ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VII, July 2025

Deepfake Video Detection: A Comprehensive Review

Petchiammal M, Vignesh Kumar N

Kristu Jayanti Deemed to be University, India

DOI: https://doi.org/10.51583/IJLTEMAS.2025.1407000109

Abstract: Deepfake technology, driven by Generative Adversarial Networks (GANs) and diffusion models, presents significant political, social, and economic threats. This review consolidates insights from over 30 scholarly contributions on deepfake detection techniques, datasets, evaluation metrics, and ongoing challenges. We examine both traditional methods and modern deep learning strategies, including convolutional neural networks (CNNs), transformers, multimodal architectures, and ensemble frameworks. Key benchmark datasets—DFDC, FaceForensics++, and Deepfake-Eval-2024—are comparatively analyzed. Performance metrics such as accuracy, AUC, F1-score, and Matthew's correlation coefficient (MCC), along with adversarial robustness, are critically assessed. Identified limitations include poor cross-domain generalization, suboptimal real-time performance, and dataset bias. The review proposes future directions including adaptive detection models, enhanced multimodal fusion, model interpretability, and the need for unified global standards in forensic validation.

Keywords: Deepfake, Video Forensics, Detection, CNN, GAN, Diffusion Models, Benchmark Datasets, Adversarial Robustness, Multimodal Fusion

I. Introduction

Defining Deepfakes & Their Evolution

Deepfakes, a blend of "deep learning" and "fake," are artificially created media that produce highly realistic images, videos, and audio through sophisticated artificial intelligence (AI) methods, especially generative adversarial networks (GANs), variational autoencoders (VAEs), and diffusion models (Tolosana et al., 2020). The deepfake phenomenon began around 2017 when Reddit users first brought attention to face-swapping methods utilizing open-source AI resources. These initial techniques allowed users to overlay celebrity images onto performers in adult films, triggering ethical and technological concerns throughout various sectors.

At first, the creation of deepfakes was constrained by processing capabilities and basic algorithms, leading to apparent artifacts and deformations (Korshunov & Marcel, 2018). Nevertheless, ongoing progress in deep learning has resulted in the creation of models such as StyleGAN and diffusion-based frameworks, greatly improving the realism and quality of synthetic content (Karras et al., 2019). Contemporary tools such as Synthesia, DeepFaceLab, and HeyGen allow for face-swapping, voice cloning, and complete body reenactments, making it progressively harder for the untrained eye to tell apart authentic and fabricated media.

The progression of deepfakes is typically classified into generations:

• First Generation: Simple face-swapping showing noticeable artifacts.

• Second Generation: Enhanced texture and resolution, allowing for photorealistic quality.

• Third Generation: Multi-modal deepfakes combining synchronized audio and video, voice replication, and complete body synthesis.

This development underscores the technology's dual-function nature: while facilitating inventive advancements in fields such as filmmaking, education, and accessibility, it also poses considerable dangers of misuse in social, political, and economic domains.

Forensic Relevance: The Arms Race in Digital Forensics

The rise of deepfakes has profound consequences for digital forensics, which aims to verify digital content and maintain the integrity of evidence in legal and investigative scenarios (Verdoliva, 2020). Conventional forensic methods that depend on identifying visual discrepancies like blending mistakes, compression artifacts, and lighting mismatches are becoming less effective against sophisticated generative models (Guarnera et al., 2020).

A significant progress in forensic science is GAN fingerprinting, which detects subtle patterns characteristic of images produced by particular AI models (Marra et al., 2019). These fingerprints, identifiable in the frequency domain, enable forensic specialists to track the synthetic source of media. Moreover, methods based on physiological signals have surfaced, utilizing biological indicators like irregular eye-blinking, variations in skin tone from heartbeats, and discrepancies in lip synchronization to detect possible deepfakes (Ciftci et al., 2020).

The active interaction between creating deepfakes and identifying them has resulted in an "arms race." With the advancement of deepfake technology, detection methods need to quickly evolve to combat emerging tactics of fraud. This ongoing cycle offers both a challenge and a chance for forensic researchers to develop and strengthen the reliability of detection methods.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VII, July 2025

Societal Impacts

Misinformation & Trust Erosion

Deepfakes significantly contribute to spreading false information, undermining public trust in media, institutions, and democratic structures. The term "liar's dividend" describes how deepfakes allow individuals to dismiss authentic evidence by asserting it is false, thus reducing accountability (Chesney & Citron, 2019). This increasing doubt leads to "truth decay," a societal issue where distinguishing between truth and falsehood becomes increasingly difficult (RAND Corporation, 2018).

Political Manipulation & Election Interference

The ability of deepfakes to alter political environments is significant. Cases of deepfake material targeting political leaders, disseminating propaganda, or swaying voter opinions have been recorded. Deepfake robocalls were employed to decrease voter participation in U.S. elections (Vaccari & Chadwick, 2020). In India, videos with deepfake technology showing political figures have spread extensively, intensifying divisions in public opinion (Nicas & Conger, 2020).

Although the 2024 elections saw minimal use of deepfakes, experts warn that the swift evolution of this technology may lead to more advanced and widespread electoral manipulation in the future (Time, 2024).

Financial Scams & Identity Fraud

Deepfake technology is being more frequently used in financial scams and identity theft. Voice cloning has been utilized in social engineering schemes, where fraudsters mimic CEOs to approve fake transactions. A significant incident saw a Hong Kong company losing $25.6 million from a deepfake video conference featuring a fraudulent executive (Springer, 2025).

Estimates suggest that fraud facilitated by deepfakes led to worldwide losses of around $12 billion in 2024, with forecasts predicting an increase to $40 billion by 2027 (PwC, 2024). This concerning pattern highlights the pressing necessity for strong detection systems and legal structures to address financial exploitation.

Personal Harm & Psychological Effects

Aside from financial and political consequences, deepfakes cause personal and psychological damage. Deepfake pornography without consent primarily affects women, leading to emotional turmoil, damage to their reputation, and social stigma (West, 2019). Victims frequently endure anxiety, depression, and an overwhelming feeling of insecurity, underscoring the urgent requirement for protective laws and assistance frameworks.

Detection as Defense: Forensic and Technological Countermeasures

Given the various risks associated with deep pace, detection techniques serve as the first level of protection. Various methods have been developed for recognition, and the risk of recoil created by synthetic carriers has been developed.

1. Artifact-Based Detection: Methods using Sparkle Neural Networks (CNNs) such as XCception and ResNet analyze space and frequency functions to identify specific artifacts in Gan (Rossler et al., 2019).

2. Physiological analysis of signals: A method for detecting biological inconsistencies such as non-natural velocity, micro-representation abnormalities, and remote light fields (RPPGs) to detect heartbeats (Ciftci et al., 2020).

3. Multi-Model Fusion: Combining audio data, visual, and text improves the accuracy of detection by mutual checking of conflicts between methods (Mittal et al., 2020).

4. Blockchain and Digital Source: Protect the reliability of digital content by using blockchain systems to establish constant and nonexistent recordings of media origin and change (Hasan and Salah, 2019).

5. AI (XAI): Development of an interpretive model that emphasizes the area manipulated by legal health professionals and legal authorities in the assessment of evidence (Simek et al., 2017). Despite these achievements, the problems are preserved. In particular, the generalization of detection models, invisible options in the deep phase, stability against conflicting attacks, and scalability of real applications.

Contextual Safeguards: Policy, Regulation & Public Literacy

Technical solutions should be supplemented by complete political measures, normative frameworks and national education for an effective fight against the threat of deep features.

•Regulations and Standards: International organizations such as the International United Nations Telecommunication Union (IUT) protect standardized water panels, monitoring of origin, and cross-couperation (Reuters, 2025).

• Law: Laws such as the American law on falsehood and European Union regulations aim to criminalize the malicious use and transparency of mandatory mandate of the deep rhythms of content generated by AI. • State education: With the increase in digital literacy through information campaigns, people critically evaluate the credibility of the media and contribute to social stability.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VII, July 2025

Structure & Scope of This Review

This review document has been organized to propose a detailed study of deepfakes, particularly.

• Technological advances: Mapping deep creative development based on simple face changing methods in complex multimodal manufacturing.

•Judicial Methods: Evaluation of detection methods such as artifact analysis, physiological detection of signals, multimodal fusion, original monitoring, and more.

•Social Impact: An analysis of the effects of deep scale on disinformation, democracy, financial security, and individual well-being.

• Defense measures: Assessing the efficiency and limitations of tools for detecting current and legal frameworks.

• Future orientation: Identify research gaps and identify ways to increase detection reliability, dataset diversity, real applications, and integrated political responses.

Thanks to the entry between technical, judicial and social perspectives, this review aims to develop an overall strategy to counter the threats in the development of deep features.

Deepfake Generation Techniques

Deepfake's generation methods have undergone rapid success through the development of complex AI models and the development of computing power. The main methodologies include model-based models, diffusion models, and judicial indicators left as artifacts.

GAN-Based Face Swapping and Reenactment

Generated Competition Network (GAN) was essential to ensure people's use and reconstruction. Goodfellow et al. (2014), GANS uses discriminatory device generators to create realistic synthetic environments.

•Face Wap: This open-source tool replaces one person's face with another person in an image or video based on detection of faces and alignment guides for transparent charges. •VID2VID: A prominent way to broadcast video with video, VID2VID provides facial representation and posture reconstruction while maintaining a temporary sequence.

These GAN-based approaches contribute significantly to deepfake availability and quality.

Diffusion Model-Based Forgeries

Since 2024, diffusion models are the last development of generative modeling. Unlike GANS, the diffusion model gradually improves random noise to obtain high quality images (Hoetal., 2020). • Notable examples include a stable Dall-E 3 distribution that successfully creates light-realistic images with thin details and rich textures (Rombach et al., 2022).

These models demonstrate the special ability to create a variety of visually consistent outings, pushing the limits of creating synthetic environments.

Traces of Artifacts

Despite achievements in the field of generational ectors, judicial analysis shows clear indications of manipulation.

• Eye irregularity: Composite videos often show abnormal flashing models as the model may not repeat the natural frequencies of the eye flash (Li et al., 2018).

• Pixelia and deformation artifacts: Artifacts such as Pixelia remain common model limitations with smooth integration of facial offices (Rossler et al., 2019). These artifacts act as important medico legal markers to aid in the detection and analysis of deep fakes.

Detection Approaches

A sophisticated method of deep furk generation has been developed, and there is a need for reliable and reliable detection methods. These approaches can, in principle, be divided into traditional forensic methods, deep learning models, multimodal strategies, and holistic or hybrid systems.

Traditional&ForensicMethods

Traditional methods for detecting deep tasks rely on hand-developed functions and medicolegal testing to detect physiological and statistical abnormalities present in synthetic environments.

Two notable approaches include:

• Eye flashing detection: The first deep-fark model could not reproduce the natural flashing model due to lack of images of the eyes closed in the training set. Li et al. (2018) introduced methods to detect irregular eyes in videos, exposing characteristic abnormalities to deep standards.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VII, July 2025

•Twisted artifacts: Mother et al. (2019) identified artifacts related to facial deformations and refined transformations used during mixing. These artifacts often appear around the face of the lighting and the contradiction. This can be found using detailed forensic analysis.

These judicial markers, particularly combined with field experiences of image and video analysis, contribute to the decision of manipulated content.

Deep Learning Approaches

Deep learning models, particularly Sparkling Neural Networks (CNNs), have greatly improved the detection of deep characteristics and independently identify complex models with detailed datasets.

•CNN Model: Architectures such as XCPT, RESNET, VGG are widely appreciated in datasets such as DFDC (Deep Fark Detection Task) and FaceFornsics++. In particular, the Xceptal model reached an impressive accuracy of ~89.2% in DFDC data (Rossler et al., 2019).

•Transformers and two flow-based networks: Latest development included models of transformers and attention mechanisms that analyse spatial and temporary functions within the video. These models improve detection accuracy by identifying inconsistencies between staff and detecting irregular motion movements in different video sequences (Mittal et al., 2020).

Deep learning models offer scalability and adaptability, but can result in poor performance along with invisible methods and deep tail generation regions.

Multimodal Detection

Multimodal detection methods incorporate different types of data, such as audio and visual input data, to improve stability compared to incorrect and advanced methods.

• Audiovisual fusion: Detection speed has been improved by a method of integrating facial movement, lip synchronization and audio motifs. Mittal et al. (2020) emphasize that emotional signals and recognition influence additional validation layers and find inconsistencies between auditory and visual signals. These methods are necessary to identify deep criteria that include both visual manipulation and sound.

Ensemble & Hybrid Models

The overview and hybrid approach merges the benefits of various detection methods by integrating detailed learning algorithms and forensic analysis to improve detection accuracy and robustness.

• Fusion frame: Guarnera et al. (2020) proposes an approach to integrating CNN-based features with forensic markers, leading to higher detection points compared to model solutions.

•Installation detection systems: Some systems use a coherent discovery layer that filters suspicious content in subsequent deep tests, based on the first judicial analysis based on a full evaluation. These integrated systems are the limits of deep properties detection, balancing accuracy, generalization and interpretation.

Datasets & Benchmarks

The progress of deepfake detection methods depends primarily on access to various extended datasets. Standardized datasets and control metrics provide the necessary basis for comparing training, testing and detection models in a variety of conditions and operations.

DFDC (Deepfake Detection Challenge Dataset)

Facebook AI introduced in 2019, DFDC data is one of the largest public resources created specifically for DeepFakes detection. This includes over 100,000 videos generated using several deep pharmacy methods, modifying a wide range of operations in a variety of environmental and demographic conditions (Dolhansky et al., 2020). This dataset played an important role in stimulating the development of reliable detection algorithms within the framework of DFDC competition.

FaceForensics++

Faceforesics++ is another important data widely used in the academic and research community. Developed by Rossler et al. (2019), it contains alved videos prodhed through oven separate deepfake generation technical. All data provides a low-quality compressed version and model real scenarios where compression artifacts can affect detection accuracy.

Deepfake Bench

Deepfake Bench is a recent set for comparison and is designed to assess the effectiveness of detection models in a wide range of synthetic methods. This standard includes a variety of styles of manipulation and solution problems, such as interemotion generalization, where models studying on the same dataset do not focus on invisible datasets (Dang et al., 2020).

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VII, July 2025

Deepfake-Eval-2024

Published in 2024, Deepfake-Eval-2014 is an advanced standard designed to evaluate deep lenses from real multilingual sources. This represents the important evolution of dataset conservation, including content from various cultural and linguistic layers, reflecting the global nature of disinformation campaigns. An impressive withdrawal of this data evaluation is the decline in region of the region of the Curve Indicator (AUC) (AUC) compared to indicators in older datasets such as DFDC and FaceForensics++ (Jain et al., 2024). This gap highlights the limitations of existing models when faced with subtle complexity of actual deep oceans.

Importance of Datasets

The diversity and integrity of these datasets are necessary to:

•Model Summary: Ensure that detection models work effectively in different types of deep contexts.

• Account Progress: Provides a standardized reference point for measuring detection technology outcomes. • Identifying bias: Assisting in identifying dataset displacements that can lead to heterogeneous accuracy in demographic group detection.

Continuing development and clarification of datasets and standards is necessary to attract innovation in deep characteristics detection and to ensure the relevance of detection systems in digital landscapes in rapid development.

Metrics & Evaluation

Performance of Deepfake detection models should use standardized measurements that quantitatively determine the accuracy, reliability and reliability of various data sets and handling methods. Some important indicators are integral parts of this assessment process.

Key Metrics

• Accuracy: Reflects the share of deep brightness that is properly identified in all cases marked deep, indicating the number of accurate predictions.

•Reminder (Sensitivity): Measures the power of the model to detect calculations of the depth ratio correctly identified by the actual deep rhythm, total number of depth depths.

• F1 rating: Combining accuracy and inspection with metrics to calculate harmonic averages to provide a balanced look when two aspects are equally important.

•AUC-ROC (area below the curve of receiver working characteristics): Evaluate the model's capacity to distinguish between real and false environments by building a compromise between actual positive and false positive indicators at various thresholds. A higher AUC means stronger discriminatory forces.

•MCC (Matthew's correlation coefficient): Provides a balanced rating, taking into account real positives, real negatives, false power, false negatives. This makes it particularly effective to evaluate models of unbalanced datasets. These measures provide a multidimensional perspective on model performance, and not only accurately determine deep criteria, they also help select models that generally broaden different contexts.

Adversarial Robustness

An important aspect of Deep Paris' deep detection bet evaluation is their strength against conflicting attacks. Collaborative stability measures how well the model continues to work when it meets a deliberately modified entry intended for detours.

•FGSM (Method of Rapid Gradient Signaling): This widely used contention method modifies the input data and introduces the computational noise obtained according to the gradient of the loss function. Research has shown that deep function detection models can significantly reduce performance when attacked by FGSM, highlighting current system vulnerabilities (Sabir et al., 2019).

•Other competitive methods: Apart from FGSM, methods such as DPI (planned gradient descent) and DeepFool introduce more complex interference that also checks the limits of the detection model. Adversarial stability management is important to ensure that deep detection detection systems remain deep detection detection systems in real applications where specially designed methods can be deployed to bypass security measures.

Benchmarking and Standardization

This assessment is often controlled by standardized datasets such as DFDC, FaceFornsics++, and Deepfake-Eval-2014, and ensures consistency of productivity reports in a variety of studies. Continuous comparative analysis of updated datasets is important for capturing new methods to generate deep characteristics and validate the generalization of detection systems. Using these reliability measures and ratings, researchers can develop more reliable adaptive detection models that can protect digital integrity.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VII, July 2025

Challenges & Limitations

Deep properties have achieved notable advances, but there are still various problems and limitations that prevent the actual implementation of these systems under real conditions. These limitations are highlighted in the gaps facing current technologies and areas where new research and innovation are needed.

Cross-Domain Generalization and Real-World Adaptability

Many models for detecting deep respect are trained on specific datasets, which limits their ability to summarize different types of operations with deep characteristics, media formats, and environmental conditions. This phenomenon known as the task of summarizing internal generalizations means that models that are properly executed on controlled datasets such as DFDCs are uncertain during testing of actual, invisible data (Agarwal et al., 2020). Due to the various video resolutions, compression levels, lighting conditions and cultural content, true adaptability is the main obstacle. The nature of the development of generative models further exacerbates this problem. This is because new ways of generating OUTKs can effectively surpass detectors before.

Real-Time Constraints and Computational Cost

Highly computational efficiency is required for the deployment of deep task detection systems in real-world applications, such as streaming widespread and social network mitigation. Nevertheless, many modern models, particularly deep solutions based on training, such as CNNs and transformers, are computationally intense and require significant therapeutic power and memory (Guarnera et al., 2020). The high computational requirements of these models make it difficult to deploy them to limited resources such as smartphones and built systems, leading to a break between research and practical and evolving implementations.

Bias in Datasets and Global South Detection Gap

Bias in the data training set can lead to inequality in findings across different demographic groups. It especially affects people around the world. Most existing datasets are primarily the presence of western subjects, and when applied to people in unused groups and ethnic regions, lead to less effective models (Mehrabi et al., 2021). This gap in detection effectiveness raises important questions of justice and equality, potentially expanding digital differences, making marginalized groups more vulnerable to deep levels of abuse.

Interpretability and forensic admissibility

Interpretability includes the ability to understand and formulate how detection models can reach conclusions. Many detailed learning detectors act like black boxes and provide very accurate, but understand how the conclusions are drawn (Rudin, 2019).

Lack of interpretation is a serious issue in legal terms; it should be transparent and resist legal control. The courts require clear and understandable excuses about the validity of digital evidence, and it is possible that opaque AI models do not meet these strict standards.

Future Directions

Continuing advancements in Deepfake Generation Technologies require constant innovation in detection methods. To solve current limitations and future problems, researchers are studying several promising areas to increase the efficiency, stability and applicability of deep feature detection systems.

Multimodal Detection Frameworks

The new detection system pays more attention to multimodal methods that combine data from several sources, such as visual, audio, and text elements. Simultaneous analysis of several modalities allows these executives to achieve higher accuracy and stability for false complexes (Mittal et al., 2020). For example, the combination of voice models and lip motion analysis with facial dynamics can help determine contradictions that can neglect unique systems. This integrated perspective is essential for the detection of deep, complex fragments that gently mix audio with visual elements.

Domain Adaptation and Continual Learning

Detection models are often attempted to effectively generalize when faced with new ways of creating deep properties. Domain adaptation solves this problem and allows the model to adapt to unknown data models without the need for complete recycling (Wang and Deng, 2018).

Furthermore, the continued teaching method allows the model to gradually include new information while maintaining the knowledge it has already received. This approach is important to maintain modern detection systems as deep farm methods develop quickly.

Embedding Provenance Metadata and Watermarking

Origin-based approaches include the integration of metadata or digital watermarks when creating legal media and verifying its reliability later. Methods such as content authentication and blockchain have been developed to follow the origins and changes of

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VII, July 2025

digital content (McGregor et al., 2020). Such mechanisms not only help identify manipulated content, but also help to strengthen precautions in relation to deeper standards spread.

Standardized Global Comparison Support

The creation of standardized global standards potentially coordinated by international organizations such as the International Telecommunication Union (ITU) is essential for a consistent assessment of detection models for different countries and use cases (ITU, 2022).

Global standards combine evaluation criteria to ensure detection systems are carefully tested for reliability, justice, and scalability in a variety of cultural and technical contexts.

Human-Algorithm Collaboration in Detection

An encouraging approach is to strengthen cooperation between human testing and detection systems controlled by artificial intelligence. Algorithms contribute to the speed and ability to recognize models, but human analysts add valuable contextual understanding and ethical decision-making. This collaborative approach is particularly valuable in judicial and journalistic research where subtle notes are important (Chesney and Lemon, 2019).

Conclusion

Deepfakes has become a double-edition sword of digital landscapes. It provides innovative applications in the fields of entertainment, education and creative arts, while representing the unprecedented risks of information, confidentiality and the integrity of democratic processes. Since its creation in 2017, methods monitored by modern complex methods based on GANS and diffusion models have evolved in both technical complexity and social impact. This development requires an urgent, complete and interdisciplinary response, in particular within the framework of digital criminals' and to ensure the authenticity of the media.

The judicial importance of deep fake is profound. The ability of synthetic media to create persuasive false narratives raises important issues in legal context, cognitive activities, and public discourse. It should be noted that deepfakes have been used in disinformation campaigns, political manipulation and financial fraud, indicating the potential for a major damage technology. Multimodal detection systems that incorporate visual, audio and text signals are particularly effective in increasing the reliability of deep task detection. The hybrid model, which incorporates deep education into forensic function, also offers a balanced strategy, accuracy in interpreting mixtures. However, these detection methods are not without limitations. The key issue is the generalization of interdieman, where models trained on a particular dataset (e.g. DFDC, FaceFornsics++) are often not underlined sufficiently when exposed to real data. The computer costs of deploying modern models limit scalability, particularly in real-time or resource media limited. Furthermore, certain biases in existing datasets, often skewed in relation to demographics that are directed towards the West, create gaps in detection of populations in the southern world, representing serious fears about justice and inclusivity. The scope of evaluation has progressed along with indicators such as accuracy, accuracy, inspection, F1-indicator, AUC-ROC, and MCC, but is always insufficient to solve problems related to opponent reliability. Methods such as FGSM are subject to vulnerabilities. Vulnerabilities can fluctuate with minimal digging even in high-performance models, highlighting the need for a more stable and safe detection methodology. I look forward to some future instructions being mandatory. Multimodal detection systems provide a way to more complete analysis by capturing intermodal inconsistencies. Domain adaptation and constant training allow detection models to remain flexible and adapt to new ways of deep generation without the need for complete recycling. When digital watermarks are introduced directly in the pipeline of metadata and content creation, preventive protection mechanisms are provided, ensuring source validation and media monitoring. Additionally, the development of standardized global control indicators, possibly led by organizations such as the International Telecommunication Union (IUT), ensures uniform standards for evaluating and developing international cooperation. These criteria help overcome detection differences between cultures, languages and technological infrastructures and enable detection systems to be fair and globally applicable. Finally, human cooperation is distinguished as an important strategy. Algorithms provide scalability and speed, but human judgment is important for contextual analysis, especially in judicial research and journalistic testing. Creating an interface that promotes smooth cooperation between people and artificial intelligence systems experts can greatly improve the accuracy and reliability of deep task detection.

Therefore, solutions to deep fund problems go beyond the scope of technology alone. This is a social need and requires joint efforts in the domains such as law, politics, and ethics. At a time when synthetic environments continue to erode the boundary between reality and manufacturing, appropriate, interpretive, reliable, and fair construction detection systems are needed to maintain the integrity of digital information. Thanks to sustainable innovation, international cooperation and ethical forecasting, we want to alleviate the associated risks and protect reliability at the pace of the digital world.

References

1. Greenberg, J., White, H. C., Carrier, S., & Scherle, R. (2009). A metadata best practice for a scientific data repository. Journal of Library Metadata, 9(3-4), 194-212.
2. Mathis, R. M., & Caughey, L. (2005, January). A metadata model for electronic images. In Proceedings of the 38th Annual Hawaii International Conference on System Sciences (pp. 112a-112a). IEEE.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VII, July 2025

3. Mani, R. G., Parthasarathy, R., Eswaran, S., & Honnavalli, P. (2022). A survey on digital image forensics: Metadata and image forgeries. In Workshop on Applied Computing, January 27-28, 22 (Vol. 55, pp. 22-55).
4. Chen, P. L., Cheng, Y. C., & Chen, K. (2018). Analysis of social media data: an introduction to the characteristics and chronological process. Big Data in Computational Social Science and Humanities, 297-321.
5. Spyrou, E., & Mylonas, P. (2016). Analyzing Flickr metadata to extract location-based information and semantically organize its photo content. Neurocomputing, 172, 114-133.
6. Varthis, E., Poulos, M., Giarenis, I., & Papavlasopoulos, S. (2020). Automatic metadata extraction via image processing using Migne's Patrologia Graeca. International Journal of Metadata, Semantics and Ontologies, 14(4), 265-278.
7. Le Bourgeois, F., & Kaileh, H. (2004). Automatic metadata retrieval from ancient manuscripts. In Document Analysis Systems VI: 6th International Workshop, DAS 2004, Florence, Italy, September 8-10, 2004. Proceedings 6 (pp. 75-89). Springer Berlin Heidelberg.
8. Bharati, A., Moreira, D., Brogan, J., Hale, P., Bowyer, K., Flynn, P., ... & Scheirer, W. (2019, January). Beyond pixels: Image provenance analysis leveraging metadata. In 2019 IEEE winter conference on applications of computer vision (WACV) (pp. 1692-1702). IEEE.
9. Ingale, S., & Mehta, M. (2013). Characterizing suspicious images in social media using exif metadata. International Journal of Advance Computational Engineering and Networking.
10. Sugiantoro, B., & Prayudi, Y. (2018). Corelation Analysis Of Forensic Metadata For Digital Evidence. International Journal of Computer Science & Information Security, 16(3), 85.
11. Liu, X., Wang, M., & Huet, B. (2016). Event analysis in social multimedia: a survey. Frontiers of Computer Science, 10, 433-446.
12. Mombelli, S., Lyle, J. R., & Breitinger, F. (2024). FAIRness in digital forensics datasets' metadata–and how to improve it. Forensic Science International: Digital Investigation, 48, 301681.
13. Saranya, K., Paulraj, M., & Brindha, M. (2022, April). A survey on feature selection and classification techniques for EEG signal processing. In Proceedings of International Conference on Deep Learning, Computing and Intelligence: ICDCI 2021 (pp. 155-165). Singapore: Springer Nature Singapore.
14. McAuley, J., & Leskovec, J. (2012). Image labeling on a network: using social-network metadata for image classification. In Computer Vision–ECCV 2012: 12th European Conference on Computer Vision, Florence, Italy, October 7-13, 2012, Proceedings, Part IV 12 (pp. 828-841). Springer Berlin Heidelberg.
15. Riggs, C., Douglas, T., & Gagneja, K. (2018, October). Image mapping through metadata. In 2018 Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC) (pp. 1-8). IEEE.
16. Näslund, A. (2024). Image metadata. From information management to interpretative practice. Museum Management and Curatorship, 39(4), 398-418.
17. Kumar, P. R., Srikanth, C., & Sailaja, K. L. (2016). Location Identification of the Individual based on Image Metadata. Procedia Computer Science, 85, 451-454.
18. Smith, K. R., Saunders, S., & Kejser, U. B. (2014, June). Making the case for embedded metadata in digital images. In Archiving Conference (Vol. 11, pp. 52-57). Society for Imaging Science and Technology.
19. Tavakoli, M., Elias, M., Kismihók, G., & Auer, S. (2021, April). Metadata analysis of open educational resources. In LAK21: 11th International Learning Analytics and Knowledge Conference (pp. 626-631).
20. Hossain, M. A., & Haque, B. I. (2022, January). An Analytic Solution for the Helmholtz-Duffing Oscillator by Modified Mickens' Extended Iteration Procedure. In International Conference on Mathematics and Computing (pp. 689-700). Singapore: Springer Nature Singapore.
21. Noufal, P. P. (2005). Metadata: Automatic generation and extraction.
22. Sarvas, R., Herrarte, E., Wilhelm, A., & Davis, M. (2004, June). Metadata creation system for mobile images. In Proceedings of the 2nd international conference on Mobile systems, applications, and services (pp. 36-48).
23. Holland, R., Leingang, O., Bogunović, H., Riedl, S., Fritsche, L., Prevost, T., ... & Menten, M. J. (2024). Metadata-enhanced contrastive learning from retinal optical coherence tomography images. Medical Image Analysis, 103296.
24. Linkert, M., Rueden, C. T., Allan, C., Burel, J. M., Moore, W., Patterson, A., ... & Swedlow, J. R. (2010). Metadata matters: access to image data in the real world. Journal of Cell Biology, 189(5), 777-782.
25. Tesic, J. (2005). Metadata practices for consumer photos. IEEE MultiMedia, 12(3), 86-92.
26. Lim, S., & Li Liew, C. (2011, September). Metadata quality and interoperability of GLAM digital images. In Aslib Proceedings (Vol. 63, No. 5, pp. 484-498). Emerald Group Publishing Limited.
27. Chakraborty, C., Gupta, B., & Ghosh, S. K. (2014). Mobile metadata assisted community database of chronic wound images. Wound Medicine, 6, 34-42.
28. Haucke, M., Heinzel, S., & Liu, S. (2024). Social mobile sensing and problematic alcohol consumption: Insights from smartphone metadata. International Journal of Medical Informatics, 188, 105486.
29. Chen, Y., Sherren, K., Smit, M., & Lee, K. Y. (2023). Using social media images as data in social science research. New Media & Society, 25(4), 849-871.
30. McAuley, J., & Leskovec, J. (2012). Image labeling on a network: using social-network metadata for image classification. In Computer Vision–ECCV 2012: 12th European Conference on Computer Vision, Florence, Italy, October 7-13, 2012, Proceedings, Part IV 12 (pp. 828-841). Springer Berlin Heidelberg.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VII, July 2025

31. Schreck, T., & Keim, D. (2012). Visual analysis of social media data. Computer, 46(5), 68-75.
32. Ramesh Kumar P., Ch Srikanth, KL Sailaja. “Location Identification of the Individual based on Image Metadata.” Procedia Computer Science, vol. 85, 2016, pp. 451-454.