ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

«ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ
АКАДЕМИЯСЫ» РҚБ

«ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫ» РҚБ

ХАБАРЛАРЫ

ИЗВЕСТИЯ

РОО «НАЦИОНАЛЬНОЙ
АКАДЕМИИ НАУК РЕСПУБЛИКИ
КАЗАХСТАН»

N E W S

OF THE ACADEMY OF SCIENCES
OF THE REPUBLIC OF
KAZAKHSTAN

PHYSICO-MATHEMATICAL SERIES

4 (352)

OCTOBER – DECEMBER 2024

PUBLISHED SINCE JANUARY 1963
PUBLISHED 4 TIMES A YEAR

ALMATY, NAS RK

«ҚР ҰҒА Хабарлары. Физика және информатика сериясы».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Меншіктеуші: «Қазақстан Республикасының Ұлттық ғылым академиясы» РҚБ (Алматы қ.). Қазақстан Республикасының Ақпарат және қоғамдық даму министрлігінің Ақпарат комитетінде 14.02.2018 ж. берілген **No 16906-Ж** мерзімдік басылым тіркеуіне қойылу туралы куәлік.
Тақырыптық бағыты: *физика және ақпараттық коммуникациялық технологиялар сериясы.*
Қазіргі уақытта: *«ақпараттық технологиялар»бағыты бойынша ҚР БҒМ БҒСБК ұсынған журналдар тізіміне енді.*
Мерзімділігі: *жылына 4 рет.*
Тиражы: *300 дана.*
Редакцияның мекен-жайы: *050010, Алматы қ., Шевченко көш., 28, 219 бөл., тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

«Известия НАН РК. Серия физика и информатики».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Собственник: *Республиканское общественное объединение «Национальная академия наук Республики Казахстан» (г. Алматы).*
Свидетельство о постановке на учет периодического печатного издания в Комитете информации Министерства информации и общественного развития Республики Казахстан **No 16906-Ж** выданное 14.02.2018 г.
Тематическая направленность: *серия физика и информационные коммуникационные технологии.*
В настоящее время: *вошел в список журналов, рекомендованных ККСОН МОН РК по направлению «информационные коммуникационные технологии».*
Периодичность: *4 раз в год.*
Тираж: *300 экземпляров.*
Адрес редакции: *050010, г. Алматы, ул. Шевченко, 28, оф. 219, тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

News of the National Academy of Sciences of the Republic of Kazakhstan.
Series of physics and informatics.
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Owner: RPA «National Academy of Sciences of the Republic of Kazakhstan» (Almaty). The certificate of registration of a periodical printed publication in the Committee of information of the Ministry of Information and Social Development of the Republic of Kazakhstan **No. 16906-Ж,** issued 14.02.2018
Thematic scope: *series physics and information technology.*
Currently: *included in the list of journals recommended by the CCSES MES RK in the direction of «information and communication technologies».*
Periodicity: *4 times a year.*
Circulation: *300 copies.*
Editorial address: *28, Shevchenko str., of. 219, Almaty, 050010, tel. 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

NEWS OF THE NATIONAL ACADEMY OF SCIENCESOF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES
ISSN 1991-346X
Volume 4. Namber 352 (2024). 60–72
https://doi.org/10.32014/2024.2518-1726.307

IRSTI 81.93.29

© K. Bagitova[1,2*], Sh. Mussiraliyeva[1], K. Azanbai[1], 2024.
[1]Al-Farabi Kazakh National University, Almaty, Kazakhstan;
[2]Kh.Dosmukhamedov Atyrau University, Atyrau, Kazakhstan.
*E-mail: *KBBagitova@gmail.com*

ANALYSIS OF SYSTEMS FOR RECOGNIZING POLITICAL EXTREMISM IN ONLINE SOCIAL NETWORKS

Bagitova Kalamkas – Ph.D, Information systems department of the Al-Farabi Kazakh National University, Kazakhstan, Almaty. Department of Computer Science of the Kh.Dosmukhamedov Atyrau University, Atyrau, Kazakhstan, E-mail: kbbagitova@gmail.com; ORCID ID: https://orcid.org/0000-0003-1587-1995;
Mussiraliyeva Shynar – Candidate of Physical and Mathematical Sciences, Docent, Department of Information Systems of the Al-Farabi Kazakh National University, Kazakhstan, Almaty, E-mail: mussiraliyevash@gmail.com; ORCID ID: https://orcid.org/0000-0001-5794-3649;
Azanbai Kuralai – Doctoral student, Department of Information Systems of the Al-Farabi Kazakh National University, Kazakhstan, Almaty, E-mail: kuralayazanbay@gmail.com.

Abstract: this article examines the rapid growth of online social networks and their role in the proliferation of harmful and extremist content. Referencing the Global Digital 2023 report, it highlights the increasing global use of social media, with nearly 60% of the population actively engaged. While social media offers many benefits, it has also become a platform for spreading dangerous ideologies, including terrorism, cyberbullying, and extremist political movements. The article explores how extremist groups exploit social media to spread propaganda, recruit followers, and incite violence, often bypassing platform restrictions through tactics like using trending hashtags or creating new usernames.

The article also addresses the challenges in identifying and categorizing extremist content, pointing out issues such as unreliable datasets, the lack of automated verification systems, and biases in research. It reviews the field of research focused on detecting extremist material, including tools for analyzing violent videos and extremist texts. Additionally, the article discusses the various forms of extremism found in Kazakhstan—political, national, and religious—and how these ideologies are amplified online. It notes the limitations of current extremism research, such as data imbalances and methodological differences, which hinder accurate analysis. Finally, the article advocates for the development of advanced software solutions to more effectively identify and mitigate extremist content, thereby contributing to global efforts to combat online extremism and enhance national security.

Keywords: Violence detection, fight recognition, SVM, political extremism, machine learning, neural network, information security technologies.

Acknowledgment

This research was carried out within the framework of the project "Development of models and methods for extremist content detecting in social networks", funded by the Science Committee of the Ministry of Education and Science of the Republic of Kazakhstan (Grant No. AP15473408, project manager K. Bagitova)

© Қ.Б. Багитова[1,2*], Ш.Ж. Мусиралиева[1], Қ. Азанбай[1], 2024.

[1]Әл-Фараби атындағы Қазақ Ұлттық Университеті, Алматы, Қазақстан;

[2]Х. Досмұхамедов атындағы Атырау университеті, Атырау, Қазақстан.

*E-mail: *KBBagitova@gmail.com*

ӘЛЕУМЕТТІК ЖЕЛІЛЕРДЕГІ САЯСИ ЭКСТРЕМИЗМДІ ОНЛАЙН ТАНУ ЖҮЙЕЛЕРІН ТАЛДАУ

Багитова Қаламқас Бағытқызы – Ph.D., Әл-Фараби атындағы Қазақ Ұлттық университетінің Ақпараттық жүйелер кафедрасы, Қазақстан, Алматы; Х. Досмұхамедов атындағы Атырау университеті, Информатика кафедрасы, Қазақстан, Атырау, E-mail: kbbagitova@gmail.com, https://orcid.org/0000-0003-1587-1995;

Мүсіралиева Шынар Женісбекқызы – физика-математика ғылымдарының кандидаты, доцент, Әл-Фараби атындағы Қазақ Ұлттық университетінің Ақпараттық жүйелер кафедрасы, Қазақстан, Алматы, E-mail: mussiraliyevash@gmail.com, https://orcid.org/0000-0001-5794-3649;

Азанбай Құралай – докторант, Әл-Фараби атындағы Қазақ Ұлттық университетінің Ақпараттық жүйелер кафедрасы, Қазақстан, Алматы, E-mail: kuralayazanbay@gmail.com.

Аннотация: мақала желідегі әлеуметтік желілердің қарқынды өсуін және олардың зиянды және экстремистік мазмұнды таратудағы рөлін қарастырады. Global Digital 2023 есебіне сілтеме жасай отырып, ол халықтың 60%-ға жуығы белсенді түрде қатысатын әлеуметтік медианы жаһандық қолданудың артып келе жатқанын көрсетеді. Әлеуметтік желі көптеген артықшылықтарды ұсынса да, ол қауіпті идеологияларды, соның ішінде терроризмді, киберқорлауды және экстремистік саяси қозғалыстарды тарату алаңына айналды. Мақалада экстремистік топтардың үгіт-насихат тарату, ізбасарларды тарту және зорлық-зомбылыққа шақыру үшін әлеуметтік медианы қалай пайдаланатыны, трендті хэштегтерді пайдалану немесе жаңа пайдаланушы атын жасау сияқты тактика арқылы платформа шектеулерін жиі айналып өтетіні зерттеледі.

Мақалада сондай-ақ экстремистік мазмұнды анықтау және санаттаудағы қиындықтар, сенімсіз деректер жиынтығы, автоматтандырылған тексеру жүйелерінің жоқтығы және зерттеулердегі біржақтылық сияқты мәселелер қарастырылған. Ол экстремистік материалдарды, соның ішінде зорлық-зомбылық бейнелері мен экстремистік мәтіндерді талдауға арналған құралдарды анықтауға бағытталған зерттеу саласын қарастырады. Сонымен қатар, мақалада Қазақстандағы экстремизмнің әртүрлі түрлері – саяси,

ұлттық және діни – және бұл идеологиялардың желіде қалай күшейетіні талқыланады. Ол нақты талдауға кедергі келтіретін деректер теңгерімсіздігі мен әдіснамалық айырмашылықтар сияқты қазіргі экстремизмді зерттеудің шектеулерін атап өтеді. Мақала экстремистік мазмұнды тиімдірек анықтау және азайту үшін озық бағдарламалық шешімдерді әзірлеуді жақтайды, осылайша онлайн экстремизммен күресу және ұлттық қауіпсіздікті нығайту бойынша жаһандық күш-жігерге үлес қосады.

Түйін сөздер: зорлық-зомбылықты анықтау, күресті тану, SVM, саяси экстремизм, машиналық оқыту, нейрондық желілер, ақпараттық қауіпсіздік технологиялары.

© К.Б. Багитова[1,2*], Ш.Ж. Мусиралиева[1], К. Азанбай[1], 2024.
[1]Казахский Национальный Университет имени аль-Фараби, Алматы, Казахстан;
[2]Атырауский университет имени Х. Досмухамедова, Атырау, Казахстан.
*E-mail: *KBBagitova@gmail.com*

АНАЛИЗ СИСТЕМ РАСПОЗНАВАНИЯ ПОЛИТИЧЕСКОГО ЭКСТРЕМИЗМА В СОЦИАЛЬНЫХ СЕТЯХ ОНЛАЙН

Багитова Каламкас Багитовна — PhD, кафедра информационных систем, Казахский национальный университет имени аль-Фараби, Алматы, Казахстан; Кафедра Информатики, Атырауский университета имени Х. Досмухамедова, Атырау, Казахстан, E-mail: kbbagitova@gmail.com, https://orcid.org/0000-0003-1587-1995;
Мусиралиева Шынар Женисбековна — кандидат физико-математических наук, доцент кафедры информационных систем, Казахский национальный университет имени аль-Фараби, Алматы, Казахстан, E-mail: mussiraliievash@gmail.com, https://orcid.org/0000-0001-5794-3649;
Азанбай Куралай — докторант, кафедра информационных систем, Казахский национальный университет имени аль-Фараби, Алматы, Казахстан, E-mail: kuralayazanbay@gmail.com.

Аннотация. В статье рассматривается быстрый рост социальных сетей в интернете и их роль в распространении вредного и экстремистского контента. Ссылаясь на отчет Global Digital 2023, он подчеркивает рост глобального использования социальных сетей, в котором активно задействовано почти 60% населения. Хотя социальные сети предлагают множество преимуществ, они также стали платформой для распространения опасных идеологий, включая терроризм, кибербуллинг и экстремистские политические движения. В статье рассматривается, как экстремистские группы используют социальные сети для распространения пропаганды, вербовки подписчиков и подстрекательства к насилию, часто обходя ограничения платформы с помощью таких тактик, как использование популярных хэштегов или создание новых имен пользователей.

В статье также рассматриваются проблемы выявления и категоризации экстремистского контента, указывая на такие проблемы, как ненадежные наборы данных, отсутствие автоматизированных систем проверки и предвзятость в исследованиях. В ней рассматривается область исследований, сосредоточенная на обнаружении экстремистских материалов, включая

инструменты для анализа жестоких видеороликов и экстремистских текстов. Кроме того, в статье обсуждаются различные формы экстремизма, встречающиеся в Казахстане — политические, национальные и религиозные — и то, как эти идеологии усиливаются в интернете. В статье отмечаются ограничения современных исследований экстремизма, такие как дисбаланс данных и методологические различия, которые мешают точному анализу. Также в статье предлагается разработка передовых программных решений для более эффективного выявления и нейтрализации экстремистского контента, тем самым внося вклад в глобальные усилия по борьбе с онлайн-экстремизмом и укреплению национальной безопасности.

Ключевые слова: обнаружение насилия, распознавание драк, SVM, политический экстремизм, машинное обучение, нейронная сеть, технологии информационной безопасности.

Introduction. A new field of study, online social networks, also known as virtual or online communities, will be spurred by the internet's and social services' quick development and growth as well as the widespread notion of Web 2.0. Users' varied behaviors, or a collection of distinct processes, comprise social media. Examples include using email services, starting chat rooms and blogs, getting information from homepages linked to links, altering and sharing images and videos through the media exchange system, and so on. The primary findings of the Global Digital 2023 research state that:

- The population of the globe surpassed 8 billion on November 15, 2022, and reached 8.01 billion at the start of 2023.
- 6.8% of the world's population, or 5.44 billion people, used mobile phones as of the beginning of 2023.
- Additionally, 64.4% of people have internet access worldwide. Their number rose by 1.9% throughout the course of the year.
- Nearly 60% of the global population, or 4.76 billion individuals, were active on social networks as of the start of 2023.

These figures show that social media is increasingly being used as a communication tool in many different nations, including as a handy venue for individuals who disseminate extreme viewpoints.

There is no doubt that the most recent changes in the world will have an impact on every aspect of life. Protecting our people from the harmful news, violent films, and terrorist ideas that proliferate on social media is getting harder and harder. Additionally, a large number of political strategists, advertisers, agitators, criminals, radicals, and organizers of harmful groups are among the numerous professional manipulators that work in social networks. Social media is a great instrument for spreading propaganda, informing people about crimes, altering awareness, advertising, extremist propaganda, and inciting riots.

Materials and methods. Social networks are becoming the primary medium via which harmful ideas and phenomena are disseminated:

1. Cyberbullying, harassment, and trolling;
2. Terrorism and extremism;
3. Politically charged destructive movements;
4. Drug addiction, pedophilia, and sexual promiscuity;
5. Risky Games and "challenges";
6. Dangerous Subcultures (the cult of school shooters, maniacs, and killers);
7. Consciousness manipulation;
8. SME content, etc.

Inciting social, racial, national, or religious animosity; elevating someone's sense of superiority or inferiority according to their language, social, racial, national, religious, or attitude toward religion are examples of *extremism*.

Behind each crime of an extremist (terrorist) nature are certain ideological views and beliefs of the people who committed it. Moreover, the absolute majority of such crimes are committed in a group, and the ideology inherent in its representatives goes far beyond its borders and serves as the basis for the formation and functioning of large-scale associations of extremist (terrorist) orientation. In this regard, it seems possible to determine the main ideological directions of the above associations and identify some of their features.

In addition to the international community's efforts to combat terrorism and violent extremism, Kazakhstan has produced important publications in this regard. It goes without saying that the strategy is extensive and has a wide range of hard and soft components that take into account stakeholders, laws, and work areas.

According to the Republic of Kazakhstan's "on Combating Extremism" statute, there are three different kinds of extremism in the country. They are:

- *Political extremism* - forcibly changing the constitutional order, violating the sovereignty of the Republic of Kazakhstan, the integrity, inviolability and inalienability of its territory, undermining the national security and defense capability of the state, forcibly seizing power or forcibly retaining power, creating, managing and participating in illegal paramilitary formations, organizing and participating in an armed uprising, inciting social and class hatred;

- *National extremism* - inciting racial, national and tribal hatred, including the incitement to violence or violence;

- *Religious extremism* - inciting religious hatred or Discord, including the use of any religious practices associated with violence or calls for violence, as well as threatening the safety, life, health, morality or rights and freedoms of citizens.

Based on the direction of political ideology in other countries, including European ones, we can conditionally distinguish between "left" extremism (left extremism) and "right extremism" (right extremism) (Chernyshev, 2021).

"Left" extremism takes on the ideas of revolutionism, anarchism, declares itself the most consistent representative and defender of the working masses, all the disadvantaged and the poor.

The objects of their criticism are social inequality, suppression of the individual,

exploitation, bureaucratization in society. They are ready to eliminate these phenomena by any means, including armed uprisings.

"Right-wing" extremists (fascist, neo-fascist, far-right, nationalist, racist movements) criticize modern society for "lack of order", "dominance of plutocracy", "decline of morality", selfishness. Right-wing extremists are often used to fight progressive public organizations and political figures. Many of them work under the guise of the state.

How social networks affect extremism. National security experts are concerned about the connection between social media and political division, as they caution about the persistent threat of extremism (terrorist) worldwide. The United States Department of Homeland Security (DHS) declared 2022 to be a "high-risk environment" because of internet activity that disseminated false information and conspiracies.

Use of social networks in extremism (terrorism). Social media threats, in addition to inciting political extremism, can also come from foreign and domestic organizations that want to harm the United States. According to the DHS, these "dangerous entities" often present or disseminate extremist messages to promote beliefs that can trigger terrorism.

In addition, global terrorist organizations have tried to increase their level of activity, attract new followers and cause panic through social networks using the following tactics:

- We announce our plans;
- Involve social media users in online communication;
- Use of messages that attract a young audience;
- Show violent acts;
- Take responsibility for terrorist acts;
- Redirect social network users to their group sites;
- Find funding.

Social media platforms act to limit content, resulting in extremists using their actions to their advantage. It is easy for such extremist groups to bypass the prohibitions of social networking platforms by creating a new username. They also use various algorithms to their advantage by adding trending words or hashtags to increase their visibility.

Analysis of tools for identifying political extremist texts in online social networks. Every kind of extremist literature and discourse, including radicalization, propaganda, and engagement in their ideologies, has distinct traits and repercussions. They are clarified as well (Gaikvad, and others, 2021). Because social networking platforms are becoming more and more widespread, extremist groups utilize them to spread propaganda, radicalize individuals, and recruit them for violent acts. Therefore, it is necessary to develop methods of radicalization, propaganda, and determination of attractiveness to their beliefs in order to limit the development of extremism in social networks (Kennedy, 2020). The following challenges arise when analyzing messages containing extremist information on social networks:

1.There aren't many publicly accessible data sets on texts related to extremism.

2.The text on extremism lacks balanced and ideologically neutral data sets.

3.The absence of automated techniques for data verification to assess data quality.

4.The absence of reliable automated techniques for identifying extremist texts on the web.

5.Restraint in the effort to categorize extremist information into groups like recruiting, promotion, and radicalization.

27,000 posts were gathered by Kennedy (Kennedy, 2020) from the social network Gab. In an effort to protect the right to free speech, the social media platform Gab has developed into a safe haven for the transmission of hate speech. The recordings are categorized by the writers as verbal abuse (VO), calls for violence (CV), and assaults on human dignity (HD).

13,369 anti-terrorist, 16,506 non-terrorist, and 38,617 random tweets were gathered by Abrar et al. (Abrar, and others, 2019). However, the authors did not apply data validation procedures to the gathered data collection, nor did they disclose any primary accounts or keywords relevant to terrorism that were utilized to collect tweets.

Asif and associates (Asif, and others, 2020) gathered extremist materials on the Facebook accounts of news organizations including PTV News, Dawn, and Geo. 19,497 posts in all were gathered. 109 randomly selected participants took the questionnaire-based test that the authors used. The authors, however, may not have included all the data because they only used 25 message samples.

The researchers collected data on the ideology of far-right white supremacy from various sources and places. Jackie and De Smedt (Jaki, and others, 2019) gathered fifty thousand tweets from around one hundred Twitter users who were thought to be German far-right supporters. Also, the writers gathered fifty thousand impartial tweets. The writers omitted all information regarding techniques for data verification.

Problems in the network of existing extremism data. The text data collection on extremism on the internet reveals a number of study gaps. The following issues are noted in the internet extremism text data set:

Data imbalances and binary classification. One of the main issues with extremism's internet datasets is data imbalance. It's challenging to compile a balanced class dataset because extremism data makes just a small portion of all social media data.

The binary, or at most three-class classification of extremism data is another issue with data sets. Furthermore, extremism takes many different forms and evolves throughout time. As a result, classifications based on the context of extremist literature are required.

The binary, or at most three-class classification of extremism data is another issue with data sets. Furthermore, extremism takes many different forms and evolves

throughout time. As a result, classifications based on the context of extremist literature are required.

Words. Extremism propagates across languages and across diverse ideologies. As a result, defining an extremist literature gets harder. As a global language, English is used by most scholars. The radical utilizes a lot of English to disseminate his beliefs worldwide.

Conventional data sets are no longer relevant. Social networks' stringent data exchange standards that prevent the updating of outdated data sets. One of the reasons for the limited number of standard data sets is this stringent policy around data sharing.

Verify. The manual verification of evaluators' agreement is a common practice among researchers. A limited number of randomly selected samples are utilized to verify the data because not all data can be verified by hand. Bias is thereby unintentionally introduced.

Evaluation of the quality of the data. Researchers frequently gather their own data while examining extremism on the internet (Berger, 2018; Fernandez, and others, 2018). Legacy user data sets are not accessible to the general public due to social media policies and other problems. Comparing data sets is therefore a major issue in the internet research of extremism. This creates even another issue when comparing the outcomes. It is challenging to compare the outcomes of studies on online extremism detection that employ various techniques and methodologies as no two studies use the same data set.

Accounts that are blocked. Social networking sites prohibit hate speech and acts of violence (Bagitova, and others, 2023; Twitter, 2020). As a result, many accounts with such extreme ideologies are blocked right away. Because there aren't any blocked accounts, other researchers are unable to generate results even after gathering data.

Analysis of tools for identifying political extremist content in graphic resources of social networks. The identification of political extremist content from the limited number of video resources available on internet social networks is a significant issue. As a result, it was thought that visual resources enhanced textual. As a result, numerous scientific articles and notes were read throughout the investigation. This review's primary goal is to present a thorough, methodical analysis of techniques for detecting video violence. A number of techniques have been developed in the last ten years to recognize aggressive conduct and violent videos. These techniques must be categorized, examined, and summarized. The following is a description of this systematic review's primary scientific findings:

- An overview of contemporary techniques for recognizing violence, emphasizing their uniqueness, salient characteristics, and limits;
- A study of the relative merits of several feature descriptors for detecting violence in videos;
- An analysis of data sets and assessment standards for identifying violence in videos;

- A discussion of the shortcomings, challenges, and unanswered issues surrounding video-based violence detection.

Acknowledge the action. A technology that can identify human actions is called action recognition. Based on the number of body parts involved and the complexity of the action, human activity is categorized into four divisions. Four categories comprise gestures, actions, interactions, and group activities. A gesture is a sequence of motions used to express a certain idea with the hands, head, or other body parts. A single person's activities are made up of numerous gestures. A group of human behaviors in which two or more individuals take part is called an interaction. In a scenario involving two performers, one of them needs to be a human, while the other can be either.

A group action consists of a mixture of gestures, actions, or interactions when there are more than two players and one or more interacting objects (Ye, and others, 2018; Galassi, and others, 2021).

What constitutes violence. The wider subject of identifying activities includes a distinct problem with the concept of violence. Finding out if violence happens automatically and successfully in a brief amount of time is the goal of violence detection. In the past few years, automatic video identification of human activity has gained importance for applications such content-based video search, video surveillance, and human-computer interaction (Rothman, 2022). Finding out if violence happens automatically and successfully is the goal of violence detection. In any case, because the concept of violence is subjective, it is challenging to define it precisely. The definition of violence is a complicated issue both in terms of application and study since it contains characteristics that set it apart from simple acts.

Categorization of techniques for detecting violence. Violence in daily life is characterized by unusual occurrences or behaviors. In the subject of activity recognition, using computer vision to identify these kinds of actions in security cameras has gained popularity (Naik, and others, 2018). Scientists have developed a variety of methods and approaches to recognize violent or unusual events, pointing to the steep increase in crime as proof that more accurate identification is required. In the last few years, numerous methods for identifying violence have been created. Depending on the classifier used, three categories are created: violence detection by deep learning, violence detection by SVM, and violence detection by machine learning (Omarov, and others, 2022; Mashechkin, and others, 2019). SVM and deep learning are categorized separately because of their widespread applications in computer vision. The features of each approach are explained in the tables.

Results and discussion. During the study of technologies for improving competencies in the field of internet extremism prevention, the idea of developing software for identifying political extremist texts and graphic resources in online social networks was born. At the same time, long-term research was carried out, a review of world-class software systems was carried out, and various models and methods were used. Since the content in social networks is of several nature, the

goal was to increase the accuracy of identifying the content of political extremism from text and graphic resources.

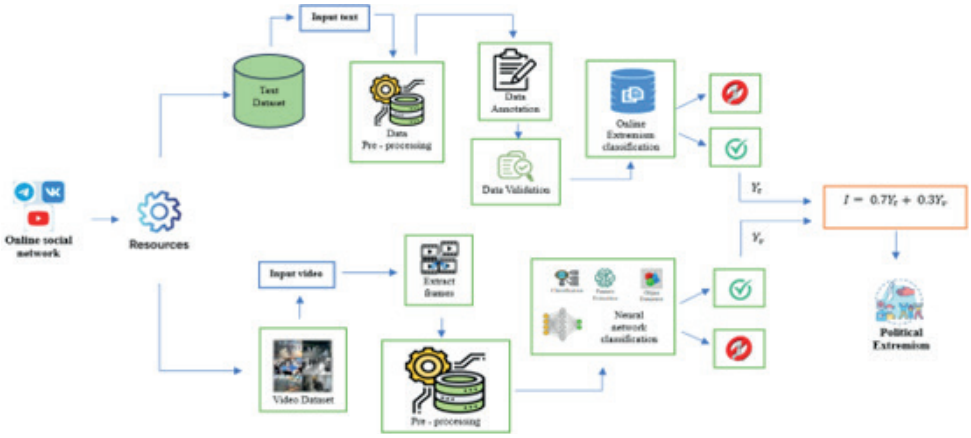

Figure 1. General model of the methodology for determining political extremism

As for the general model of the methodology for identifying political extremism, first, text and graphic resources are taken from posts posted on social networks, several processes are carried out, and then, in accordance with the conditions of an integral assessment, it is determined whether the resources received contain political extremist content. The following chapters provide a clear description of all stages of the developed software (Kotzé, and others, 2020) We examine techniques for detecting violence that make use of traditional machine learning techniques. We provide a summary of the different classification approaches for identifying violent video content in Fig. 2. The methods include definitions, feature extraction, classification, application to various manifestations, and evaluation parameters for different data sets.

Serrano Gracia et al. (2015)	Motion blob acceleration measure vector method for detection of fast fighting from video	Ellipse detection method	An algorithm to find the acceleration	Spatio-temporal features use for classification	Both crowded and less crowded	Accuracy about 90%
Zhou et al. (2018)	FightNet for Violent Interaction Detection	Temporal Segment Network	Image acceleration	Softmax	Both crowded and uncrowded	97% in Hockey, 100% in Movies dataset
Ribeiro, Audigier & Pham (2016)	RIMOC method focuses on speed and direction of an object on the base of HOF	Covariance Matrix method STV based	Spatio-temporal vector method (STV)	STV uses supervised learning	Both crowded and uncrowded	For normal situation 97% accuracy
Yao et al. (2021)	Multiview fight detection method	YOLO-V3 network	Optical flow	Random Forest	Both crowded and uncrowded	97.66% accuracy, 97.66 F1-score
Arceda et al. (2016)	Two step detection of violent and faces in video by using ViF descriptor and normalization algorithms	Vif object recognition CUDA method and KLT face detector	Horn shrunk method for histogram	Interpolation classification	Less crowded	Lower frame rate 14% too high rate of 35% fs/s 97%
Wu et al. (2020a), Wu et al. (2020b)	HL-Net to simultaneously capture long-range relations and local distance relations	HLC approximator	CNN based model	Weak supervision	Both crowded and uncrowded scene	78.64%
Xie et al. (2016)	SVM method for recognition based on statistical theory frames	Vector normalization method	Macro block technique for features extractions	Region motion and descripton for video classification	Crowded	96.1% accuracy
Febin, Jayasree & Joy (2020)	A cascaded method of violence detection based on MoBSIFT and movement filtering	MoBSIFT	Motion boundary histogram	SVM, random forest, and AdaBoost	Both Crowded and uncrowded scene	90.2% accuracy in Hockey, 91% in Movies dataset
Senst et al. (2017)	Lagrangian fields of direction and begs of word framework to recognize the violence in videos	Global compensation of object motion	Lagrangian theory and STIP method for extract motion features	Late fusion for classification	Crowded	91% to 94% accuracy

Figure 2. Different classification methods for detecting video violence

Techniques for employing SVM to detect violence. Fig. 3 displays a collection of techniques for identifying a violent incident based on SVM. SVM is a supervised learning technique that addresses issues with classification. SVM is a well-liked computer vision technique because it considers digitized and trustworthy data. It is applied to jobs involving binary classification.

Ye et al. (2020)	A Video-Based DT- SVM School Violence Detecting Algorithm	Motion Co-occurrence Feature (MCF)	Optical flow extraction	Crowded	97.6%
Zhang et al. (2016)	GMOF framework with tracking and detection module	Gaussian Mixture model	OHFO for optical flow extraction	Crowded	82%–89% accuracy
Gao et al. (2016)	Violence detection using Oriented VIF	Optical Flow method	Combination of VIF and OVIF descriptor	Crowded	90%
Deepak, Vignesh & Chandrakala (2020)	Autocorrelation of gradients based violence detection	Motion boundary histograms	Frame based feature extraction	Crowded	91.38% accuracy in Crowd Violence; 90.40% in Hockey dataset
Al-Nawashi, Al-Hazaimeh & Saraee (2017)	Framework includes preprocessing, detection of activity and image retrieval. It identifies the abnormal event and image from data-based images.	Optical flow and tempora difference for object detection CBIR method for retrieving images.	Gaussian function for video future analysis	Less crowded	97% accuracy
Kamoona et al. (2019)	Sparsity-Based Naive Bayes Approach for Anomaly Detection in Real Surveillance Videos	Sparsity-Based Naive Bayes	C3D feature extraction	Both crowded and uncrowded	64.7% F1 score; 52.1% precision; 85.3% recall in UCF dataset
Song, Kim & Park (2018)	SGT-based and SVM-based multi-temporal framework to detect violent events in multi-camera surveillance.	Late fusion	Multi-temporal Analysis (MtA)	Variety fight scenes from minimum two to maximum fifteen people include various movements	78.3% (SGT-based, BEHAVE), 70.2% (SVM-based, BEHAVE), 87.2% (SGT-based, NUS-HGA), and 69.9% (SGT-based, YouTube)
Vashistha, Bhatnagar & Khan (2018)	An architecture to identify violence in video surveillance system using VIF and LBP	Shape and motion analysis	VIF and Local Binary Pattern (LBP) descriptors	Both crowded and non-crowded scenes	89.1% accuracy in Hockey dataset, 88.2% accuracy in Violent-Flow dataset

Figure 3. Methods for detecting violence using SVM

Methods for identifying violence through deep learning. Research work on the use of deep learning algorithms for detecting violence in graphic resources is improving day by day. Convolutional neural networks (CNNs) and their enhancements are widely used to detect violence in videos.

Ding et al. (2014)	Violence Detection using 3D CNN	3D convolution is used to get spatial information	Backpropagation method	Crowded	91% accuracy
Arandjelović et al. (2016)	Deep architecture for place recognition	VGG VLAD method for image retrieval	Backpropagation method for feature extraction	Crowded	87%–96% accuracy
Perif et al. (2019)	Framework for football stadium comprising of big data analysis and deep learning through bidirectional LSTM	Bidirectional LSTM	HOG, SVM	Crowded	94.5% accuracy
Mu, Cao & Bin (2016)	Violent scene detection using CNN and deep audio features	MFB	CNN	Crowded	Approximately 90% accuracy
Mohtavipour, Saeidi & Arabsorkhi (2021)	A multi-stream CNN using handcrafted features	A deep violence detection framework based on the specific features (speed of vmovement, and representative image) derived from handcrafted methods.	CNN	Both crowded and uncrowded	
Sudhakaran & Lanz (2017)	Detect violent videos using ConvLSTM	CNN along with the ConvLSTM	CNN	Crowded	Approximately 97%
Naik & Gopalakrishna (2021)	Deep violence detection framework based on the specific features derived from handcrafted methods	Discriminative feature with a novel differential motion energy image	CNN	Both crowded and uncrowded	
Meng, Yuan & Li (2017)	Detecting Human Violent Behavior by integrating trajectory and Deep CNN	Deep CNN	Optical flow method	Crowded	98% accuracy
Rendón-Segador et al. (2021)	ViolenceNet: Dense Multi-Head Self-Attention with Bidirectional Convolutional LSTM	3D DenseNet	Optical flow method	Crowded	95.6%– 100% accuracy
Xia et al. (2018)	Violence detection method based on a bi-channels CNN and the SVM.	Linear SVM	Bi-channels CNN	Both crowded and uncrowded scenes	95.90 ± 3.53 accuracy in Hockey fight, 93.25 ± 2.34 accuracy in Violence crowd
Meng et al. (2020)	Trajectory-Pooled Deep Convolutional Networks	ConvNet model which contains 17 convolutionpool-norm	Deep ConvNet model	Both crowded and	92.5% accuracy in Crowd Violence, 98.6% in

Figure 4. Identifying violence using deep learning techniques

A set of deep learning-based recognition techniques is displayed in Fig. 4. Deep learning is based on neural networks. The technique is used to categorize forced recognition according to the data set and the acquired capabilities by adding more convolutional layers.

Conclusion

Social media sites have a significant impact on people's beliefs, attitudes, and perceptions, which helps to propagate extremism. These platforms are being utilized more and more to disseminate propaganda from extremist groups, radicalize youth, and entice them to join them. Thus, studies on identifying extremism in social networks are required to limit its impact and negative consequences. The concept of extremism is constrained by a distinct ideology, a binary classification with a narrow textual meaning of extremism, and manual data review techniques to ensure data quality, according to a survey of the literature on the subject. Researchers employed a data collection that was restricted to a specific ideology in earlier experiments.

The following outcomes of this study's efforts to develop models and procedures for spotting political extremism in online social network text and graphic resources were attained:

1. for the first time, a method for the formation of a set of signs, taking into account the peculiarities of the Kazakh language, was developed and a model for identifying texts of political extremism in the Kazakh language was created in online social networks;

2. for the first time, a corpus of texts on political extremism in the Kazakh language was created to identify signs of political extremism in online social networks;

3. developed a neural method for detecting political extremism on online social network graphic resources;

4. developed a model of processing online social network graphic resources and neuronet analysis to identify political extremism;

5. software for identifying extremist texts and graphic resources in the Kazakh language in online social networks has been created as a result of the developed models and methods.

The novelty of this study is the development of a deep neural network model for identifying extremist texts in the Kazakh language. Based on the application of the TF-IDF method to bigrams, in which the preliminary stemming algorithm was performed, a deep neural network model was built, and the results show the effectiveness of the proposed model in identifying extremist texts in comparison with classical machine learning methods with the highest accuracy for the task of identifying texts of extremist orientation in the Kazakh language.

References

https://online.zakon.kz/Document/?doc_id=30004865

Chernyshev, E. (2021). Kaspersky: A window into the criminal world in every child's pocket. Retrieved from *https://www.nakanune.ru/news/2021/05/12/22601520/*

Gaikvad, M., Ahirrao, S., Fansalkar, S., & Kotecha, K. (2021). Detecting extremism on the Internet: A systematic review of the literature focusing on datasets, classification methods, verification methods, and tools. IEEE Access, 48364–48404. *https://doi.org/10.1109/ACCESS.2021.3068313*

The Main Purpose of the Event Is to Promote the Development of the Kazakh Language. The concept of extremist data and a systematic review of projects to combat extremism. (2023). NEWS OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN PHYSICO-MATHEMATICAL SERIES, 3(347), 112–130. Retrieved from *https://journals.nauka-nanrk.kz/physics-mathematics/article/view/5792/4039*

Kennedy, B. (2020). The Hate Corps: A collection of 27,000 posts annotated on hate speech. Retrieved from *https://psyarxiv.com/hqjxn/*

Abrar, M. F., Arefin, M. S., & Hossein, M. S. (2019). The structure of real-time analysis of tweets to identify terrorist activities. In Proceedings of the 2nd International Conference on Electrical Engineering, Computer and Communication Technology (ECCE 2019), Khaldia, India (pp. 1-6). *https://doi.org/10.1109/ECCE.2019.123456*

Asif, M., Ishtiaq, A., Ahmad, H., Al Junaid, H., & Shah, J. (2020). Analysis of extremist sentiments in social networks based on text information. Telematics and Informatics. *https://doi.org/10.1016/j.tele.2020.101345*

Jaki, S., & De Smedt, T. (2019). Right-wing German hate speech on Twitter: Analysis and automatic detection. Retrieved from *https://arxiv.org/abs/1910.07518*

Berger, J. M. (2018). The Census of the Alternative Right on Twitter: Defining and describing the audience of alternative right-wing content on Twitter. Retrieved from https://www.voxpol.eu/new-research-report-the-alt-right-twitter-census-by-jm-berger/

Fernandez, M., Asif, M., & Alani, H. (2018). Understanding the roots of radicalization on Twitter. In Proceedings of the 10th ACM Web Science Conference (pp. 1-10). Boston, Massachusetts, USA. *https://doi.org/10.1145/3201064.3201083*

Bagitova, K. B., Musiralieva, Sh. Zh., Bolatbek, M. A., & Ospanova, R. K. (2023). Development of ExWeb software for detecting extremist content on the Internet. News of the National Academy of Sciences of the Republic of Kazakhstan. Physics and Computer Science Series, 2(346), 81–95. Retrieved from *https://journals.nauka-nanrk.kz/physics-mathematics/article/view/5414/3871*

Twitter. (2020). Updating our rules against hateful behavior. Retrieved from https://blog.twitter.com/en_us/topics/company/2019/hatefulconductupdate.html

Ye, L., Wang, P., Wang, L., Ferdinando, H., Seppänen, T., & Alasaarela, E. (2018). A combined motion-audio school bullying detection algorithm. International Journal of Pattern Recognition and Artificial Intelligence, 32(12). *https://doi.org/10.1142/S0218001418470123*

Galassi, A., Lippi, M., & Torroni, P. (2021). Attention in Natural Language Processing. IEEE Transactions on Neural Networks and Learning Systems, 32(10). *https://doi.org/10.1109/TNNLS.2020.3019893*

Rothman, D. (2022). Transformers for Natural Language Processing: Build, train, and fine-tune deep neural network architectures for NLP with Python, PyTorch, TensorFlow, BERT, and GPT-3 (2nd ed.). Packt Publishing.

Naik, A. J., & Gopalakrishna, M. T. (2018). Violence detection in surveillance video-a survey. International Journal of Latest Research in Engineering and Technology (IJLRET), 1, 1–17.

Omarov, B., Narynov, S., Zhumanov, Z., Gumar, A., & Khassanova, M. (2022). State-of-the-art violence detection techniques in video surveillance security systems: A systematic review. PeerJ Comput Sci, 8, e920. *https://doi.org/10.7717/peerj-cs.920*

Mashechkin, I., Petrovskiy, M., Tsarev, D., & Chikunov, M. (2019). Machine Learning Methods for Detecting and Monitoring Extremist Information on the Internet. Programming and Computer Software, 45, 99–115.

Kotzé, E., Senekal, B. A., & Daelemans, W. (2020). Automatic classification of social media reports on violent incidents in South Africa using machine learning. South African Journal of Science, 116(3), 1–8. *https://doi.org/10.17159/sajs.2020/6501*

Hu, Z., Tereikovskyi, I., Tereikovska, L., Tsiutsiura, M., & Radchenko, K. (2020). Applying Wavelet Transforms for Web Server Load Forecasting. In Z. Hu, S. Petoukhov, I. Dychka, & M. He (Eds.), Advances in Computer Science for Engineering and Education II. ICCSEEA 2019. Advances in Intelligent Systems and Computing, vol 938 (pp. 13-22). Springer, Cham. *https://doi.org/10.1007/978-3-030-16621-2_2*

CONTENTS

INFORMATION AND COMMUNICATION TECHNOLOGIES

МАЗМҰНЫ

АҚПАРАТТЫҚ-КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР

СОДЕРЖАНИЕ

ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

Publication Ethics and Publication Malpracticein the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethicalguidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any otherlanguage, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайтах:
www:nauka-nanrk.kz
http://physics-mathematics.kz/index.php/en/archive
ISSN2518-1726 (Online),
ISSN 1991-346X (Print)

Директор отдела издания научных журналов НАН РК *А. Ботанқызы*
Редакторы: *Д.С. Аленов, Ж.Ш.Әден*
Верстка на компьютере *Г.Д.Жадыранова*

Подписано в печать 2.12.2024.
Формат 60x881/8. Бумага офсетная. Печать –ризограф.
16,0 п.л. Тираж 300. Заказ 4.

Национальная академия наук РК
050010, Алматы, ул. Шевченко, 28, т. 272-13-19