



Delft University of Technology

Misinformation Detection on Social Media Challenges and the Road Ahead

Ahvanooney, Milad Taleby; Zhu, Mark Xuefang; Mazurczyk, Wojciech; Choo, Kim Kwang Raymond; Conti, Mauro; Zhang, Jing

DOI

[10.1109/MITP.2021.3120876](https://doi.org/10.1109/MITP.2021.3120876)

Publication date

2022

Document Version

Final published version

Published in

IT Professional

Citation (APA)

Ahvanooney, M. T., Zhu, M. X., Mazurczyk, W., Choo, K. K. R., Conti, M., & Zhang, J. (2022). Misinformation Detection on Social Media: Challenges and the Road Ahead. *IT Professional*, 24(1), 34-40. <https://doi.org/10.1109/MITP.2021.3120876>

Important note

To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Copyright

Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy

Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

Green Open Access added to TU Delft Institutional Repository

'You share, we take care!' - Taverne project

<https://www.openaccess.nl/en/you-share-we-take-care>


Otherwise as indicated in the copyright section: the publisher is the copyright holder of this work and the author uses the Dutch legislation to make this work public.

Misinformation Detection on Social Media: Challenges and the Road Ahead

Milad Taleby Ahvanooeey  and Mark Xuefang Zhu , Nanjing University (NJU), Nanjing, Jiangsu, 210023, China

Wojciech Mazurczyk , Warsaw University of Technology (WUT), Warszawa, 00-665 Nowowiejska, Warszawa, Poland

Kim-Kwang Raymond Choo , University of Texas at San Antonio (UTSA), San Antonio, TX, 78249-1644, USA

Mauro Conti , University of Padua (UNIPD), 63 - 35121, Padua, Italy, and also TU Delft (TUD), 2600 AA, Delft, The Netherlands

Jing Zhang , Nanjing University of Science and Technology (NJUST), Nanjing, Jiangsu, 210094, China

It is increasingly challenging to deal with the volume, variety, velocity, and veracity of misinformation (e.g., dissemination of fake news contents, spurious posts, and fabricated images/videos) from different online platforms. In this article, we present an overview of existing machine learning and information hiding-based misinformation detection techniques and discuss the current threats and limitations of these approaches. Based on the discussion, we identify a number of potential countermeasures.

As our society becomes increasingly Internet-savvy, the importance of online news platforms (ONPs) and social media applications (SMAs) in our daily communication (e.g., information retrieval and dissemination) is becoming more pronounced. For example, end-users of these platforms share information (e.g., news articles or product reviews) and stay informed concerning various events, such as political campaigns and global pandemics. Unlike traditional news outlets, information such as user-generated content posted on SMAs is generally unvetted and subject to potential manipulation to mislead readers. As a result of such forged contents, misinformation, i.e., the dissemination of fake news, can have political and real-world social impacts, as partly evidenced during the 2016 U.S. presidential election campaign. Thus, it is not surprising that the term “fake news” has become a popular idiom and was recently featured as “Word of the Year” in a recent post by Collins Language Publications (note that the usage of this term increased by 365% since 2016). It has also attracted the attention of researchers and other stakeholders in investigating fake news source identification,

analyzing the impacts of spurious information, and their potential distribution.^{1,2}

When a news content is spread on ONPs, which may contain attachments (e.g., images, video, and audio), it can be easily manipulated and rapidly replicated by malicious users. Such activities can potentially generate a massive volume of untrustworthy contents.³ In practice, state-of-the-art machine learning (ML)-based fake news detection algorithms involve calculating the similarity rate between the fake/spurious content and the original one from a reliable corpus, i.e., available datasets generated from the legitimate resources.^{4–6} For example, user A creates a news content and shares it via LinkedIn. On the other hand, user B copies and manipulates the user A’s content as well as broadcasts the forged news article via Facebook. If user C intends to check the content integrity of this article on Facebook, and if this platform utilizes the ML-based methods, it needs to compute the similarity rate of the current article with all the collected data from the legitimate resources (e.g., websites or other SMAs). Essentially, these approaches have very high computational complexity and cannot provide sufficient results for real-time applications, i.e., where users create new articles that are not available on any other ONPs. To address this problem, researchers have proposed information hiding (IH)-based content authentication techniques that can embed a hidden watermark or signature for verifying the integrity of news content

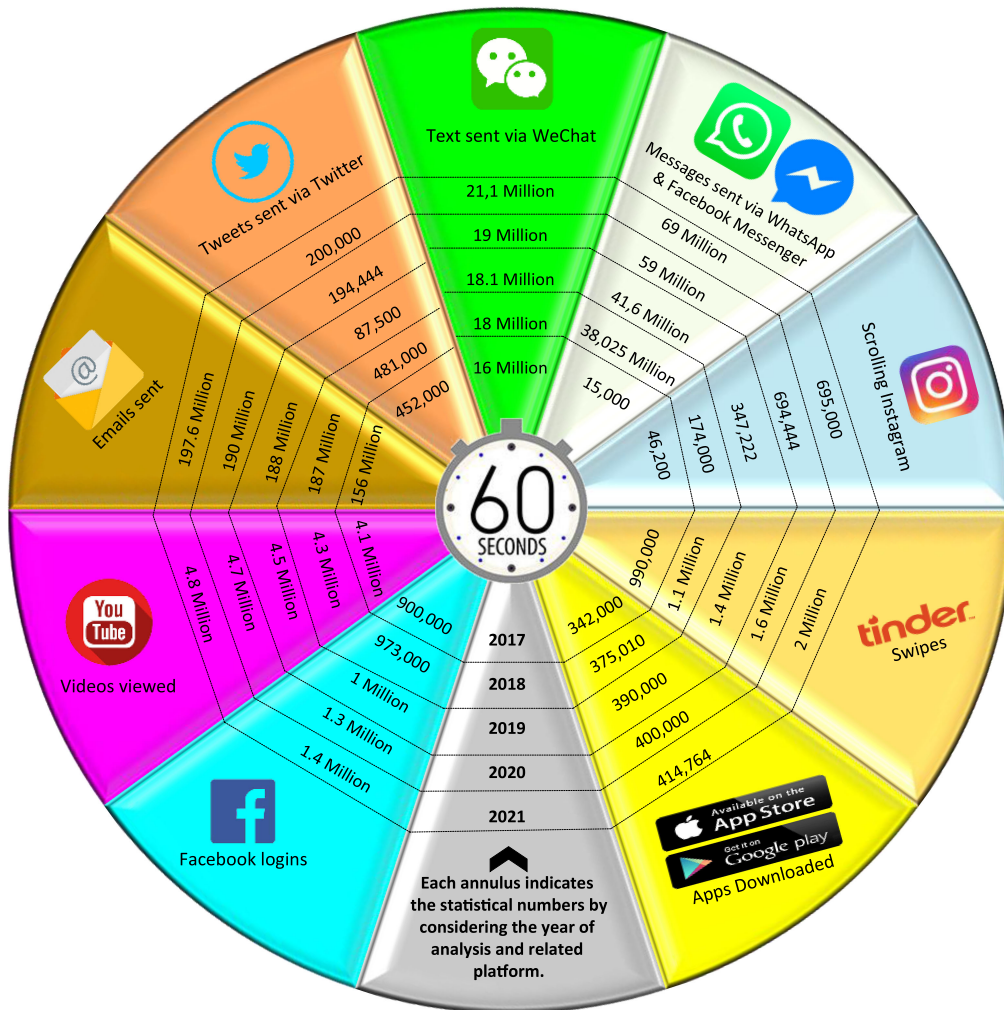


FIGURE 1. Statistical analysis of the shared messages, logins, and downloaded apps in an Internet minute.¹¹

while being copied/re-shared by malicious users on SMAs.⁷⁻¹⁰ However, the content integrity and the goal of fact statement cannot be often evaluated by either the ML or the IH-based technologies. Hence, we believe that investigators should take the collaboration between the aforementioned misinformation detection methods as well as human cognitive knowledge-based approaches into account while performing the integrity analysis. For instance, there are only a limited number of valid resources that mostly share fact news contents and these may unintentionally or intentionally mislead readers, which degrades the performance of state-of-the-art techniques.⁵

According to a statistical report presented by the Modern Luxury team during an Internet minute in 2017–2021,¹¹ there has been a massive growth in the use of SMAs and the number of shared contents on the most popular ONPs (see Figure 1). In general, a news content

is composed of one or more types of digital information, such as text, image, video, and audio. Among these types of data, textual information is the most sensitive to tampering compared to others. This sensitivity is related to the fact that a small semantic change in a sentence or a word may modify the factual meaning of the whole content; thus, it may result in the generation of untrustworthy content. Therefore, cybersecurity investigators and law enforcement agencies (LEAs) must rethink and enhance their strategies concerning online sharing platforms. For instance, the LEAs need to make ONPs to be compliant with the General Data Protection Regulation, which can reduce the number of fake news contents, while security investigators should focus on proposing new mechanisms to control a multidisciplinary task that involves several disciplines, including computer science, criminal justice, law, commerce, and economics.^{1,11-14}

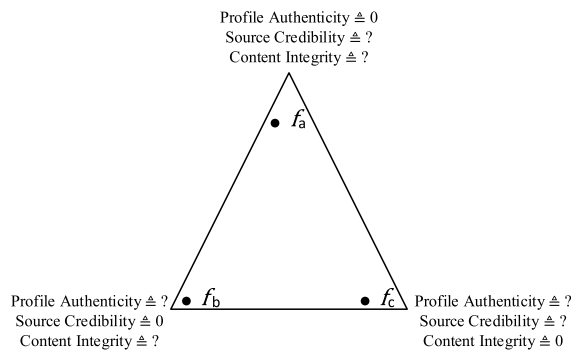


FIGURE 2. Magic triangle of the performance criteria.

In this article, we present a critical overview of the most crucial challenges that need to be considered when developing security tools for assessing the integrity of news contents on ONPs. Hence, the main contribution of this article is to bring a new perspective and the recognition of the most significant mid- and long-term opportunities and problems to be considered by both LEAs and cybersecurity experts investigating the phenomenon of misinformation analysis and its potential impacts on public opinion.

FAKE NEWS DETECTION CRITERIA

In this section, we discuss specific characteristics of fake news on SMAs, such as profile authenticity, source credibility, and content integrity, which are exposed to tampering attacks by malicious end-users on SMAs.

- *Profile authenticity*: It involves identifying the reliability of an account that generates automatic news contents on SMAs to advertise or make propaganda by impersonating someone else’s identity or signing up a fake profile.² Note that most users of SMAs are legitimate, but some of them might act maliciously or not even be actual persons. Since signing up/creating accounts on SMAs is typically cost-free, malicious users (e.g., cyborgs, trolls, and social bots) are encouraged to create multiple fake profiles for their purposes.⁶ Such profiles could act as spyware, in particular, to misdirect readers, such as creating, manipulating, and broadcasting fake news contents or ads on ONPs.¹⁵ This criterion must be certified by verifying the profile owner’s identity via ID cards or by evaluating his/her historical records or activities.
- *Source credibility*: In journalism, a source is a place, publisher, person, etc., that has timely information on a particular subject. Outside of

journalism, a “source” refers to a “news source” or a platform, such as television, radio, newspapers, and online social media.^{2,3} Although SMAs are quickly substituting traditional news sources, there is still a possibility that a malicious user may share or manipulate news content, making it a kind of unreliable source.¹⁴ In the case where a person who has a legitimate track record or profile on the ONPs (e.g., a certified reporter, a judge, or a minister), the news content shared via such profiles on SMAs can be considered a reliable source by verifying their ID cards from affiliated departments. If the content of a news article includes a cited source, the credibility of the source must be validated from the linked resource using ML-based techniques.

- *Content integrity*: When a certified user shares a news article on the SMAs, it is vulnerable to malicious attacks, such as forgery and tampering that violate the integrity and copyright of the original news content. Technically, news article integrity authentication is the process of verifying whether a given content matches the original one or not.⁵ Technically, the content integrity rate of news articles can be authenticated using the ML- or IH-based techniques.

As depicted in Figure 2, when developers design an efficient misinformation detection system, these criteria must be taken into account sequentially due to their significance. However, these criteria are inconsistent and influential on the system’s results separately; thus, their relationships can be expressed using a magic triangle model. Here, f_a indicates that the misinformation detection system has identified the spreader’s account as a fake profile. Afterward, other features are automatically considered as zero because they depend on the profile authenticity. Next, f_b implies that the system has processed the source of news content, and identified it as unreliable one. Similarly, f_c denotes that the system has authenticated the content integrity of the news article and detected it as a tampered version. In the best case, if the system processes a specific news content considering the above three criteria and classifies the results as authentic, reliable, and original, this article is classified as trustworthy to prove its reliability.

CHALLENGES OF THE STATE-OF-THE-ART TECHNIQUES

In general, news contents have influential impacts on social opinions and their editable structures on the

ONPS (or SMAs) make them potential targets for malicious actions, such as fake profile generation, forgery, and tampering attacks,⁵ which can cause the violation of the content integrity and copyright of sensitive news. In the case that a malicious user manipulates the title and news caption by changing some words of the content, the readers will receive falsified information. Technically, content integrity authentication is the practice of verifying whether a given content is similar to its original version or not. Here, we categorize the state-of-the-art authentication approaches into two main groups: whole document-based (or IH-based) and knowledge-based (or pattern-based) algorithms.⁶ In the following, we briefly describe both of these approaches.

Whole Document-Based or IH-Based Approaches

This type of authentication methods involves embedding a robust or fragile watermark (or invisible signature) into news content before broadcasting it and extracting the signature when it is required to identify its integrity rate. In general, they can be classified into two different types based on their embedding characteristics: structural and linguistic.

- › *Structural-based algorithms*: It modify the layout structures of news content, such as font type/size, spaces between words/lines, and homoglyphs for marking the signature. Technically, these characteristics depend on character encoding (e.g., Unicode or ASCII), which do not alter the original content. Such methods could preserve the invisible signature from tampering and forgery attacks to some extent through the watermarked news content,^{6–9,16}
- › *Linguistic-based algorithms*: It involve replacing linguistic features (semantic or syntactic), such as acronyms, abbreviations, and synonyms, for hiding a signature which may change the original meaning of some words or terms in a news content. Therefore, such modifications could generate falsified information, making them inefficient for authenticating sensitive text contents.^{7,17}

Practically, most of the existing IH-based algorithms can only provide proof of ownership (except a recent technique introduced by Ahvanooy *et al.*⁵), which does not protect the signed text content against tampering and forgery attacks. In the case that an attacker manipulates some portion of a signed news article, the corresponding detection algorithm cannot discover the invisible signature. However, the existence of a signature

can also be considered as evidence of authenticity. Hence, such methods could be partially used for misinformation detection when verifying the integrity of signed content for real-time online applications.

Knowledge-Based or Pattern-Based

Since the aim of fake news is to share false claims in the form of an article, the most obvious means of detecting uncertainty is to validate the veracity of the primary claims to decide on their content integrity, which is called fact-checking. These methods attempt to employ external sources to detect the truthfulness of claims mentioned in news content.² Technically, these predictive models involve computing a pattern of given article and determining the similarity rate of words with the available data in benchmark datasets, such as BuzzFeed-News, LIAR, and BS Detector,³ which could be collected from various available sources, such as search engines, online news, and SMA websites. In practice, they process the knowledge and linguistic structures using ML-based methods, such as neural networks, vector-based models, knowledge graphs, and distance measures).^{17–20} Since computer scientists have defined the fact-checking problem as a classification task, it includes the following phases for evaluating the factual claims of fake news detection.^{2,18}

- › *Data collection and labeling*: This phase involves processing the trustworthy ONPs for collecting and labeling data. Most of the existing approaches utilize feature selection methods to assign efficient labels to relevant factual data based on limited linguistic characteristics. In practice, the selection of trustworthy sources is a very challenging task. Moreover, most state-of-the-art approaches do not include visual features during their data collection, which may lead to a false result. Even if the textual content is identified as authentic, there is still a possibility that it is associated with a tampered image or video.^{4,10}
- › *Classification and ranking*: This phase involves extracting some linguistic characteristics, such as frequency of words, sentences, etc., and visual (video or image) features, such as similarity distribution histogram, coherence score, clarity score, and diversity score from the claimed news content using ML-based methods. Most of the existing algorithms only utilize limited linguistic features and eliminate the nonfactual words based on their predefined strategies as well as they do not evaluate the visual features during their analysis. However, some recent studies employ multimodal-based algorithms for

TABLE 1. Performance analysis of the state-of-the-Art fake news detection algorithms.

References	Type of method		Performance criteria: Yes:(✓) No: (×)			Applications		Type of considered features
	IH	ML	Profile authenticity	Source credibility	Content integrity	Offline	Real-time	
Por <i>et al.</i> ⁹	✓	×	×	✓	×	✓	✓	Textual
Zheng <i>et al.</i> ¹⁰	×	✓	×	×	×	✓	×	Textual+Visual
Rizzo <i>et al.</i> , ^{8,16}	✓	×	×	✓	×	✓	✓	Textual
Ahvanooy <i>et al.</i> ⁵	✓	✓	×	✓	✓	✓	✓	Textual
Shu <i>et al.</i> ³	×	✓	×	✓	✓	✓	×	Textual
Gravanis <i>et al.</i> ¹³	×	✓	×	✓	✓	✓	×	Textual
Ozbay and Alatas ¹⁴	×	✓	×	✓	✓	✓	×	Textual
Khattar <i>et al.</i> ¹⁵	×	✓	×	✓	✓	✓	×	Textual + Visual
Meral <i>et al.</i> ¹⁷	✓	×	×	×	×	✓	✓	Textual
Hassan <i>et al.</i> ¹⁸	×	✓	×	×	✓	✓	×	Textual
Singh <i>et al.</i> ¹⁹	×	✓	×	×	✓	✓	×	Textual+Visual
Nguyen <i>et al.</i> ²⁰	×	✓	×	×	✓	✓	×	Textual

processing the text data and image data during the fake news detection analysis, which suffer from very high computational complexity for training and data collection.^{15,19} Due to the sensitivity of a news article, any kind of conceptual elimination can result in a false detection rate.¹⁸

- › **Decision-making:** This phase involves measuring the three criteria (see Figure 2) by employing the above two phases as preliminary inputs. Most of the existing fake news detection techniques do not consider these criteria and simply rely upon the textual content analysis of news articles. Essentially, these features need be considered in the real-time analysis of news content on SMAs for identifying its reliability.^{15,20}

Most of the state-of-the-art ML-based methods consider the detection of “fake news” as a classification task. However, in practice, it can also be defined as a clustering task, where malicious users create/share new articles on the SMAs. Because of the variety of news content structures, a new article is not annotated (or unlabeled) and the process of data collection and labeling is a very time-consuming task for all available data from the trustworthy ONPs. For real-time applications, since there is no accessible annotated dataset for instant news contents, the supervised learning approaches do not provide efficient results as they depend on the quality of the collected

data. Table 1 summarizes the performance features of the state-of-the-art solutions considering their merits and limitations.

ROAD AHEAD

In the modern digital age, SMAs have become a common means of sharing or reading news articles by their end-users. Simultaneously, they have also provided the broad dissemination of fake news challenges to the international society, i.e., fake news content can spread falsified or spurious information, resulting in critical negative impacts on public opinions. However, there are several solutions for fake news detection based on ML and IH methods from offline datasets. But, the lack of efficient techniques for real-time application is one of the primary drawbacks in this area. We have to remark that there are still some open research issues that require to be solved to achieve the desired efficiency in future works. In the following, we suggest some guidelines aimed at leading developers and researchers on how to apply proper state-of-the-art algorithms considering real-world application requirements.

- › An efficient technique must be able to process three fundamental criteria, namely, profile authenticity, source credibility, and content integrity, by considering the multimodal (textual and visual) features during the detection analysis.

- › Because the authentication of a profile is a very complicated task, developers can certify it by employing a combination of scanned images of the ID card or the driving license, and one-time phone number or email verification using deep learning algorithms. This idea can limit the number of fake account generation with the same e-mail or phone number.
- › SMAs can utilize a combination of ML- and IH-based methods for providing a predictive tool that generates an integrity rate for each news content. This tool can provide more insights on the trustworthiness of a news article when end-users read it and realize its reliability. In addition, such predictive models can block or warn malicious users about their violent actions and set an untrustworthy label on their profiles.
- › Since malicious spreaders create/share fake advertisements to sell their illicit goods/services, or attract investments in cryptocurrencies, they need to be authenticated using ML-based predictive models considering the past activities of the spreaders' posts to label them as untrustworthy profiles.
- › Essentially, the ML-based predictive models that are based on multimodal features suffer from high computational complexity, and their results depend on the quality of data collection and labeling phases. To address this issue, future research efforts should focus on the development of new solutions to reduce the computational cost by considering hidden signatures through text contents, attachments, and profile authenticity analysis as preliminary steps before processing the multimodal features.

To summarize, if an expert wishes to address the uncertainty of real-time fake news detection on SMAs with higher efficiency, then he/she must take into account multimodal (textual and visual) features as well as three performance criteria together considering the suggestions, which we have outlined above.

CONCLUSION

Billions of users interact with each other on SMAs every day, and they use popular ONPs for sharing news contents. Through broadcasting such news articles, malicious users try to misdirect the trust of readers by manipulating news contents toward their intentional purposes (e.g., global panic, elections, intrusions, etc.).

Therefore, real-time fake news detection in SMAs has become the primary concern of users as well as the research community. SMA platforms require to provide real-time fake news detection tools for

ensuring the necessary level of trustworthy news contents. Cybersecurity investigators, LEAs, and governments must step forward and attempt to develop new paradigms and technologies for sharing and manipulating the quality of news articles on SMAs.

Moreover, misinformation detection should not be considered as an optional tool, but must be the main phase of the design procedure in SMAs. Hence, it can play a crucial role in facilitating our future, essentially in ONPs, by teaching to raise awareness of a balance between trust and action, and to consider a new proactive adoption in our policy.

ACKNOWLEDGMENTS

This article was supported in part by the National Natural Science Fund of China (NSFC) under Grant 6211101164, Grant 62076130, and Grant 91846104, and in part by the National Centre for Research and Development, Poland, under Grant EIG CONCERT-JAPAN/05/2021.

REFERENCES

1. X. Zhang and A. A. Ghorbani, "An overview of online fake news: Characterization, detection, and discussion," *Inf. Process. Manage.*, vol. 57, no. 2, 2020, Art. no. 102025, doi: [10.1016/j.ipm.2019.03.004](https://doi.org/10.1016/j.ipm.2019.03.004).
2. K. Shu *et al.*, "Fake news detection on social media: A data mining perspective," *ACM SIGKDD Explorations Newslett.*, vol. 19, no. 1, pp. 22–36, 2017, doi: [10.1145/3137597.3137600](https://doi.org/10.1145/3137597.3137600).
3. K. Shu, D. Mahudeswaran, and H. Liu, "FakeNewsTracker: A tool for fake news collection, detection, and visualization," *Comput. Math. Org. Theory*, vol. 25, no. 1, pp. 60–71, 2019, doi: [10.1007/s10588-018-09280-3](https://doi.org/10.1007/s10588-018-09280-3).
4. A. Bondielli and F. Marcelloni, "A survey on fake news and rumour detection techniques," *Inf. Sci.*, vol. 497, pp. 38–55, Sep. 2019, doi: [10.1016/j.ins.2019.05.035](https://doi.org/10.1016/j.ins.2019.05.035).
5. M. T. Ahvanooy, Q. Li, X. Zhu, M. Alazab, and J. Zhang, "ANiTW: A novel intelligent text watermarking technique for forensic identification of spurious information on social media," *Comput. Secur.*, vol. 90, no. 3, 2020, Art. no. 101702, doi: [10.1016/j.cose.2019.101702](https://doi.org/10.1016/j.cose.2019.101702).
6. C. Matteo *et al.*, "(Mis)Information operations: An integrated perspective," *J. Inf. Warfare*, vol. 18, pp. 83–98, 2019.
7. M. T. Ahvanooy, Q. Li, J. Hou, A. R. Rajput, and C. Yini, "Modern text hiding, text steganalysis, and applications: A comparative analysis," *Entropy*, vol. 21, no. 4, pp. 1–31, 2019, doi: [10.3390/e21040355](https://doi.org/10.3390/e21040355).

8. S. G. Rizzo, F. Bertini, and D. Montesi, "Fine-grain watermarking for intellectual property protection," *EURASIP J. Inf. Secur.*, vol. 10, pp. 1–20, 2019, doi: [10.1186/s13635-019-0094-2](https://doi.org/10.1186/s13635-019-0094-2).
9. L. Y. Por, W. KokShei, and K. O. Chee, "A text-based data hiding method using Unicode space characters," *J. Syst. Softw.*, vol. 85, no. 5, pp. 1075–1082, 2012, doi: [10.1016/j.jss.2011.12.023](https://doi.org/10.1016/j.jss.2011.12.023).
10. J. Zeng, Y. Zhang, and X. Ma, "Fake news detection for epidemic emergencies via deep correlations between text and images," *Sustain. Cities Soc.*, vol. 66, 2021, Art. no. 102652, doi: [10.1016/j.scs.2020.102652](https://doi.org/10.1016/j.scs.2020.102652).
11. L. Lewis, "Infographic: What happens in an internet minute 2020 & 2021," Retrieved: data from 2017 to 2021. Accessed: Oct. 13, 2021. [Online]. Available: <https://www.allaccess.com/merge/archive/32972/>
12. D. Domenico et al., "Fake news, social media and marketing: A systematic review," *J. Bus. Res.*, vol. 124, pp. 329–341, 2021, doi: [10.1016/j.jbusres.2020.11.037](https://doi.org/10.1016/j.jbusres.2020.11.037).
13. G. Gravanis, A. Vakali, K. Diamantaras, and P. Karadais, "Behind the cues: A benchmarking study for fake news detection," *Expert Syst. Appl.*, vol. 128, pp. 201–213, 2019, doi: [10.1016/j.eswa.2019.03.036](https://doi.org/10.1016/j.eswa.2019.03.036).
14. F. A. Ozbay and B. Alatas, "Fake news detection within online social media using supervised artificial intelligence algorithms," *Physica A: Stat. Mechanics Appl.*, vol. 540, 2020, Art. no. 123174, doi: [10.1016/j.physa.2019.123174](https://doi.org/10.1016/j.physa.2019.123174).
15. D. Khattar, J. S. Goud, M. Gupta, and V. Varma, "MVAE: Multimodal variational autoencoder for fake news detection," in *Proc. ACM World Wide Web Conf.*, 2019, pp. 2915–2921, doi: [10.1145/3308558.3313552](https://doi.org/10.1145/3308558.3313552).
16. F. Bertini, S. G. Rizzo, and D. Montesi, "Can information hiding in social media posts represent a threat?," *Computer*, vol. 52, no. 10, pp. 52–60, 2019, doi: [10.1109/MC.2019.2917199](https://doi.org/10.1109/MC.2019.2917199).
17. H. M. Meral, B. Sankur, A. S. Özsoy, T. Güngör, and E. Sevinç, "Natural language watermarking via morphosyntactic alterations," *Comput. Speech Lang.*, vol. 23, no. 1, pp. 107–125, 2009, doi: [10.1016/j.csl.2008.04.001](https://doi.org/10.1016/j.csl.2008.04.001).
18. N. Hassan, F. Arslan, C. Li, and M. Tremayne, "Toward automated fact-checking: Detecting check-worthy factual claims by ClaimBuster," in *Proc. 23rd ACM SIGKDD Int. Conf. Knowl. Discov. Data Mining*, 2017, pp. 1803–1812, doi: [10.1145/3097983.3098131](https://doi.org/10.1145/3097983.3098131).
19. V. K. Singh, I. Ghosh, and D. Sonagara, "Detecting fake news stories via multimodal analysis," *J. Assoc. Inf. Sci. Technol.*, vol. 72, no. 1, pp. 3–17, 2021, doi: [10.1002/asi.24359](https://doi.org/10.1002/asi.24359).
20. T. T. Nguyen, M. Weidlich, H. Yin, B. Zheng, Q. V. H. Nguyen, and B. Stantic, "User guidance for efficient fact checking," *Proc. VLDB Endowment*, vol. 12, no. 8, pp. 850–863, 2019, doi: [10.14778/3324301.3324303](https://doi.org/10.14778/3324301.3324303).

MILAD TALEBY AHVANOOEY is currently a Faculty Member at Nanjing University, Jiangsu, China. Ahvanooeey received the Ph.D. degree in computer engineering (Cybersecurity), Nanjing University of Science and Technology, Xuanwu, China, in December 2019. He is the corresponding author of this article. Contact him at M.Taleby@IEEE.org.

MARK XUEFANG ZHU is currently a Full Professor and the Head of the Institute of Multimedia Information Processing at the School of Information Management, Nanjing University, Jiangsu, China. He is the co-corresponding author of this article. Contact him at xfzhu@nju.edu.cn.

WOJCIECH MAZURCZYK is currently a University Professor at the Warsaw University of Technology, Warszawa, Poland. He is also the head of the Computer Systems Security Group. Since 2018, he has been an Associate Editor for the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY and series editor for the *IEEE Communications Magazine*. Contact him at wojciech.mazurczyk@pw.edu.pl.

KIM-KWANG RAYMOND CHOO holds the Cloud Technology Endowed Professorship at The University of Texas at San Antonio, San Antonio, TX, USA. He was the recipient of the 2019 IEEE Technical Committee on Scalable Computing Award for Excellence in Scalable Computing. Contact him at raymond.choo@fulbrightmail.org.

MAURO CONTI is currently a Full Professor in computer science and the head of SPRITZ Security and Privacy Group University of Padua, Padua, Italy. He is also an IEEE Senior Member, and associate editor for the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, IEEE COMMUNICATIONS SURVEYS AND TUTORIALS. Contact him at conti@math.unipd.it.

JING ZHANG is currently an Associate Professor with the School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing, China. His research interests include machine learning and data mining and their applications in cyberspace security. Contact him at jzhang@njust.edu.cn.