Received: Added at production | Revised: Added at production | Accepted: Added at production

DOI: xxx/xxxx

RESEARCH ARTICLE

Debunking War Information Disorder: A Case Study in Assessing the Use of Multimedia Verification Tools

Sohail Ahmed Khan[1] | **Laurence Dierickx**[1] | **Jan-Gunnar Furuly**[2,5] | **Henrik Brattli Vold**[3,5] | **Rano Tahseen**[4,5] | **Carl-Gustav Linden**[1] | **Duc-Tien Dang-Nguyen**[1]

[1]University of Bergen, Norway

[2]Aftenposten, Norway

[3]Institute of Journalism, Norway

[4]TV2, Norway

[5]Faktisk, Norway

Correspondence

Corresponding authors: Sohail Ahmed Khan and Duc-Tien Dang-Nguyen, University of Bergen, Bergen, Norway

Email: {sohail.khan, ductien.dangnguyen}@uib.no

Abstract

This paper investigates the use of multimedia verification, in particular, computational tools and Open-source Intelligence (OSINT) methods, for verifying online multimedia content in the context of the ongoing wars in Ukraine and Gaza. Our study examines the workflows and tools used by several fact-checkers and journalists working at Faktisk, a Norwegian fact-checking organisation. Our study showcases the effectiveness of diverse resources, including AI tools, geolocation tools, internet archives, and social media monitoring platforms, in enabling journalists and fact-checkers to efficiently process and corroborate evidence, ensuring the dissemination of accurate information. This research provides an in-depth analysis of the role of computational tools and OSINT methods for multimedia verification. It also underscores the potentials of currently available technology, and highlights its limitations while providing guidance for future development of digital multimedia verification tools and frameworks.

KEYWORDS

verification, multimedia verification, osint, verification journalism, misinformation detection, fake news, osint journalism, social media monitoring, user-generated content

1 | INTRODUCTION

Social media platforms play a crucial role in news consumption and dissemination (Hermida et al., 2012; Nielsen & Fletcher, 2023), offering instant access to global news stories and vast real-time multimedia content. Notably, journalists and news media organisations actively utilise these platforms to stay updated on high-profile news events (Djerf-Pierre et al., 2020; Schifferes et al., 2017). However, using social media platforms in journalism acts as a double-edged sword. While it enables news media companies to reach wider audiences and stay connected with global news events, it also serves as a conduit for the dissemination of mis- and dis-information, especially during significant events like wars, elections, and pandemics (Cotter et al., 2022; Goțiu, 2023; Ireton & Posetti, 2018).

In the global landscape of journalism and news media, disentangling truth from falsehood has become a critical response to the proliferation of information disorders which can have various forms, from unintentional misinformation to intentional disinformation that intends to cause harm (Haider & Sundin, 2022; Wardle & Derakhshan, 2017). This necessity has given rise to the specialised field of fact-checking and verification, acknowledged as a cornerstone for objective, ethical, and accountable reporting (Mena, 2019; Singer, 2021).

In many ways, fact-checking and verification is reflected in investigative journalism, a practice deeply rooted in critical and global approaches consistent with journalism's watchdog role (Cancela et al., 2021). It involves addressing the rapid dissemination of information disorder on social media, necessitating the ability to scrutinise various forms of content, whether textual or audiovisual. However, verifying content spread on social media is challenging due to the difficulty of assessing the accuracy and validity of both sources and content (Brandtzaeg et al., 2016; Lecheler & Kruikemeier, 2016).

Computational tools and Open-source Intelligence (OSINT) methods have great potential to support fact-checkers in this process. OSINT refers to the process of gathering information from publicly available resources, meaning that they must be legally accessible, and there are a plethora of tools designed to facilitate this information gathering (Hassan et al., 2018). Similar to investigative journalism, certain fact-checking organisations have used OSINT techniques to support their professional practice. This involves new methods and skills to complement journalistic methods and know-how (Müller & Wiik, 2023). For instance, in Norway, Faktisk[1] is engaged in such a way. This fact-checking organisation has the particularity of having been created through a partnership between several large media companies in the country. In 2022, Faktisk created a dedicated team, Faktisk Verifiserbar, comprising reporters, researchers and fact-checkers from various Norwegian media outlets, collaboratively verifying visual content and stories from the ongoing war in Ukraine.

This paper aims to understand how computational tools and OSINT methods are practically used by fact-checkers involved in Faktisk Verifiserbar in verifying the (mostly) visual information shared online in relation to ongoing wars in Ukraine and Gaza. We study their methodologies, verified cases, utilised tools, requirements, and challenges with the aim of mapping out current practices, identify limitations, and propose enhancements in fact-checking and verification tools. Hence, this research focuses on one primary question: What limitations do existing tools face, and what potential advancements in computational methods could enhance multimedia verification in the future? In essence, we investigate: (i) The verification workflows adopted by fact-checkers in multimedia content verification; (ii) The rationale behind their selection and utilisation of computational tools in multimedia verification; (iii) Real-world cases from the Russia-Ukraine, Gaza-Israel wars authenticated by the Faktisk Verifiserbar team; and (iv) The limitations of existing tools and prospects for future computational advancements in multimedia verification.

This paper is organised as follows: In Section 2, we provide an overview of the literature to establish the state of the knowledge in the use of fact-checking technologies by human fact-checkers. Section 3 outlines the methodology employed for data collection by delineating the verification workflows adopted by fact-checkers in multimedia content verification. Section 4 presents the procedures utilised at Faktisk Verifiserbar for multimedia content verification, focusing on the context of the Russia-Ukraine war with some cases from the war in Gaza, and explains the rationale behind the selection and utilisation of computational tools. Section 5 showcases notable cases investigated by Faktisk Verifiserbar regarding the Russia-Ukraine war. Section 6 highlights key insights for the advancement of multimedia verification. Lastly, Section 7 discusses the research question and summarises the findings of the study and its contribution to the field.

2 | FACT-CHECKING AND THE CHALLENGES OF MULTIMEDIA VERIFICATION

Fact-checking processes and practices encompass a variety of strategies, including social media monitoring, traditional journalistic techniques, online research and investigative methods, and multimedia verification (Amazeen, 2020; Dierickx & Lindén, 2023; Graves, 2017; Shapiro et al., 2013). At the heart of these practices, verification refers to all the methods and techniques that make it possible to test a claim's reliability, accuracy and truthfulness. Verification includes traditional methods of journalism, such as phone calls to trusted sources and the use of a wide range of digital tools (Lecheler & Kruikemeier, 2016). The term 'debunking' is increasingly associated with verification in fact-checking, reflecting a growing link between manipulated multimedia content and sophisticated forensic tools (Graves et al., 2023). However, debunking content goes beyond searching for evidence, as it involves detecting and revising misinformation and disinformation (Weikmann & Lecheler, 2023).

In an evolving digital environment, content verification faces many challenges. Social media is complicated to deal with, firstly because user-generated content makes it challenging to identify the source and assess its accuracy, and secondly, because it involves real-time information flows and different types of content (Brandtzaeg et al., 2018). The decontextualisation of multimedia content is another challenge, as there may be a contradiction between what is shown and what is portrayed, such as scenes of previous events that were recorded elsewhere but reused in several different contexts (Weikmann & Lecheler, 2023). Furthermore, images and videos are likely to misrepresent a claim if the context is not explained (Brandtzaeg et al., 2018).

Verifying video content is more challenging because a frame-by-frame approach often reveals errors, alterations, or hidden elements (Weikmann & Lecheler, 2023). The emergence of deepfake technology, characterised by hyper-realistic audiovisual manipulation, has made it increasingly difficult to distinguish between authentic and fake media through visual inspection alone (Mukta et al., 2023). Therefore, manipulating faces in images and videos, whether partial or complete, has become a prominent and ongoing area of research, as it poses a significant challenge in the fight against disinformation (Montoro Montarroso

et al., 2023). The widespread use of generative AI adds complexity in terms of generating and detecting harmful content (Dierickx et al., 2023b). Detection also challenges extend to cheapfakes and non-AI manipulations using image or video editing software to alter context (Dang-Nguyen et al., 2024; Khan et al., 2023).

In such a complex manipulated multimedia landscape, fact-checking technologies are also helpful in verifying sources, news discovery, multimedia verification, search and automated translation (Lecheler & Kruikemeier, 2016; Micallef et al., 2022). Hence, they are part of the fact-checking apparatus for verifying and debunking multimedia content. However, although many tools are available, fact-checkers tend to use the same because they are unaware of the existence of a plethora of tools or do not have the time to discover or learn to use them (Dierickx & Lindén, 2023; Picha Edwardsson et al., 2023). Moreover, even in a tech-savvy market such as Norway, there can be discrepancies between the effective use of technology and the narratives about its potential. Nevertheless, the most advanced technological skills were found among fact-checkers in Faktisk (Samuelsen et al., 2023).

Fact-checking digital content is often associated with OSINT techniques, which refer to publicly available digital platforms and tools for digital forensics (Picha Edwardsson et al., 2023). However, research has shown that investigators may lack the awareness and skills to use such tools, relying instead on their powers of logical deduction and critical evaluation (Himma-Kadakas & Ojamets, 2022). Such skills are nevertheless valuable in OSINT practice, as analytical techniques are considered necessary to mitigate accuracy (Siegel, 2018). OSINT methods were notably popularised after the 2021 US Capitol riot, enabling an understanding of the underlying complex social structure behind the event (Reese, 2023). They were also brought to the fore in the context of the Russian-Ukrainian war, where photographic evidence was used to prove the Boutcha massacres (Ledoux, 2022).

OSINT methods and tools are at the heart of the practices of specialist open-source investigative organisations. One of the most influential actors in this field, Bellingcat[2], was launched three days before the downing of Malaysian Airlines flight MH-17 over eastern Ukraine in 2014, demonstrating the efficiency of advanced multimodal analytical methods in the search for truth (Higgins, 2021; Kotišová & van der Velden, 2023). Such organisations, primarily led by non-journalists, are now considered to have brought a new dynamic to investigative journalism, both in terms of competencies and tools (Müller & Wiik, 2023). They are also a reference for fact-checking organisations involved in OSINT.

Addressing the many challenges associated with multimedia verification is the focus of a considerable body of research in data, computer and information sciences. The pitfall is to assume that technology alone will suffice in the fight against information disruption, whereas the benefits of considering human-computer interactions have been demonstrated (Dierickx et al., 2023a). Understanding the needs of end-users is not only related to the functionalities provided by the tool, as it participates in a socio-technical process that considers professional and cultural perspectives (de Haan et al., 2022; Diakopoulos et al., 2021; Nakov et al., 2021). Other challenges relate more directly to fact-checkers as end-users of technology. These relate to the fragmented use of computational tools in that they have a limited function in the fact-checking process and are rarely integrated with each other, and multiple tools perform the same task with similar but not identical results (Micallef et al., 2022).

3 | METHOD

This research draws on a case study design to explore the challenges of verifying multimedia content in the context of the Russian-Ukrainian war. The study, conducted between April and December 2022, captures the real-time dynamics of the verification process during an ongoing event in which open-source news methods gained prominence in journalism (Ledoux, 2022). The case study as a research strategy was developed to enable the production of contextual knowledge, which is crucial for understanding complex phenomena in real-life situations and providing a nuanced perspective on the observed reality (Flyvbjerg, 2006). As the aim of this study is to collect evidence to improve verification workflows and used technologies from an operational perspective, the research strategy aligns with human-computer interaction methods, where the focus is placed on the user when conducting specific tasks in context (Chen & Atwood, 2007).

The data collection includes 60 days of on-site observation, which was necessary to understand the fact-checkers' workflows, considering the project brought together fact-checkers at Faktisk Verifiserbar from multiple different Norwegian news media companies, including, TV2, VG and Aftenposten. This privileged position implied a proximity with the observed fact-checkers, which necessitated a constant search for establishing a balance between the researcher engagement and the needed critical distance (Döös & Wilhelmson, 2014). The research method also involved close collaboration three fact-checkers, who were asked to actively participate in this research by writing about their experiences with the tools and detailing their verification

processes. This approach helped gather valuable information that wouldn't have been possible to collect otherwise. Such an experimental research approach improved the understanding how the fact-checkers interact with verification tools and their workflows in real situations.

The method also involved one-to-one semi-structured interviews, a strategy that provided flexibility, helping to better understand the fact-checking workflows and tasks carried out with the available tools. Furthermore, the research included a comprehensive analysis of over 200 fact-checks related to the Russian-Ukrainian war, published by Faktisk Verifiserbar between April 2022 and December 2022. This analysis involved a close examination of the content, sources, and methodologies used in each verification, providing empirical data on the types of misinformation encountered, the strategies employed to counter it, and the effectiveness of various verification tools. We would like to highlight that in this manuscript, new cases from war in Gaza have also been included to confirm the process.

Ethical considerations were not only related to the researcher's position in the newsroom but also about the collection of social media data posed unique challenges. Since social media users were not informed about this research and could not therefore withdraw their consent, and considering the fundamental respect for the privacy of users despite the publicly available content being shared on a private platform, the sensitive nature of the content, and the study's focus on the interactions between fact-checkers and fact-checking technology, all collected social media data was anonymised to ensure the protection of users' privacy (Williams et al., 2017).

4 | MULTIMEDIA VERIFICATION PROCESS AND ROUTINES IN FAKTISK

In this section, we describe the workflows and computational tools used at Faktisk Verifiserbar to verify multimedia content related to the wars in Ukraine and Gaza. We'll briefly explain the 5-step multimedia verification process, known as the 5 Ws (Waisbord, 2019), which is key to Faktisk Verifiserbar's approach. Additionally, we'll outline the data collection and publishing process used during verification.

Faktisk is the only Norwegian fact-checking organisation in Norway. It was launched before the 2017 Norwegian general election through a partnership between several large media companies (Larsen, 2019; Steensen et al., 2023). It is owned by two commercial news companies (VG and Dagbladet), two public broadcasters (NRK and TV 2) and two media companies (Polaris Media and Amedia) (Larsen, 2019; Sheikhi et al., 2023; Steensen et al., 2023). Faktisk is organised according to a newsroom model (Cherubini & Graves, 2016), which reflects a democratic-corporative perspective typical of Nordic countries (Larssen, 2020).

As a member of the International Fact-Checking Network (IFCN), Faktisk is committed to impartiality and fairness, transparency of sources, transparency of funding and organisation, transparency of methodology, and open and honest corrections (Graves, 2018; Larssen, 2020; Mena, 2019). In 2022, Faktisk set up a special team called *Faktisk Verifiserbar*, which consists of reporters, researchers and fact-checkers from different media companies across Norway, working together to verify visual content and stories from the ongoing wars in Ukraine and Gaza. In terms of process when it comes to verifying online multimedia content, they follow a five-step method widely used within fact-checking organisations insofar as they align with standard journalistic practice.

4.1 | A Five-step Method to Verify Multimedia Content

The verification of online multimedia content at Faktisk addresses the basic set of questions, referred to as the five Ws, that are the foundation of any journalistic process (Waisbord, 2019). However, the 'what', which relates to the incident, event or other circumstance that is the story's focus, is replaced by the criteria of 'originality', which relates to the newsworthiness of the content to be fact-checked. In practice, this also means ensuring it has not been reported in another context.

Once the originality is established, the 'Who' relates to the process of identifying the individual or group responsible for creating or capturing the original content. It involves the investigation of the source, including the content they shared in the past, and their social media footprint, valuable insights can be gained regarding the authenticity and credibility of the multimedia content being verified. Moreover, verifying the source is instrumental in detecting instances where the content has been misrepresented, repurposed, or taken out of context.

The 'When' involves determining the precise time frame or temporal context in which the content was captured or occurred. This process is critical to assessing the authenticity and relevance of the content element. By analysing various indicators such

TABLE 1 Useful methods of finding out time and date of the events being presented in images/videos. In the left column we present the methods, whereas on the right side we write a brief description about each method.

Method	Description
Metadata	Nearly all the digital photos/videos have embedded metadata information including the date and time the photo/video was captured among other details. This metadata information can be examined using most freely available photo editing software or online tools.
Check the upload date	Most social media platforms show the date and time a photo/video was shared along with other details such as, name of the person who shared the post, and on some platforms the location from where the post was shared. This information can also sometimes lead to the date and time at which the photo/video was actually captured.
Check for context clues	Look for other visible elements in the photo/video that can be helpful in verifying the time and date, such as the sun's position, weather details (rain, snow), presence of people, or clothing people are wearing.
Look for visible time stamps	Digital devices such as some video cameras, security cameras etc embed a visible time stamp in the footage which can also be helpful.
Compare with other sources	If the photo/video was taken/shared in the course of a specific event (festival, bombing), compare it with other photos/videos taken/shared at the same event. This can also sometimes lead to the exact time and date of the acquisition of a photo/video.
Analyse weather data	Historical weather data can help in estimating the date/time of an event being presented in an image/video. As mentioned in the case above, Faktisk Verifiserbar was able to roughly estimate the date of a highly important event by analysing the historical weather patterns using Weather.com. For reference, please see Figure 5.
Analyse shadows	When there is no metadata information available, or any other contextual clues about the photo/video, the length of shadows can be utilised to establish the time of day when a photo/video was captured. Shadows are longest during the early morning hours and late afternoon, and shortest at noon. To determine the time, measure the length of the shadow cast by a known object inside the photo/video, and then compare it to the object's height. The ratio of the shadow's length to the object's height can then be utilised to estimate the time of the day. SunCalc is a freely available online tool which helps in inferring the time at which a photo/video was captured using shadow analysis.
Contact the user	If still unsure of the time and date, one can try to reach out to the user who shared the photo/video online, and ask for more information.

as metadata information or contextual clues within the image/video itself, such as shadows, weather, time of day, etc., fact-checkers can attempt to determine the specific moment or period when the event occurred, or the content was captured. This verification process helps to identify instances of potential misrepresentation, manipulation or outdated information.

The 'Where' refers to the geographical location where the content was captured, or the location displayed in the content. Geolocation is central to Faktisk Verifiserbar's fact-checking efforts, especially for visual content (image or video). Through careful analysis of visual cues, landmarks and distinctive elements within the multimedia content, fact-checkers attempt to geolocate the content and determine its alignment with the claimed location. This process often involves using geolocation tools, satellite imagery and mapping data to cross-reference the visual information presented in the content. Verification of the "Where" component can determine whether instances of potential misattribution or misassociation of the content with a specific location can be identified.

Finally, the 'Why' usually seeks to understand the reasons or motivations behind the content. However, finding out why someone shared a particular image/video is almost impossible, as the act of sharing something online is driven by different motivations. While some people may genuinely share content without malicious intent, others may have ulterior motives, such as promoting a particular political or personal agenda. Understanding the underlying motivation behind online posts is crucial to effectively assessing their credibility. If you come across a post from someone who is known to spread misinformation, conspiracy theories or biased content, it is wise to exercise caution and conduct extensive verification to ensure the accuracy and reliability of the information being shared.

In Table 1, we have summarised several methods for inferring the date and time when the multimedia content was created or captured.

4.2 | The Data Collection and Publishing Process

In addition to this five-step method, Faktisk Verifiserbar has incorporated some internal steps during and after verification has completed. First, Faktisk Verifiserbar has devised a database comprising comprehensive reports and is limited for internal use only. All events to be verified are added to this verification database. The structure of the database is organised around a unique identifier given to each case being verified, the date of the occurrence of the event, and the date on which the image/video relating

TABLE 2 Frequently used computational and multimedia verification tools utilised by Faktisk Verifiserbar.

Application	Tool
Reverse image search	Google Images, Google lens, Yandex Images, Bing Images, Tineye
Facial recognition	PimEyes(Paid service), Search4faces.com
Image verification	ImgOps, InVid-WeVerify, FotoForensics
Social media	Facebook, Twitter, Telegram, TikTok, VKontakte
Social media monitoring	Dataminr, Tweetdeck
Geolocation	Google Maps/Streetview, Yandex Maps/Streetview, Bing Maps, Apple Maps
Chronolocation	NASA FIRMS, SunCalc, Yr.no, Weather.com
Satellite imagery	NASA FIRMS, Google Earth Pro, Sentinel Hub Playground, Planet.com
Workflow	Slack and Google sheets, docs, drive, and Gmail
Publishing platform	NTB Mediebank

to the event was shared online. The database also contains the date of publication (if any), a link to the job status (“Completed”, “Work in process”, “On hold”, “For control”, “Not a priority”), the verification status (“Verified”, “Not verifiable”, “Partially verified”, “False”, “Misleading”), the name of the person/s who worked on the case, the name of the person/s who ensured a peer control, the coordinates of the location presented in the video/photo being verified, and the location where the event took place.

The other fields are related to the sender (identified as “Pro-Russia”, “Pro-Ukrainian”, “Neutral”, and “Other”), the description of what is being presented in the multimedia content, the link to the originally shared content, the link of the content on Faktisk’ server, and relevant comments to other Faktisk Verifiserbar colleagues. Each case under review is assigned a specific category. There are nine different predefined categories: “Injured civilians”, “Troop transfer”, “Combat actions”, “Demonstrations”, “Damaged infrastructure”, “Hope and heart”, “Mass grave”, “Cluster bomb” and “Other”. Insofar as multimedia content are likely to be disturbing, a level of violence is assigned to each content, through five different categories: “None - Military presence”, “Mild - Explosion/ Destruction/ Mild damage”, “Moderate - Bombing/Moderate damage”, “Heavy - Serious damage/Wounded corpse”, and “Very strong - Dead or injured bodies/Explicitly gross or particularly close violence”.

Data collection begins when the team receives requests from parent media companies. Team members also monitor social media platforms (X, Facebook, Telegram, Reddit). They also follow specific Telegram channels, X accounts and Discord servers. In addition, they use online resources to gather real-time information and track the situation on the ground. When a relevant event/case is identified for review, it is added to the database. The content is stored in a new folder containing various resources such as raw files (images/videos), screenshots and geolocation details (coordinates). A base template generates a verification document within the project folder. The template comprises several main sections, including “The public report text”, “What does the video/picture actually show?”, “Publishing context”, “Geolocation”, and “Time verification” Each section provides a brief explanation of the verification process, outlining the steps taken, tools utilised, and other relevant information.

Once the verification document is complete, the case is updated to ‘Ready for inspection’ for a buddy check, a standard procedure at Faktisk Verifiserbar. This step ensures a second opinion on the verification, confirms the document’s accuracy and involves another person thoroughly reviewing and approving the document. After a positive evaluation, the document can be published on the Mediebank platform developed by Norwegian News Agency, NTB. The Mediebank platform allows fact-checkers working at the Faktisk Verifiserbar to share images, videos that they have verified with other journalists working at major Norwegian news media companies. An email is sent to the tipster, usually a journalist in Norway, and if the event is newsworthy, another email is sent to a predefined list of media people. Sometimes, a full news story is written and published on the Faktisk Verifiserbar platform, mainly if the event attracts the attention of their journalists.

In Table 2 provides a concise overview of the primary tools consistently used by Faktisk Verifiserbar to verify multimedia content. These tools are an integral part of the verification workflow and contribute significantly to the accuracy and reliability of our investigative processes.

5 | VERIFYING THE RUSSIAN-UKRAINIAN WAR

This section provides an overview of Faktisk Verifiserbar's process for verifying multimedia content related to the wars using the 5 step verification process described in the preceding section. At the end of this section, we also present notable cases from the war where satellite imagery and related tools were specifically employed for verification. Following this, we highlight the specific challenges associated with using satellite imagery and geolocation. This section is specifically focused on achieving the first three aims listed in Section 1, i.e., (1) The verification workflows adopted by fact-checkers in multimedia content verification; (2) The rationale behind their selection and utilisation of computational tools in multimedia verification; (3) Real-world cases from the Russia-Ukraine, Gaza-Israel wars authenticated by the Faktisk Verifiserbar team.

5.1 | Following the Five-step Process

To determine the originality of content, an image or video must first be authenticated. There are several methods available, one of which is reverse image search to detect any alterations or contextual misuse of the image or video if possible. If an earlier version of the same image or video is found online, this strongly suggests that it has been recycled and presented out of context. Another method is to analyse the metadata associated with an image or video. Metadata contains valuable information about the time and place of the content's creation, which can help assess its authenticity. However, they are often missing from visual content downloaded from social media platforms (Pasquini et al., 2021). Caution should also be exercised when dealing with metadata information, as it may be subject to modification or manipulation.

Reverse image search can be performed with tools like Google, Bing, and Yandex for images, or dedicated tools like TinEye and Google Lens. For video verification, InVid-WeVerify plugin, VLC, and Adobe Premiere are commonly used. The embedded watermarks or logos found in particular images and videos can also sometimes help identify the content's source and provide valuable clues for further investigation. Journalists also conduct keyword searches on various social media platforms, such as Telegram channels, Twitter and Discord servers, using queries related to the events depicted in the image or video. These approaches help them gather additional information about the origin of the content. Facial recognition software such as PimEyes and Search4faces is also occasionally used when images or videos contain identifiable faces, helping to identify the source.

An example of the misuse of old images to spread misinformation during the Russia-Ukraine war was the case of an alleged Ukrainian soldier, who was depicted in a viral post with a swastika carved into his back by Russian soldiers. This image resurfaced on social media platforms and was circulated by various users, including a retired Norwegian military officer and a well-known Ukrainian war specialist, retired lieutenant general, who often appears in Norwegian media. To verify the image's authenticity, Faktisk Verifiserbar conducted a simple reverse image search, revealing that the same image had previously been used in unrelated contexts (Figure 1). Another recent instance of employing reverse image search to debunk mis-contextualised media relating to the recent war in Gaza. A particular video circulating on Instagram purported to show "European Zionists" seizing Palestinian homes (Figure 1). However, through reverse image searches conducted on frames extracted from the video, coupled with geolocation tools, journalists at Faktisk Verifiserbar determined that the video was actually recycled, having been originally shared in May 2022, and was recorded in Hebron, West Bank. The investigations revealed that the house was not seized forcibly but rather acquired through purchase.

The second step, related to the 'Who' question, aims to identify the content's original creator, uploader or sharer. Fact-checkers begin by asking direct questions of the individual or people who shared the content on social media to assess whether they are the source of the story. However, this technique does not often produce probing results, as people do not necessarily share their footage. The responses collected through such interviews can be cross-checked with available information, such as checking the Exif data in a photo or comparing the video with Google Street View. Suppose the photo/video is uploaded to a social media platform. In that case, metadata information is often lost. Still, journalists can also request the original file or additional corroborating evidence, such as other images or footage, to verify the person's presence at the location.

When it is impossible to contact the person/entity who uploaded or shared the content online, journalists use alternative methods to authenticate it. One method is to conduct a social media analysis by searching for the users (using their usernames and other relevant information) who shared the content on other prominent social media platforms, online forums and people search engines such as PeopleFinder.com[3], Spokeo.com[4], Webmii.com[5] and Pipl.com[6]. If a website is being investigated, online tools such as Who.is[7], DNSChecker.org[8] and similar domain search engines can be used. The other solution is to analyse any

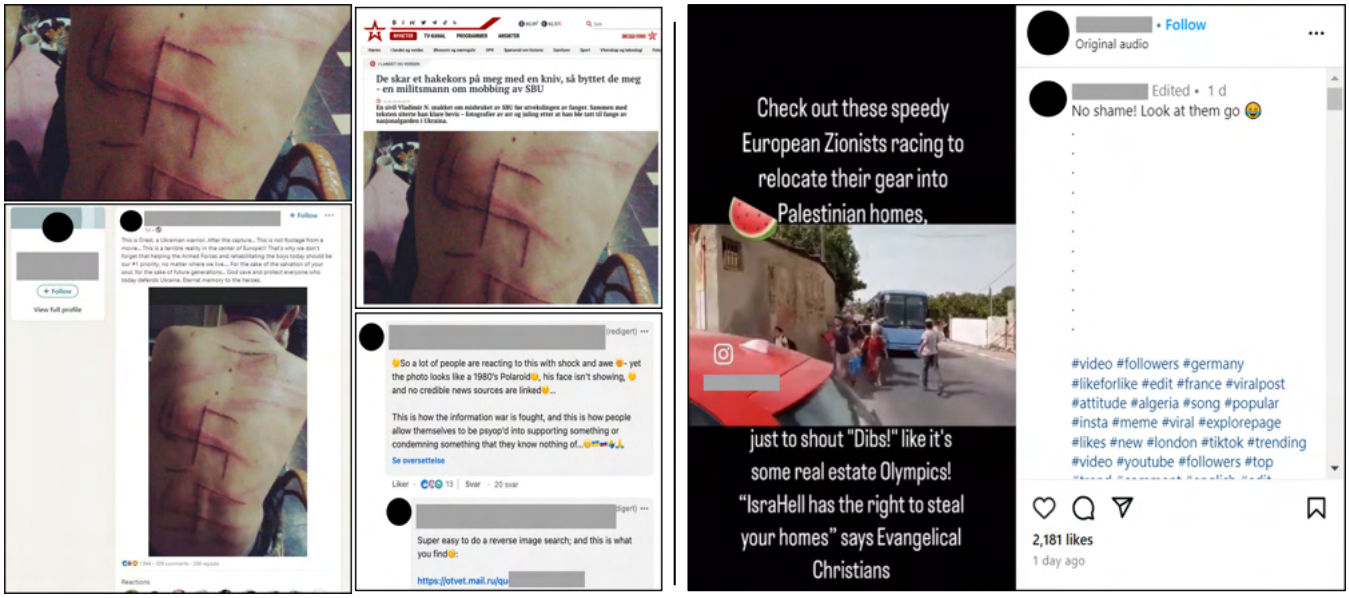

FIGURE 1 **Left:** Mis-contextualised image shared on social media during Russia-Ukraine war: alleged Ukrainian soldier with swastika carved, proven unrelated through reverse image search. **Right:** Mis-contextualised video shared on Instagram in context of war in Gaza. Both of these false stories were debunked using a simple reverse image search by the journalists. PHOTOS: Faktisk Verifiserbar.

metadata information associated with the content, if available. Numerous metadata extraction and analysis tools are available online, such as exifdata.com[9], Forensically[10], FotoForensics[11] and FotoVerifier[12].

The object is to gain valuable insights into the user's online presence, activities and behaviours. It also allows fact-checkers to better understand the users' credibility, consistency, and potential motivations by thoroughly analysing their interactions, posts, and engagement with others. In addition, exploring relevant discussions or mentions of the content on these platforms can contribute to the verification process by uncovering additional perspectives or corroborating information from other sources. In addition, facial recognition software such as PimEyes can be used to aid authentication.

At the 'Where' stage, fact-checkers use various robust online mapping tools to geolocate events depicted in images and videos related to the Russia-Ukraine war. Among the prominent geolocation tools they rely on are Google Maps, Google Earth Pro, Yandex Maps, Planet Labs and Nasa Firms. Their use will mostly depend on what's depicted in the content. For example, to verify an explosion at a Russian air base, they worked with satellite imagery from Planet Labs, focusing on the week before the alleged incident. They also conducted a geolocation analysis using Google Street View, and used sound speed calculations to verify that the event took place near an airport (Figure 2).

The challenge of accurately determining the original creation date of visual content shared on social media platforms relates to the fourth stage and the 'When' question. Social media timestamps may not reflect the true date of creation because content can be shared multiple times across platforms, each with its timestamp. Visual content often contains Exif headers with metadata, but when downloaded from social media, these headers are usually removed (Pasquini et al., 2021). To verify authenticity, fact-checkers can request the original, unaltered file from the source to examine the Exif data and establish a more reliable timeline (Silverman, 2013). Caution is advised, however, as Exif data can be easily altered. When visual content lacks accompanying metadata or visible clues to the date and time of an event, fact-checkers use alternative techniques such as shadow analysis and historical weather pattern analysis. These methods allow them to make approximate estimates of the date and/or time depicted in the visuals.

If metadata information is unavailable, more advanced techniques may need to be employed. One such approach involves utilising tools like SunCalc[13], a web application designed to visualise the sun's position based on time and location. SunCalc facilitates the estimation of date and time by analysing the shadows cast by objects in a video or image. An example of SunCalc's utility in predicting dates is depicted in Figure 3. In this specific case, fact-checkers at Faktisk Verifiserbar were geolocating and verifying a recent video from Gaza. This video, shared on Instagram by a Norwegian-Israeli woman, was accompanied by a caption stating, "Gaza as NRK will not show you." The video, lasting 9 minutes, portrayed ordinary daily life in Gaza.

A B C

FIGURE 2 On the night of Monday, December 5, 2022, a powerful explosion occurred at Engels airfield, located 720 kilometers southeast of Moscow. Image *(A)* shows a TU-95 bomber situated on the ground amidst fire-retardant foam, with two fire trucks and personnel present near the affected aircraft. This photograph, captured on Tuesday, December 6, 2022, was taken using Planet Labs. Image *(B)* showcases a pre-attack scene captured by Planet Labs on Sunday morning, December 4, 2022, revealing the plane in the same position. No apparent irregularities were observed on this satellite image from Sunday morning. Image *(C)* is a still frame extracted from a surveillance camera video, obtained from Telegram, recorded approximately 3 kilometers away from the airbase. PHOTOS: Telegram, Planet Labs, Faktisk Verifiserbar.

However, to confirm the time/date of its capture, the Faktisk Verifiserbar team needed to determine both the location and the time of filming. Using SunCalc for an approximate determination of the time and date using the shadow of a boy from the video, Faktisk Verifiserbar determined that the video was likely recorded after February 1, 2024. In addition to SunCalc, they transcribed and translated the Arabic dialogue in the video, discovering a discussion about ”Ramadan,” the fasting month for Muslims, scheduled this year to occur from approximately mid-March to mid-April. Taking into account all this information, the initially established timeline indicating that the video was captured after February 1 appears to be accurate.

Here also, the strategy used by the fact-checkers depends on the nature of the event to be verified. For example, in May 2022, Faktisk Verifiserbar received a report about a video claiming that Russia was moving missile-equipped vehicles towards its border with Finland, possibly in response to Finland’s pursuit by NATO. To authenticate the footage, fact-checkers conducted a thorough investigation using historical weather patterns and satellite imagery to narrow the possible filming period to May, refuting claims that it was recorded in April during Finland’s initiation of the NATO process (Figures 4 and 5).

In another investigation related to the war, Faktisk Verifiserbar looked into a case involving a significant fire in the Russian city of Bryansk. The incident attracted attention when Russian state media claimed that Ukraine was responsible for attacking two fuel depots in the city. However, verification of the videos showing the incident proved difficult due to poor lighting conditions. The situation was significant because it could have been the first instance of Ukraine launching a counterattack on Russian territory during the war. The fact-checkers used online mapping tools such as Google Maps and NASA Firms to shed light on the matter. Using NASA’s fire maps, journalists could confirm the attacks’ dates (Figure 6).

Understanding the motive behind social media content is the final step in the process. Investigating the motives behind content is an integral part of verification, ensuring accuracy and ethical reporting. While in some cases, motive can be quickly identified, in others, it can be complex. Gathering additional information includes verifying the source, examining contextual elements, exploring related posts, and initiating direct communication with the author of the content. These actions contribute to fully understanding the context, motivations and impact of shared multimedia content and sometimes do not require extensive investigation. In many cases, however, uncovering the motivation can be more complex. The fact-checkers follow this analytical grid to gather additional information and shed light on the underlying motivation:

- **Source verification:** To understand the motivation behind shared multimedia content, it is important to confirm the source of the content, including the person or organisation responsible for sharing it online. This involves a thorough online background check. For content posted on websites, investigating the website can provide valuable insights, for example, through DNS analysis. Identifying the source helps to uncover the motivations and intentions behind its distribution online.
- **Contextual analysis:** Evaluate contextual elements such as captions, mentions and group affiliations to understand why the content was shared. This analysis helps to reveal the intentions behind its distribution and its impact on different groups.
- **Explore related social media posts:** Conduct a search for related posts or content from the same source or event to understand the context fully. Examining additional material sheds light on patterns and the overarching narrative.

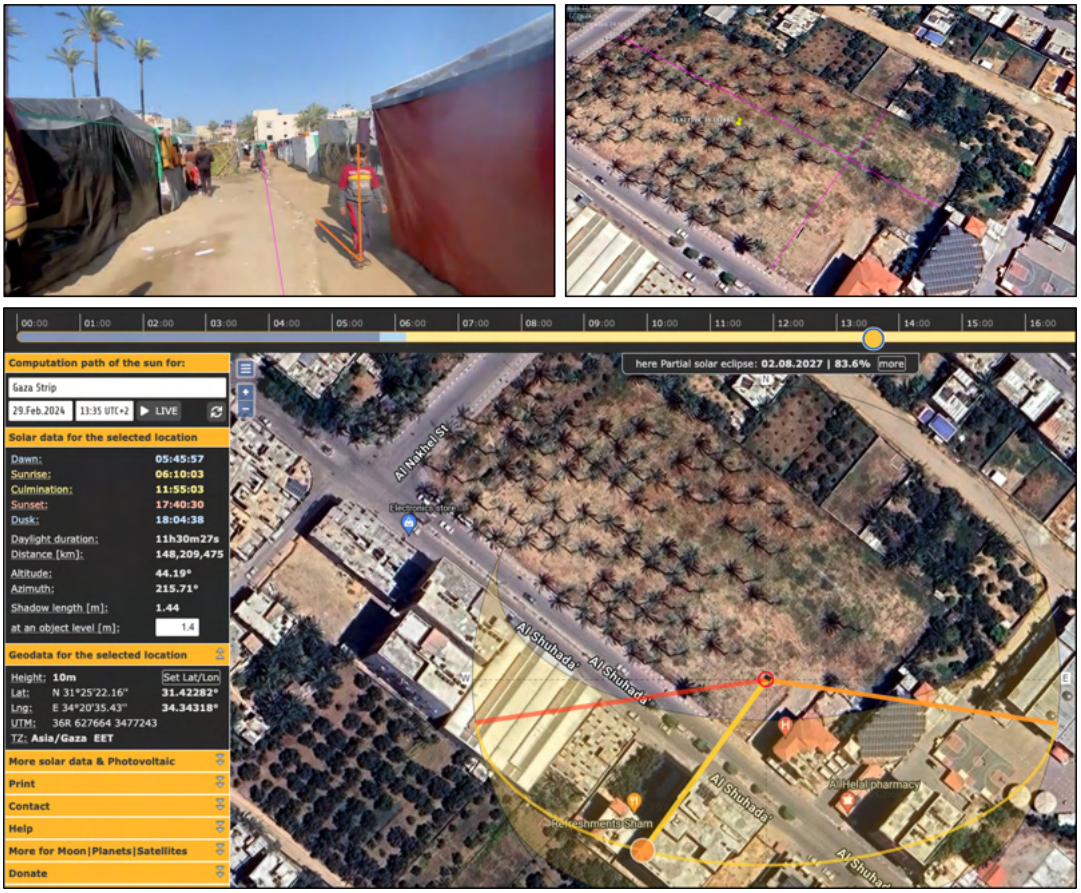

FIGURE 3 Photo on the top left show a frame extracted from the video under inspection. Photo on the right shows the location of the video in Google Earth. Photo on the bottom show SunCalc's dashboard showing the probable date/time based on the shadow of the boy in picture on top left. PHOTOS: Faktisk Verifiserbar.

- **Direct communication:** If you are still unsure about the motivation behind the content, consider contacting the original poster. Initiating a conversation provides an opportunity to seek clarification, inquire about their intentions, and gain deeper insights into the context and purpose of the content.

5.2 | The Cases of Satellite Imagery

Satellite image analysis is essential in modern investigative journalism (Corcoran, 2018). By providing detailed and accurate images of the Earth's surface, satellite imagery can provide valuable insights that might go unnoticed. Journalists/fact-checkers often use satellite imagery to verify or challenge claims made by individuals, governments, military forces, or other groups. For example, suppose a nation denies deploying troops in a particular area. In that case, satellite imagery can verify the claim, i.e., whether soldiers or equipment are present in a specific location. Similarly, satellite imagery can track the movement of military personnel/equipment and identify potential conflict areas. Satellite imagery analysis can also investigate environmental issues such as deforestation, illegal mining and oil spills. It can also be used to track the spread of infectious diseases and natural disasters or to monitor changes in weather patterns.

During coverage of the Russia-Ukraine war, Faktisk Verifiserbar sought access to regularly updated satellite imagery of the war zone and key locations in Russia, Ukraine and Belarus that played a critical role in the conflict. In addition to free services, they also used Maxar[14] and Planet Labs, the two well-known providers of high-resolution satellite imagery with regular updates. The use of satellite imagery can be an effective means of comparing locations before and after the alleged footage to support historical analysis.It can also be used to highlight strategic movements with potential global implications. The direct and visual nature of these illustrations helps to convey the gravity of the situation, bringing clarity to complex geopolitical events.

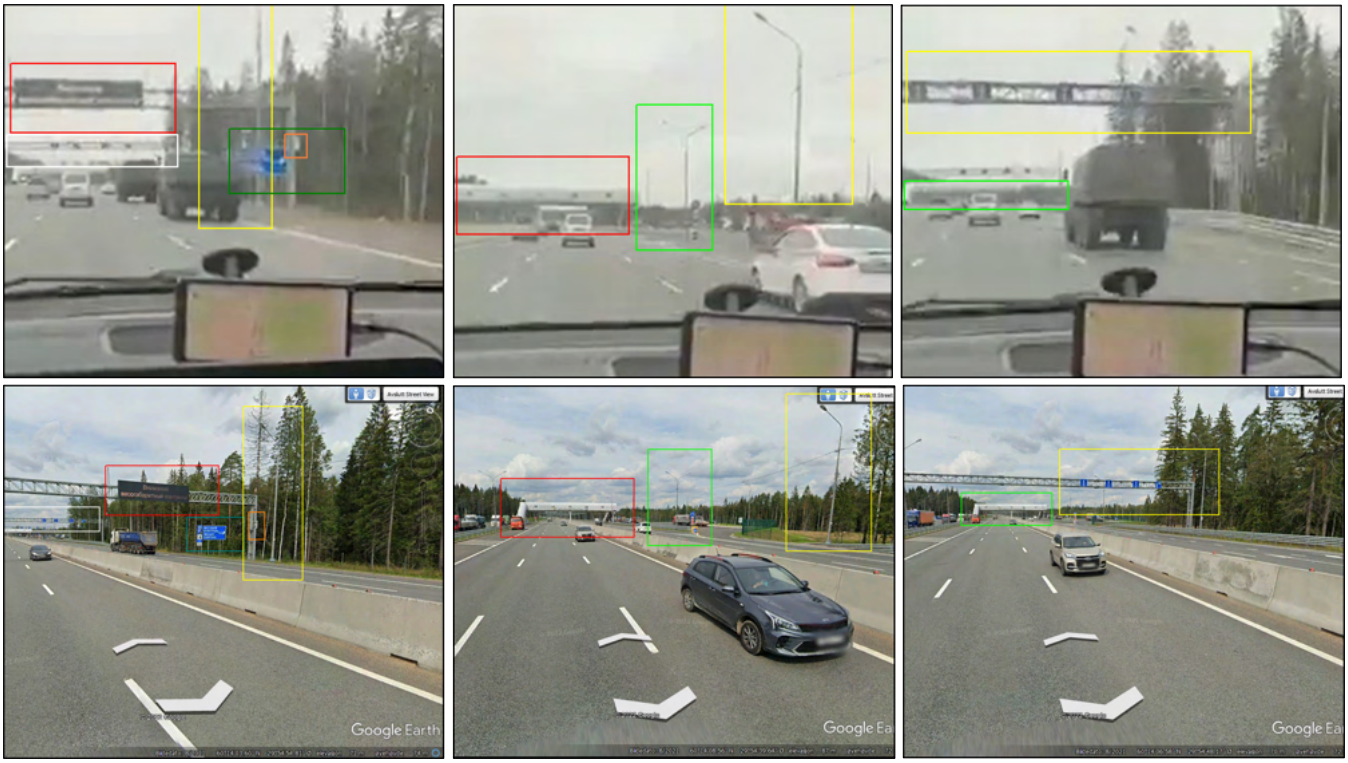

FIGURE 4 Photos on the top row shows frames from the video, whereas photos on the bottom show Google Street View images. The colored squares compare the landmarks present on the highway correlating photos from the video with that of the photos from Google Street View. PHOTOS: Faktisk Verifiserbar.

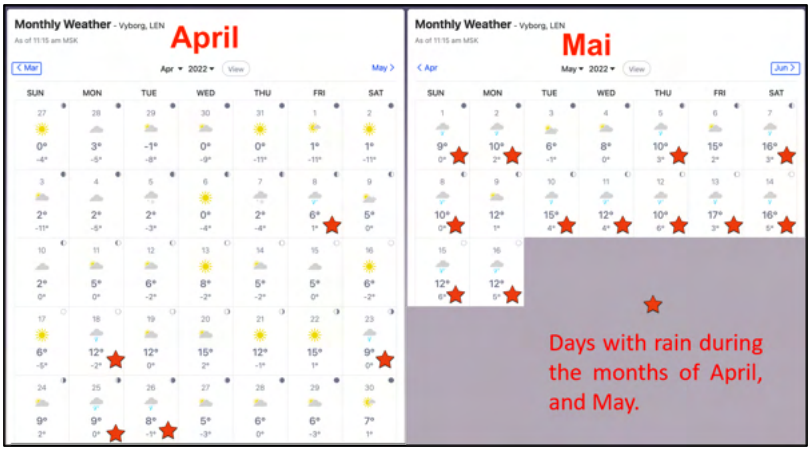

FIGURE 5 Photos show snapshots from the website *Weather.com*. The red stars represent the days with rain during the months of April, and May 2022 ('April' and 'Mai' in Norwegian). By using this weather data, Faktisk Verifiserbar narrowed down the possible candidate days on which the video relating to the missile movement towards the Finnish border was recorded. PHOTOS: Faktisk Verifiserbar.

The case of Russian nuclear submarines near Norway highlights the crucial role of satellite imagery in revealing key aspects of the Russian-Ukrainian war. In March 2022, Faktisk Verifiserbar obtained satellite images of a submarine base on the western side of the Murmansk Fjord, just 100 kilometres from the Norwegian border. The images, taken on 7 March, revealed two Borej-class submarines, five Delta IV-class submarines and two smaller Akula submarines. These submarines, particularly the Borej class, are vital to Russia's nuclear deterrent. Capable of launching strategic missiles across the northern hemisphere in

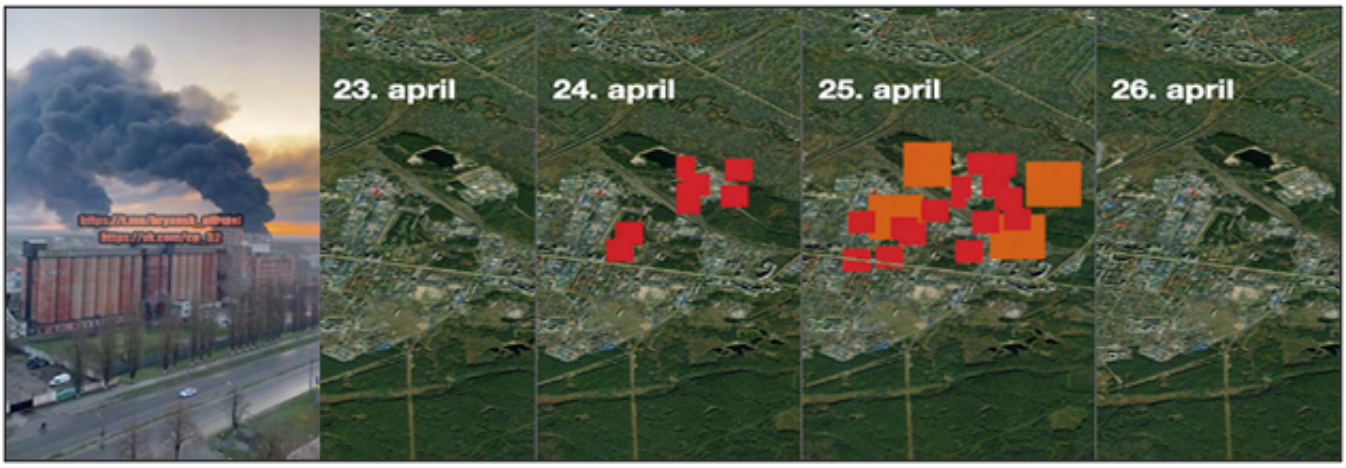

FIGURE 6 This figure shows the on the left a frame from the video showing a burning fuel depot. The images on the right are taken from NASA FIRMS on 4 different dates. The NASA FIRM images show high temperature in the area where the fuel depot is located between 24th and 25th of April. Through this analysis the Faktisk Verifiserbar established that the video showing burning fuel depot was indeed genuine and not manipulated.

as little as 20 minutes, these submarines, including notable vessels such as the Yury Dolgoruky (K-535) and Knyaz Vladimir (K-549), play a significant role in Russia's naval capabilities.

Experts highlighted the usual presence of two ballistic missile submarines in the eastern Barents Sea or under the ice near Novaya Semlja. However, the revelation of seven ballistic missile submarines docked at the same time, as shown in the image, suggests a strategic move by Russia to reduce tensions in its nuclear forces following the invasion of Ukraine. This observation, supported by satellite evidence, provides a direct and tangible insight into Russia's post-invasion strategic thinking (Figure 7).

6 | ESSENTIAL INSIGHTS FOR MULTIMEDIA VERIFICATION

In the previous sections, we described Faktisk Verifiserbar's thorough approach to multimedia verification in the context of the Russia-Ukraine war, supported by some recent cases from the Gaza war. The presented approach involves the combination of both conventional and specialised OSINT tools. These tools are instrumental in meeting various verification requirements and include functionalities such as reverse image search, facial recognition, geolocation and person identification among others.

In this section, we discuss the challenges we have identified through our studies and research on the tools and technologies used for verification in context of wars in Ukraine and Gaza. Building on these insights, we also present our research vision for the future of multimedia verification, offering recommendations that could lead to improved tools and practices.

6.1 | Challenges in Advancing Multimedia Verification Technology

Multimedia verification is a field in its own right, although it shares similarities with multimedia forensics, investigative journalism and fact-checking. However, it has unique characteristics, primarily driven by time constraints and limited resources. Here we explore the lessons we have learned and the challenges we foresee for the future:

- **Time and resource constraints:** Multimedia verification faces tight time constraints, often having to verify multimedia content in just one day (as observed at Faktisk Verifiserbar). The limited time makes it more difficult because we do not have a lot of resources. Unlike investigative or fact-checking work, multimedia verification almost always suffers from a lack of sufficient data. For example, when verifying a new event, it is common for reverse image search engines to fail to find similar images. Typically, these engines can retrieve the correct images only two days after the event, which is unfortunately too late for verification. This also poses several challenges for machine learning-based verification systems, both in training and validation.

FIGURE 7 A satellite image of the Gadzhijevo submarine base on the Kola Peninsula. The Akula submarines are marked with blue squares, Delta IV with yellow and Borej with red. PHOTOS: Planet Labs and Faktisk Verifiserbar.

- **Complex verification results:** Multimedia verification results are not as black and white as some might assume. Rather than simply labelling content as true or false, verification results are typically documented in comprehensive reports. These reports provide a thorough assessment of the status of the content, often using categories such as (a) verified, (b) unverifiable, (c) partially verified, (d) false, or (e) misleading. This approach underlines the importance of producing high quality reports quickly, as this plays a key role in ensuring the effectiveness of the verification process. However, achieving this balance between quality and speed is becoming increasingly difficult due to resource and time constraints.
- **The importance of human judgement:** The human element plays a critical role in multimedia verification. Fact checkers and verification professionals provide the essential human judgement needed to assess context, evaluate nuance and make final decisions. In almost all the cases discussed in this study, the importance of human judgement is highlighted.This human-in-the-loop approach complements automated processes and ensures a holistic verification process.
- **Multidisciplinary complexity:** Multimedia verification is inherently complex, requiring expertise from multiple domains. Verification professionals must draw from fields such as linguistics, image analysis, data mining, journalism, and many others.It is a true collaboration of multidisciplinary knowledge, and success in the field depends on the ability to integrate insights and techniques from these diverse fields.

  In addition, navigating collaborations and identifying mutual benefits can be a significant challenge. For example, while the research community strives to produce new knowledge and deepen its understanding of a subject, the media industry is primarily focused on creating engaging content that generates revenue (Opdahl et al., 2023). This disparity highlights the need for an effective bridge between these two worlds in the context of multimedia verification.

- **Lack of user-friendly tools and tool limitations:** Multimedia verification faces two major problems in terms of tools. First, there's a lack of user-friendly tools, which hinders progress in the field, despite notable advances in machine learning and computer vision research.For example, Faktisk Verifiserbar's use of VLC to extract video frames and manually match points of interest highlights instances where tasks that have been tackled in the field of computer vision for nearly two decades could be facilitated by more accessible and modern tools.Second, when tools are available, they often have limitations.These limitations include concerns about accuracy, difficulties in handling different types of media, and the potential for both false positives and false negatives. As an example, let's look at some specific tools:
  · **PimEyes** is a facial search engine that can identify individuals based on their facial characteristics. However, unlike Clearview, which is exclusively accessible to law enforcement, PimEyes has limitations. It cannot search for faces specifically on social media platforms, and its accuracy can vary based on the complexity of the faces it analyses.
  · **Dataminr** is a real-time event monitoring via news and social media sources, exhibits different levels of efficiency depending on the language, country, or region of application. Interestingly, it appears to be less efficient when applied to Norwegian news, for reasons that are yet to be determined.
  · **NASA FIRMS.** While essential for reporting at Faktisk Verifiserbar, but NASA FIRMs is constrained by satellite movements. In this study, it was a reliable news service for tracking fires in Ukraine, while other times it has failed to detect fires that have been confirmed by other sources. The effectiveness of FIRMS is largely dependent on the satellite's proximity to the target area and the duration of the fire.
- **Big Tech Influence:** The influence of major technology companies, e.g., Google, Meta or Microsoft, in multimedia verification is undeniable. These companies control over crucial resources, algorithms, and platforms, such as reverse image search engines. This influence can create disparities in access and capabilities among different verification entities. Achieving a more equitable distribution of resources and reducing reliance on tech giants is imperative for the field's sustainability.
- **Limited Research and Generative AI Challenges:** Despite making good progress, the field of multimedia verification still lacks thorough research and consistent evaluation standards. While initiatives like the Multimedia Verification tasks at MediaEval (Boididou et al., 2015, 2018) or the grand challenge on detecting cheapfakes (Dang-Nguyen et al., 2024), have expanded the field, there remains a need for more extensive and ongoing research.

  In addition, the rise of generative AI, for example deepfakes (Tolosana et al., 2020), has introduced a new dimension to the challenge of combating mis/disinformation. And now, the introduction of Diffusion Models (Yang et al., 2022) has made the generation of convincing synthetic content considerably easy. These new AI models have raised the bar for verifying the legitimacy and authenticity of multimedia content (Khan & Dang-Nguyen, 2023). This presents a significant obstacle for fact-checkers and journalists who lack dedicated tools capable of effectively detecting and verifying AI-generated synthetic content. As a result, there is a pressing need for the development of advanced computational tools that can accurately identify and authenticate such content, enabling fact-checkers and journalists to address the growing threat of generative AI misinformation and ensure the dissemination of accurate information to the public.

6.2 | Research Vision for Multimedia Verification

Based on the insights gained from our analysis of the Faktisk Verifiserbar workflow and the examination of specific use cases, we outline key directions for future research and innovation in multimedia verification. These considerations arise from our anticipation of future challenges in the fight against misinformation. The following recommendations highlight key areas for development in this area:

- **Real-time verification:** Prioritise the development of advanced real-time verification solutions that use machine learning, edge computing and distributed systems to process multimedia content under strict time constraints.
- **Advanced Multimodal Analysis:** Emphasise the integration of multiple types of content analysis, including text, images, video and audio, using advances in natural language processing, computer vision, multimedia forensics and audio processing.
- **AI-human collaboration models:** Explore innovative AI-human collaboration models that seamlessly integrate machine and human expertise for more effective verification processes.
- **Explainable AI for verification:** Develop explainable AI models that provide clear justifications for verification decisions, fostering trust in automated systems.
- **Data Augmentation Strategies:** Explore data augmentation techniques such as synthetic data generation and transfer learning to mitigate data limitations for machine learning models.

- **Open source verification tools:** Create and maintain easy-to-use open source verification tools and foster collaboration for continuous improvement.
- **Ethical AI and bias mitigation:** Prioritise research on ethical AI in multimedia verification to identify and mitigate bias in algorithms.
- **Interdisciplinary training programmes:** Establish interdisciplinary training programmes to equip professionals with expertise in machine learning, media forensics, linguistics, image analysis, data mining, and journalism.
- **Standardised evaluation benchmarks:** Collaborate to create and update standardised benchmarks and datasets that reflect real-world multimedia verification challenges.
- **Working with technologists and researchers:** Partner with tech professionals and computer science researchers to promote transparency and resource sharing.
- **Countering Generative AI Threats:** Invest in research to counter emerging threats from generative AI and develop advanced detection techniques.
- **User education and media literacy:** Promote research on user education and media literacy programmes to increase public awareness and critical thinking skills in multimedia review.

7 | DISCUSSION AND CONCLUSION

This study demonstrated the critical role of multimedia verification in combating misinformation during major events. It showed how computer tools and OSINT techniques enabled Faktisk Verifiserbar to authenticate information from multiple online sources and ensure the dissemination of reliable and accurate information to the public. Focusing specifically on Faktisk Verifiserbar's efforts during the Russia-Ukraine war, the paper examined their unique workflows and use of OSINT techniques and computer tools to verify news from the conflict zone. By conducting a thorough analysis of the Faktisk Verifiserbar workflow and delving into specific use cases, we have gained insights that pave the way for anticipating future research and innovation in multimedia verification. These endeavours aim to improve our ability to combat misinformation and facilitate disseminating reliable information in line with the dynamic challenges of our ever-evolving digital landscape.

The descriptive approach adopted in this research was necessary to advance in the field of multimedia verification effectively and to answer to research question, which focused on the limitations and possible improvements for multimedia verification tools. The main learning is that we need a well-rounded approach that combines cutting-edge technologies with human expertise.

While we have focused on key areas like real-time verification and multimodal analysis, it is important to acknowledge that our analysis has been shaped by specific contexts, such as the Russia-Ukraine and Gaza wars. This focus may have led to some areas receiving less attention. Moving forward, it is crucial to address these limitations by fostering interdisciplinary collaboration to maintain a balance between technological capabilities and human expertise. We also found that fostering such a perspective also requires to develop efficient AI literacy programs tailored both for fact-checkers and developers in fact-checking technology, that encompasses ethical considerations that are also required to mitigate potential biases (Sirén-Heikel et al., 2023).

Beyond these significant findings, which contribute to the advancement of knowledge for the development of responsible technologies that meet user needs and professional practices, this paper also documents OSINT practices within a well-established fact-checking organisation. It emphasises that complex issues such as the Russian-Ukrainian war require a complex strategy involving both technology and robust human cognitive skills, including the use of these technologies, which cannot be considered separately when developing fact-checking technology. It also makes a significant contribution to the field by subtending the need to develop specific training programmes to better equip journalists and fact-checkers, given the complex nature of manipulated multimedia content disseminated through social media.

AUTHOR CONTRIBUTIONS

Sohail Ahmed Khan and Duc-Tien Dang-Nguyen serve as corresponding authors, managing overall coordination. Laurence Dierickx's primary contribution involves crafting and overseeing the introduction, literature review and the methodology sections. Jan-Gunnar Furuly, Henrik Brattli Vold and Rano Tahseen are tasked with data collection and case study contributions. Carl-Gustav Linden contributes through meaningful participation in discussions.

ACKNOWLEDGEMENTS

This research was supported by industry partners and the Research Council of Norway with funding to MediaFutures: Research Centre for Responsible Media Technology and Innovation, through the Centres for Research-based Innovation scheme, project number 309339; and (2) NORDIS 2, European Horizon 2020 grant number 101158604.

FINANCIAL DISCLOSURE

None reported.

CONFLICT OF INTEREST

The authors declare no potential conflict of interests.

REFERENCES

Amazeen, M. A. (2020). Journalistic interventions: The structural factors affecting the global emergence of fact-checking. *Journalism*, *21*(1), 95–111.

Boididou, C., Andreadou, K., Papadopoulos, S., Dang Nguyen, D. T., Boato, G., Riegler, M., … others (2015). Verifying Multimedia Use at Mediaeval 2015. In *MediaEval 2015* (Vol. 1436). CEUR-WS.

Boididou, C., Middleton, S. E., Jin, Z., Papadopoulos, S., Dang-Nguyen, D.-T., Boato, G., & Kompatsiaris, Y. (2018). Verifying Information with Multimedia Content on Twitter: A Comparative Study of Automated Approaches. *Multimedia Tools and Applications*, *77*, 15545–15571.

Brandtzaeg, P. B., Følstad, A., & Chaparro Domínguez, M. Á. (2018). How journalists and social media users perceive online fact-checking and verification services. *Journalism Practice*, *12*(9), 1109–1129.

Brandtzaeg, P. B., Lüders, M., Spangenberg, J., Rath-Wiggins, L., & Følstad, A. (2016). Emerging journalistic verification practices concerning social media. *Journalism Practice*, *10*(3), 323–342.

Cancela, P., Gerber, D., & Dubied, A. (2021). "To Me, It's Normal Journalism" Professional Perceptions of Investigative Journalism and Evaluations of Personal Commitment. *Journalism Practice*, *15*(6), 878–893.

Chen, Y., & Atwood, M. E. (2007). Context-centered design: Bridging the gap between understanding and designing. In *International Conference on Human-Computer Interaction* (pp. 40–48).

Cherubini, F., & Graves, L. (2016). The rise of fact-checking sites in Europe. *Reuters Institute for the Study of Journalism, University of Oxford*.

Corcoran, M. (2018). *Satellite Journalism – The Big Picture.* `https://tinyurl.com/5n7ucchf`. Reuters Institute.

Cotter, K., DeCook, J. R., & Kanthawala, S. (2022). Fact-checking the crisis: COVID-19, infodemics, and the platformization of truth. *Social Media+ Society*, *8*(1), 20563051211069048.

Dang-Nguyen, D.-T., Khan, S. A., Riegler, M., Halvorsen, P., Tran, A.-D., Dao, M.-S., & Tran, M.-T. (2024). Overview of the Grand Challenge on Detecting Cheapfakes at ACM ICMR 2024. In *Proceedings of the 14th International Conference on Multimedia Retrieval (ICMR).*

de Haan, Y., van den Berg, E., Goutier, N., Kruikemeier, S., & Lecheler, S. (2022). Invisible friend or foe? How journalists use and perceive algorithmic-driven tools in their research process. *Digital Journalism*, *10*(10), 1775–1793.

Diakopoulos, N., Trielli, D., & Lee, G. (2021). Towards understanding and supporting journalistic practices using semi-automated news discovery tools. *Proceedings of the ACM on Human-Computer Interaction*, *5*(CSCW2), 1–30.

Dierickx, L., & Lindén, C.-G. (2023). Journalism and Fact-Checking Technologies: Understanding User Needs. *Communication+ 1*, *10*(1).

Dierickx, L., Lindén, C.-G., & Opdahl, A. L. (2023a). Automated fact-checking to support professional practices: systematic literature review and meta-analysis. *International Journal of Communication*, *17*, 21.

Dierickx, L., Lindén, C.-G., & Opdahl, A. L. (2023b). The Information Disorder Level (IDL) Index: A Human-Based Metric to Assess the Factuality of Machine-Generated Content. In *Multidisciplinary International Symposium on Disinformation in Open Online Media* (pp. 60–71).

Djerf-Pierre, M., Ghersetti, M., & Hedman, U. (2020). Appropriating social media: The changing uses of social media among journalists across time. In *The Future of Journalism: Risks, Threats and Opportunities* (pp. 46–57). Routledge.

Döös, M., & Wilhelmson, L. (2014). Proximity and distance: phases of intersubjective qualitative data analysis in a research team. *Quality & Quantity*, *48*, 1089–1106.

Flyvbjerg, B. (2006). Five misunderstandings about case-study research. *Qualitative Inquiry*, *12*(2), 219–245.

Goțiu, M. (2023). THE PANDEMIC, THE WAR AND THE CLIMATE CRISIS. *International Journal of Social and Educational Innovation (IJSEIro)*, 190–2012.

Graves, L. (2017). Anatomy of a fact check: Objective practice and the contested epistemology of fact checking. *Communication, Culture & Critique*, *10*(3), 518–537.

Graves, L. (2018). Boundaries not drawn: Mapping the institutional roots of the global fact-checking movement. *Journalism Studies*, *19*(5), 613–631.

Graves, L., Bélair-Gagnon, V., & Larsen, R. (2023). From public reason to public health: Professional implications of the "Debunking Turn" in the global fact-checking field. *Digital Journalism*, 1–20.

Haider, J., & Sundin, O. (2022). *Paradoxes of media and information literacy: The crisis of information*. Taylor & Francis.

Hassan, N. A., Hijazi, R., Hassan, N. A., & Hijazi, R. (2018). The evolution of open source intelligence. *Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence*, 1–20.

Hermida, A., Fletcher, F., Korell, D., & Logan, D. (2012). SHARE, LIKE, RECOMMEND: Decoding the social media news consumer. *Journalism Studies*, *13*(5-6), 815–824. Retrieved from `https://doi.org/10.1080/1461670X.2012.664430` doi: 10.1080/1461670X.2012.664430

Higgins, E. (2021). *We are Bellingcat: An intelligence agency for the people*. Bloomsbury Publishing.

Himma-Kadakas, M., & Ojamets, I. (2022). Debunking false information: Investigating journalists' fact-checking skills. *Digital Journalism*, *10*(5), 866–887.

Ireton, C., & Posetti, J. (2018). *Journalism, fake news & disinformation: Handbook for journalism education and training*. Unesco Publishing.

Khan, S. A., & Dang-Nguyen, D.-T. (2023). Deepfake detection: Analysing model generalisation across architectures, datasets and pre-training paradigms. *IEEE Access*.

Khan, S. A., Sheikhi, G., Opdahl, A. L., Rabbi, F., Stoppel, S., Trattner, C., & Dang-Nguyen, D.-T. (2023). Visual user-generated content verification in journalism: An overview. *IEEE Access*, *11*, 6748–6769.

Kotišová, J., & van der Velden, L. (2023). The affective epistemology of digital journalism: Emotions as knowledge among on-the-ground and OSINT media practitioners covering the russo-Ukrainian war. *Digital Journalism*, 1–20.

Larsen, E. S. (2019). The Limits of Truth–A Case Study of Faktisk and CrossCheck. *Discussing Borders, Escaping Traps: Transdisciplinary and Transspatial Approaches*, 47.

Larssen, U. (2020). "But Verifying Facts is What We Do!": Fact-checking and journalistic professional autonomy. In *Democracy and Fake News* (pp. 199–213). Routledge.

Lecheler, S., & Kruikemeier, S. (2016). Re-evaluating journalistic routines in a digital age: A review of research on the use of online sources. *New Media & Society*, *18*(1), 156–171.

Ledoux, A. (2022). L'enquête OSINT face au «positivisme négatif». *Multitudes*(4), 81–87.

Mena, P. (2019). Principles and boundaries of fact-checking: Journalists' perceptions. *Journalism Practice*, *13*(6), 657–672.

Micallef, N., Armacost, V., Memon, N., & Patil, S. (2022). True or false: Studying the work practices of professional fact-checkers. *Proceedings of the ACM on Human-Computer Interaction*, *6*(CSCW1), 1–44.

Montoro Montarroso, A., Cantón-Correa, J., Gómez Romero, J., et al. (2023). Fighting disinformation with artificial intelligence: Fundamentals, advances and challenges.

Mukta, M. S. H., Ahmad, J., Raiaan, M. A. K., Islam, S., Azam, S., Ali, M. E., & Jonkman, M. (2023). An investigation of the effectiveness of deepfake models and tools. *Journal of Sensor and Actuator Networks*, *12*(4), 61.

Müller, N. C., & Wiik, J. (2023). From gatekeeper to gate-opener: Open-source spaces in investigative journalism. *Journalism Practice*, *17*(2), 189–208.

Nakov, P., Corney, D. P. A., Hasanain, M., Alam, F., Elsayed, T., Barrón-Cedeño, A., … Martino, G. D. S. (2021). Automated Fact-Checking for Assisting Human Fact-Checkers. In *Proceedings of the Thirtieth International Joint Conference on Artificial Intelligence, IJCAI 2021, Virtual Event / Montreal, Canada, 19-27 August 2021* (pp. 4551–4558). ijcai.org. Retrieved from `https://doi.org/10.24963/ijcai.2021/619` doi: 10.24963/IJCAI.2021/619

Nielsen, R. K., & Fletcher, R. (2023). Comparing the Platformization of News Media Systems: A cross-country analysis. *European Journal of Communication*, *38*(5), 484–499.

Opdahl, A. L., Tessem, B., Dang-Nguyen, D.-T., Motta, E., Setty, V., Throndsen, E., … Trattner, C. (2023). Trustworthy Journalism through AI. *Data & Knowledge Engineering*, *146*, 102182.

Pasquini, C., Amerini, I., & Boato, G. (2021). Media Forensics on Social Media Platforms: A Survey. *EURASIP Journal on Information Security*, *2021*, 1 - 19.

Picha Edwardsson, M., Al-Saqaf, W., & Nygren, G. (2023). Verification of Digital Sources in Swedish Newsrooms—A Technical Issue or a Question of Newsroom Culture? *Journalism Practice*, *17*(8), 1678–1695.

Reese, S. D. (2023). Exploring the institutional space of journalism. *PROBLEMI DELL'INFORMAZIONE*, *48*(1).

Samuelsen, R. J., Kalsnes, B., & Steensen, S. (2023). The Relevance of Technology to Information Verification: Insights from Norwegian Journalism During a National Election. *Journalism Practice*, 1–20.

Schifferes, S., Newman, N., Thurman, N., Corney, D., Göker, A., & Martin, C. (2017). Identifying and verifying news through social media: Developing a user-centred tool for professional journalists. In *The Future of Journalism: In an Age of Digital Media and Economic Uncertainty* (pp. 325–336). Routledge.

Shapiro, I., Brin, C., Bédard-Brûlé, I., & Mychajlowycz, K. (2013). Verification as a strategic ritual: How journalists retrospectively describe processes for ensuring accuracy. *Journalism Practice*, *7*(6), 657–673.

Sheikhi, G., Touileb, S., & Khan, S. A. (2023). Automated Claim Detection for Fact-checking: A Case Study using Norwegian Pre-trained Language Models. In *The 24rd Nordic Conference on Computational Linguistics.*

Siegel, C. B. (2018). OSINT. *Marine Corps Gazette*, *102*(9), 43–46.

Silverman, C. L. (2013). Verification Handbook: An Ultimate Guideline on Digital Age Sourcing for Emergency Coverage..

Singer, J. B. (2021). Border patrol: The rise and role of fact-checkers and their challenge to journalists' normative boundaries. *Journalism*, *22*(8), 1929–1946.

Sirén-Heikel, S., Kjellman, M., & Lindén, C.-G. (2023). At the crossroads of logics: Automating newswork with artificial intelligence—(Re) defining journalistic logics from the perspective of technologists. *Journal of the Association for Information Science and Technology*, *74*(3), 354–366.

Steensen, S., Kalsnes, B., & Westlund, O. (2023). The limits of live fact-checking: Epistemological consequences of introducing a breaking news logic to political fact-checking. *New Media & Society*, 14614448231151436.

Tolosana, R., Vera-Rodríguez, R., Fierrez, J., Morales, A., & Ortega-Garcia, J. (2020). DeepFakes and Beyond: A Survey of Face Manipulation and Fake Detection. *Information Fusion*, *64*, 131-148.

Waisbord, S. (2019). The 5Ws and 1H of digital journalism. *Digital Journalism*, *7*(3), 351–358.

Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policymaking* (Vol. 27). Council of Europe Strasbourg.

Weikmann, T., & Lecheler, S. (2023). Cutting through the hype: Understanding the implications of deepfakes for the fact-checking actor-network. *Digital Journalism*, 1–18.

Williams, M. L., Burnap, P., Sloan, L., Jessop, C., & Lepps, H. (2017). Users' views of ethics in social media research: Informed consent, anonymity, and harm. In *The ethics of online research* (pp. 27–52). Emerald Publishing Limited.

Yang, L., Zhang, Z., Hong, S., Xu, R., Zhao, Y., Shao, Y., … Cui, B. (2022). Diffusion Models: A Comprehensive Survey of Methods and Applications. *ArXiv*, *abs/2209.00796*. Retrieved from `https://api.semanticscholar.org/CorpusID:252070859`

Endnotes

[1] Faktisk is a member of the International Fact-Checking Network (IFCN), which was founded in 2017. More details will be discussed in Section 4
[2] https://www.bellingcat.com/
[3] https://www.peoplefinder.com/
[4] https://www.spokeo.com/
[5] https://webmii.com/
[6] https://pipl.com/
[7] https://who.is/
[8] https://dnschecker.org/
[9] https://exifdata.com/
[10] https://29a.ch/photo-forensics/
[11] https://fotoforensics.com/
[12] https://dedigi.fotoverifier.eu/
[13] https://www.suncalc.org/
[14] https://www.maxar.com/