalized user experiences, thus offering a comprehensive solution to address the pressing challenges faced by online media today. The usage of these capabilities, makes biometrics a distinctive and promising avenue to not only restore trust but also combat the pervasive issue of misinformation, ultimately fostering a secure and resilient online media ecosystem.

Keywords: digital media crisis, social media, Sybil attack, fake news, artificial intelligence, online media ecosystem

Conflicts of interest. The author declares that there is no conflict of interest.

Article history: submitted June 14, 2023; revised July 20, 2023; accepted August 24, 2023.

For citation: Shilina, S. (2023). Biometrics in online media: An anti-crisis paradigm shift. *RUDN Journal of Studies in Literature and Journalism*, 28(4), 741–748. <http://doi.org/10.22363/2312-9220-2023-28-4-741-748>

Биометрия в онлайн-СМИ: антикризисная смена парадигмы

А.Г. Шилина 

Парадайм Ресерч, Грузия, 6000, Батуми, Горгасали, д. 86

 sasha@paradigmfund.io

Аннотация. Интернет-СМИ в настоящее время борются с кризисом, обусловленным распространением дезинформации и снижением доверия к медиа. Цель исследования – рассмотреть проблемы, с которыми сталкиваются цифровые медиа, и предложить при-

© Shilina S., 2023



This work is licensed under a Creative Commons Attribution 4.0 International License
<https://creativecommons.org/licenses/by-nc/4.0/legalcode>

менение биометрических технологий в качестве потенциального решения. Биометрия как передовая технология – это сложный процесс количественной и статистической оценки уникальных физических и поведенческих характеристик, отличающих людей друг от друга. Ее многогранный потенциал простирается далеко за пределы идентификации. Установлено, что биометрия легко справляется с задачами проверки личности, аутентификации контента и борьбы с вредоносными действиями, такими как боты и атаки Сивиллы. Кроме того, с ее помощью можно персонализировать пользовательский опыт, предоставляя уникальные преимущества для решения насущных проблем, стоящих перед онлайн-медиа сегодня. Использование этих возможностей делает биометрию уникальным и многообещающим средством не только для восстановления доверия, но и для борьбы с проблемой дезинформации, в конечном итоге способствуя созданию безопасной и устойчивой экосистемы онлайн-медиа.

Ключевые слова: кризис цифровых медиа, социальные сети, атака Сивиллы, фейк ньюс, искусственный интеллект, экосистема онлайн-медиа

Заявление о конфликте интересов. Автор заявляет об отсутствии конфликта интересов.

История статьи: поступила в редакцию 14 июня 2023 г.; отрецензирована 20 июля 2023 г.; принята к публикации 24 августа 2023 г.

Для цитирования: *Shilina S.* Biometrics in online media: an anti-crisis paradigm shift // Вестник Российского университета дружбы народов. Серия: Литературоведение. Журналистика. 2023. Т. 28. № 4. С. 741–748. <http://doi.org/10.22363/2312-9220-2023-28-4-741-748>

Introduction

The contemporary media landscape is characterized by hybridization, porosity, and technological saturation. It is grappling with a severe crisis characterized by the proliferation of misinformation, a decline in public trust, and the rampant spread of fake news, largely fueled by social media platforms. The accessibility and rapid sharing of information have compromised the integrity and reliability of media content, posing significant challenges to society. This crisis undermines the public's ability to make informed decisions, erodes democratic processes, and fosters division among individuals and communities.

The issue of trust in media has generated a substantial body of research that has investigated the causes and effects of trust in media (Engelke et al., 2019; Prochazka et al., 2019) measured and understood trust dynamics (Fink, 2019; Park et al., 2020; Usher, 2018). Recently-published systematic reviews explored specific types of online misinformation, particularly fake news, their characteristics and impact (Di Domenico et al., 2020; Pennycook, Rand, 2021). Detection methods for identifying and countering misinformation, including both human-generated and AI-generated content (Shin, Chan-Olmsted, 2023; Kolo et al., 2022), have also been extensively examined in the literature (Zhang, Ghorbani, 2020). The fusion of traditional and digital media, the permeability of information across various platforms, and the pervasive influence of technology have tested the media by transforming its environment in unprecedented ways.

Today, social networks are a key contributor to online awareness, and trust in them as a source of information is predicted to rapidly grow, posing the lack of trust in media and journalism as a “challenge” (Fink, 2019) and leading to an industry “crisis”. Social media platforms as a phenomenon have reshaped the structure, dimensions, and complexity of news dissemination. The widespread use of them

has accelerated misinformation dissemination, enabling individuals to generate and share false information quickly and anonymously (Del Vicario et al., 2016). Major social media platforms serve as spaces for social interaction, communication, and entertainment while being significant channels for the broad sharing of information and news (Vosoughi et al., 2018), not necessarily true or relevant.

On top of that, the online media landscape has become a breeding ground for Sybil attacks (Douceur, 2002) with the utilization of multiple fake identities and social media bots (Aldayel, Magdy, 2022). Such bots, automated accounts controlled by algorithms or humans, have been weaponized to influence search algorithms, amplify and spread false narratives, manipulate public opinion, and create artificial trends (Shao et al., 2017), rumors and conspiracy theories (Ferrara, 2018; Algavi et al., 2023), create fake reputations, suppress political competitors, and even affect presidential election (Cresci et al., 2017). This manipulation has led to biased information flow, favouring specific perspectives, products, or organizations, hindering users' access to accurate and diverse information, ultimately disrupting the human ecology (Volkova, Lazutova, 2017). In recent years, researchers have dedicated a significant amount of attention to social media bot detection (Aljabri et al., 2023; Ferrara, 2018; Shao et al., 2018) and prevention (Kavazi et al., 2021; Thakur, Breslin, 2021), and defense.

In order to address this crisis, it is imperative for the media to seek innovative alternative solutions that have the potential to restore trust, promote authenticity, and ensure the delivery of accurate and reliable information to the public. We believe that the solution lies in the utilization of biometric technology, which offers unique capabilities in verifying identity and authenticating user interactions, ensuring content integrity, and enhancing user experiences.

This paper explores the crisis in media and examines how the utilization of biometrics can serve as a viable solution. It discusses the challenges faced by the media industry and explores the potential benefits and considerations associated with the implementation of biometric solutions in the media landscape.

The paper aims to achieve the following objectives:

- investigate the extent and impact of the crisis in digital media, including the prevalence of misinformation, declining trust, and the proliferation of fake news;
- explore the potential benefits of biometric technology in addressing the challenges faced by the media industry;
- analyze the considerations associated with implementing biometrics in the digital media landscape;
- provide examples of biometrics initiatives for online media.

Based on the research objectives outlined above, the following hypothesis is proposed: ‘The integration of biometric technology can serve as an effective solution to the crisis in online media by enhancing trust, combating misinformation, and fostering a more secure and personalized media environment’.

Unlocking the power of biometrics for media

Biometrics, the science of recognizing and verifying individuals based on their unique physiological or behavioral characteristics, has rapidly advanced in recent years (Kaur, Verma, 2014). Significantly enhancing the accuracy, efficiency,

and reliability of biometric systems, the introduction of machine learning techniques, such as deep learning and convolutional neural networks (Cherrat et al., 2020; Jin, 2022) has revolutionized biometric recognition algorithms. The benefits of biometrics for identity verification have expanded. Flexible and user-friendly biometric verification provides a high degree of authenticity, it can be done quickly and effortlessly, reducing the time and effort required, and enhancing security measures, particularly in high-risk environments, by providing an extra layer of authentication. Still, while biometrics can offer effectiveness and reliability, it is crucial to acknowledge the challenges it presents like privacy concerns, algorithm biases, adoption rate, and integration complexity, as well as susceptibility to potential attacks. Striking the right balance between security, privacy, and usability is of utmost importance to ensure the responsible and ethical utilization of biometric technologies. This approach is vital in effectively addressing the aforementioned threats within the media landscape.

With biometric technologies, media organizations can enhance authentication, verification, and identification processes, thereby ensuring the integrity and reliability of information disseminated through digital platforms.

First, biometrics can play a crucial role in ensuring the credibility of users on online platforms. By requiring individuals to authenticate themselves using their unique biometric traits, media organizations can establish a higher level of confidence in user identities, reducing the risk of impersonation, and unauthorized access. This authentication process can enhance security and contribute to a more trustworthy media environment.

Second, biometrics can assist in verifying the authenticity and integrity of media content, including images, videos, and audio recordings. By embedding biometric markers during the creation or capture of content, media organizations can establish a verifiable link between the content and its original source, reinforcing the credibility of information.

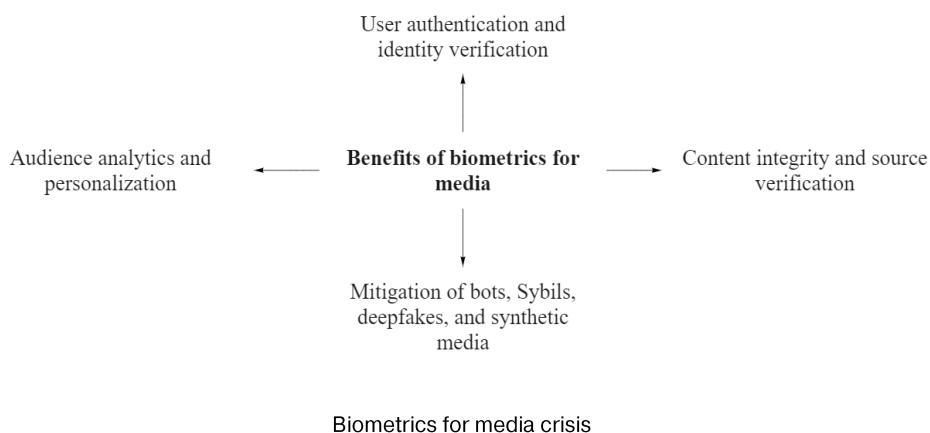
Biometrics can play a vital role in combating bots and Sybil attacks within the media landscape. Biometric analysis can aid in differentiating between human users and automated accounts, distinguishing real content from synthetic media.

In the context of combating Sybil attacks, facial recognition alongside liveness detection (Raheem et al., 2019) can play a significant role in verifying that the captured biometric traits belong to a live human user and not a manipulated or fake representation. Introduced in 2020, the Humanode project has emerged as an innovative initiative leveraging cutting-edge cryptography, and blockchain alongside liveness detection biometric technology. It aims to bring Sybil resistance to the digital environment and the media landscape in particular (Kavazi et al., 2021). By harnessing the power of biometrics, the project aims to ensure that each user account within the media platform corresponds to a unique, verifiable human identity. Through biometric authentication and verification processes, the Humanode project seeks to eliminate the presence of automated accounts and establish a trust-based space for content creation and consumption. By prioritizing user privacy and security, the project establishes a transparent and accountable environment that

encourages responsible content creation and consumption. In 2023, the project introduced the BotBasher tool which has already been implemented in hundreds of Discord servers authenticating over 220K of verified unique users¹.

It is worth noting, that multimodal biometric fusion increases the reliability of detection systems and reduces the chances of false positives or false negatives, and implementation of continuous authentication can help monitor user behavior and detect any suspicious activities in real time (Cherrat et al., 2020).

On top of that, biometrics can enable media organizations to gain insights into audience engagement and preferences. Media platforms can measure emotional reactions, identify engagement levels, and tailor content delivery to individual preferences by analyzing biometric data such as facial expressions, gaze patterns, or physiological responses. This personalized approach enhances user experience, improves content relevance, and fosters deeper audience engagement.



Navigating the biometric frontier: overcoming hurdles in implementing biometrics in the media

Despite the apparent advantages, implementing biometrics in the media landscape requires addressing several challenges. First, there are technical challenges and infrastructure requirements, involving upgrading hardware, software, and network capabilities to support the processing and storage of biometric data securely.

To implement and deploy biometric solutions effectively media organizations also need to collaborate with biometric technology providers, accessing to state-of-the-art biometric algorithms and software development kits (SDKs).

Additionally, implementing biometrics in the media industry necessitates careful consideration of legal and regulatory aspects, ensuring compliance with privacy regulations, such as the General Data Protection Regulation (GDPR), etc.

Moreover, media organizations should consider establishing clear policies and guidelines for the responsible use of biometric data, including data retention, access controls, and data-sharing practices. Transparency in data practices builds trust with users and demonstrates a commitment to protecting their privacy.

¹ BotBasher latest version is out. Retrieved September 23, 2023, from <https://blog.humanode.io/botbasher-new-version-is-out/>

Conclusion

Biometric technology offers unique advantages in restoring trust in media. Robust biometric authentication systems enable media organizations to verify the authenticity of users, thereby mitigating risks such as impersonation and identity theft. Integrating biometric traits as authentication factors, an additional layer of security is added, instilling confidence in users regarding the reliability and credibility of the information they consume and share. Furthermore, biometrics can effectively combat the influence of social media bots and Sybil attacks by differentiating between human users and automated accounts, thereby enhancing the quality and integrity of user-generated content.

However, implementing biometric technology in the media industry presents its own set of challenges. Technical considerations, such as infrastructure requirements and compatibility, must be carefully addressed to ensure seamless integration and optimal performance. Collaborating with biometric technology providers becomes crucial to access the necessary expertise and tools for successful implementation. Additionally, legal and regulatory aspects, including obtaining informed consent and protecting user privacy, must be diligently navigated to uphold ethical standards and ensure compliance with data protection regulations.

Despite these challenges, the potential benefits of biometrics for media are substantial. Biometric technology can play a pivotal role in restoring trust, combating misinformation, and establishing a more secure and personalized media environment. Leveraging biometric verification mechanisms, media organizations can build a foundation of trust with their audience, guaranteeing the authenticity and reliability of the content they deliver.

It is important to recognize that biometrics alone cannot single-handedly solve the crisis in media. It should be part of a holistic approach that incorporates education, media literacy, and transparency in journalistic practices.

Biometrics will reshape the way media organizations operate and engage with their audiences. As technology continues to evolve, biometrics will play a pivotal role in creating a more secure, personalized, and trustworthy media ecosystem that fosters credibility, authenticity, and user satisfaction.

References

- Aldayel, A., & Magdy, W. (2022). Characterizing the role of bots' in polarized stance on social media. *Social Network Analysis and Mining*, 12, 30. <https://doi.org/10.1007/s13278-022-00858-z>
- Algavi, L., Volkova, I., Kovalev, G., & Budtsov, G. (2023). Qanon as a transmedia storytelling. *Media Education*, 19(1), 3–9. <https://doi.org/10.13187/me.2023.1.3>
- Aljabri, M., Zagrouba, R., Shaahid, A., Alnasser, F., Saleh, A., & Alomari, D.M. (2023). Machine learning-based social media bot detection: A comprehensive literature review. *Social Network Analysis and Mining*, 13, 20. <https://doi.org/10.1007/s13278-022-01020-5>
- Shin, J., & Chan-Olmsted, S. (2023). User perceptions and trust of explainable machine learning fake news detectors. *Journal of Communication*, 17, 518–540.
- Cherrat, E., Alaoui, R., & Bouzahir, H. (2020). Convolutional neural networks approach for multimodal biometric identification system using the fusion of fingerprint, finger-vein and face images. *PeerJ Computer Science*, 6, e248. <https://doi.org/10.7717/peerj-cs.248>

- Cresci, S., Di Pietro, R., Petrocchi, M., Spognardi, A., & Tesconi, M. (2017). Paradigm-shift of social spambots: Evidence, theories, and tools for the arms race. *WWW '17 Companion: Proceedings of the 26th International Conference on World Wide Web Companion* (pp. 963–972). <https://doi.org/10.1145/3041021.3055135>
- Del Vicario, M., Bessi, A., Zollo, F., Petroni, F., Scala, A., Caldarelli, G., Stanley, H.E., & Quattrociocchi, W. (2016). The spreading of misinformation online. *Proceedings of the National Academy of Sciences*, 113(3), 554–559. <https://doi.org/10.1073/pnas.1517441113>
- Di Domenico, G., Sit, J., Ishizaka, A., & Nunan, D. (2021). Fake news, social media and marketing: A systematic review. *Journal of Business Research*, 124, 329–341. <https://doi.org/10.1016/j.jbusres.2020.11.037>
- Douceur, J.R. (2002). The Sybil attack. In P. Druschel, F. Kaashoek, & A. Rowstron (Eds.), *Peer-to-Peer Systems. IPTPS 2002. Lecture Notes in Computer Science* (vol. 2429, pp. 251–260). Berlin, Heidelberg: Springer. https://doi.org/10.1007/3-540-45748-8_24
- Engelke, K.M., Hase, V., & Wintterlin, F. (2019). On measuring trust and distrust in journalism: Reflection of the status quo and suggestions for the road ahead. *Journal of Trust Research*, 9(1), 66–86. <https://doi.org/10.1080/21515581.2019.1588741>
- Ferrara, E. (2018). Measuring social spam and the effect of bots on information diffusion in social media. *Complex Spreading Phenomena in Social Systems* (pp. 229–255). Cham: Springer. https://doi.org/10.1007/978-3-319-77332-2_13
- Fink, K. (2019). The biggest challenge facing journalism: A lack of trust. *Journalism*, 20(1), 40–43. <https://doi.org/10.1177/14648849188070>
- Jin, J. (2022). Convolutional neural networks for biometrics applications. *SHS Web of Conferences: 2022 International Conference on Science and Technology Ethics and Human Future*, 144, 03013. <https://doi.org/10.1051/shsconf/202214403013>
- Kaur, G., & Verma, C.K. (2014). Comparative analysis of biometric modalities. *International Journal of Advanced Research in Computer Science and Software Engineering*, 4(4).
- Kavazi, D., Smirnov, V., Shilina, S., MOZGIII, Li, M., Contreras, R., Gajera, H., Lavrenov, D. (2021). *Humanode. Whitepaper v. 0.9.6 “You are [not] a bot”*. <https://doi.org/10.13140/RG.2.2.25572.91528>
- Kolo, C., Mütterlein, J., & Schmid, S.A. (2022). Believing journalists, AI, or fake news: The role of trust in media. *Proceedings of the 55th Hawaii International Conference on System Sciences*. Retrieved September 21, 2023, from <http://hdl.handle.net/10125/79727>
- Park, S., Fisher, C., Flew, T., & Dulleck, U. (2020). Global mistrust in news: The impact of social media on trust. *International Journal on Media Management*, 22(2), 83–96. <https://doi.org/10.1080/14241277.2020.1799794>
- Pennycook, G., & Rand, D.G. (2021). The psychology of fake news. *Trends in Cognitive Sciences*, 25(5), 388–402. <https://doi.org/10.1016/j.tics.2021.02.007>
- Prochazka, F., & Schweiger, W. (2019). How to measure generalized trust in news media? An adaptation and test of scales. *Communication Methods and Measures*, 13(1), 26–42. <https://doi.org/10.1080/19312458.2018.1506021>
- Raheem, E.A., Ahmad, S.M.S., & Adnan, W.A.W. (2019). Insight on face liveness detection: A systematic literature review. *International Journal of Electrical and Computer Engineering*, 9(6), 5865. <http://doi.org/10.11591/ijece.v9i6.pp5165-5175>
- Shao, C., Ciampaglia, G.L., Varol, O., Yang, K., Flammini, A., & Menczer, F. (2018). The spread of low-credibility content by social bots. *Nature Communications*, 9, 4787. <https://doi.org/10.1038/s41467-018-06930-7>
- Thakur, S., & Breslin, J.G. (2021). Rumour prevention in social networks with layer 2 blockchains. *Social Network Analysis and Mining*, 11, 104. <https://doi.org/10.1007/s13278-021-00819-y>
- Usher, N. (2018). Re-thinking trust in the news: A material approach through “Objects of Journalism”. *Journalism Studie*, 19(4), 564–578. <https://doi.org/10.1080/1461670X.2017.1375391>

- Volkova, I.I., & Lazutova, N.M. (2017). Screen media and human ecology: From charming to joining. *Bulletin of Orenburg State University*, (12), 106–111. (In Russ.) <https://doi.org/10.25198/1814-6457-212-106>
Волкова И.И., Лазутова Н.М. Экранные массмедиа и экология человека: от зачаровывания к присоединению // Вестник Оренбургского государственного университета. 2017. № 12 (212). С. 106–111. <https://doi.org/10.25198/1814-6457-212-106>
- Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, 359(6380), 1146–1151. <https://doi.org/10.1126/science.aap95>
- Zhang, X., & Ghorbani Ali, A. (2020). An overview of online fake news: Characterization, detection, and discussion. *Information Processing & Management*, 57(2). <https://doi.org/10.1016/j.ipm.2019.03.004>

Bio note:

Sasha Shilina, Ph.D. in Philology, Chief Research Officer, Paradigm Research Institute, 86 Gorgasali St, Batumi, 6000, Georgia. ORCID: 0000-0003-4696-0739. E-mail: sasha@paradigmfund.io

Сведения об авторе:

Шилина Александра Геннадьевна, кандидат филологических наук, главный научный сотрудник, Парадайм Ресерч, Грузия, 6000, Батуми, Горгасали, д. 86. ORCID: 0000-0003-4696-0739. E-mail: sasha@paradigmfund.io