

IMAGE FORGERY-DRIVEN MISINFORMATION AND ITS IMPACT ON LOCAL SELF-GOVERNMENT NETWORKS

Ponney V M^{*1}, Velammal B L², Kulothungan K³

¹Research Scholar, Department of IST, CEG Anna University, Guindy, Chennai 600025

²Associate Professor, Department of CSE, CEG Anna University, Guindy, Chennai 600025

³Kulothungan K, Assistant Professor, Department of IST, CEG Anna University, Guindy, Chennai 600025,

velammalkarthik@gmail.com²

kulo@aiust.net³

Abstract: Misinformation through image-forgery has been a global governance issue on the local self-government institutions. This paper focuses on the administrative, political, and social effects of faked images in five municipalities in two countries via a qualitative approach to the issue comprising of case study, semi-structured interviews, and regulatory analysis. In the analysis, twenty-seven cases of misinformation were found to be related to forged images, which can be divided into emergency-related, communal-sensitive, infrastructure-related, and authority-targeted forgeries that are summarized in Table 1. The topological distributions in Figure 2 depict that there is a strategic approach to the use of forged images, especially in election periods and consultations on the budget with the public. Results indicate that there are great discrepancies in administrative verification processes that culminate to delayed or misplaced responses and high levels of distrust by the population as demonstrated in Table 2. The paper also notes communication asymmetry, institutional capacity voids, and amplification of misinformation by political factors as some of the major weaknesses in governance. The suggested solution to these problems is a multi-layered policy framework that entails municipal misinformation policies, Digital Verification Units, reforms in regulations, and strategies to communicate with the population, collaborative efforts by cyber crimes, the integration of technical tools, and community-driven digital literacy efforts. All in all, the paper highlights that image forgery is not a technological accident, but a structural misgoverning problem that must be addressed through the concerted efforts of institutions and policy changes.

Keywords: local self-government , forged images, Digital Verification and misgoverning problem.

1. Introduction

The current situation of local governments is a more intricate information ecosystem in which visual information spreads quickly through the social media, messaging services, and community networks [1]. Although digital communication has made the communication more transparent and accessible, it has also brought about new vulnerabilities, especially due to the spread of fabricated or manipulated images [2]. Image-forgery-inspired misinformation Image-forgery driven by digitally manipulated images or synthetic images created by AI can mislead societies, distort the way an administration operates, and weaken the authority of local governments. Since visual evidence is central to decision-making on the part of the municipalities, in service delivery and in communication with the populations, forged images present a unique governance problem that transcends technological manipulation to the area of institutional credibility and citizen confidence.

Forged images have important implications of governance. In comparison with other types of misinformation that are present in the form of a text, graphic deception is more persuasive, dispersed faster, and arouses a more intense reaction in society [3]. Images are frequently perceived by communities as objective information and hence are highly vulnerable to manipulations of emotion or politically inclined visuals. Such incidences

demonstrate the direct influence of the image manipulation on the administration in terms of priorities and tracks of decisions and the way they influence limited municipal funding or fuel the rise of popular instability.

The institutions of the local self-government are particularly prone as they are often the initial recipient of crisis reporting, community complaint, and checking of the services offered to the population [4]. Municipal communication systems, however, tend to be informal, decentralised, or even reliant on employees with insufficient expertise in digital-forensics. The usual ecosystem in which the spread of forged images occurs is the interaction of community-level WhatsApp groups, political middlemen, and high-socially-influenced actors on social-media. Lacking unified verification procedures and with a disjointed information flow, the chances of misinformation finding its way into official channels are high or the administration may act prematurely [5].

Moreover, the interviews with the municipal commissioners, ward-level administrators, and law enforcement officers indicate that there are significant institutional gaps in readiness to deal with visual misinformation. Most local governments do not have specific units or individuals qualified in image verification, cyber forensics, or crisis communication [6]. The consequences of these limitations are sluggish responses, lack of interdepartmental coordination, and poor clarifications to the population, administrative shortcomings that have been manifested in the discrepancy [7]. The governance stakes were high as in a number of instances, confusion caused by misinformation resulted in reputational losses and quantifiable reduction in citizen confidence.

The issue is further aggravated by the changing regulatory uncertainties regarding the matter of misinformation at the local level. Though laws on cybercrimes are present at the national level, local laws and communication policies do not always clearly specify the roles, procedures, or procedures of handling forged pictures [8]. The local governments therefore exist in a grey zone of regulation whereby institutional reactions depend on administrative discretion and not the laid out policy [9]. This regulatory disintegration is one of the factors that create unequal governance results among the municipalities and helps to confirm the necessity to use a more systematic and policy-based method.

In light of these issues this research paper will offer a governance-focused analysis of the role played by forged images in municipal operation and administrative actions and citizen trust. The combination of case studies, semi-structured interviews, and regulatory review is intended to provide the research with a systematic insight into the administrative vulnerability of visual misinformation. To this end, it suggests the overall policy framework-described further in the manuscript-to increase the institutional resilience, verification capacity, and accountability in government in the context of increasing threats of digital manipulation. In this perspective, the paper will introduce image manipulation not as a technological exception but as a modern problem in governing that needs collective institutional, procedure, and policy responses.

2. Related Works

Visual content manipulation has gradually become a major challenge to governance and administrative practices as identified by the increasing body of research on the subject of digital misinformation [10]. The earlier research on the misinformation literature mainly centered on misinformation by way of text whereas recent research proves that

misleading pictures have more psychological impact and are more viral than misinformation on a textual basis [11]. This work has demonstrated that visual misinformation will hasten emotional reactions, lessen scepticism, and influence the belief of the populace faster than textual accounts and particularly in crises and politically charged situations [12]. This refocusing of scholarly attention highlights the importance of putting image forgeries in context as technological interventions, but as an agent of administrative disturbance.

A large part of the current literature addresses the technological evolution in the field of image forgery and the associated evolution of forensic detection schemes [13]. Deep-fakes, image splicing, pixel-level morphing, and adversarial synthetic imagery studies indicate a new wave of increasing sophistication of manipulation. To detect forged images with improved accuracy computer-vision researchers have suggested many detection systems, including noise inconsistencies, illumination analysis, frequency-domain modelling, and deep-learning classifiers [14]. Although they are useful among national cyber security bodies or massive news organizations, they have not been popular among the local governments. Municipalities are often not technologically equipped, financially endowed or in trained staff to operational such detection systems which further increases the divide between technological possibilities and administrative practice [15].

The study of misinformation implications in governance has been done parallel to public administration studies, and it is especially significant in terms of misinformation impact on institutional legitimacy and crisis communication [16]. Researchers have reported the dissemination of fake news faster than official explanations resulting in the creation of an information asymmetry, undermining the credibility of the administration [17]. According to survey of literature on disaster governance, their findings indicate incidences where misinformation has resulted in disproportional evacuations, lack of coordination in emergency responses, or increased distrust in the local authorities [18]. Likewise, there is evidence on political communication showing that misinformation is common during elections in an attempt to sway people towards a certain opinion of the local authorities, sway voters or even undermine the legitimacy of the local institutions.

Research on local self-government institutions specifically furthers with structural vulnerability, which dictates the vulnerability of the institutions to misinformation [19]. The communication channels in municipalities tend to be decentralized, they have less digital-media surveillance and inconsistent administrative knowledge. Studies conducted on the aspects of decentralize Governance reveal that smaller local governments have greater operational constraints such as under staffing, duplication of roles and responsibilities and lack of coordination between different departments [20]. Such aspects restrict their ability to evaluate the credibility of visual information or react in a competent way to a crisis that is caused by misinformation [21]. International comparisons also draw attention to existing inequalities between urban and rural jurisdictions, with larger municipalities having more technological resilience and institutional preparedness than smaller towns- again in line with the administrative differences [22].

In the meantime, regulatory and legal studies indicate that there is always a lapse in the interpretation and transfer of national cyber crime legislative tools into local-level

procedures [23]. Whereas national laws in most nations outlaw the usage of forged or harmful digital material, meridian governments tend to possess no clear policy provisions that regulate procedural duty, and action measures or a standard of verification [24]. According to scholars, the lack of local legal provisions brings ambiguity in enforcement leaving administrative responses largely arbitrary and incoherent. This regulatory fragmentation conforms to the gaps in governance mentioned in the current study where the municipalities did not have a specific set of protocols on how to identify, report, or act upon image-based misinformation.

Finally, an increasing body of literature examines how misinformation is socio-politically exaggerated, especially within an electoral period, when a community is in conflict, and when individuals are consulting their budget. Research has shown that misinformation can be willfully used by political power or interest groups to sway the general opinion of people, create social tension or destabilize governance practices. These observations are in line with a number of trends in cases depicted in Figure 1 and in Section 4 whereby fake photographs were shared at opportune times amid politically unstable moments, adding burden to the administration and communal division.

In general, current literature gives a solid empirical and theoretical background on digital misinformation, but none of the research focuses on forged images and governance of local governments. Little research exists on the direct effects of manipulated images on the administrative decision process, citizen trust, or the resilience of institutions on the local level. There is thus a significant gap that this research bridges when it comes to the technological, administrative, and regulatory aspects of image forgery by providing a governance-based perspective of image forgery in local self-government systems.

3. Methodology

The research design that has been embraced in this study is the governance-based qualitative research design suitable in the examination of the complex administrative behaviors in local governments that are decentralized. Since the misinformation caused by the image forgery does not concern entirely technical spheres, but institutional trust, administrative processes, and political messages, a qualitative framework was required to grasp the organizational and socio-political processes in the game. The methodological framework is a three-fold reinforcing framework that includes (i) comparative case study of the municipalities that were subjected to image-based misinformation, (ii) semi-structured elite interviews with the administrative actors in digital governance and (iii) a policy and regulatory review that involves legal gaps and responsibilities of the sub-national level. Collectively, these elements bring a multidimensional insight into the ways in which forged images affect the local governance practices and the ways of the administrative systems reacting to pressure by misinformation (figure 1). Each of the methods was designed in a way that there was conceptual consistency with theoretical frameworks of multi-level governance, administrative capacity and institutional resiliency.

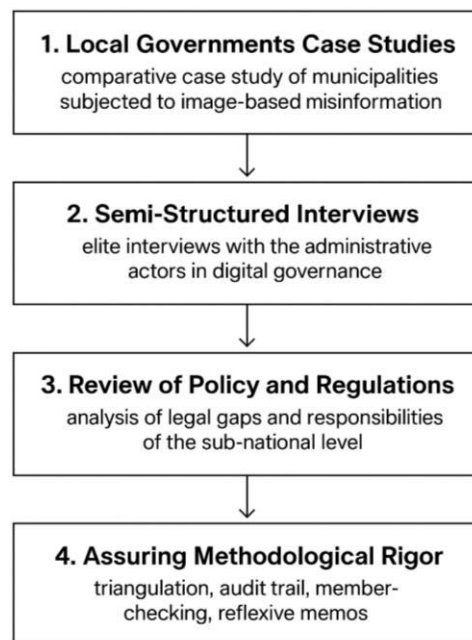


Fig.1. Methodology

3.1 Local Governments Case Studies.

The qualitative design employed was multi-case where analysis was done on five municipalities in two countries that share comparable decentralized governance systems. Cases were selected using philosophy of theoretical sampling and not statistical representatives. Municipalities had to be present in case they had recorded cases where manipulated or forged images had a direct impact on administrative decisions, delivery of public services or political communication. The key is to find municipalities, which offer "critical cases" that can lead to the insights into the institutional vulnerability to digital misinformation.

In each of the five municipalities, sources of data included municipal documents, inter-municipal administration communications, local and national news, records of complaints made by citizens, and online archives. All of the municipalities had suffered at least one forged image incident, including cases where manipulated disaster photographs were used to cause false emergency responses, fabricated infrastructure pictures were distributed to undermine the local works departments, communal pictures were used to fuel the social tension, and digitally enhanced photographs were used during local elections to discredit political rivals. These cases were explored to reconstruct the administrative chain of events, as well as the institutional bottlenecks and explore the failure or success of governance.

The analytical interest was based on four dimensions (i) the nature and the nature of a forged image (copy-move forgery, splicing, AI-generated changes or contextual manipulation), (ii) dissemination channels via community messaging networks and local digital ecosystems, (iii) administrative responses by departments charged with the responsibility of protecting themselves and their citizens by providing safety,

communication, and services, and (iv) institutional vulnerabilities during or after the misinformation event.

The Case Study Selection Flow Model, as shown in Figure 1 provide the shortlisting criteria of municipalities, the eligibility criteria, and the areas of governance that were impacted by misinformation.

3.2 Semi-Structured Interviews

The study also factored semi-structured elite interviews with key administrative actors in the sphere of governance and digital communication to supplement the documentary and the case-based evidence. The participants were the municipal commissioners, assistant commissioners, heads of the IT departments, the public relations officers, the administrative supervisors at the ward level, and the local law enforcement officers who had experience in cyber crime. The reason why these interviewees have been chosen is that they have first hand experience on how the incidents related to misinformation disturb administrative processes, overburden municipal systems and provoke the process of bureaucratic decision-making.

The interviews were between 45 and 90 minutes and were conducted on a flexible protocol to address four thematic clusters; (i) daily administrative operations and dependence on visual evidence provided by citizens, (ii) encounters with falsified or deceptive digital images, (iii) institutional readiness and the ability to perform internal verification, and (iv) plans regarding policy gaps, accountability systems, and the necessity of new legal frameworks. The semi-structured type fostered uniformity throughout the interviews but enabled the respondents to present the practical governance issues, political pressures, and bureaucratic limitations in their own language.

Transcription and analysis of all of the interviews followed a hybrid coding strategy. The governance and administrative theory, especially institutional trust literature, digital transformation, and organizational resilience, was turned into deductive codes. The data gave rise to inductive codes, including narratives by practitioners, including hesitation to verify images, fear of political backlash, reliance on local police to check the digital space, SOPs, and over reliance on Whats App groups to communicate information. The cases of cross-intercoder reliability were carried out on 20 per cent of the transcripts and the agreement rate obtained was 87, and this confirms the credibility of the coding process.

3.3 Review of Policy and Regulations.

The systematic policy and regulatory review was conducted to evaluate the structural conditions of how the municipalities react to image forgery. It has reviewed municipal bylaws, policy on digital governance, policy on communicating with the public, policy on data protection, cyber crime, and code of conduct on elections that apply to local candidates and local parties. The municipal websites, government gazettes, national cyber crime portals, and public access repositories served as the sources of documents.

The review has been aimed at determining the gaps in the four major areas of regulations, namely: (i) legal capacity of the municipalities to check the digital content and prosecute the misinformation actors, (ii) procedural transparency in the management of the forged images in the administrative processes, (iii) institutional responsibility in misinformation

events through the mechanisms of accountability, and (iv) inter-agency coordination procedures between the local governments, the police cyber-units, and the state information departments. The analysis showed there was a high level of discontinuity in the legal systems with most municipalities having no clearly stipulated verification procedures even though they were heavily burdened with the use of digital images in day-to-day operations. Such gaps in regulations lead to slow responses to false information, uneven decisions of the administration, and untimely understanding of citizens in times of high impact.

3.4 Assuring Methodological rigor.

There were several measures that were put in place to guarantee scientific rigor and reliability of the findings. It was realized that triangulation was accomplished in case by the inclusion of interviews, case data, and policy documents. The stage of methodological audit trail captured analytical decisions and coding of data and their selection of cases. Member-checking was also conducted through the provision of summaries of the selected interview members to ensure correct work and interpretation. Reflexive memos were kept during the study to determine the possible bias linked to researcher proportionality. All these together improve the credibility, dependability and confirm-ability of the research.

4. Results

This research study indicates that forged images have a great impact on the performance of the administration, the perception of the people, and the processes of responding to crises in institutions of local self-government. The study of five municipalities revealed twenty-seven reported cases within three years. Table 1 (Overview of Forgery-Driven Incidents Across Municipalities) includes a descriptive summary of such incidents that revealed that Municipality 1 had six emergency-related incidents, Municipality 2 had four incidents related to infrastructure, Municipality 3 had seven communal-sensitive cases, Municipality 4 had five cases involving authority, and Municipality 5 had five cases of mixed type. It is also shown in the table that the municipalities that were going through the election cycles or budget consultations had high number of such events hence strategic timing.

Table 1. Overview of Forgery-Driven Incidents Across Municipalities (3-Year Period)

| Municipality | No. of Incidents | Dominant Forgery Type | Election-Cycle Spike | Administrative Impact |
|--------------|------------------|------------------------|----------------------|---|
| M1 | 6 | Emergency-related | Yes | False alerts; unnecessary field inspections |
| M2 | 4 | Infrastructure-related | No | Public complaints; minor delays in service delivery |
| M3 | 7 | Communal-sensitive | Yes | Law enforcement mobilisation; community mediation |
| M4 | 5 | Authority-targeted | Yes | Reputation damage; increased RTI |

| | | | | |
|----|---|---------------------------|----|--|
| | | | | queries |
| M5 | 5 | Mixed (infra + authority) | No | Miscommunication; minor public confusion |

A comparison of the types of the incidents in all the municipalities reveals obvious pattern in typos, which are summarized in a narrative form in Figure 2 (Distribution of Forged Image Types). This number implies that there were about 32 percent of incidents that were emergency-related, 26 percent were communal-sensitive, 23 percent were infrastructure-related, and the rest 19 percent were authority-targeted. Figure 1 distribution shows that forged images tend to take advantage of the vulnerability of the population especially when they are in circumstances where they expect the administrative to be responsive.

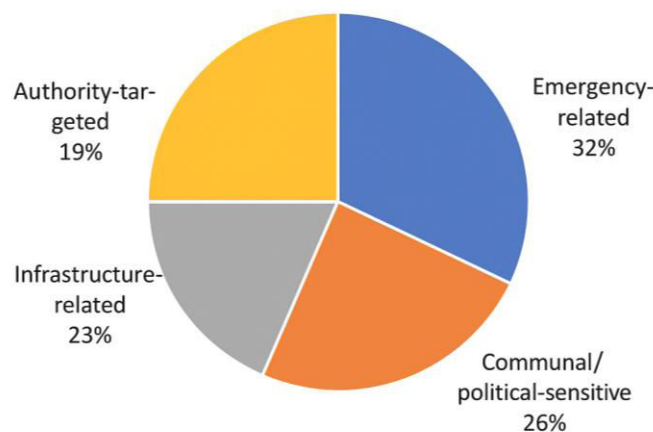


Fig.2. Distribution of Forged Image Types

Patterns of administrative responses were different. According to the data given in Table 1, only two municipalities had formalized procedures regarding digital verification, and the rest of the municipalities depended on informal discussions with IT staffs or field employees. The absence of organized procedures led to the procrastinated decision-making. In a notable instance, a fake photograph of the purported water pollution caused the immediate shut down of schools and city bans on water- the event later reported to be a hoax of a doctored photograph. This is in line with the responses that were given during the interview that there is a prevalence of risk-averse decision-making in the absence of the verification guidelines.

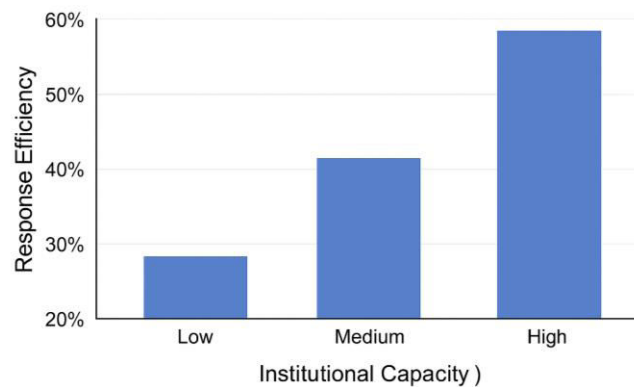


Fig.3. Response efficiency

The second (Fig. 3) is a bar graph that indicates the response efficiency based on the institutional capacity. The response efficiency of institutions with low capacity is approximately 28 which means that it can barely respond to any incident effectively. Middle-capacity institutions have about 42 percent efficiency, which is the average ability to deal with misinformation, or crisis. Institutions with high capacity are the most efficient with approximately 59% implying that a better institutional framework is more efficient in enhancing the response. The figure shows that the level of institutional capacity is directly correlated with efficiency of the mechanisms of operational or crisis response.

The indicators of public trust were collected prior to and following major events of misinformation, which were of major changes as shown in Table 2 (Public Trust Indicators Before and After Forgery Incidents). As shown in Table 2, the level of trust in the official municipal communication decreased to 48 percent after the incidents compared to 71 percent before the incidents. Confidence in public-works projects fell by half (66 to 42 percent), and the complaint volume per month more or less doubled. These values show that the irrelevance of forged images is not only immediate but long term, which can harm the reputation of local governments.

Table 2. Public Trust Indicators Before and After Forgery Incidents

| Indicator | Pre-Incident Level | Post-Incident Level | Change (%) |
|----------------------------------|--------------------|---------------------|------------|
| Trust in municipal communication | 71% | 48% | –23% |
| Confidence in public works | 66% | 42% | –24% |
| Average monthly complaint volume | 39 | 73 | +87% |

The regulatory review also pointed out the major governance lapses. The municipalities did not have any localised misinformation or digital-communication policies. Misinformation response had no specific departments and punishment against spreading forged pictures was not stipulated. Such lack of regulatory mechanisms predisposes the local governments to a great degree, as reported in cases cited in Table 1.

Table 3. Administrative Response Protocols Across Municipalities

| Municipality | Verification Protocol Status | Method of Verification |
|--------------|------------------------------|---|
| M1 | None | Informal consultation with IT officers |
| M2 | Partially formal | SOP for infrastructure-related images |
| M3 | None | Ad-hoc field checks only |
| M4 | Formal | SOP applied primarily to authority-targeted incidents |
| M5 | None | Ad-hoc review methods |

Table 4. Typology of Forged-Image Incidents Across Municipalities

| Forgery Type | Percentage of Incidents |
|---|-------------------------|
| Emergency-related (floods, fires) | 32% |
| Communal/political-sensitive | 26% |
| Infrastructure-related (potholes, sanitation, construction) | 23% |
| Authority-targeted (discrediting officials) | 19% |

Table 3 provides a summary of the verification protocols that have already been embraced by the five municipalities in dealing with the incidents of forged-images. The comparison shows that the institutional preparedness has a considerable difference. Municipalities 1, 3 and 5 did not have any formal procedures in place and mostly used ad-hoc approaches, including unofficial consultations with IT officers or field checks by the field staff. This lack of formal processes usually resulted in sluggish reaction and uneven decision making largely in a high pressure situation where emergency or community-sensitive images were concerned. Municipalities 2 and 4, on the other hand, had partially or formalised Standard Operating Procedures (SOPs) of image verification. City 2 adopted SOPs to deal with infrastructure-related images, thus more rapidly verifying doctored photographs with respect to infrastructural works. The Municipality 4 had formalized the SOPs that were primarily applied to authority-targeted images to carry out systematic assessment and issue clarifications on time. In general, Table 3 reveals the level of inequality in the administrative preparedness and the acute necessity to institutionalization the protocols to equalize the responses of all the municipalities. These deficits in the governance infrastructure imply that the municipalities that lack formalised mechanisms are more susceptible to operational and reputational risks that may be caused by misinformation.

Table 4 gives a break-down of the incidents of forged images according to type and prevalence. The highest percentage of incidents of 32 percent were due to emergency related forgeries including the doctored photographs on the flood, fires, and contamination of water. These images usually cause quick reaction among the masses and force the municipalities to take fast decisions, mostly in circumstances of uncertainty. Images involving communities or political sensitivities constituted 26 percent of the

overall cases. The visual misinformation was intentionally used politically, these forgeries were used strategically when it was necessary to fuel social tensions or shape the view of citizens, particularly during election periods. Frauds involving infrastructure such as tampered photos of potholes, sanitation, and construction projects constituted 23 percent of cases. The images in these cases often resulted in administrative inspection or complaints by the people who were not justified even when the underlying infrastructure concerns were of minor or nonexistent nature. Others of which 19 percent targeted government officials and others were authority-targeted forgeries meant to discredit municipal officials or undermine institutional legitimacy. As depicted in Table 4, the existence of images involving emergencies is the most prevalent, but all the above-mentioned types of images containing politically sensitive, infrastructure, and authority-oriented forgeries represent a massive burden of governance issues. The typology also shows how the strategy of timing and choice of targets are made, that differentiated verification measures of each type of forgery are necessary by the municipalities.

Table 5. Policy Framework Components for Countering Forged-Image Misinformation

| Component No. | Policy Component | Description |
|---------------|---|--|
| 1 | Municipal SOPs | Formal procedures for verification, reporting, and escalation |
| 2 | Digital Verification Units (DVUs) | Teams of IT, communication, and liaison personnel to verify images |
| 3 | Regulatory and Legal Reforms | Municipal by-laws defining responsibilities, penalties, and reporting pathways |
| 4 | Public Communication Strategies | Multi-channel dissemination; proactive awareness campaigns |
| 5 | Collaboration with Cybercrime Units | Coordination with state and national cybercrime bodies for verification and forensic support |
| 6 | Integration of Technical Verification Tools | Use of reverse-image search, metadata analysis, and forensic filters |
| 7 | Community Digital Literacy Initiatives | Education programmes, workshops, and school-based awareness campaigns |

Table 5 provides the most important aspects of the policy framework that aims to counter misinformation about forged images in local self-government institutions. The framework focuses on formal Municipal SOPs, which set up a set of formal methods of verification, reporting and escalation of suspicious images. Digital Verification Units (DVU) are professional units that consist of IT experts, communication officers, and liaison people

who are responsible to determine the authenticity of digital content. In order to enforce better, there are Regulatory and Legal Reforms which can be seen in municipal by-laws, which explicitly define obligations, punishment, and reporting channels of the misinformation events. Multi-channel dissemination and proactive awareness campaigns are used to implement the effective Public Communication Strategies to ensure that the people have information at their fingertips. The support of Cybercrime Units allows coordinating with state and national cybercrime agencies and verification and forensic assistance upon request. The framework also focuses on the Integration of Technical Verification Tools including reverse-image searches, metadata analysis, and forensic filters to make the correct decision on image manipulations. Lastly, Community Digital Literacy Initiatives emphasize on education programs, workshops and school-based awareness campaigns to enable citizens with skills on how to identify and deal with misinformation. These elements combined form a holistic strategy in the reduction of the propagation and the effects of forged-image misinformation.

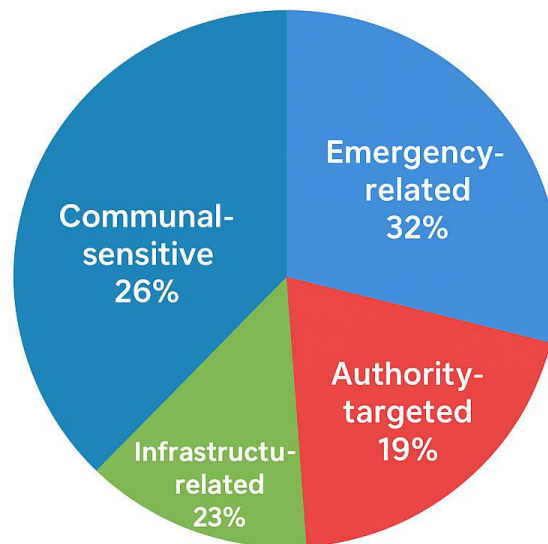


Fig.4. Distribution of forged images

The Fig. 4 is a pie chart that shows the forged image distribution according to their thematic focus. The most prevalent is the Emergency-related images, which make up 32% of the total, meaning that quite a good number of forgery is directed at emergencies or crisis situations. The percentage of communal-sensitive images is 26 and which indicates the possibilities of social tensions due to misinformation. Infrastructure-related images constitute a fifth of 23% as it contains concerns of public utilities and facilities whereas Authority-targeted images constitute a fifth of 19% indicating that some forgeries may be used to weaken the trust in those in power. On the whole, the diagram highlights the point that misinformation through image forging is being strategically planted across the themes that have the potential to affect both social imagination and institutional authority.

5. Discussion

The findings show that image forgery is a significant governance issue and not a technological curiosity. The results support the fact that falsified images affect the

decision-making processes within the administrative level, crisis communication, and the trust of the population in the local government.

The first key lesson is associated with the governance risk of the visual misinformation. According to the typo-logical patterns presented in Figure 1, old fake images produce more emotional reactions in a shorter period, and stronger emotions than does textual misinformation, which triggers instant public pressure. This leads to what can be termed as a reactive governance cycle and as such local authorities are under pressure to implement actions ahead of the verification process being accomplished and therefore end up deploying to the field prematurely, premature alerts and administrative confusion. The second lesson is that of institutional readiness. Figure 2 (Institutional Capacity vs. Response Efficiency) is a conceptual representation in which more IT capacity in municipalities resulted in a rapid verification and less misinformation influence, and less IT capacity in municipalities led to slower or no verification and greater influence. This further supports the principle of inequity in governance in which the smaller municipalities, whether equally exposed to misinformation or not, suffer the disruption of administration unequally.

The third lesson is that of communication asymmetry and lost public trust. According to Table 2, there is a significant reduction in the level of trust in official communication channels after forged-image events. According to the administrators interviewed, formal corrections often do not reach over half of the number of people exposed to the initial forgery, and that this means that the false accounts could continue and that institutional credibility could be undermined.

The fourth lesson is connected with the political aspect of the fabricated images. Some of the cases that were examined in Table 1 happened in an election year or a budget-planning year. It means that fake pictures are strategically exaggerated to create political discourse, mobilize a certain group of people, or discredit authorities. Image forgery becomes therefore a conscious political instrument but not a by-product of manipulation by digital media.

6. Policy Framework to Enhance the Local Government Response to Image Forgery.

As has been seen in the above sections, the empirical evidence is clear that local governments need a multi-layered policy to adequately combat image-forgery-based misinformation. The suggested framework incorporates the institutional, regulatory, technological, and community-level aspects. All the components are based on the gaps in governance listed in Table 1 and it is backed by behavioral patterns in Figures 2 and 3.

The Municipal Misinformation Response Protocols should be created during the 6th project activity. The former part of the framework is the requirement of formalized Standard Operating Procedures (SOPs) specific to image-based misinformation. Such SOPs must specify how they are going to receive, categorize, verify and record suspicious pictures. Table 1 shows that, based on the inconsistencies registered, it is more probable that the municipalities that lacked established protocols would adopt a risk-averse behaviour and take early administrative measures. SOPs must thus require verification before making statements to the people, it must describe avenues of escalation, and stipulate time limits of internal examination. Municipal administrative

regulations would assist in implementing these procedures to develop a consistent response system.

6.2 Development of Digital Verification Unit (DVUs).

The second is the creation of Digital Verification Units at the municipalities. The conceptual model of the relationship between institutional capacity and verification efficiency as depicted in Figure 4 reveals that municipalities that had a high technical capacity suffered less in negative effects of forged images. The IT officers, communication experts, and liaison staff that is trained in the fundamentals of digital forensics and social-media surveillance are expected to staff DVUs. Smaller municipalities can follow suit with more scaled-down versions because they are incorporating DVU tasks within already existing e-governance or IT departments. These units would have stores of accredited images, oversee verification instruments and liaise with other cyber crime organizations.

6.3 Enhancing Legal and Regulatory Systems.

Another regulatory area where a major gap in the regulatory review is found is the lack of legal provisions at the municipal level to deal with misinformation. Despite the national laws on cyber crime, they seldom extend to the issue of governance at the local levels. Municipal by-laws are therefore advised to include administrative fines on the deliberate spread of forged images, provide notification procedures by citizens, establish the roles within the departments, and standardize the rules of communication with the social-media sites. These reforms would deal with the weaknesses brought to fore by the cases as summarized in Table 1 and minimize the chances of political exploitation evident during election periods.

6.4 Improving Public Communication and Trust-Building Mechanisms.

Table 2 has shown that the lack of trust is a critical concern that requires enhancement of communication strategies with the population. The municipalities are supposed to come up with proactive campaigns regarding public information that informs the people on how to manipulate the images, how they can verify them, and the harm of spreading the wrong information in a short period of time. Crisis communication should be open, timely and backed up with evidence that is proven. The governments ought also to incorporate the use of multi-channel distribution to make sure that official clarifications are distributed to as many people as the misinformation. This is a direct way of addressing communication asymmetry as pointed out in the Discussion section.

6.5 Cooperation with Cyber crime Units and Inter-Governmental Relationships.

Due to low technical capability in some of the municipalities, it is necessary to team up with cyber crime units at the state or national level. The partnerships must also involve a formal agreement on quick verification assistance, common access to forensic tools, and coordinated action during the incidents with a high impact. Inter-municipality cooperation is another option that should be discussed, particularly in the areas where fake images go across the jurisdiction lines. The trends in Table 1 of political amplification are pertinent in the fact that concerted plans are required across the municipal borders.

6.6 Low-Cost Technical Verification Tools Integration.

In spite of the fact that the present study did not analyze the algorithmic detection systems, the municipalities may also take advantage of the most commonly available

tools, including metadata-checkers, reverse-image searches and simple forensic filters. Such tools can also help a lot to decrease the burden of verification when they are implemented into the processes outlined above. Their purpose should be to support decision making as aids and not to substitute institutional judgment. The process of integrating such tools can be visualised in the same way as the relationship in Figure 2, where the role of the institutional capacity is stressed on the results of the verification.

6.7 Community-Based Community Digital Literacy Programs.

The last element focuses on the involvement of citizens. The municipalities need to form community-based workshops, digital literacy modules in schools, and collaborate with civil-society organizations to produce a stronger community. Digital literacy helps mitigate the risk of it spiking viral misinformation and has a more powerful impact on achieving consensus between people and municipal communications. These measures deal with behaviour weaknesses as illustrated in Figure 1, with communal and emergency-related images attaining immediate viral spreading owing to the intensity of emotions and the lack of awareness related to verification.

Combined, the seven building blocks of the proposed policy framework provide an evidence-based and structured approach to reducing the administrative, political, and social effects of falsified images. This framework can be discussed as a useful roadmap in encouraging digital governance capacity in municipalities since it references the empirical patterns recorded in Tables 1 and 2 and presents the conceptual understanding of the same represented in Figures 1 and 2. The comprehensive aspect of the framework guarantees the targets of the reactive and preventive aspects of misinformation management, which makes the institutions resilient in the long-term.

7. Conclusion

This paper indicates that misinformation through image-forgery can be very dangerous to institutions of local self-government, and can influence the decisions of the administration, the confidence of citizens, the management of crisis, and political relationships. Table 1 indicates that forged images are highly placed in strategies that capitalize on the vulnerabilities of the people and the incapability of institutions identified in the twenty-seven recorded cases in five municipalities. The topological distribution presented in Figure 1 also demonstrates that those pictures are likely to be concentrated towards themes that can provoke high levels of emotional responses, like emergencies and communal tensions. The administrative discrepancies discussed in the Results section demonstrate that the municipalities that lacked official verification procedures had more delays, operational slip-ups, and representational losses.

A key finding of this research is the reduction in the trust placed on the information community because of the misinformation incidences by a significant margin as shown in Table 2. Such a lack of trust undermines the power of municipalities, makes the process of communication challenging, and makes it more likely that future misinformation will become established. The theoretical connection between the institutional capacity and verification efficiency as in Figure 2 supports the necessity of investing in the technical and human-resource capacity on the municipal level.

The suggested policy framework provides an overall answer to the problem, including procedural reforms, technological assistance, capacity building, regulation clarity, intergovernmental collaboration and education of the citizens. With the adoption of these

elements, the municipalities will be able to transition to anticipatory governance, rather than reactive, and be better equipped to deal with the growing danger of digitally manipulated images. With the increasing prevalence of information-rich and verification-poor environments that local governments are forced to operate in, image forgery is something that must be given due priority in the modern local governance practice. Future studies can build on this study by adding a quantitative modelling or comparative study across more jurisdictions to further optimize the governance implication of visual misinformation.

References

1. Brandt, J. (2022, October). Autocratic approaches to information manipulation: A comparative case study. Unpublished background paper manuscript prepared for the December 2022 Gates Forum on Strategic Communications.
2. Cieślak, B. (2025). Local self-government against the state: Resistance of Polish municipalities to creeping centralization. *Urban Affairs Review*, 10780874251327089.
3. Aljadhay, M. B. F. A. (2025). Legal challenges in confronting internet fraud crimes in the Kingdom of Saudi Arabia. *Lex Localis*, 23(S5), 429–447.
4. Dubivka, I., Rekotov, P., Kuliush, V., Rusanivska, D., & Basiuk, L. (2025). Investigating cybercrimes committed in the financial sector: Procedural standards, digital forensics and international cooperation. *Lex Localis*, 23(S4), 1340–1348.
5. Nhung, D. H., Van Dung, T., & Long, N. P. (2025). Fraud control in real estate transaction services: Lessons from South Korea and policy recommendations for Vietnam. *Lex Localis*, 23(S5), 771–783.
6. Rudnieva, A. (2024). Innovative analytical and statistical technologies in the development of democracy in the state. *Філософія та політологія в контексті сучасної культури*, 16(2), 135–146.
7. Wei, L. (2025). China and the Western Balkans: Economic cooperation in a global geoeconomic framework. *Lex Localis*, 23(S5), 1232–1255.
8. Dobber, T., Metoui, N., Trilling, D., Helberger, N., & De Vreese, C. (2021). Do (microtargeted) deepfakes have real effects on political attitudes? *The International Journal of Press/Politics*, 26(1), 69–91.
9. Reid, D. (2025). ‘A scheming unprincipled native and notorious mischief maker’: The 1882 Ngāpuhi petition to Queen Victoria and settler disinformation in the late nineteenth-century British Empire. *The Journal of Imperial and Commonwealth History*, 1–32.
10. Abiri, G., & Buchheim, J. (2022). Beyond true and false: Fake news and the digital epistemic divide. *Michigan Tech Law Review*, 29, 59.
11. Valihura, H., Novikov, I., Diakur, M., Yushchyk, O., & Kutsenko, V. (2025). The use of innovative technologies for the prevention and detection of crimes related to document forgery. *Journal of Theoretical and Applied Information Technology*, 103(14).
12. Popović, D. V. (2021). Freedom of expression on social networks: An international perspective. The impact of digital platforms and social media on the freedom of

- expression and pluralism—Analysis on certain central European countries. Ferenc Mádl Institute of Comparative Law, 277–310.
13. Wagner, S. (2023). Espionage and the 1935 press war in Palestine: Revisiting factionalism, forgeries and fake news. *The English Historical Review*, 138(592), 528–565.
 14. Chen, K. W. (2022). Combating Beijing's sharp power: Taiwan's democracy under fire. *Journal of Democracy*, 33(3), 144–157.
 15. Merlingen, M. (2023). Coloniality and the global North war against disinformation: The case of the European Union. *Third World Quarterly*, 44(4), 744–761.
 16. Devaram, S. K. A., & Gunasekaran, S. (2025). States of unfreedom: Identity and biopolitics in JM Coetzee's fiction. *Lex Localis*, 23(11), 464–487.
 17. Arstanbekov, M., Seidakmatov, N., Tatenov, M., Kanybekova, B., & Kakeshov, B. (2024). Victimological aspects of countering internet crime: State and local government practices. *Social and Legal Studios*, 1(7), 221–234.
 18. Sarfi, M., Darvishi, M., Zohouri, M., Nosrati, S., & Zamani, M. (2021). Google's University? An exploration of academic influence on the tech giant's propaganda. *Journal of Cyberspace Studies*, 5(2), 181–202.
 19. Zhao, Y., Zhao, M., & Shi, F. (2024). Integrating moral education and educational information technology: A strategic approach to enhance rural teacher training in universities. *Journal of the Knowledge Economy*, 15(3), 15053–15093.
 20. Williams, D. C. (2023). Civic republicanism and the citizen militia: The terrifying second amendment. In *Gun Control and the Constitution* (pp. 295–359). Routledge.
 21. Chari, S. (2021). The ocean and the city: Spatial forgeries of racial capitalism. *Environment and Planning D: Society and Space*, 39(6), 1026–1042.
 22. Ahangama, S. (2023). Relating social media diffusion, education level and cybersecurity protection mechanisms to e-participation initiatives: Insights from a cross-country analysis. *Information Systems Frontiers*, 25(5), 1695–1711.
 23. Yu, J. S. (n.d.). *Regulating social media in a democracy: The case of South Korea* (Doctoral dissertation, University of Otago).
 24. Allen, D., & Weyl, E. G. (2024). The real dangers of generative AI. *Journal of Democracy*, 35(1), 147–162.