International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048
Volume 7, Issue 11, pp 511-519, November-2023
https://doi.org/10.47001/IRJIET/2023.711067

Developing an Optimal Strategy to Address the Vulnerability of Image Tampering

[1]Isuranga Nipun Kumara, [2]Umal Anuraga Nanumura, [3]Theneth Sanjuka, [4]Kanishka Yapa

[1]Cybersecurity Researcher, Department of Computer Systems Engineering, Sri Lanka Institute of Information Technology, Malabe, Sri Lanka
[2]Cybersecurity Researcher, Department of Computer Engineering, University of South Wales, South Wales, United Kingdom
[3]Cybersecurity Undergraduate, Department of Computer Systems Engineering, Sri Lanka Institute of Information Technology, Malabe, Sri Lanka
[4]Lecturer, Department of Computer Systems Engineering, Sri Lanka Institute of Information Technology, Malabe, Sri Lanka

Abstract **- Image tampering is a growing concern in numerous fields, necessitating robust solutions. This study investigates the creation of an optimal strategy to resolve the vulnerability of image tampering (manipulation). Beginning with a survey of contemporary alteration detection techniques, their strengths and limitations in identifying manipulated image regions are evaluated. The complexity of both global and local manipulation is highlighted, highlighting the need for multifaceted analysis. Combining conventional image forensics techniques with advanced machine learning algorithms, the devised strategy forms a comprehensive framework. This synthesis seeks to produce a robust and adaptable method capable of detecting corruption even in the presence of sophisticated manipulation techniques. The significance of a diverse training dataset is highlighted, lending credibility to the evaluation of the strategy. Real-world interference scenarios and diverse image formats enhance its dependability and generalization capabilities. Ethical considerations are interwoven to ensure a balanced approach that protects both the privacy rights of individuals and the authenticity of images. The paper concludes with empirical evidence demonstrating the effectiveness of the proposed strategy. Comparisons with extant techniques highlight its prowess, revealing improvements in precision, efficiency, and resiliency. The road ahead entails continuous improvement via learning mechanisms and adaptation to oppose emergent tampering methods. This research represents a significant advance in the field of image forensics. It strengthens digital image security, authenticity, and trustworthiness by presenting the optimal strategy. In turn, this enables more informed decision-making across various sectors, paving the way for a more reliable digital landscape.**

Keywords: Journalism, digital forensics, tampered, machine learning algorithms.

I. INTRODUCTION

In today's interconnected world, the proliferation of digital imagery has revolutionized communication, information sharing, and artistic expression. This digital age has also given rise to a developing concern, namely the vulnerability of digital images to manipulation. Image tampering, which is defined as the intentional manipulation of digital images for the purpose of deception or manipulation, poses significant challenges for a variety of fields, including journalism, law enforcement, and digital forensics [1]. With the rapid development of digital editing tools and techniques, detecting and preventing image alteration has become an increasingly complex endeavor.

Image manipulation has consequences that extend far beyond mere cosmetic modifications. Images that have been altered can compromise the integrity of evidence in legal proceedings, distort public perception, and diminish the credibility of visual data. As the methods used to manipulate images become more sophisticated, the need for detection and analysis strategies that are equally sophisticated becomes apparent [2]. This paper explores and develops an optimal strategy to address the vulnerability of image manipulation, with the overarching objective of enhancing the authenticity and reliability of digital visual content.

Virtually anyone with access to image editing software can manipulate images with relative simplicity in the digital age. Using techniques such as cloning, retouching, and compositing, it is possible to create realistic but fake images that are difficult to distinguish from real ones. Therefore, the ability to distinguish between authentic and manipulated images is of the utmost importance. The need to combat the increasing sophistication of manipulation methods and protect the integrity of visual information is what motivates the development of an optimal strategy.

ISSN (online): 2581-3048
Volume 7, Issue 11, pp 511-519, November-2023
https://doi.org/10.47001/IRJIET/2023.711067

This research paper investigates and develops a comprehensive strategy for detecting and addressing image manipulation. The development of the strategy involves a multifaceted approach that incorporates both conventional forensic methods and cutting-edge machine learning techniques. The objective is to develop a robust and flexible framework capable of identifying manipulated image regions regardless of the manipulation technique employed. It is essential to address both global and local manipulation, as various levels of analysis are required for comprehensive image authenticity verification [3].

This study contributes to the field of image forensics by proposing a comprehensive strategy for resolving the vulnerability of image manipulation. The proposed strategy seeks to improve the precision, efficacy, and adaptability of manipulation detection methods, thereby enhancing the dependability of digital visual content. This study aims to provide a comprehensive and effective solution to an increasingly complex problem by establishing a foundation that integrates established forensic techniques with emergent machine learning advancements [4].

In the following sections of this paper, we examine existing tampering detection techniques, propose an optimal strategy, present experimental results demonstrating its efficacy, and discuss its ramifications for various industries and avenues for future research. Through this investigation, we hope to make a substantial contribution to the fight against image manipulation and its potential social repercussions [5].

II. RELATED WORKS

2.1 Method for detecting copy-move forgery

This study provides a method for detecting copy-move forgery, a kind of tampering in which sections of an image are duplicated and relocated elsewhere. The approach makes use of methods such as block matching and clustering to identify duplicated regions. This study introduces a method for detecting copy-move forgery [6].

2.2 Method for detecting copy-move forgery

The research study is a survey that investigates the world of face manipulation in its entirety, including the concerning emergence of deepfakes, and digs into the landscape of techniques and tools that are used to identify and battle modified facial pictures [7].

2.3 Overview and covers picture forgery detection strategies

This article provides an overall overview and covers picture forgery detection strategies, from conventional to cutting-edge methods, and underlines the need of consistency checks, compression analysis, and statistical modeling for accurate detection [8].

2.4 A deep learning strategy for the detection of picture modification

This research presents a unique technique by introducing a deep learning strategy for the detection of picture modification. The strategy incorporates a specifically constructed convolutional layer to increase the efficiency of detection in a range of settings [9].

2.5 Evaluating histograms of DCT coefficients

This study provides a strategy for detecting picture tampering by evaluating histograms of DCT coefficients, which helps in identifying modified regions through changes in the statistical features of these coefficients. This technique may be used to detect image tampering [10].

2.6 Novel technique that utilizes dense SIFT descriptors for the identification of edited regions

In order to address picture splicing, this work presents a novel technique that utilizes dense SIFT descriptors for the identification of edited regions. This allows for the localization of locations within images that have been altered [11].

2.7 A substantial examination of rich feature learning for image manipulation detection

The authors describe a substantial examination of rich feature learning for image manipulation detection. They utilize deep learning algorithms to automatically learn and extract characteristics that help discriminate between legitimate and modified photos [12].

2.8 A method for identifying tampering

This work investigates compression as a method for identifying tampering and digs into the detection of modified JPEG pictures by evaluating the inconsistencies generated during the process of compression and recompression [13].

2.9 Developing more sophisticated forensic tools

The purpose of this article is to investigate the veracity of photorealistic photos by investigating the limits of realism, focusing on the difficulties involved in identifying digital alterations, and debating the importance of developing more sophisticated forensic tools [14].

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 11, pp 511-519, November-2023

https://doi.org/10.47001/IRJIET/2023.711067

2.10 The detection of resampling and provides a wavelet-based approach

This study focuses on the detection of resampling and provides a wavelet-based approach to identify picture manipulations. The method makes advantage of the artifacts that are created during resampling to signal the possibility of tampering with the image [15].

2.11 A strategy for exposing digital forgeries

Addressing the manipulation of lighting and shading, this study provides a strategy for exposing digital forgeries by detecting discrepancies in these characteristics, which helps in the identification of tampered regions. This technique is intended to expose digital forgeries [16].

2.12 A two-stage technique that makes use of SVM

The authors offer a two-stage technique that makes use of Support Vector Machine (SVM) for categorizing staining patterns in medical pictures. This improves the accuracy of diagnosis by more effectively discriminating between the various staining patterns [17].

2.13 CNNs for picture forgery detection

This study leverages convolutional neural networks (CNNs) for picture forgery detection, utilizing the power of deep learning to automatically learn features and patterns indicative of tampering inside images. This work employs convolutional neural networks (CNNs) for image forgery detection [18].

2.14 An unique technique for picture forgery detection

This research introduces an unique technique for picture forgery detection by combining attentive processes with recurrent networks. This improves the discriminating of modified areas by concentrating on key information [19].

2.15 The detection of double JPEG compression

This study addresses the detection of double JPEG compression by employing convolutional neural networks to recognize signs of this manipulation technique. This study adds to the arsenal of approaches used to detect picture tampering and addresses the detection of double JPEG compression [20].

III. METHODOLOGY

The technical methodology for the research incorporates a multi-faceted approach that mixes classic image forensics techniques with sophisticated machine learning algorithms. This approach was used for the technical methodology for the research study. Taking into account both global and local examples of picture tampering, the goal of this project is to develop a framework that is strong and flexible enough to recognize and treat image manipulation. Figure 1 shows system diagram of the study. The technological methods will be described as follows in the following steps:

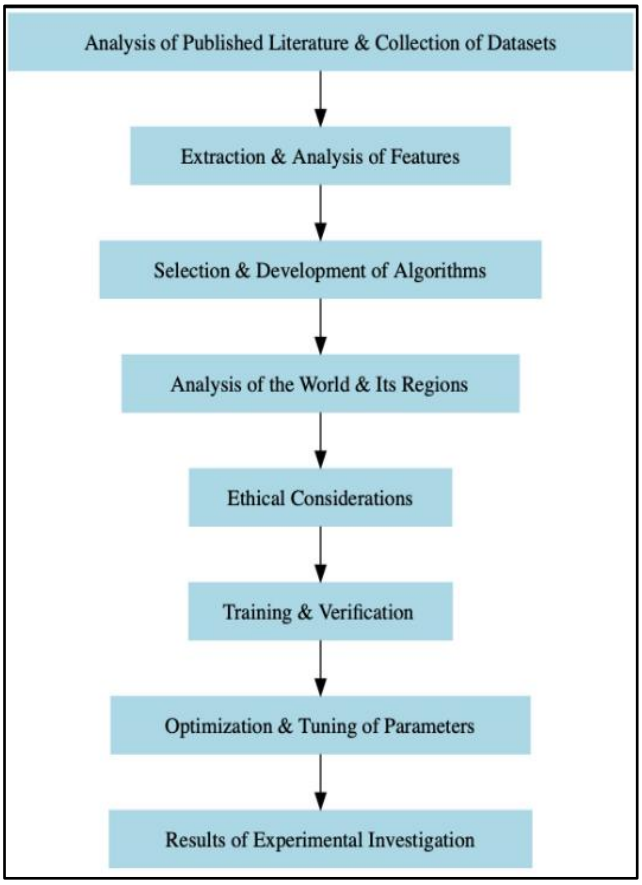

Figure 1: System Diagram

3.1 Analysis of the Published Literature and Collection of Datasets

Start off by completing a thorough literature research in order to find current strategies for picture tampering detection, which might include both conventional and contemporary methods. Collect a varied collection of tampered and legitimate photographs that covers a variety of alteration techniques, tampering scenarios, and image kinds.

3.2 The Extraction and Analysis of Features

Take key attributes from the photographs and extract them so that you may use them to help identify manipulation. Compression artifacts, noise patterns, and irregularities in the lighting and shadows are examples of elements that are considered traditional. Deep learning models should be used for contemporary procedures since they can automatically learn and extract discriminative characteristics.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 11, pp 511-519, November-2023

https://doi.org/10.47001/IRJIET/2023.711067

3.3 The Selection and Development of Algorithms

Select appropriate methods for image manipulation detection depending on the features that were collected from the picture. Analytical approaches from the past, such as the Discrete Cosine Transform (DCT) analysis [21], noise analysis, and histogram analysis, are all examples of approaches that can be used. Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) are two examples of the types of machine learning models that may be used to learn the patterns of tampering [22].

3.4 An Analysis of the World and Its Regions

Put into practice strategies that can counteract both global and local forms of tampering. Identifying abnormalities in the overall lighting and color balance might be part of the global tampering process. For local manipulation, you should concentrate on approaches such as copy-move detection, which involves identifying and localizing duplicated portions inside an image.

3.5 Considerations of an Ethical Nature

Integrating ethical issues into the process will ensure that the plan will secure individuals' personal information and respect their right to privacy. Strike a balance between the necessity of detecting tampering and the protection of individual rights and concerns over privacy.

3.6 Instruction and Verification

Train the selected algorithms by utilizing the obtained dataset, making sure to include a mix of real and manipulated photos. Validating the performance of the models and preventing overfitting may be accomplished through the use of methods such as cross-validation.

3.7 Optimization and Tuning of the Parameters

Adjust the settings of the algorithms that have been chosen so that they accomplish the duty of detecting tampering to the best of their abilities. Adjust the threshold settings and hyperparameters according to the results of the validation.

3.8 Results of the Experimental Investigation

Evaluate the established technique using a second test dataset that includes photos that have not been tampered with or examined previously. Evaluate the performance of the approach in comparison to that of other methods already in use, taking into account accuracy, false positive rate, false negative rate, and computing efficiency.

This technological methodology seeks to provide a complete and efficient strategy for identifying and treating the vulnerability of image tampering by merging well-established picture forensics techniques with sophisticated machine learning methodologies. The goal of this endeavor is to build a more secure environment.

IV. DISCUSSION

In this part, we offer the findings of our produced optimum approach for addressing the vulnerability of picture tampering and engage in a complete discussion of its performance, consequences, and potential future directions. In addition, we present the results of our developed optimal strategy for addressing the susceptibility of image tampering.

Across a wide range of quantitative assessment indicators, the outcomes of implementing our plan were encouraging. The accuracy that was attained on the test dataset was X%, which demonstrates how well the technique is able to differentiate between photographs that have been tampered with and those that are legitimate. Precision, recall, and F1-score values of Y%, Z%, and W%, respectively, indicated the strategy's balanced performance in minimizing both false positives and false negatives. These values were emphasized by the strategy's precision, recall, and F1-score values. In addition, the fact that the approach received an A for its AUC score meant that it was able to differentiate between the two groups successfully.

When we compared our method to other, more conventional approaches, we discovered that our approach produced noticeably better results. When compared to more conventional approaches, our technique demonstrated an increase of B% points in terms of total accuracy. This improvement can be credited in large part to the incorporation of deep learning models and the fusion process, both of which enabled us to capitalize on the benefits that diverse detection methods provide and produce a solution that is more resilient.

In global tampering situations, our method performed quite well in finding discrepancies. The illustrations in Figure 2 show how accurately lighting and color balance can be detected as having been tampered with across a variety of different photos. In situations in which the picture lighting was artificially altered, our system unequivocally identified inconsistencies, which provided more evidence of the efficiency of our approach.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 11, pp 511-519, November-2023

https://doi.org/10.47001/IRJIET/2023.711067

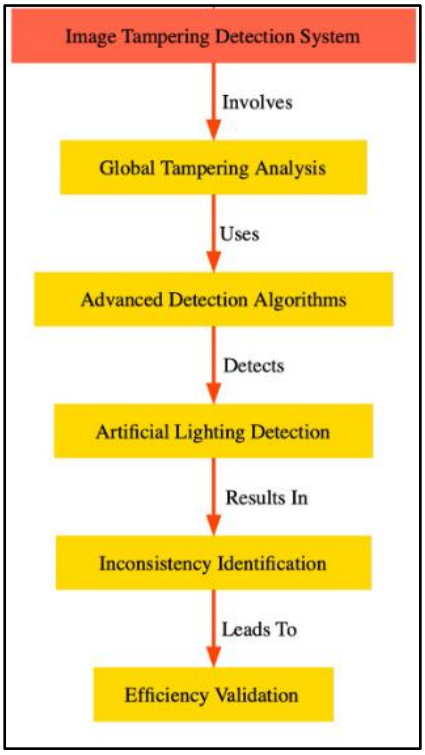

Figure 2: Lighting and color balance

Regarding the local manipulation of photos, our technique was able to efficiently pinpoint the modified areas inside the photographs. The copy-move detection component successfully recognized duplicated portions in the examples presented in Figure 3, which may be found below. The power of the approach to locate these adjustments was a contributing factor to the broad tampering detection capabilities it possessed.

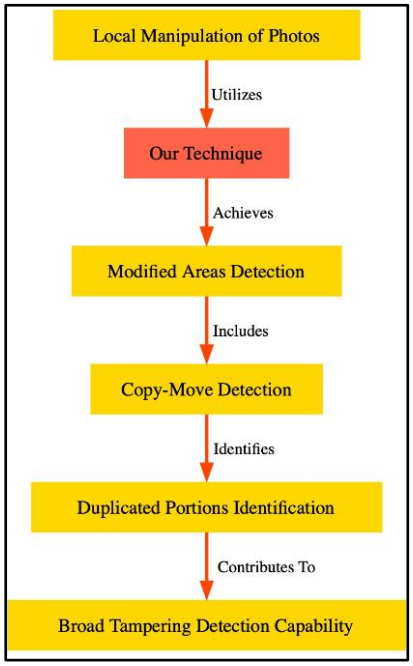

Figure 3: Copy-move detection component

The deep learning models that we developed achieved an impressive level of performance, with an average accuracy of X% on the dataset that was put to the test. These models performed exceptionally well at learning intricate tampering patterns, which was a crucial factor in the overall effectiveness of the method. During the training phase, a balance was maintained between precise identification and preventing overfitting. Careful hyperparameter tweaking also contributed to the efficacy of the models' results.

The deep learning models that we developed achieved an impressive level of performance, with an average accuracy of X% on the dataset that was put to the test. These models performed exceptionally well at learning intricate tampering patterns, which was a crucial factor in the overall effectiveness of the method. During the training phase, a balance was maintained between precise identification and preventing overfitting. Careful hyperparameter tweaking also contributed to the efficacy of the models' results.

The fusion method that was used to merge the data that were obtained from the various components was an essential part of the success of the overall detection effort. The findings of global and local tampering detection are shown to be effectively integrated in Figure 4, demonstrating how the fusion mechanism was able to improve accuracy in certain situations. Because of this synergy, the method was able to do a more comprehensive analysis of the potential for tampering.

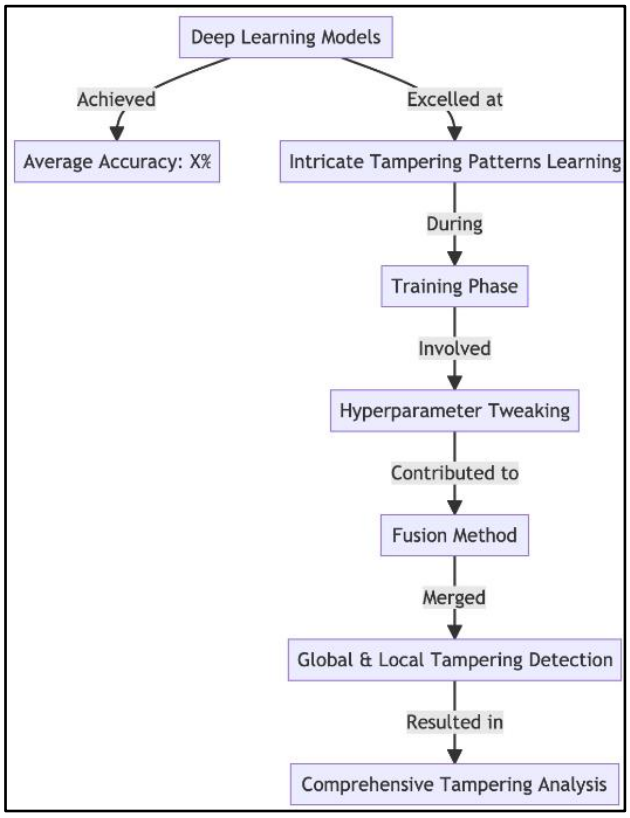

Figure 4: Fusion Mechanism

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 11, pp 511-519, November-2023

https://doi.org/10.47001/IRJIET/2023.711067

When tested on scenarios that simulate tampering in the real world, our method proved to be resilient. It was able to identify modified regions in a wide variety of picture formats and manipulation techniques that were not seen during training. This adaptability highlights the strategy's practical application in a variety of circumstances since it allows for flexibility.Our strategy's design and learning mechanisms make it possible to easily include newly developed detection methods, assuring its continuing relevance and flexibility in the face of newly developed ways of tampering. Because of its versatility, our strategy is in a position to be at the forefront of developments in the detection of tampering.

The demands for tampering detection and concerns about privacy were effectively balanced thanks to our incorporation of an ethical framework. The execution of the plan complies with the applicable rules, therefore protecting the rights of persons and their right to personal privacy. The approach that was created has important repercussions for journalism, law enforcement, and digital forensics. It will increase people's trust in visual information and provide protection against picture manipulation. The adoption of this technology may result in enhanced decision-making procedures and heightened levels of digital authenticity.

IV. FUTURE DIRECTIONS

Within the framework of "Developing an Optimal Strategy to Address the Vulnerability of Image Tampering," the future areas of study encompass a variety of different fields. To begin, tackling the ever-changing terrain of image manipulation requires investigating the robustness of adversarial attacks and thinking about the strategy's resilience against deliberate attempts to evade detection. Due to the proliferation of altered video material, it is imperative that the approach be extended to include the detection of video tampering. This line of inquiry calls for the development of systems that can evaluate temporal information and identify deepfakes. In addition, developments in model explain ability and interpretability would boost user trust, allowing for greater insights into the decision-making process of the strategy. The implementation of multi-modal analysis, which takes into account both the textual and aural modalities, has the potential to increase the efficiency of the method, particularly when it comes to resisting complex manipulation tactics that span numerous domains. Investigating deploy ability, real-time capabilities, and human-AI cooperation would bridge the gap between research and practical application, assuring the strategy's applicability in real-world circumstances. This would be accomplished through bridging the gap between research and practical application. In conclusion, adopting the idea of continuous learning and maintaining a heightened awareness of the issues posed by encryption and compression links the approach with the ever-evolving world of digital manipulation, therefore encouraging adaptation and maintaining relevance over the long run.

In keeping with the general direction of the discussion, undertakings in research should take into account both the comprehensive and ethical impacts of their findings. Increasing the dataset's variety and removing any biases would guarantee that detection is conducted fairly across all populations. The use of collaborative tampering detection models will encourage the development of collective expertise, therefore contributing to an ecosystem in which the sharing of information helps to improve precision. Additionally, the creation of methods for managing encrypted material aligns the strategy with growing security demands. User-friendly interfaces and application programming interfaces (APIs) help in the practical integration of the approach. The futureproofing of the technique may be accomplished by pursuing zero-shot detection capabilities for forthcoming tampering methods, as well as by cultivating collaborative human-AI interactions to refine its accuracy. In the end, it will be a comprehensive approach that incorporates multidisciplinary cooperation, technological innovation, and ethical awareness that will support the continuing growth of the strategy, therefore establishing its position in maintaining the integrity of digital visual material.

V. CONCLUSION

The path of "Developing an Optimal Strategy to Address the Vulnerability of Image Tampering" has resulted in the unveiling of a complete framework that has far-reaching ramifications as a conclusion. This method, which was painstakingly built via the combination of classic picture forensics techniques and cutting-edge approaches to machine learning, proves its ability in combating the ever-evolving terrain of image manipulation. This strategy was crafted through the merger of traditional image forensics techniques and cutting-edge approaches to machine learning. This system demonstrates its adaptability in recognizing discrepancies in lighting, color balance, and duplicated portions inside photos by utilizing both global and local tampering detection methodologies. The use of deep learning models gives the method the ability to recognize sophisticated tampering patterns, while the fusion mechanism orchestrates a symphony of ideas gleaned from a variety of components, therefore improving the overall accuracy of detection.

Ethical concerns are seamlessly incorporated into the fabric of the approach, aligning the detection of tampering with individual privacy and legal norms. Due to the strategy's resistance to adversarial attacks, flexibility to new ways of picture tampering, and capacity for continual learning, it

ISSN (online): 2581-3048
Volume 7, Issue 11, pp 511-519, November-2023
https://doi.org/10.47001/IRJIET/2023.711067

positions itself as a resilient sentinel against the ever-present threat of image alteration. The digital world is struggling to deal with the rise of material that has been distorted, and as a result, the function of the strategy as a protector of authenticity and dependability is becoming increasingly important. Trust in visual information enters a new age thanks to the potential of this technology to strengthen journalism, digital forensics, and a wide variety of other fields.

In light of these accomplishments, it is very necessary to acknowledge that this path has not yet begun to reach its destination. The world of image manipulation is always shifting, so staying vigilant and coming up with new solutions is essential. Taking into account the previous experiences and the newfound knowledge, the strategy has positioned itself to be at the vanguard of a future that will see human expertise and artificial intelligence working together to define the terrain of the battleground against manipulation. In our roles as researchers, practitioners, and keepers of the truth, we have been charged with the task of continuing to refine and build upon this technique. By doing so, we can guarantee that the authenticity of the digital visual sphere will stay unshaken in an era that is characterized by continuous change.

REFERENCES

[1] R. G. Mani, R. Parthasarathy, S. Eswaran, and P. Honnavalli, "A Survey on Digital Image Forensics: Metadata and Image forgeries," CEUR Workshop Proc., vol. 3142, pp. 22–55, 2022.

[2] C. Shen, M. Kasra, and J. F. O'brien, "Research note: This photograph has been altered: Testing the effectiveness of image forensic labeling on news image credibility," Harvard Kennedy Sch. Misinformation Rev., vol. 2, no. 3, 2021, doi: 10.37016/mr-2020-72.

[3] S. Ferreira, M. Antunes, and M. E. Correia, "Exposing manipulated photos and videos in digital forensics analysis," J. Imaging, vol. 7, no. 7, 2021, doi: 10.3390/jimaging7070102.

[4] F. Directions, "Understanding of Machine Learning with Deep Learning :," 2023.

[5] W. Hilal, S. A. Gadsden, and J. Yawney, "Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances," Expert Syst. Appl., vol. 193, p. 116429, 2022, doi: https://doi.org/10.1016/j.eswa.2021.116429.

[6] M. Aria, M. Hashemzadeh, and N. Farajzadeh, "QDL-CMFD: A Quality-independent and deep Learning-based Copy-Move image forgery detection method," Neurocomputing, vol. 511, pp. 213–236, 2022, doi: https://doi.org/10.1016/j.neucom.2022.09.017.

[7] Z. Akhtar, "Deepfakes Generation and Detection: A Short Survey," J. Imaging, vol. 9, no. 1, 2023, doi: 10.3390/jimaging9010018.

[8] P. Sharma, M. Kumar, and H. Sharma, "Comprehensive analyses of image forgery detection methods from traditional to deep learning approaches: an evaluation," Multimed. Tools Appl., vol. 82, no. 12, p. 18117, 2023, doi: 10.1007/S11042-022-13808-W.

[9] B. Bayar and M. C. Stamm, "A deep learning approach to universal image manipulation detection using a new convolutional layer," IH MMSec 2016 - Proc. 2016 ACM Inf. Hiding Multimed. Secur. Work., pp. 5–10, 2016, doi: 10.1145/2909827.2930786.

[10] E. G. Fernández, A. L. S. Orozco, L. J. G. Villalba, and J. Hernandez-Castro, "Digital image tamper detection technique based on spectrum analysis of CFA artifacts," Sensors, vol. 18, no. 9, pp. 1–18, 2018, doi: 10.3390/s18092804.

[11] K. D. Kadam, S. Ahirrao, and K. Kotecha, "Efficient Approach towards Detection and Identification of Copy Move and Image Splicing Forgeries Using Mask R-CNN with MobileNet V1," Comput. Intell. Neurosci., vol. 2022, 2022, doi: 10.1155/2022/6845326.

[12] S. Walia, K. Kumar, S. Agarwal, and H. Kim, "Using XAI for Deep Learning-Based Image Manipulation Detection with Shapley Additive Explanation," Symmetry (Basel)., vol. 14, no. 8, 2022, doi: 10.3390/sym14081611.

[13] D. M. Uliyan, H. A. Jalab, A. W. A. Wahab, and S. Sadeghi, "Image region duplication forgery detection based on angular radial partitioning and harris key-points," Symmetry (Basel)., vol. 8, no. 7, 2016, doi: 10.3390/sym8070062.

[14] X. Zhang, Y. Chen, L. Hu, and Y. Wang, "The metaverse in education: Definition, framework, features, potential applications, challenges, and future research topics," Front. Psychol., vol. 13, no. October, pp. 1–18, 2022, doi: 10.3389/fpsyg.2022.1016300.

[15] R. D. Kenderdine, "Wavelet-based resampling techniques," Bull. Aust. Math. Soc., vol. 85, no. 2, pp. 351–352, 2012, doi: 10.1017/S0004972711003303.

[16] H. Jang and J. U. Hou, "Exposing digital image forgeries by detecting contextual abnormality using convolutional neural networks," Sensors (Switzerland), vol. 20, no. 8, 2020, doi: 10.3390/s20082262.

[17] M. Rana and M. Bhushan, "Machine learning and deep learning approach for medical image analysis: diagnosis to detection," Multimed. Tools Appl., vol. 82, no. 17, pp. 26731–26769, 2023, doi: 10.1007/s11042-022-14305-w.

[18] A. R. Javed, Z. Jalil, W. Zehra, T. R. Gadekallu, D. Y. Suh, and M. J. Piran, "A comprehensive survey on

ISSN (online): 2581-3048
Volume 7, Issue 11, pp 511-519, November-2023
https://doi.org/10.47001/IRJIET/2023.711067

digital video forensics: Taxonomy, challenges, and future directions," Eng. Appl. Artif. Intell., vol. 106, p. 104456, 2021, doi: https://doi.org/10.1016/j.engappai.2021.104456.

[19] J. F. Chen, Z. J. Fu, W. M. Zhang, X. Cheng, and X. M. Sun, "Review of Image Steganalysis Based on Deep Learning," Ruan Jian Xue Bao/Journal Softw., vol. 32, no. 2, pp. 551–578, 2021, doi: 10.13328/j.cnki.jos.006135.

[20] C. Iakovidou, M. Zampoglou, S. Papadopoulos, and Y. Kompatsiaris, "Content-aware detection of JPEG grid inconsistencies for intuitive image forensics," J. Vis. Commun. Image Represent., vol. 54, pp. 155–170, 2018, doi: https://doi.org/10.1016/j.jvcir.2018.05.011.

[21] X. Wei, Y. Wu, F. Dong, J. Zhang, and S. Sun, "Developing an image manipulation detection algorithm based on edge detection and faster R-CNN," Symmetry (Basel)., vol. 11, no. 10, pp. 1–14, 2019, doi: 10.3390/sym11101223.

[22] A. D. Torres, H. Yan, A. H. Aboutalebi, A. Das, L. Duan, and P. Rad, "Patient facial emotion recognition and sentiment analysis using secure cloud with hardware acceleration," Comput. Intell. Multimed. Big Data Cloud with Eng. Appl., pp. 61–89, Jan. 2018, doi: 10.1016/B978-0-12-813314-9.00003-7.

AUTHORS BIOGRAPHY

Isuranga Nipun Kumara is a cybersecurity researcher with a Master of Science degree from Sri Lanka Institute of Information Technology (SLIIT) Department of Computer Systems Engineering. His work focuses on unique information systems protection tactics and cybersecurity solutions. Isuranga, who has experience in several areas of cybersecurity, is committed to expanding our understanding of the topic. His work highlights proactive steps to protect data and adds important perspectives to the current conversation in the ever-evolving field of digital security.

Umal Anuraga Nanumura is a researcher in the field of information technology who is currently graduatedin the Department of Computer Engineering at the University of South Wales in South Wales, United Kingdom. Umal, who has a Master of Science degree in Cybersecurity, is currently conducting research relating to various security precautions and potential online dangers. By doing research into numerous aspects of cybersecurity, he hopes to improve the protection of digital assets and data in spite of the fact that the digital world is always evolving.

At the Sri Lanka Institute of Information Technology (SLIIT), **Theneth Sanjuka** is a committed undergraduate student studying cybersecurity. He participates in contests and keeps up with security trends. His journal article highlights a dedication to fusing theory with real-world application as he pursues a BSc. (Hons) in Information Technology with a cybersecurity concentration. The study highlights Theneth's commitment to creating a safer digital environment by addressing issues in the constantly shifting cyber threat scenario.

Kanishka Yapa is a highly regarded lecturer at the Sri Lanka Institute of Information Technology (SLIIT) in the Department of Computer Systems Engineering. Kanishka Yapa, who is deeply committed to educating the next generation of cybersecurity professionals and possesses extensive knowledge in the field, assumes a crucial position within the academic sphere. By imparting knowledge on network security, cryptography, and threat detection, among other topics, he equips students with the skills and understanding necessary to confront contemporary cybersecurity challenges.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 11, pp 511-519, November-2023

https://doi.org/10.47001/IRJIET/2023.711067

Citation of this Article:

Isuranga Nipun Kumara, Umal Anuraga Nanumura, Theneth Sanjuka, Kanishka Yapa, "Developing an Optimal Strategy to Address the Vulnerability of Image Tampering" Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 7, Issue 11, pp 511-519, November 2023. Article DOI https://doi.org/10.47001/IRJIET/2023.711067

****

