International Journal of Science, Strategic Management and Technology
Volume **02** Issue **04** April-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

TrustNet a Deep Learning based intelligent system for digital image authenticity and forgery avoidance

Mrs. K. Vinotha
year Final year
Information Technology
M.I.E.T Engineering
Tiruchirappalli, Tamil Nadu.
vinothakcse@gmail.com

S. Madhu Priya
Final year Department Of
Information Technology
M.I.E.T Engineering
Tiruchirappalli, Tamil Nadu.
smadhupriya1309@gmail.com

A. Selciya
Department Of
Information Technology
M.I.E.T Engineering,
Tiruchirappalli, Tamil Nadu.
aselciyaselciya@gmail.com

P. Karthikha
Department of
Information Technology
M.I.E.T Engineering College,
Tiruchirappalli, Tamil Nadu.
pkarthikha17050@gmail.com

S. Ramya Assistant professorFinal year Final
Department of Department Of
Information TechnologyM.I.E.T Engineering
College, College, College, College,
Tiruchirappalli, Tamil Nadu.
msbramya2005@gmail.com

https://doi.org/10.55041/ijsmt.v2i4.094
Cite this Article: Vinotha, K., Priya, S. M., Selciya, A., Karthikha, P. & Ramya, S. (2026). TrustNet a Deep Learning based intelligent system for digital image authenticity and forgery avoidance. International Journal of Science, Strategic Management and Technology, *02*(04). https://doi.org/10.55041/ijsmt.v2i4.094

***Abstract*—**Secure transmission of sensitive information is a critical requirement in modern cyber and defence communication systems. Although conventional encryption techniques provide strong protection, they remain vulnerable when encryption keys are compromised or encrypted data is intercepted. To address this limitation, this paper proposes a Multi-Security Image Cyber Model for highly confidential data transmission. The framework employs a multi-image–based architecture in which five cover images are initially processed, and three are dynamically selected to reduce predictability.

Sensitive data is embedded into the selected images using amatrix-based embedding approach. A single reconstruction password generated at a predefined reference point serves as the key to combine the images and recover the hidden information. Additionally, the framework utilizes both original and compressed forgery data to learn a compression sensitive embedding feature space, improving robustness against compression-related distortions and attacks. By distributing security parameters across multiple images and requiring a tri- component reconstruction process, the model significantly enhances resistance to brute-force attacks, interception, and unauthorized decoding while maintaining efficient transmission performance

Keywords—deep learning, digital image, Cyber Security, encryption

I. INTRODUCTION

With rapid advancements in Artificial Intelligence, forged facial content has become increasingly sophisticated, making it difficult for the human eye to distinguish between fake and real faces. Moreover, the complexity of real-world deployment environments further degrades the performance of existing detection models. Therefore, developing generalized and robust face forgery detection systems to counter malicious attacks remains a significant challenge. The rapid evolution and widespread availability of advanced image processing tools have made it increasingly difficult to trust digital images. The accessibility and sophistication of these tools have significantly contributed to the proliferation of image forgery, as highlighted by Liu et al. (2018). Digital image forgery techniques, including copy-move manipulation, are widely used to compromise imageauthenticity, often leading to misinformation dissemination and fraudulent activities (Wu et al., 2018).

With the growing popularity of social media platforms, users frequently share images and videos from their daily lives. Both expert and non-expert forgers can manipulate such content for malicious purposes Piva et al.(2013). Consequently, several intelligent methods Wu et al.(2022), Hussain et al. (2021), Dong et al. (2022), and Marra et al. (2018) have been proposed to detect manipulation traces and ensure image authenticity. However, modern cyberattacks often conceal manipulation artifacts, thereby misleading existing cybersecurity systems. Additionally, as cyber threats continuously evolve, security mechanisms must be regularly updated; otherwise, they risk becoming ineffective against emerging attack strategies.

Conventional cryptographic frameworks, such as the Advanced Encryption Standard (AES) and Rivest–
Shamir–Adleman (RSA), have long served as the foundation of secure digital communication. These algorithms provide strong mathematical protection by ensuring data confidentiality and integrity through key-based encryption. However, despite their effectiveness, they suffer from a critical limitation: the presence of a single point of failure. If an adversary gains access to the encryption key through side channel attacks, social engineering, or cryptanalysis or intercepts encrypted data for offline brute-force attacks, the entire security model is compromised. Furthermore, the existence of a single encrypted file may itself attract adversarial attention, increasing the risk of targeted attacks.

To address these limitations, this paper proposes a Multi Security Image Cyber Model with the following key contributions:

- **Dynamic Carrier Selection:** A controlled selection mechanism that reduces predictability in transmission patterns, thereby mitigating vulnerabilities associated with static steganographic systems.
- **Tri-Component Reconstruction:** A novel architecture where data recovery depends on the correct combination of three independent carrier images along with a unified password, effectively eliminating the single-point-of-failure inherent in traditional encryption methods.
- **Efficient Performance:** The proposed framework ensures enhanced multi-layer security while

maintaining efficient computational and transmission performance, making it suitable for bandwidth- and latency-constrained environments such as military and defence communication systems.

The remainder of this paper is organized as follows: Section 2 reviews related work in cryptography, steganography, and multi-carrier security models. Section 3 presents the proposed Multi-Security Image Cyber Model, including the carrier selection mechanism, embedding strategy, and reconstruction protocol. Section 4 discusses the experimental setup, results, and comparative security analysis. Finally, Section 5 concludes the paper with key findings and outlines directions for future research.

II. Literature Review

Digital image forgery has become a critical concern due to the rapid advancement of image processing tools and the widespread use of social media platforms. Techniques such as copy-move forgery (CMF) are commonly used to manipulate image content by copying and pasting regions within the same image to conceal or duplicate objects (Wu et al., 2018; Mohammed et al., 2018). These manipulations can lead to serious societal and political consequences, including misinformation and tampered evidence, thereby highlighting the need for reliable detection mechanisms.

Detecting and localizing CMF is a challenging task due to variations in texture, rotation, scaling, and illumination (Cozzolino et al., 2015). Traditional approaches for CMF detection are broadly categorized into block-based and key point-based methods. Block-based methods analyse local image regions, while key point-based techniques identify distinctive features using algorithms such as SIFT, SURF, ORB, and triangle-based matching (Ardizzone et al., 2015; Silva et al., 2015; Manu & Mestre, 2016; Yang et al., 2017). However, these conventional methods often struggle to detect complex and subtle manipulations, especially under geometric and intensity transformations (Lin & Wu, 2011).

Recent advancements in deep learning have significantly improved forgery detection performance. Convolutional Neural Networks (CNNs) enable automatic feature extraction and have demonstrated promising results, although they may lack robustness against highly sophisticated manipulations (Gajjar et al., 2022). Emerging techniques such as Generative Adversarial Networks (GANs) and Vision Transformers (Vitis) further enhance detection capabilities. GANs are used to generate realistic forged samples for training, improving model generalization (Goodfellow et al., 2014), while Vitis leverage self-attention mechanisms to capture global contextual information (Dudovskiy et al., 2020; Mogan et al., 2023). Despite these improvements, challenges remain in achieving robustness and efficiency across diverse and complex scenarios.

III. Steganographic Models

S. Venkatesh et al. (2023) proposed a multi-layer steganographic framework for secure military communication using Least Significant Bit (LSB) substitution and Discrete Wavelet Transform (DWT). The model incorporates encryption prior to embedding, enhancing security through a dual-layer approach. While it achieves good visual quality and robustness, the use of a single carrier image introduces a single point of failure.

M. K. Sharma et al. (2022) introduced a multi-image steganographic technique that distributes secret data across multiple carrier images using matrix encoding. This approach improves embedding capacity and reduces distortion while providing basic distributed security. However, the static selection of carrier images limits randomness and makes the system predictable.

A. K. Mishra et al. (2024) developed a hybrid framework combining Advanced Encryption Standard (AES) with image steganography. The model ensures strong data confidentiality through encryption but relies on a single carrier image and key, making it vulnerable if either is compromised.

A. Summary

Although significant progress has been made in forgery detection and stenographic security, existing methods face limitations in handling complex transformations, ensuring robustness, and avoiding single points of failure. Additionally, high computational complexity restricts their real-world applicability. These challenges highlight the need for a more efficient and generalized **Multi-Security Image Cyber Model**, which distributes sensitive information across multiple carriers while improving detection robustness and security against advanced attacks.

B. Proposed Methodology

To address the limitations discussed earlier, this paper proposes a **Multi-Security Image Cyber Model**, a robust framework designed using *TrustNet*, a deep learning-based intelligent system for digital image authenticity and forgery prevention. The proposed model is particularly suitable for highly confidential data transmission environments such as military communication networks.

The system follows a modular architecture comprising the following components:

- **Frontend:** Python-based interface for system interaction and control
- **Backend:** Dataset management and query processing module
- **Authentication:** Image-based authentication mechanism
- **AI Integration:** Deep learning model (TrustNet) implemented using PyCharm
- **Background Services:** Image security processing, including embedding and reconstruction Unlike conventional approaches, the proposed framework introduces a novel multi-layered security mechanism by distributing sensitive information across multiple carrier images. The system employs a **tri- component reconstruction process**, where successful data recovery requires the correct combination of multiple images along with a valid authentication parameter.

This design significantly enhances security by eliminating the single point of failure present in traditional cryptographic and steganographic systems. Even if an adversary intercepts one or more carrier images or partially compromises the authentication mechanism, the original confidential data remains inaccessible. The reconstruction process depends on precise alignment and correct sequencing of all components, thereby creating a highly secure and resilient architecture. Overall, the proposed model establishes a multi-level defense strategy that substantially increases the computational complexity for unauthorized access while maintaining efficient performance for secure communication.

IV. Multi-Security Image Cyber Model Methodology

To overcome the limitations of conventional encryption and single-image steganography methods, this work proposes a **Multi-Security Image Cyber Model** for the secure transmission of confidential data. The proposed system introduces a multi-layer protection mechanism in which sensitive information is distributed across multiple images rather than relying on a single carrier. This significantly reduces the risk of unauthorized reconstruction, even if part of the transmitted data is intercepted.

In the proposed framework, the system initially collects five different images that serve as potential carriers for secure data embedding. From this pool, three images are dynamically selected using a controlled selection mechanism. This selection process enhances randomness and unpredictability, making it difficult for attackers to identify the actual carrier images.

Once selected, the confidential data is embedded into these images using a matrix-based embedding structure. The three images are logically arranged in a matrix format, enabling the distribution of encoded data across multiple image layers. This ensures that no single image contains sufficient information to reconstruct the original data independently.

To further strengthen security, the system generates a single reconstruction password at a predefined reference point. This password serves as a unified authentication key required to combine the selected images and retrieve the hidden information. Data reconstruction is only possible when the correct set of images and the corresponding password are provided at the authorized reconstruction point.

A key advantage of the proposed model is its strong resistance to attacks. Even if an adversary intercepts the transmitted images or partially obtains the authentication key, reconstructing the original data remains extremely challenging. Without the exact combination of selected images and the correct reconstruction parameters, the hidden information cannot be accurately recovered.

Overall, this multi-layered framework provides enhanced protection against brute-force attacks, interception, and unauthorized decoding, making it highly suitable for secure communication in sensitive environments.

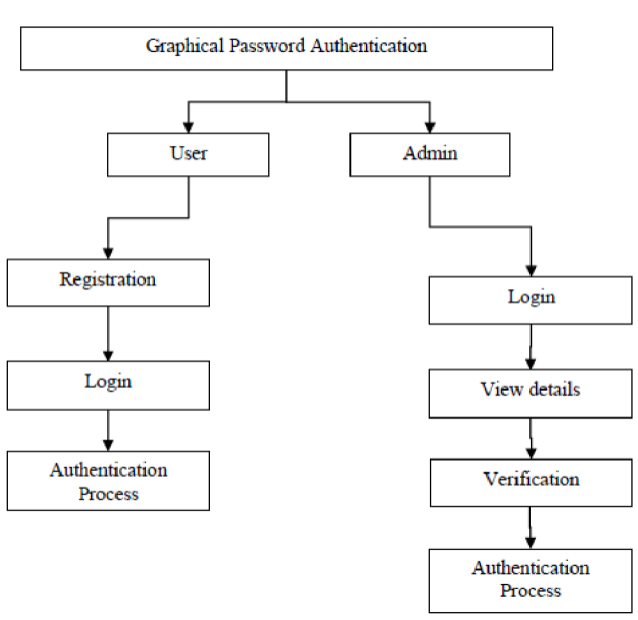

Figure.1: System Architecture

The figure.1 illustrates a **Graphical Password Authentication System** designed to provide secure access through image-based credentials. The system is structured around two primary roles: user and administrator. In the user workflow, a new user begins with registration, during which a graphical password (such as images, patterns, or click points) is created and stored. After registration, the user proceeds to the login stage, where the selected graphical password is entered. The system then performs an authentication process to verify the input against the stored credentials and grants access only if a match is found.

In the administrator workflow, the admin logs into the system using authorized credentials and is provided with additional privileges. After login, the admin can view system or user details and perform a verification step to monitor authenticity or detect suspicious activities. This is followed by an authentication process to ensure secure administrative access. Overall, the system employs a multilevel authentication mechanism with role-based access control, enhancing security by combining graphical password techniques with verification processes. This approach strengthens protection against unauthorized access and can be effectively integrated into secure frameworks such as the proposed Multi-Security Image Cyber Model.

V. Result and Discussion

System testing was conducted to evaluate the overall performance, reliability, and robustness of the proposed system. The objective was to ensure that all components including the frontend, backend, authentication module, and AI integration function cohesively and meet the specified requirements. The testing process validated that the system operates correctly under various conditions and is free from major defects.

Figure.2: Registration link

The figures 2 show the **user registration and login interfaces** of the authentication system. The registration page allows new users to create an account by entering basic details such as username, email, and password, ensuring secure access setup. In Figure.3, the login page enables registered users to access the system by providing their credentials. Both interfaces are designed with a simple and user-friendly layout, supporting secure authentication and smooth user interaction within the system.

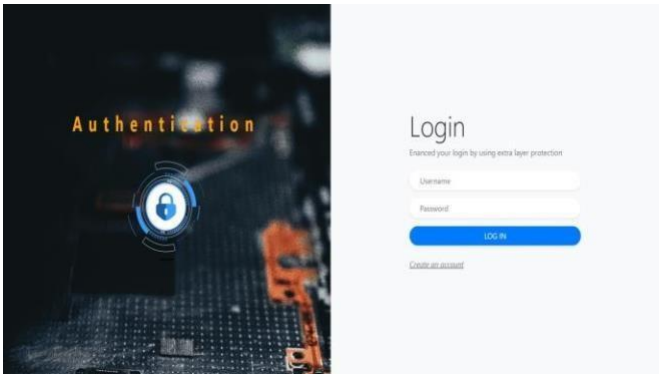

Figure.3: login page for authentication

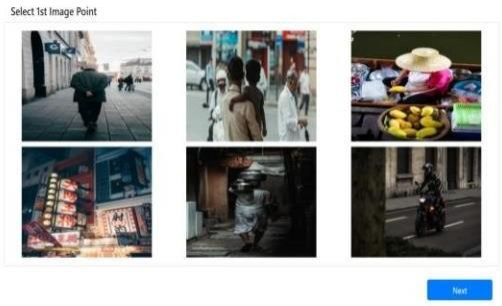

Figure.4: Image capture for a authentication

The figure 4 illustrates the **graphical password selection interface**, where users choose specific image points as part of their authentication process. Multiple images are displayed, and the user selects one or more images or points, which act as a secure graphical password. This approach enhances security by making passwords harder to guess compared to traditional text-based methods.

VI. Conclusion

This work presents a **Multi-Security Image Cyber Model** for enhancing the protection of confidential data during digital communication. By distributing sensitive information across multiple carrier images and integrating a unified authentication mechanism, the proposed framework effectively overcomes the limitations of conventional single image and single-key security approaches. The use of dynamic image selection, matrix-based embedding, and a reconstruction password ensures that data recovery is only possible under strictly valid conditions.

The experimental and system-level evaluation demonstrates that the proposed model provides strong resistance against interception, unauthorized access, and brute-force attacks. The multi-layered architecture significantly increases the complexity for attackers while maintaining efficient performance suitable for secure communication environments.

Overall, the proposed framework offers a reliable and scalable solution for safeguarding sensitive information, particularly in high-security domains such as military and defence communication systems. Future work may focus on integrating advanced deep learning techniques, adaptive carrier selection strategies, and stronger cryptographic methods to further enhance robustness and applicability in evolving cyber threat landscapes.

References

[1] Liu, Y., Guan, Q., Zhao, X., & Cao, Y. (2018). Image forgery localization based on multiscale convolutional neural networks. In Proceedings of the 6th ACM Workshop on Information Hiding and Multimedia Security (pp. 85–90).

[2] Wu, Y., Abd-Almageed, W., & Natarajan, P. (2018). Buster net: Detecting copy-move image forgery with source/target localization. In Proceedings of the European Conference on Computer Vision (ECCV) (pp. 168–184).

[3] A. Piva, An overview on image forensics, Int. Scholarly Research Notices, 2013. do: https://doi.org/10.1155/2013/496701

[4] H. Wu, J. Zhou, J. Tian, J. Liu, Robust image forgery detection over online social network shared image, in: Proceedings of the IEEE Conference on Comp. Vision and Pattern Recognize., New Orleans, Louisiana, USA, ISBN: 978-1-6654-6946-3, 2022, pp. 13440-13449.

[5] I. Hussain, S. Tan, B. Li, X. Qin, D. Hussain, J. Huang, A novel deep learning framework for double JPEG compression detection of small size blocks, Journal of Visual Commun. and Image Represent. 80(2021) 103269. do: https://doi.org/10.1016/j.jvcir.2021.103269

[6] W. Dong, H. Zeng, Y. Peng, X. Gao, A. Peng, A deep learning approach with data augmentation for median filtering forensics, Multi. Tools and Apply. 81(2022) 11087-105. do:

https://doi.org/10.1007/s11042-022-12040-w

[7] F. Marra, D. Gragnani Ello, D. Cozzolino, L. Verdolaga, Detection of gang-generated fake images over social networks, in: Proceedings of the IEEE Conference on Mult. Inf. Process. and Retrieval, Miami, FL, USA, ISBN: 978-1-5386-1857-8, 2018, pp. 384-389

[8] Cybersecurity Ventures. (2025). Cybercrime to cost the world $10.5 trillion annually by. Cybersecurity Ventures Report.

[9] IBM Security. (2020). Cost of a data breach report. IBM Report.

[10]Mohammed, T. M., Bunk, J., Nataraj, L., Bappy, J. H., Flenner, A., Manjunath, B. S., Chandrasekaran, S., Roy-Chowdhury, A. K., & Peterson, L. (2018). (Preprint 1802.03154v2) URL. http://arxiv.org/abs/1802.03154v2.

[11] Cozzolino, D., Poggi, G., & Verdolaga, L. (2015). Efficient dense field copy–move forgery detection. IEEE Transactions on Information Forensics and Security, 10(11), 2284–229
[12] Ardizzone, E., Bruno, A., & Mazzola, G. (2015). Copy–move forgery detection by matching triangles of key points. IEEE Transactions on Information Forensics and Security., 10, 2084– 2094.
[13] Manu, V., & Mestre, B. M. (2016). Detection of copy-move forgery in images using segmentation and surf. Advances in signal processing and intelligent recognition systems (pp. 645–654).
[14] Silva, E. A., Carvalho, T., Ferreira, A., & Rocha, A. (2015). Going deeper into copy-move forgery detection: Exploring image telltales via multi-scale analysis and voting processes. Journal of Visual Communication and Image Representation, 29, 16–32.
[15] Yang, B., Sun, X., Guo, H., Xia, Z., & Chen, X. (2017). A copy- move forgery detection method based on CMFD-SIFT. Multimedia Tools and Applications, 77, 837–855.
[16] Lin, S. D., & Wu, T. (2011). An integrated technique for splicing and copy-move forgery image detection 2011. In 4th International Congress on Image and Signal Processing (IEEE). https://doi.org/10.1109/cisp.2011.6100366.
[17] Gajjar, P., Saxena, A., Shah, H., Kiani, N., Lakhani, K., Shah, P., Sharma, A., & Limbachia, K. (2022). Copy move forgery detection: The current implications and contemporary practices. *Journal of Physics: Conference Series, 2325*(1), Article 012050. https://doi.org/10.1088/1742-6596/2325/1/012050
[18] Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial nets. Advances in Neural Information Processing Systems, 27
[19] Dudovskiy A., Beyer L., Kolesnikov A., Weissenborn D., Zhai X., Entertainer T., Dehghani M., Hinderer M., Hei gold G., Gelly S. et al. (2020) An image is worth 16x16 words: Transformers for image recognition at scale. arid preprint arXiv:2 010.11
[20] Mogan, J. N., Lee, C. P., Lim, K. M., Ali, M., & Alqahtani, A. (2023). Gaitan-vit: Multimodal gait recognition with convolutional neural networks and vision transformer. Sensors, 23(8), 3809.