Algorithmic Censorship in Modern Wars: Case of the Encryption for Digital Resilience during the Latest Israeli War of 2023 on Gaza

HASSAN RAMMAL*
Al Maaref University, Lebanon

ABSTRACT

Social media has significantly reshaped traditional concepts of free media, steering it toward greater independence. After decades of control by ministries of communication and gatekeepers over audio-visual content, these institutions have gradually lost their influence, leading to a more decentralized media landscape. In this new environment, social media platforms have become powerful tools, shaping social and political narratives by controlling information dissemination, often aligning with their policies. Artificial intelligence's rise has amplified algorithms' role, particularly during geopolitical wars and conflicts. For instance, during the latest Israeli war in Gaza that erupted in October 2023, thousands of accounts supporting the Palestinian cause were banned, raising concerns about freedom of expression due to algorithms' ability to manipulate public opinion. In response, users have adopted various tactics, such as employing encryption and content modification techniques to evade algorithmic censorship. Despite the widespread use of these tactics across the Arab world, no research has systematically explored their effectiveness in countering algorithms, especially in crisis-prone regions. This study aims to fill this gap by examining the most common encryption techniques used by users during the Gaza war, particularly in resistance axis countries. This study will utilize a mixed-methods approach to analyse a sample of 80 social media posts sourced from X, TikTok, WhatsApp, and Instagram. The analysis will identify the most effective methods for circumventing AI-based censorship and highlight the sophisticated strategies used to protect freedom of expression in the digital age.

Keywords: *Algorithmic censorship, Gaza conflict, data encryption, social media bias, crisis communication strategies.*

INTRODUCTION

Today, social networks remain one of the key means of communication throughout the world that alters the ways individuals communicate and share information. Social media like WhatsApp, Instagram, X and TikTok among others have greatly revolutionized how people communicate in particular during wars and conflicts. Social media enables individuals to share ideas within a couple of moments and are also able to connect with anyone regardless of geographic boundaries (Ermoshina & Musiani, 2022). For the people living in politically sensitive states, social means more than a medium of communication. It lets them report on their daily experiences, tell firsthand witnessing of certain events, and amplify marginalized voices (Fedoruk et al., 2021).

However, this newfound freedom to communicate and connect is increasingly under threat. Although Social Media platforms provide the world with new opportunities for self-representation, they are sites of control and surveillance (Abokhodair et al., 2024). These platforms now have automatic content filtering systems, often known as algorithmic repression. Designed to weed out unwanted content including vulgar and lewd content, such systems employ machine learning and Artificial Intelligence algorithms to analyse and rate

*Corresponding author: hassan.rammal@mu.edu.lb
E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2025-4104-26
Received: 3 August 2025 | Accepted: 12 November 2025 | Published: 12 December 2025

posts including comments and images. The primary purpose is to maintain the allocated community standards and promote compliance with the legal and ethical standards.

Though the goal of these systems is to make interaction on the Internet more secure and to prevent the appearance of dangerous material such as hate speech, fake news, or violence, they are far from perfect. These algorithms cannot often interpret cultural, linguistic, or contextual nuances, leading to the removal of legitimate content (Buckley & Schafer, 2022). This is particularly problematic for users in war zones, where communication is often laden with subtle cultural codes and context-specific meanings. Algorithmic censorship can harm marginalized communities, by extraditing them from public space and denying them an active place in the digital public sphere (Wells, 2024).

Motivation for this Study

Algorithmic censorship, fuelled by social media platforms' tools for detecting 'inappropriate' content, poses a significant threat to free expression, especially in politically sensitive or war zones (Tanczer et al., 2020). These systems aim to ensure safety but fail to address cultural, political, and contextual nuances, often suppressing voices from marginalized regions like Gaza, where social media plays a key role in mobilizing support and fostering resilience (Al-Dala'ien et al., 2023).

This study explores how people in war zones adapt their communication strategies, with a focus on the Middle East, a region marked by censorship and prolonged conflict, making it an ideal case for examining the intersection of digital surveillance, algorithmic control, and user resistance. For example, Arab users bypass algorithmic restrictions by coding hashtags with mixed languages, emojis, and Unicode symbols to convey clear meanings beyond automated detection (Öztürk, 2024). These strategies represent a form of digital resilience, empowering users in increasingly oppressive digital environments.

Another motivation is the lack of research on cultural and linguistic encryption methods used by individuals to resist censorship, despite a growing focus on technical encryption and cybersecurity (Oltmann et al., 2022). This study aims to bridge the gap between technology and human creativity, showing how users in war zones repurpose digital tools to fight censorship.

Ultimately, this research aims to promote digital freedom and social justice by shedding light on these resistance techniques. It offers valuable insights for policymakers, platform developers, and activists working to safeguard online free expression, particularly in contexts like Gaza, where each post holds profound social and political importance (Huang, 2022).

Problem Definition

The implementation of algorithmic censorship by social media platforms has created significant barriers to free expression (Gohdes, 2024). Despite being designed to combat fake news and harmful content, automated algorithmic bots often filter out legitimate information, silencing crucial voices and hindering the dissemination of vital information (Tanczer et al., 2020).

To counteract this censorship, social media users in the Axis of Resistance countries have adopted innovative encryption techniques to obscure their messages from algorithmic detection. These techniques include the use of Unicode symbols, intentional misspellings, separating characters, text strike-through, prolonged characters, blurred text, mixed languages, and emojis. Even though these strategies tell a lot about resilience and creativity, there is still a paucity of research on how often they are used, and if they are effective when used. Little empirical research is known about the most frequent encryption strategies being applied and adopted by users to avoid censorship (Nadesan, 2021).

This gap in knowledge highlights a pressing need for research that systematically examines these emerging encryption techniques and strategies. Understanding their usage patterns can offer valuable insights into how individuals navigate censorship and safeguard their freedom of expression in the digital age. Furthermore, such research could catalyse the development of more equitable content moderation practices that respect cultural and political sensitivities in conflict regions.

Research Questions

a) What encryption techniques do social media users in the Axis of Resistance use to bypass algorithmic censorship during the Gaza conflict?
b) How do the usage patterns of encryption techniques vary across different social media platforms, such as WhatsApp, Instagram, X, and TikTok?

LITERATURE REVIEW

The following section explores key concepts related to algorithmic censorship, the role of social media in war zones, and encryption techniques used to bypass automated content moderation. It begins with an examination of the limitations of algorithmic censorship, particularly in war contexts mainly Gaza, where these systems usually suppress critique voices. The discussion then shifts to the significance of social media in wars and crises situations, highlighting both its capacity to spread vital information and the challenges it faces from censorship and surveillance. Encryption techniques are explored next, focusing on how individuals in war zones use linguistic and visual methods to circumvent censorship. The section concludes with an analysis of semiotic theory, illustrating how signs and symbols on social media are employed to convey meaning in ways that evade algorithmic detection. This provides a comprehensive understanding of the socio-technical dynamics of digital resistance in crisis environments.

Algorithmic Censorship

Algorithmic censorship involves the use of automated algorithms by social media platforms to moderate content based on predefined criteria, often driven by company policies, user reports, or government regulations (Rumata & Nugraha, 2020). While effective at removing toxic or obscene content, these algorithms frequently overreach, suppressing legitimate political discourse. For example, X and Instagram have faced criticism for removing posts and accounts documenting abuse in war zones, citing violations of platform standards (Zhang, 2024; Zhang & Díaz-Kommonen, 2024). Instagram publicly apologized in May 2023 after users reported systematic removal of posts about Palestinian evictions in Sheikh Jarrah. Similarly, X (Twitter) has been accused of locking accounts of activists and journalists in conflicts like Kashmir and Myanmar while allowing popular accounts spreading misinformation to remain active. These actions highlight how algorithmic decision-making often disregards cultural and political nuances, undermining free speech.

In war zones like Gaza, algorithmic censorship poses significant challenges, as it restricts the dissemination of critical information and documentation of human rights violations. Platforms claim their algorithms aim to curb violent or graphic content, but this often results in the removal of firsthand accounts from conflict areas (Tomasev et al., 2021). Activists in Gaza report that posts documenting attacks, or humanitarian crises are frequently flagged as "sensitive" or removed, silencing marginalized voices and skewing global narratives. This censorship exacerbates power imbalances, limiting activists' and journalists' ability to counter disinformation and propaganda (Matthiesen, 2022). It also hinders humanitarian organizations from using these platforms for fundraising and awareness campaigns.

To counter algorithmic censorship, many turn to encryption and alternative platforms to protect their messages from surveillance or removal. Encryption ensures secure communication, accessible only to intended recipients (Zhang et al., 2023), making it vital for activists and journalists in oppressive regimes. Tools like Signal and WhatsApp, which use end-to-end encryption, are widely used, alongside decentralized platforms like Mastodon. However, while encryption safeguards against censorship, its potential misuse by malicious actors creates a regulatory dilemma, highlighting the challenges of balancing free speech and security.

Social Media in Crisis and War Zones

Social media has become a vital source of information during wars, conflicts and crises, amplifying voices from affected regions. Platforms like X and Instagram enable real-time updates, resource sharing, and global awareness. For instance, during natural disasters, social media facilitates the dissemination of life-saving information, such as safety measures and relief locations (Mahlouly & Erhaim, 2023). The 2015 Nepalese earthquake demonstrated this, with Twitter playing a key role in coordinating rescue efforts and international aid (Olise, 2021). In war zones, where traditional media is often restricted, social media serves as a critical tool for reporting human rights abuses. During the Syrian civil war, activists used YouTube to share videos of atrocities, countering official narratives. However, the democratization of information through social media also brings challenges, such as the spread of fake news and competing narratives from state and non-state actors (Musdalifah et al., 2023), highlighting its dual nature in crisis communication.

In conflict areas like Gaza, social media is a lifeline for Palestinians to share their struggles under blockade and garner global support (Wok et al., 2016). Platforms like Instagram and X are filled with images and stories that humanize the conflict, raising international awareness. Hashtags like #SaveSheikhJarrah and #GazaUnderAttack trended globally during the 2021 escalation, amplifying on-ground voices and pressuring international responses. Similarly, during what so called the Arab Spring, platforms like Facebook were instrumental in organizing protests and mobilizing communities, offering an alternative to state-controlled media (Vorhies & Heckenlively, 2021). The practical application of social media in conflict areas offers analytical material indicating both benefits and failures. In Gaza, for instance, social media is the only tool Palestinians use to express the misery of living under blockade and gain the support of the outside world (El Zein & Abusalem, 2015).

However, maintaining digital communication in war zones is fraught with challenges, including surveillance and censorship. Governments and powerful actors often monitor and control online activity, targeting activists and journalists (Youvan, 2024). In Gaza, posts documenting Israeli airstrikes or calling for solidarity are frequently removed or shadow-banned under platform policies, silencing marginalized voices. In Myanmar, internet shutdowns and surveillance have forced activists to rely on encrypted apps like Signal or VPNs, though these measures carry risks like metadata exposure (Youvan, 2024). Additionally, algorithmic censorship often misinterprets culturally specific content, removing legitimate criticism. These challenges underscore the need for decentralized platforms, encryption technologies, and international advocacy to protect digital communication during wars and conflicts.

Encryption Techniques

Encryption techniques for bypassing censorship have appeared as an instant reaction to increasing restrictions on online speech particularly in politically or militarily sensitive regions. These techniques aim to obscure or alter the content of digital messages in such a way that they remain intelligible to human audiences but evade detection by automated censorship algorithms (Sangwan et al., 2021). These specific means of encryption have moreover been associated with the expansion of algorithmic content moderation by social networks. In the early stages, internet censorship was mainly focused on completely blocking access to entire websites or social media platforms (Latif et al., 2025). As digital censorship evolved to include more nuanced content monitoring, users began to adapt by developing various methods to subvert these restrictions. According to Wadho et al. (2023), encryption techniques evolved in response to the changing tactics of online surveillance, from simply using proxy servers to more sophisticated approaches that involve modifying the content itself. These adaptations reflect a broader trend of digital resistance, where users leverage creative strategies to reclaim their ability to communicate freely online.

Encryption techniques, as presented in Table 1, are essential for securing data and ensuring privacy in communication. There are two primary categories of encryption methods: symmetric encryption and asymmetric encryption.

Table 1: Comparison between symmetric and asymmetric encryption

Aspect	Symmetric Encryption	Asymmetric Encryption
Keys Used	Single key (same key for encryption and decryption).	Two keys: public key for encryption, private key for decryption.
Speed	Faster and more efficient for large amounts of data.	Slower due to complex mathematical computations.
Security	Less secure if the key is intercepted during sharing.	More secure since private keys are not shared.
Key Management	Requires secure key sharing between sender and receiver.	No need to share private keys; only public keys are exchanged.
Use Cases	Encrypting large files or data streams (e.g., disk encryption, database encryption).	Secure key exchanges, digital signatures, email encryption.
Efficiency	Highly efficient for encrypting large amounts of data.	Suitable for small data or as part of hybrid encryption.

a. Symmetric Encryption

Symmetric encryption involves using the same key for both encrypting and decrypting data. It is a fast and efficient method, ideal for securing large volumes of data. However, the primary challenge is ensuring the secure exchange of the key between parties.

b. *Symmetric Encryption*

Asymmetric encryption, also referred to as public-key encryption, uses two keys: a public key for encryption and a private key for decryption. This approach enhances security by removing the need to share a single key. However, it is more computationally demanding than symmetric encryption.

c. *Evolving Encryption Tactics*

The development of encryption techniques has been influenced by several factors, including the sophistication of censorship technologies, the technological savvy of users, and the specific demands of local contexts (Qureshi et al., 2022). For example, in regions where political oppression or violent conflict is prevalent, individuals often rely on encrypted communication methods to disseminate information without being detected by both government surveillance and platform algorithms. Over time, encryption techniques have become more refined, with users combining various approaches—such as linguistic manipulation, visual obfuscation, and the use of alternative scripts—to bypass detection (Khader & Karam, 2023). This process reflects the game between censors and the users when new algorithms are developed and in turn, the users try to crack them.

Types of Encryption Techniques Used in Text-Messaging Platform

The objective of these encryption methods is to either hide or mask the actual message from automated censorship systems meant to scrape and remove 'harmful or sensitive' content. Most algorithms powering automated content moderation are programmed in a way that can recognize certain forbidden words, phrases, or even images (Liaqat et al., 2024). Nonetheless, these systems are not perfect and generally do not have any idea of the context in which the content is being used. For this reason, people experiencing crises have created and used different tactics to hide their messages from algorithms while remaining able to communicate with others (JosephNg et al., 2025). Text-based encryption techniques primarily focus on altering or disguising the language or form of communication in such a way that it avoids detection by algorithms while still conveying a clear message to human readers. The most commonly used techniques are summarized in Table 2.

Table 2: Most common strategies for circumventing automated content moderation

Technique Name	Simplified Description	References
Unicode Symbols	Users replace letters or words with similar-looking symbols from the Unicode character set (e.g., writing "freedom" in Arabic or Cyrillic fonts). This break pattern recognition systems used by algorithms.	(Park, 2023)
Misspelling for Avoidance	Users intentionally misspell words or replace letters with symbols to evade detection. This exploits the reliance of automated systems on pattern matching rather than phonetic or visual variations.	(Raykar et al., 2023)
Separating Characters	Users insert spaces or symbols between characters in words to disrupt algorithmic detection. This prevents algorithms from recognizing the separated characters as coherent words.	(Daucé & Loveluck, 2021)
Text Strike-Through	Users apply a strike-through effect to words or characters to obscure keywords from algorithmic filters. The text remains readable to humans but is hidden from automated systems.	(Al-Jarrah et al., 2022)

Prolonging Characters	Users extend the length of characters (e.g., repeating vowels or consonants) to disrupt word recognition by algorithms. This serves as both an aesthetic choice and a subtle encryption technique.	(Iannone, 2022)
Blurring Text	Users blur or obscure text within images using visual filters (e.g., pixelization). This makes it difficult for automated systems to detect sensitive content while remaining visible to human viewers.	(Umar et al., 2023)
Mixed Language	Users mix languages or code-switch within a post to evade algorithmic detection. Algorithms may not recognize words in multiple languages, and this technique also signals solidarity or cultural identity.	(Panait & Ashraf, 2021)
Emojis	Users replace words with emojis to convey messages indirectly. Emojis act as symbolic language that bypasses algorithmic filters while retaining meaning for those familiar with the context.	(Majdawi & Jabi, 2020)

Semiotics: Theory and Application

Semiotics relates to signs and symbols and is pivotal for describing communication, especially when messages are transmitted through the use of words, images, sounds, and other digital symbols. Ferdinand de Saussure, the founder of modern semiotics is a Swiss linguist. Saussure's theory centres on the idea that meaning is constructed through the relationships between signs, which are composed of two primary components: the signifier, which refers to the form of the sign, which may be a word or an image, and the signified which is the concept that is represented by the sign.

De Saussure (1959) emphasized that meaning is derived from the difference between signs in a system of signs and not from the relationship between the signifier and the signified. He defined linguistic signs as a structure of language that belonged to the social convention and were not isolated but within a system of interdependent signs.

In the context of social media, Saussure’s theory can be used to decipher how signification (words, images, or symbols) is used. Social media platforms, such as X and Instagram, serve as sites where signs are not only linguistic but also visual (e.g., images, emojis, GIFs) and cultural (e.g., hashtags, memes). These platforms are rich in semiotic activity, and users build and communicate information using stimuli that may bear little resemblance to the manifest content of the information. A post containing mere emojis, hashtags, and misspellings will have a message that the automated censorship systems may not understand. Still, people within a particular culture or with a specific political inclination will.

Charles Peirce (1931), an American philosopher, developed a triadic model of signs that is more complex than Saussure's dyadic approach. In Peirce’s framework, a sign consists of three components: the *representamen* (the form the sign takes), the *interpretant* (the meaning or concept derived from the sign), and the object (the actual thing or concept that the sign refers to). Peirce’s theory emphasizes the dynamic relationship between the sign, its interpretation, and its object, allowing for a more fluid and open-ended understanding of meaning-making (Peirce, 1931).

Peirce’s model helps explain how individuals use signs to create meanings that evade censorship algorithms. For instance, a "thumbs-up" emoji may signify support (interpretant), solidarity in a protest (object), and vary in form (representamen) across platforms or contexts. This interplay of linguistic and visual semiotics enables cryptic, context-dependent communication in politically sensitive areas (Sikdar & Kule, 2022).

Semiotics is a valuable tool for analysing how language and symbols are used in social media. Communication on these platforms relies on multiple semiotic resources—words, images, sounds, and gestures—making multimodality essential for understanding encryption techniques. By combining linguistic elements with visual or symbolic practices, users' obscure messages while preserving meaning for specific audiences (Riaz et al., 2024).

Emojis, as semiotic signs, enhance or obscure meaning. For example, a raised fist can symbolize resistance, solidarity, or rebellion, depending on the context. In war zones, such practices help activists bypass content moderation algorithms that flag specific keywords. The strategic use of emojis and Unicode symbols is particularly effective in heavily monitored environments (Cobbe, 2021).

Similarly, misspellings or altered spellings leverage the flexibility of language, as Saussure noted that signs are relational and context dependent. By altering spellings, users preserve meaning while evading keyword-based censorship filters. This linguistic encryption is widely used in digital activism, ensuring messages are understood within communities while avoiding detection (Dawson, 2024).

RESEARCH METHODOLOGY

This section outlines the research methodology employed in this study to investigate the use of encryption techniques in social media posts, particularly in politically sensitive contexts. The study adopts a mixed-methods approach, combining quantitative and qualitative perspectives to systematically analyse and interpret the data. By integrating these two strategies, the research aims to provide a comprehensive understanding of how encryption techniques are utilized to navigate censorship and convey messages in digital communication. The following subsections detail the philosophical foundations, research strategy, data collection methods, sampling procedures, and analytical techniques used to achieve the study's objectives.

Research Philosophy and Approach

In the quantitative part of this study, it will adopt a positivist research philosophy which assumes that it is possible to quantify social events or phenomena (Ali, 2024). This philosophy is in line with the study's aim to identify and quantify the most common types of encryption techniques used in social media posts. This study is in the line of studies that believe that it is possible to use positivism in contemporary media research (Rammal et al., 2024). In addition, a semiotic perspective will be incorporated in this study to interpret the symbolic meaning behind the encryption techniques. Semiotics, as the study of signs and symbols, will help analyse how certain encryption techniques (e.g., emojis, misspellings, Unicode) carry hidden or alternative meanings that help users navigate censorship.

Research Strategy

The research will utilize a multi-strategy approach starting by a qualitative method and the findings explored sequentially by a quantitative method. It adopts a case study design, which allows for a snapshot of the current state of encryption techniques used in social media posts at a specific point in time. The research will explore text-based posts made during the Israeli war on Gaza that started in 2023 and examine the use of encryption techniques to bypass censorship.

Furthermore, a semiotic analysis framework will be employed to interpret the signs and symbols used in the encrypted posts. This will allow the researcher to assess the layers of meaning behind encryption practices and their implications for communication in sensitive contexts. By integrating quantitative analysis (frequency, distribution) and semiotic analysis (interpretation of symbols and signs), the study will provide a richer, more nuanced understanding of encryption techniques.

Data Collection Methods

The primary data collection method will involve content analysis of social media posts published following “Operation Al-Aqsa Flood (Tufan Al-Aqsa)” between 2023 and 2024. Text analysis is particularly well-suited for studying social media communication, as it enables the systematic categorization of text-based data. The researcher will analyse 80 posts from four social media platforms: WhatsApp, X (formerly Twitter), Instagram, and TikTok, with a specific focus on encryption in politically sensitive contexts. Arabic text-based posts will be extracted and analysed to identify the use of various encryption techniques, such as Unicode symbols, emojis, intentional misspellings, and other semiotic signs.

Each post will be interpreted semiotically to understand the meaning of the encryption techniques. For example, emojis may carry cultural or political meanings that go beyond their simple visual representation. Semiotic analysis will help identify whether these symbols are being used strategically to bypass censorship or to communicate certain political messages.

In this context, the researcher will examine posts across multiple platforms, collecting a sample of 20 posts from each platform to compare the frequency and type of encryption techniques used on WhatsApp, X (formerly Twitter), Instagram, and TikTok.

Sampling Procedures

The study will employ probabilistic random sampling in the quantitative to collect numerical data for statistical analysis preceded by a purposive criterion sampling in the qualitative part for textual analysis in which it selects posts based on specific criteria that align with the study's objectives. The criteria will include:

- Posts that are publicly accessible on the selected platforms (Instagram, X, TikTok) and WhatsApp groups (limited to groups that can be joined via public links only) will be analysed.
- Posts related to war situations, specifically those made during the Israeli war on Gaza and the Israeli war of 2024 on Lebanon.
- Posts that employ one or more encryption techniques (e.g., Unicode symbols, emojis, misspellings, etc.).

Data Analysis

The data analysis will combine quantitative and semiotic methods to offer a thorough understanding of the encryption techniques utilized in social media posts.

a. Statistical Analysis:

- Descriptive statistical techniques will be used to calculate the frequency of each encryption technique (e.g., emojis, Unicode, misspellings) and the distribution of these techniques across different platforms (WhatsApp, X, Instagram, and TikTok).

- Data will be analysed using IBM SPSS Statistics 26 (Statistical Product and Service Solutions (Hejase & Hejase, 2013, p. 58) to generate statistical outputs, including frequencies, percentages, and distributions across social media platforms.

b. *Semiotic Analysis:*

- Semiotic analysis will be used to interpret the symbols and signs employed in the encrypted posts. For instance, certain emojis may be interpreted as political or resistance symbols, while misspellings may act as a form of linguistic encryption.
- The study will also engage in textual semiotics to understand how language and symbols are used to convey meaning in a censored environment. This will allow the researcher to explore the intentionality behind encryption practices and how these practices serve to circumvent algorithmic censorship.

RESULTS AND DISCUSSION

This section outlines the study's findings and explores their implications regarding the encryption techniques employed in social media posts, especially within politically sensitive contexts. The results are organized to highlight the most commonly used encryption methods, their variations across different platforms, and their semiotic interpretations. Through a combination of quantitative analysis and semiotic insights, this section aims to provide a comprehensive understanding of how users navigate censorship and convey covert messages in digital spaces. The discussion further explores the strategic and adaptive nature of these techniques, shedding light on their role in contemporary digital communication.

Most Commonly Used Encryption Techniques

This section, as illustrated in Table 3, provides an overview of the various encryption techniques identified in the social media posts analysed in this study. The primary objective is to explore how users within the Axis of Resistance strategically employ these methods to circumvent algorithmic censorship. By examining the frequency and application of techniques such as Unicode symbols, misspellings, character separation, and mixed language, the study sheds light on the innovative ways users adapt their communication to evade detection while conveying politically sensitive messages. These practices not only highlight the resilience of digital activism but also underscore the ongoing cat-and-mouse game between users and automated content moderation systems. Through this analysis, the study aims to contribute to a deeper understanding of how encryption techniques are utilized in politically charged environments to maintain freedom of expression and resist oppression.

Table 3: Corresponding frequency of encryption techniques

Encryption Techniques	Presence	Frequency	Percent
Unicode	No	39	48.8%
	Yes	41	51.2%
Misspelling	No	75	93.8%
	Yes	5	6.3%
Separating	No	41	51.2%
	Yes	39	48.8%
StrikeThrough	No	76	95%
	Yes	4	5%

Prolonging	No	63	78.8%
	Yes	17	21.3%
Blurring	No	74	92.5%
	Yes	6	7.5%
MixedLang	No	64	80%
	Yes	16	20%
Emojis	No	77	96.3%
	Yes	3	3.8%

The content analysis of social media posts across four platforms revealed varying frequencies in the use of encryption techniques. Unicode symbols were among the most common methods, appearing in 41 posts (51.2%), indicating their use to encode meanings or bypass restrictions. In contrast, 39 posts (48.8%) did not use this method.

Misspelling was the least used encryption technique, found in only 5 posts (6.3%), suggesting they are not widely adopted for bypassing censorship. The majority of posts—75 (93.8%)—did not use misspellings, indicating users prefer more effective techniques.

Character separation was used in 39 posts (48.8%), while 41 posts (51.2%) did not. This highlights that character separation is fairly common but not as universal as Unicode symbols. Similarly, strike-throughs were used in only 4 posts (5%), with the majority—76 posts (95%)—not using this technique, suggesting that strikethroughs are less preferred or effective for encryption.

Prolonged characters appeared in 17 posts (21.3%), while 63 posts (78.8%) did not incorporate this method. Though more common than strikethroughs and misspellings, prolonged characters were still used in a relatively small percentage of posts. Blurring, found in 6 posts (7.5%), was another encryption method not widely adopted, with 74 posts (92.5%) not using it.

Mixed language, observed in 16 posts (20%), was another method of covert communication, though less prevalent than Unicode symbols or character separation. Emojis were among the least utilized techniques, appearing in only 3 posts (3.8%) and absent in 77 posts (96.3%), suggesting they are not a primary method for encrypted communication.

a. Encryption Techniques in Posts

This section presents key examples of the top four encryption strategies used by users affiliated with the Axis of Resistance across social networking platforms. Instead of screenshots, which may pose copyright concerns, the section includes paraphrased excerpts and summaries that reflect actual usage while preserving the anonymity and authenticity of the original posts. In several instances, multiple techniques were combined within a single post to enhance evasion and effectiveness.

These examples, aligned with the frequency analysis findings, demonstrate how users modify formatting and language to evade algorithmic detection and platform censorship. The text samples illustrate primary strategies such as Unicode manipulation, character separation, character extension, and mixed-language usage, showcasing the ingenious and contextual tactics employed in politically sensitive digital discourse.

For example, a post on Platform X from December 2024 featured a term written in Unicode-manipulated Arabic script (e.g., 'إسرا...ئيل' instead of the standard 'إسرائيل'). This encrypted style alters the text enough to bypass automated filters while remaining readable to human audiences, which helps explain why Unicode manipulation emerged as the most prevalent technique, appearing in 51.25% of posts.

Another instance from Instagram (November 2024) illustrated the implementation of character spacing, with a caption like ‘الش هداء’ instead of ‘الشهداء’. This technique disrupts keyword detection without compromising the clarity of the message for the intended audience. Character spacing appeared in 48.75% of posts, underscoring its tactical significance.

One of the August 2024 TikTok captions utilized character extension to elongate key terms such as 'الضــــاحية' and 'الضـــــربة'. This affective strategy, used in 21.3% of examples, intensified the emotional impact of the message while tactically interfering with keyword recognition algorithms.

Lastly, a TikTok post from November 2024 employed mixed language by alternating between Arabic and English within the same sentence or even the same word (e.g., “بمقاwمة” 'but the world is blind'), complicating detection while enhancing nuance. This method, found in 20% of posts, highlights how linguistic hybridity is weaponized for semiotic subversion.

Together, these examples shed light on the means through which activists employ textual creativity instead of image-driven tactics within closed digital spaces. Through the combination of creative uses of symbols, spacing, linguistic variability, and emotive content, users are capable of sustaining digital resistance without drawing notice from automated censorship systems.

b. Analysis of Results

The results, as illustrated in Figure 1, highlight the critical role of innovative and context-sensitive communication strategies within the Axis of Resistance. The analysis demonstrates that users are actively leveraging a variety of encryption techniques to circumvent censorship, with Unicode symbols and character separation emerging as the most widely adopted methods. These techniques are favoured for their ability to obscure content effectively while maintaining readability for the intended audience. In contrast, the limited use of other methods, such as misspellings, strikethroughs, and blurring, suggests that users are highly selective in their approach, prioritizing techniques that strike a balance between effectiveness and practicality.

This selectivity underscores the importance of efficiency in encrypted communication, as users navigate the challenges of censorship without compromising the clarity or accessibility of their messages. These insights offer a nuanced understanding of the strategies employed by users in politically sensitive and censored environments. They reveal a dynamic and adaptive approach to communication, where users continuously refine their methods to stay ahead of detection mechanisms. Furthermore, the findings emphasize the need for adaptive and responsive approaches to both censorship and encryption, as users and censors engage in an ongoing cycle of innovation and counter-innovation. By understanding these strategies, stakeholders can better address the complexities of communication in restricted environments, whether to support secure communication or to develop more effective censorship tools.

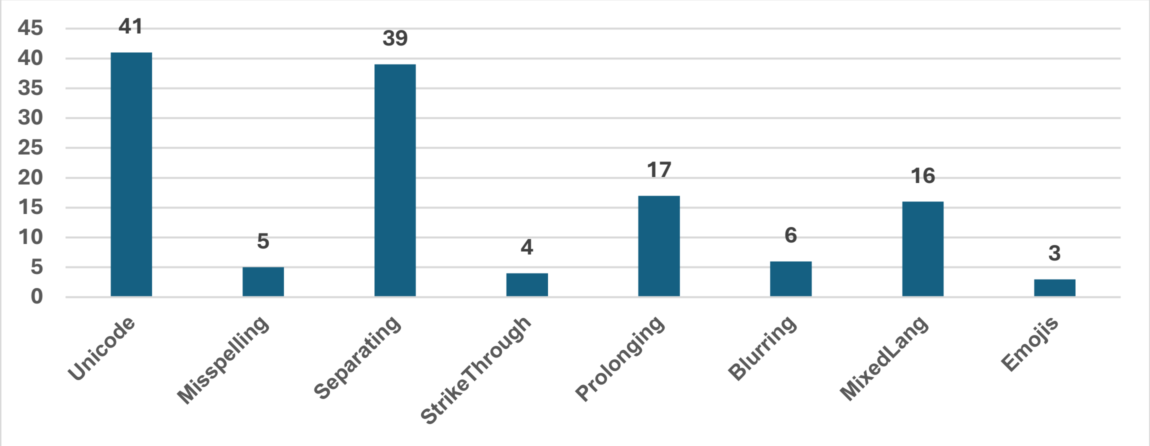

Figure 1: Encryption techniques usage

Variations in Encryption Techniques across Social Media Platforms

This section examines how encryption techniques differ across social media platforms, reflecting users' adaptation to each platform's unique features and constraints and the crosstab analysis highlights these variations.

a. Crosstab Analysis

The crosstab analysis, as depicted in Table 4, reveals significant variations in the use of encryption techniques across the four platforms.

Table 4: Crosstab analysis for encryption techniques and social media platforms

	Instagram	Tiktok	WhatsApp	X	total
Unicode	9	9	10	13	41
Misspelling	1	0	2	2	5
Separating	5	12	15	7	39
Strikethrough	3	0	1	0	4
Prolonging	5	7	1	4	17
Blurring	3	2	1	0	6
MixedLang	2	4	4	6	16
Emojis	0	1	1	1	3

Unicode symbols, the most frequently used technique, were prominently employed on X (13 instances), WhatsApp (10 instances), and equally on Instagram and TikTok (9 instances each). This suggests that Unicode is versatile and effective across platforms, particularly on X and WhatsApp, where its ability to obscure content aligns with users' needs to navigate sensitive topics.

Character separation was most common on WhatsApp (15 instances) and TikTok (12 instances), with fewer occurrences on Instagram (5 instances) and X (7 instances). This indicates that WhatsApp and TikTok users favour this technique, potentially due to the platforms' ease of use and the need to avoid censorship while maintaining clarity for intended audiences.

Prolonging characters exhibited a platform-specific distribution, with TikTok (7 instances) and Instagram (5 instances) showing higher usage, while WhatsApp (1 instance) and X (4 instances) had limited occurrences. This suggests that prolonging characters is more suited to platforms emphasizing visual or creative text expression.

Mixed language usage was observed primarily on X (6 instances) and TikTok (4 instances), reflecting the platforms' role in reaching multilingual audiences. WhatsApp and Instagram exhibited moderate mixed language usage, with 4 and 2 instances, respectively.

Techniques such as misspellings, blurring, strikethroughs, and emojis were less common overall. However, the use of strikethroughs appeared uniquely on Instagram (3 instances), while emojis were sporadically employed across TikTok, WhatsApp, and X, with just 1 instance each. These findings suggest that less prevalent techniques are employed selectively, perhaps for their symbolic value or specific communicative needs.

b. Analysis of Encryption Usage on Each Platform

This section analyses the frequency and types of encryption techniques employed by social media users in the Axis of Resistance on four major platforms: WhatsApp, X, Instagram, and TikTok. The data presented in Figure 2 reveals distinct patterns of encryption usage across these platforms, shaped by the different communication styles and content formats prevalent on each platform.

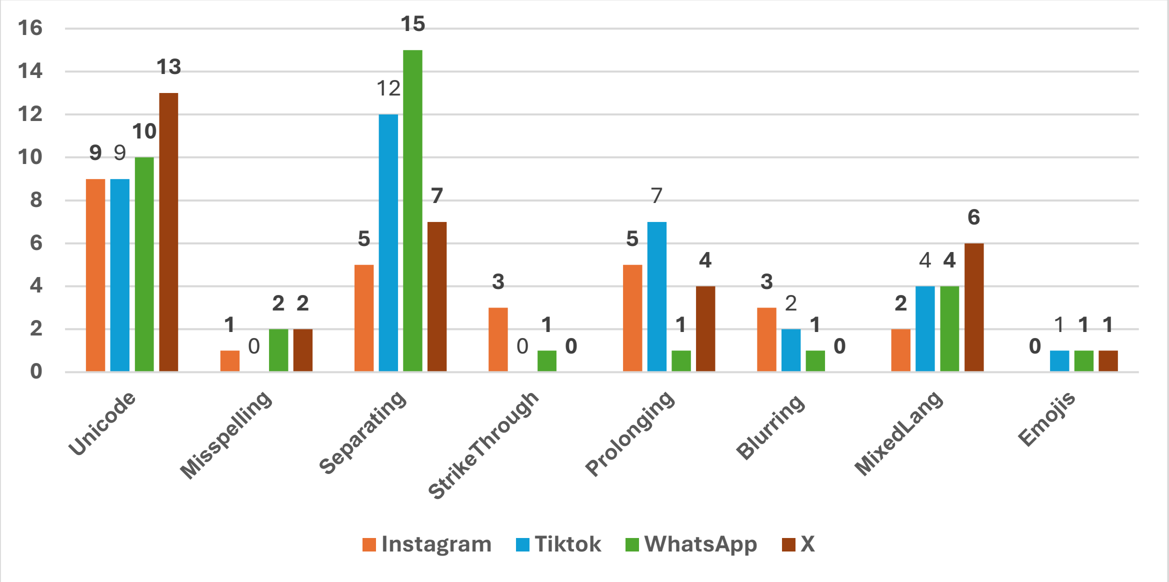

Figure 2: Encryption usage on each platform

The analysis reveals distinct patterns in encryption techniques across social media platforms. On WhatsApp, Unicode symbols (10 instances) and character separation (15 instances) are the most common, reflecting the platform's private messaging environment where clarity and evasion of censorship are prioritized. X (formerly Twitter) shows the highest use of Unicode symbols (13 instances), along with moderate use of character separation (7 instances) and mixed language (6 instances), highlighting its text-heavy and creative nature. Instagram emphasizes Unicode symbols (9 instances) and character separation (5 instances), with strikethroughs (3 instances) being uniquely popular due to their visual appeal. TikTok favours character separation (12 instances) and Unicode symbols (9 instances), aligning with its fast-paced, multimedia-driven format. Across all platforms, less common techniques like emojis and misspellings are rarely used, indicating a preference for text-based encryption strategies.

Semiotic Interpretation of Encryption Practices

Table 5 highlights a diverse range of encryption techniques used to evade censorship and convey covert political messages. These methods, which include text manipulations like misspellings and prolonged characters, as well as the creative use of emojis and mixed languages, function as semiotic tools. They serve a dual purpose: obscuring meaning from automated detection systems while simultaneously communicating resistance to political oppression. Each technique represents a strategic adaptation to the digital surveillance environment, where the goal is to preserve the integrity of politically charged messages without triggering algorithmic suppression. The combination of these techniques creates a layered and dynamic form of communication, reflecting the adaptability and creativity of users in navigating censorship.

Table 5: Illustrative examples of encryption technique usage across platforms

Encryption Technique	Category/Description	Example
Text Strike Through	Words are crossed out to indicate invalidity or censorship.	martyr → ~~martyr~~
Blurring Text	Words are made unclear or hazy to obscure meaning.	martyr → 𝒎𝒂𝒓𝒕𝒚𝒓
Separating Characters	Letters are spaced out to disrupt recognition.	explosion → e x p l o s i o n
Emojis	Emojis replace parts of words to hide or alter meaning.	Israel → 🕎
Unicode Symbols	Special characters are inserted to obscure readability.	martyr → m@rtyr
Prolonging Characters	Letters are repeated or extended unnaturally.	martyr → maaaaartyr
Misspelling for Avoidance	Words are deliberately misspelled to avoid detection.	martyr → maetyr
Mixed Language	Combines multiple languages within a single word or phrase.	resistance → resisتance
Separating Characters & Unicode	Combines spacing and symbols for maximum obfuscation.	martyr → µ @ . r † .y r
Mixed Language & Unicode	Combines language mixing with special symbols.	resistance → resi..staنce
Mixed Language & Separating	Combines language mixing with spaced-out letters.	Netanyahu → Ne t a n ياهو

DISCUSSION AND CONCLUSIONS

This research explored the encryption techniques used by social media users in the Axis of Resistance to circumvent algorithmic censorship during the latest Israeli war on Gaza that started in October 2023. The findings show that users employed a variety of encryption strategies, with Unicode symbols and character separation emerging as the most commonly used methods. These techniques reflect the adaptability and resilience of users in politically sensitive and highly censored environments.

The data revealed that over half of the posts (51.2%) employed Unicode symbols, a significant encryption method for evading detection by censorship algorithms. This supports previous research on visual encryption techniques, which often bypass content moderation systems that struggle to recognize non-Latin scripts or special characters. In contrast, simpler techniques like misspellings were less prevalent, appearing in only 6.3% of posts, suggesting limited effectiveness against sophisticated AI-based systems.

Platform-specific variations were also observed. WhatsApp, with its private messaging feature, showed a higher frequency of character separation, while TikTok’s multimedia format favoured character prolongation. This indicates that users adapt their encryption strategies based on the platform’s format and capabilities.

The semiotic analysis further illustrated the depth of meaning encoded in these techniques. For example, mixed languages and emojis not only circumvented censorship but also signified solidarity, political resistance, or cultural identity. These practices underscore the importance of digital communication in war zones, where each post carries significant socio-political implications.

The findings highlight the importance of digital resilience in politically sensitive regions, where algorithmic censorship poses a substantial threat to freedom of expression. The encryption techniques identified—such as Unicode symbols, character separation, and mixed language—are vital tools for individuals resisting algorithmic suppression. These results emphasize the need for more nuanced content moderation strategies that take cultural and political contexts into account, as well as the necessity for continued innovation in encryption methods to maintain freedom of expression in digital spaces. The variations in encryption techniques across different platforms suggest the need for platform-specific solutions that cater to the diverse ways in which users engage with digital content. Future research should explore how these techniques evolve in response to advancements in AI censorship algorithms, as well as the role of user creativity in resisting digital oppression. By understanding these adaptive strategies, policymakers, activists, and platform developers can better address the challenges posed by algorithmic censorship and work toward safeguarding free expression in the digital age.

LIMITATION OF THE STUDY

This study explores encryption techniques used by social media users in the Axis of Resistance during the latest Israeli war on Gaza that started in October 2023 but has notable limitations. With a small sample of 80 posts, it may not fully represent the diversity of techniques across regions, languages, and platforms. Additionally, focusing on just four platforms excludes others like Telegram and Signal, limiting comprehensiveness. The study’s temporal scope and focus on Arabic-language posts further reduce generalizability, while the dynamic nature of algorithmic censorship poses challenges to capturing evolving strategies. Ethical barriers also restricted access to private content, underexplored qualitative insights, and highlighted geopolitical sensitivities. To address these gaps, future research should expand sample diversity, include additional platforms, employ advanced tools, and incorporate user perspectives for deeper insights into digital resistance strategies.

BIODATA

Hassan Rammal, He is currently a Digital Graphic Course Coordinator at Al Maaref University, Beirut, Lebanon. His work experience encompasses branding, animation, and digital design. He holds Master of Fine Arts (MFA) in Motion Graphics and Master of Arts by Research (MA Res) in Arts Philosophy. He has been involved in academic activities as a lecturer and research contributor through conferences, seminars, and workshops since 2013. He is a scholar of visual communication research where he synthesizes pedagogy, creative practice, and research leadership in the field of visual communication. Email: hassan.rammal@mu.edu.lb

REFERENCES

Abokhodair, N., Skop, Y., Rüller, S., Aal, K., & Elmimouni, H. (2024). Opaque algorithms, transparent biases: Automated content moderation during the Sheikh Jarrah Crisis. *First Monday, 29*(4-1). https://doi.org/10.5210/fm.v29i4.13620

Al-Dala'ien, O. A., Al-Daher, Z., Al-Shboul, Y., & Al-Rousan, M. (2023). Analyzing verbal and pictorial Arab's Facebook posts During the Israeli attack on Gaza Strip in 2021. *GEMA Online Journal of Language Studies*, *23*(1), 114–139.

Al-Jarrah, A., Albsharat, A., & Al-Jarrah, M. (2022). Word-based encryption algorithm using dictionary indexing with variable encryption key length. *International Journal of Electrical and Computer Engineering, 12*(1), 669–683. https://doi.org/p8ds

Ali, I. M. (2024). A guide for positivist research paradigm: From philosophy to methodology. *Idealogy Journal*, *9*(2), 187-196. https://doi.org/p8dt

Buckley, N., & Schafer, J. S. (2022). 'Censorship-free' platforms: Evaluating content moderation policies and practices of alternative social media. *For(e)Dialogue, 4*(1). https://doi.org/10.21428/e3990ae6.483f18da

Cobbe, J. (2021). Algorithmic censorship by social platforms: Power and resistance. *Philosophy & Technology*, *34*(4), 739-766.

Daucé, F., & Loveluck, B. (2021). Codes of conduct for algorithmic news recommendation: The Yandex. News controversy in Russia. *First Monday, 26*(5). https://doi.org/p8dv

De Saussure, F. (1959). *Course in General Linguistics* [Trans. W. Baskin]. Philosophical Library.

Dawson, S. (2024). *You Can't Say That on TikTok: Cxnsxrshxp, Algorithmic (in) visibility, and the threat of Representation* (Doctoral dissertation, University of British Columbia).

El Zein, H., & Abusalem, A. (2015). Social media and the war on Gaza: A battle on virtual space to galvanise support and falsify Israel story. *Athens Journal of Mass Media and Communications*, *1*(2), 109-120.

Ermoshina, K., & Musiani, F. (2022). *Concealing for Freedom: The Making of Encryption, Secure Messaging and Digital Liberties*. Manchester, UK: Mattering Press.

Fedoruk, B., Nelson, H., Frost, R., & Fucile Ladouceur, K. (2021). The Plebeian Algorithm: A Democratic Approach to Censorship and Moderation. *JMIR Formative Research*, *5*(12), e32427. http://doi.org/10.2196/32427

Gohdes, A. R. (2024). *Repression in the Digital Age: Surveillance, Censorship, and the Dynamics of State Violence*. Oxford, OX: Oxford University Press.

Hejase, A. J., & Hejase, H. J. (2013). *Research Methods: A Practical Approach for Business Students* (2nd ed.). Philadelphia, PA: Masadir Inc.

Huang, T. C. (2022). Private censorship, disinformation and the first amendment: Rethinking online platforms regulation in the era of a global pandemic. *Michigan Technology Law Review, 29*(1), 137-196. https://doi.org/10.36645/mtlr.29.1.private

Iannone, A. (2022). Democracy crisis in South-East Asia: Media control, censorship, and disinformation during the 2019 Presidential and General Elections in Indonesia, Thailand and 2019 Local Election in the Philippines. *Jurnal Ilmu Sosial dan Ilmu Politik*, *26*(1), 81-97.

JosephNg, P. S., EricMok, Z. C., Phan, K. Y., Sun, J., & Wei, Z. (2025). Mitigating social media cybercrime: Revolutionising with AES encryption and generative AI. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, *46*(2), 124-154.

Khader, M., & Karam, M. (2023). Assessing the effectiveness of masking and encryption in safeguarding the identity of social media publishers from advanced metadata analysis. *Data*, *8*(6), 105. https://doi.org/10.3390/data8060105

Kshetri, N., Rahman, M. M., Rana, M. M., Osama, O., & Hutson, J. (2024). AlgoTRIC: Symmetric and asymmetric encryption algorithms for Cryptography - A comparative analysis in the AI era*. International Journal of Advanced Computer Science and Applications, 15*(12). http://doi.org/10.14569/IJACSA.2024.0151201

Latif, M. S. A., Manap, N. A., & Althabhawi, N. M. (2025). Modernising site-blocking mechanism in protecting copyright owners content against digital piracy in Malaysia. *Malaysian Journal of Syariah and Law*, *13*(1), 1-17.

Liaqat, F., Khan, M. A., & Qamar, S. S. (2024). Humanity unframed: A socio-semiotic analysis of political cartoon on Israel-Palestine Conflict. *Jahan-e-Tahqeeq*, *7*(1), 1157-1168.

Mahlouly, D., & Erhaim, Z. (2023). Pro-Palestinian activism: Resisting the digital occupation. In N. Miladi (Ed.), *Global Media Coverage of the Palestinian-Israeli Conflict: Reporting the Sheikh Jarrah Evictions* (237-250). I.B. Tauris. https://doi.org/p8dw

Matthiesen, T. (2022). Digital activism and authoritarianism adaptation in the Middle East. *Journal of Global Media Studies, 15*(2), 45–63.

Majdawi, A. M. A., & Jabi, S. I. (2020). A pragma-Semiotic analysis of emoticons in social media. *Education and Linguistics Research*, *6*(2), 139.

Musdalifah, F. S., Nasyaya, A., & Santoso, A. D. (2023). Digital voices in early days: Analysing local government social media approaches to risk communication during the initial stages of the COVID-19 pandemic in Indonesia. *Jurnal Komunikasi: Malaysian Journal of Communication*, *39*(4), 126-149. https://doi.org/10.17576/JKMJC-2023-3904-07

Nadesan, M. (2021). Technological utopia, end times and the SARS-CoV-2 crisis: A genealogy of crisis ideoscapes and mediascapes. *Communication+1*, *8*(1). https://doi.org/p8dx

Olise, F. (2021). Level of acceptance of news stories on social media platforms among youth in Nigeria. *Jurnal Komunikasi: Malaysian Journal of Communication*, *37*(2), 210-225.

Oltmann, S. M., Knox, E. J., & Mabi, M. N. (2022). Censorship is not a panacea: Access to information in a resilient society. *Proceedings of the Association for Information Science and Technology*, *59*(1), 591-594.

Öztürk, N. K. (2024). Meta's challenge with Olives and Watermelon: The case of blocking posts about Gaza. *Journal of Media and Religion Studies*, *7*(2), 101-121.

Panait, C., & Ashraf, C. (2021). AI Algorithms–(re) shaping public opinions through interfering with access to information in the online environment. *Europuls Policy Journal*, *1*(1), 46-64.

Park, D. J. (2023). US foreign policy, think tanks, control over web content, and the threat to democracy. In Y. Kamalipour, & J. V. Pavlik (Eds.), *Communicating Global Crises: Media, War, Climate, and Politics* (pp.55-74). London, UK: Bloomsbury Publishing. http://doi.org/10.5040/9798881813222.ch3

Peirce, C. S. (1931) *The Collected Papers of Charles Sanders Peirce*. Cambridge, MA: Harvard University Press.

Qureshi, M. B., Qureshi, M. S., Tahir, S., Anwar, A., Hussain, S., Uddin, M., & Chen, C.-L. (2022). Encryption techniques for smart systems data security offloaded to the cloud. *Symmetry, 14*(4), 695. https://doi.org/10.3390/sym14040695

Rammal, H., Hejase, H.J., & Hazimeh, H. (2024). Metaverse technology and its impact on the evolving landscape of communication and media: A future outlook for Lebanese satellite channels. *Saudi Journal of Humanities and Social Sciences, 9*(3), 92-117. https://saudijournals.com/media/articles/SJHSS_93_92-117.pdf

Raykar, N., Kumbharkar, P., & Jayatilal, D. H. (2023). De-duplication avoidance in regional names using an approach based on pronunciation. *International Journal of Advances in Electrical Engineering*, *4*(1), 10-17.

Riaz, N., Qureshi, Q. A., Tahir, S., & Waheed, I. (2024). Signs and symbols: A semiotic exploration of visual media and its underlying ideologies. *Journal of Arts and Linguistics Studies*, *2*(2), 705-725.

Rumata, V. M., & Nugraha, F. K. (2020). An analysis of fake narratives on social media during the 2019 Indonesian presidential election. *Jurnal Komunikasi: Malaysian Journal of Communication*, *36*(4), 351-368.

Sangwan, Y. S., Lal, S., Bhambri, P., Kumar, A., & Dhanoa, I. S. (2021). Advancements in social data security and encryption: A review. *NVEO-Natural Volatiles & Essential Oils Journal, 8*(4), 15353-15362.

Sikdar, S., & Kule, M. (2022). Recent trends in cryptanalysis techniques: A review. In R. Sarkar, S. Pal, S. Basu, D. Plewczynski, & D. Bhattacharjee (Eds.), *International Conference on Frontiers in Computing and Systems* (pp. 209-222). Singapore: Springer Nature Singapore Private Limited.

Tanczer, L. M., Deibert, R. J., Bigo, D., Franklin, M. I., Melgaço, L., Lyon, D., Kazansky, B. & Milan, S. (2020). Online surveillance, censorship, and encryption in academia. *International Studies Perspectives*, *21*(1), 1-36.

Tomasev, N., McKee, K. R., Kay, J., & Mohamed, S. (2021). Fairness for unobserved characteristics: Insights from technological impacts on queer communities. *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society* (pp. 254-265), May 19–21, Virtual Event, New York, USA. https://doi.org/p8dz

Umar, H. G. A., Aoun, M., Kaleem, M. A., Rehman, S. U., & Younis, M. (2023). Cryptographic Analysis of Blur-Based Encryption an in-depth examination of resilience against various attack vectors. *Journal of Computing and Biomedical Informatics, 5*(2). https://doi.org/10.56979/502/2023

Vorhies, Z., & Heckenlively, K. (2021). *Google Leaks: A Whistleblower's Exposé of Big Tech Censorship*. New York, NY: Simon and Schuster.

Wadho, S. A., Meghji, A. F., Yichiet, A., Kumar, R., & Shaikh, F. B. (2023). Encryption techniques and algorithms to combat cybersecurity attacks: A review. *VAWKUM Transactions on Computer Sciences*, *11*(1), 295-305.

Wells, A. (2024). Digital refugee resistance, power, representation, and algorithmic censorship. *Forced Migration Review*, *73*. https://www.fmreview.org/digital-disruption/wells/

Wok, S., Hashim, J., & Abdullah, K. (2016). Social media influence on Malay family resilience towards challenges of the Internet. *Jurnal Komunikasi: Malaysian Journal of Communication, 32*(2), 648-669.

Youvan, D. C. (2024, November 17). Conflict, crisis, and continuity: Media control, proxy wars, and the preservation of power in democratic systems. https://doi.org/p8d2

Zhang, G. (2024). Cryptographic techniques in digital media security: Current practices and future directions. *International Journal of Advanced Computer Science & Applications*, *15*(8), 933-941. http://doi.org/10.14569/IJACSA.2024.0150892

Zhang, N., & Díaz-Kommonen, L. (2024). Toward a rhetorical understanding of Chinese political internet memes amid a Chinese governance crisis. *Communication and Democracy*, *58*(2), 226-261.

Zhang, W., Hernandez-Boussard, T., & Weiss, J. (2023). Censored fairness through awareness. In B. Williams, Y. Chen. & J. Neville (Eds.), *Proceedings of the AAAI Conference on Artificial Intelligence*, *37*(12), 14611-14619. https://doi.org/p8d3