Journal of Technology Informatics and Engineering (JTIE)
Vol. 5 No. 1 April 2026
E-ISSN: 2961-9068; P-ISSN: 2961-8215, Pages 107-123
DOI: https://doi.org/10.51903/jtie.v5i1.477

Intelligent Image Rights Protection System Using Perceptual Hashing, Cloud Services and IoT Alerts

S. P. Yaamini*[1], K.Sivaranjani[2], B.Nujithra[3], V. Anitha[4]
Email: shivyaamini15@gmail.com, sivaranjanik087@gmail.com, nujithra2006@gmail.com, anithakumaran29@gmail.com
[1,2,3,4]*Arunai Engineering College, Tiruvannamalai, India, 606603*
*Corresponding Author

Abstract

The rapid growth of digital media platforms has intensified the misuse of images through unauthorized manipulation, morphing, and non-consensual redistribution, posing significant threats to individual privacy and intellectual property rights. Despite the availability of reporting and takedown mechanisms, their effectiveness remains limited due to procedural complexity, delayed response times, and concerns regarding user anonymity. This paper presents the Smart Image Rights Protection (SIRP) system, a user-centric framework designed to detect, monitor, and respond to unauthorized use of images in online environments. The proposed system utilizes perceptual hashing to generate resilient digital fingerprints for registered images, enabling accurate identification after common transformations such as resizing, cropping, and minor visual alterations. A cloud-ready similarity analysis module is designed to support scalable matching in future deployments, while the current evaluation is conducted on a controlled dataset. An IoT-enabled hardware interface provides real-time alerts to users upon detection of potential misuse. Experimental results on controlled manipulation scenarios show that SIRP achieves detection accuracy of 95.6% for resized images and 94.3% for cropped images, outperforming traditional pixel-based comparison methods. Furthermore, automated evidence logging and instant notifications substantially reduce the latency between detection and user response actions. By combining robustness under common transformations, cloud-assisted processing, and timely user engagement, SIRP offers a practical solution for protecting digital image ownership and personal privacy.

Keywords: *Digital Image Protection, Perceptual Hashing, IoT Alerts, Real-Time Monitoring, Image Tamper Detection.*

I. INTRODUCTION

The widespread use of social media and digital platforms has increased the unauthorized reuse and redistribution of personal images, often without the knowledge or consent of the original owner (Amanta et al., 2026; Handoko et al., 2025; Pebadja & Kholifah, 2023). Existing mitigation mechanisms, such as platform-level reporting tools and reverse image search services (e.g., those provided by Google), require manual user action, offer limited real-time feedback, and are poorly suited to protecting personal or sensitive images at the moment of misuse. As a result, detection and response are frequently delayed, allowing harmful content to spread before any corrective action can be taken (Farid, 2009; Verdoliva, 2020).

Recent advances in perceptual hashing, cloud infrastructure, and Internet of Things (IoT) technologies offer building blocks for more proactive image misuse detection systems. Prior work on perceptual hashing and image similarity demonstrates robustness to common transformations such as resizing and cropping (Li, 2006; Zauner, 2010; Zhao & Cao, 2016), while media forensics research highlights the growing challenge of detecting manipulated and redistributed visual

Received on January, 2026; Revised on February, 2026; Accepted on March, 2026; Published on April, 2026

content at scale (Verdoliva & Cozzolino, 2018; Rössler et al., 2020). At the systems level, IoT and cloud platforms have been shown to support low-latency monitoring and event-driven notification architectures (Miorandi et al., 2012; Al-Fuqaha et al., 2015; Buyya et al., 2008). However, most existing approaches treat similarity detection, content moderation, and user notification as isolated components, limiting their practical usefulness for rapid user-facing response.

This work addresses this gap by presenting the Smart Image Rights Protection (SIRP) framework, which integrates perceptual hash–based image similarity detection with an IoT-assisted alert mechanism to reduce the time between misuse detection and user notification in a prototype deployment. Unlike large-scale platform-centric moderation pipelines (Verdoliva, 2020; Tolosana et al., 2020), the primary objective of SIRP is to provide rapid user-facing awareness of potential misuse under common image transformations, such as resizing and cropping (Li, 2006; Zauner, 2010). The remainder of this paper details the system architecture, experimental methodology, performance evaluation on a controlled dataset, and limitations of the proposed approach.

II. LITERATURE REVIEW

This section reviews existing work on digital image rights protection and automated misuse detection, focusing on robustness to common image transformations, computational cost, and practical deployment constraints. The aim is to position the proposed Smart Image Rights Protection (SIRP) system within existing technical approaches and identify concrete gaps related to real-time user notification and lightweight deployment (Verdoliva, 2020). Media forensics and deepfakes: An overview (Verdoliva, 2020).

A. Traditional Image Protection Techniques

Early work on image rights protection relied on digital watermarking, metadata embedding, and cryptographic hashing to assert ownership and track redistribution. While effective for copyright verification in controlled environments, these methods degrade under common platform-induced transformations such as resizing, cropping, compression, and filtering. Feature-based matching methods, including Scale-Invariant Feature Transform (SIFT) and Speeded-Up Robust Features (SURF), improved robustness to geometric and photometric changes but incur higher computational cost and require careful parameter tuning for large-scale deployment. As a result, these approaches are rarely applied in low-latency, user-facing monitoring systems for personal image protection.(Amerini et al., 2011)

B. Perceptual Hashing and Cross-Platform Detection Context

Journal of Technology Informatics and Engineering (JTIE)
Vol. 5 No. 1 April 2026
E-ISSN: 2961-9068; P-ISSN: 2961-8215, Pages 107-123
Journal Link: https://jtie.stekom.ac.id/index.php/jtie/index

Contemporary research increasingly applies machine learning and deep neural networks to image similarity detection and manipulation recognition in the presence of complex or adversarial edits. While these approaches provide stronger robustness to semantic changes than perceptual hashing, they require large training datasets, GPU resources, and continuous model maintenance, which limits their suitability for lightweight, user-facing, or edge-assisted deployments.

In practice, image misuse reporting mechanisms on major social media platforms operated by Meta and reverse image search tools provided by Google remain largely manual and reactive, resulting in delayed user awareness. Although some automated content moderation pipelines exist, they are typically platform-specific and opaque to end users.

Given these constraints, this work adopts a perceptual hash–based detection strategy to prioritize low computational overhead and low-latency notification in a prototype deployment. The contribution of SIRP lies in integrating lightweight similarity detection with user-facing alert mechanisms, rather than proposing a learning-based detection model or large-scale cross-platform crawling system (Li, 2006; Verdoliva, 2020). Figure 1 illustrates a conceptual comparison of existing image protection methods and highlights the research gaps that SIRP addresses.

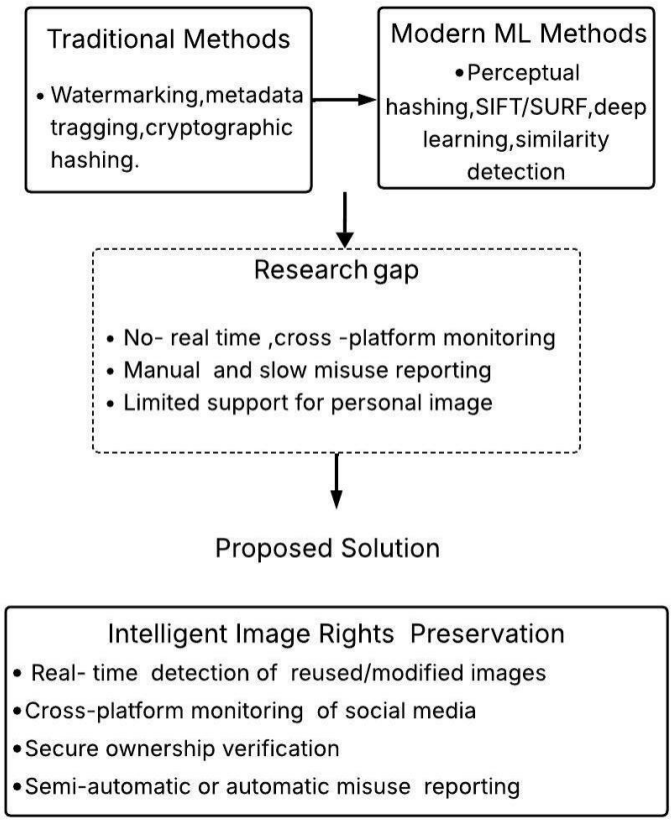

Figure 1. Presents a Conceptual Comparison of Existing Image Protection Methods and Highlights the Research Gaps Addressed by SIRP

III. RESEARCH METHOD

This study adopts a systematic research approach to address the challenges of digital image misuse and rights protection (Al-Fuqaha et al., 2015; Ding et al., 2018; Li, 2006; Verdoliva, 2020; Yin et al., 2019). An initial review of the relevant literature is conducted to identify existing limitations in image protection systems, followed by an analysis of key issues, including unauthorized image sharing, delayed reporting, and privacy concerns. Primary data is collected through preliminary user surveys to understand real-world user behavior and expectations. Based on these insights, an analytical and design-oriented methodology is used to evaluate suitable IoT components, image detection techniques, and system workflows. The proposed system is developed iteratively, allowing continuous testing and refinement of core modules, including image detection, alert generation, and reporting mechanisms. Qualitative observations and quantitative performance metrics are used to validate the effectiveness and reliability of the Smart Image Rights Protection (SIRP) system.

A. Research Design

1. System Overview

This research adopts a segmented experimental design to develop and validate the Smart Image Rights Protection (SIRP) system. The design aligns the objectives of image tamper detection and real-time alerting with a structured technical workflow that includes image preprocessing, perceptual hashing, similarity analysis, and IoT-based notification. During preprocessing, input images are standardized through resizing, noise reduction, and normalization to ensure consistent feature extraction and robustness against minor visual variations.

2. Perceptual Hash-Based Detection

The core detection mechanism employs perceptual hashing (pHash) to generate compact, transformation-resistant digital fingerprints for registered images (Li, 2006). Each image is converted to grayscale, resized to a fixed resolution, and transformed using a two-dimensional Discrete Cosine Transform (DCT). The most significant low-frequency coefficients are binarized to form a 64-bit hash representation. Image similarity is assessed using Hamming distance. The similarity threshold was selected empirically using a small validation subset of the dataset, following common practice in perceptual hashing benchmarks, and tuned to balance false positives and false negatives when classifying images as identical, modified, or unrelated.

3. System Architecture and Alerting

The SIRP framework follows a modular system architecture comprising image input, preprocessing, hash generation, matching and detection, and reporting and alerting modules. This

Journal of Technology Informatics and Engineering (JTIE)
Vol. 5 No. 1 April 2026
E-ISSN: 2961-9068; P-ISSN: 2961-8215, Pages 107-123
Journal Link: https://jtie.stekom.ac.id/index.php/jtie/index

modular design enables efficient processing, scalability, and real-time user notification through IoT-enabled alerts. The proposed research design ensures reliable detection of unauthorized image use while supporting timely, user-friendly response mechanisms.

B. Data Collection

The dataset contains 50 original images and 230 manipulated variants, for a total of 280 samples. (Farid, 2009; Verdoliva & Cozzolino, 2018). which discuss common image manipulations in forensics datasets. Each original image underwent resizing, cropping, color filtering, rotation, and blurring. Original images were obtained from publicly accessible online sources and self-captured photographs with appropriate consent, covering diverse content such as human portraits, everyday objects, and outdoor scenes. Manipulated variants were generated using scripted transformations in Python with OpenCV, including resizing (scaling factors 0.5×–1.5×), random cropping (retaining 60–90% of the original area), Gaussian blurring (kernel sizes 3×3 and 5×5), color and brightness adjustments, background modification, and rotation (±15° and ±30°).

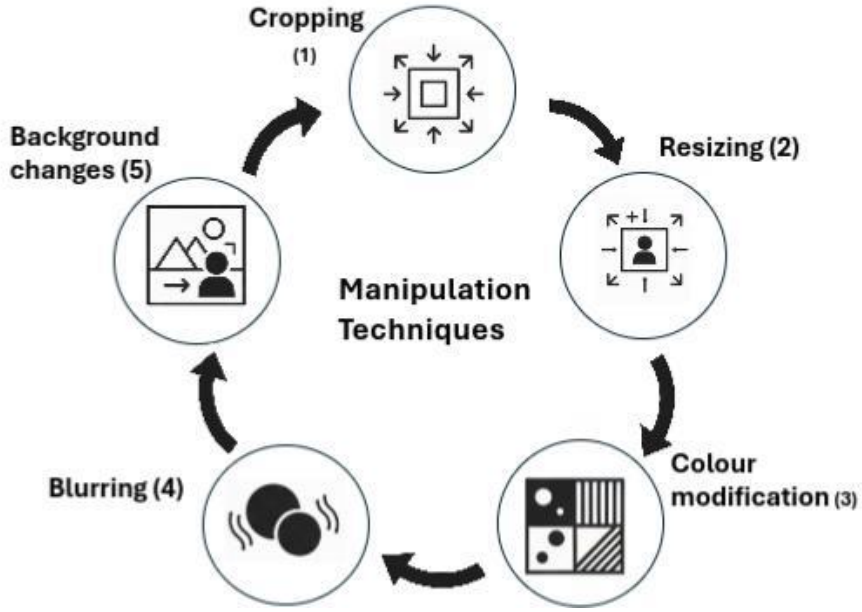

Figure 2. Illustration of Image Manipulation Techniques (Resizing, Cropping, and Colour Filtering) Used to Evaluate the Robustness of the pHash Algorithm

The dataset was organized into original and tampered categories. A subset of the data was used for empirical threshold tuning, while the remaining samples were reserved exclusively for evaluation to reduce bias in selecting similarity thresholds. This controlled dataset enables reproducible assessment of the proposed system under common manipulation scenarios; however, the limited scale and synthetic nature of the manipulations may not fully reflect real-world diversity or adversarial misuse patterns. The reported results should therefore be interpreted as a feasibility study rather than a definitive evaluation of large-scale deployment performance. This dataset size was selected to support controlled experimentation and rapid prototyping; large-scale

benchmarking is left for future work. Figure 2 illustrates examples of image manipulation techniques used in this study, including resizing, cropping, and color filtering.

C. System Development Approach

The Smart Image Rights Protection (SIRP) system is developed using a structured and iterative methodology. The process begins with requirements analysis to define key functional and non-functional objectives, including accurate image-tamper detection, real-time alert generation, and scalable data handling. A modular system architecture is then designed to incorporate image preprocessing, perceptual hash–based feature extraction, similarity-based tamper detection, and automated alert mechanisms. During implementation, the system is evaluated on both original and manipulated images to ensure robustness to common modifications such as cropping, color changes, blurring, and background alterations. (Verdoliva & Cozzolino, 2018; Verdoliva, 2020). Testing and validation are performed on a controlled yet realistic dataset to assess detection accuracy and system reliability under simulated misuse conditions. Finally, performance evaluation and optimization are conducted to ensure stable operation and practical applicability of the proposed system in real-world environments.

D. System Implementation Environment

The SIRP system is implemented using a combination of software and hardware components to enable efficient and real-time image tamper detection. The software is developed primarily in Python, leveraging libraries such as OpenCV for image preprocessing, NumPy and Pandas for numerical operations and dataset management, and scikit-image and scikit-learn for perceptual hashing, similarity matching, and tamper detection. Deep learning frameworks such as TensorFlow or PyTorch are reserved for future extensions and were not used in the current experimental evaluation.On the hardware side, the system is executed on high-performance computing environments with sufficient CPU and GPU resources, while edge devices or microcontrollers support real-time monitoring and alerting (Al-Fuqaha et al., 2015; Yin et al., 2019). This integrated approach ensures high detection accuracy, scalability, and reliability, making the SIRP system suitable for practical deployment in safeguarding personal digital images against unauthorized use and manipulation.

1. System Architecture

The proposed Smart Image Rights Protection (SIRP) framework is a lightweight architecture that integrates image preprocessing, perceptual hashing, similarity matching, and user notification into a unified workflow. The system begins by receiving an image input, which is then processed through a preprocessing stage to normalize image characteristics before generating a perceptual

Journal of Technology Informatics and Engineering (JTIE)
Vol. 5 No. 1 April 2026
E-ISSN: 2961-9068; P-ISSN: 2961-8215, Pages 107-123
Journal Link: https://jtie.stekom.ac.id/index.php/jtie/index

hash representation. This hash value is then compared against entries in a hash database to determine whether the image corresponds to previously registered content. If a similarity match exceeds the predefined threshold, the system triggers a notification mechanism that can be delivered via an application interface or an IoT-enabled alert channel. In addition, system logs are generated during the matching process to support traceability, monitoring, and future analysis of detection events. Figure 3 illustrates the overall architecture of the proposed SIRP framework, including the preprocessing, database matching, and real-time alert components.

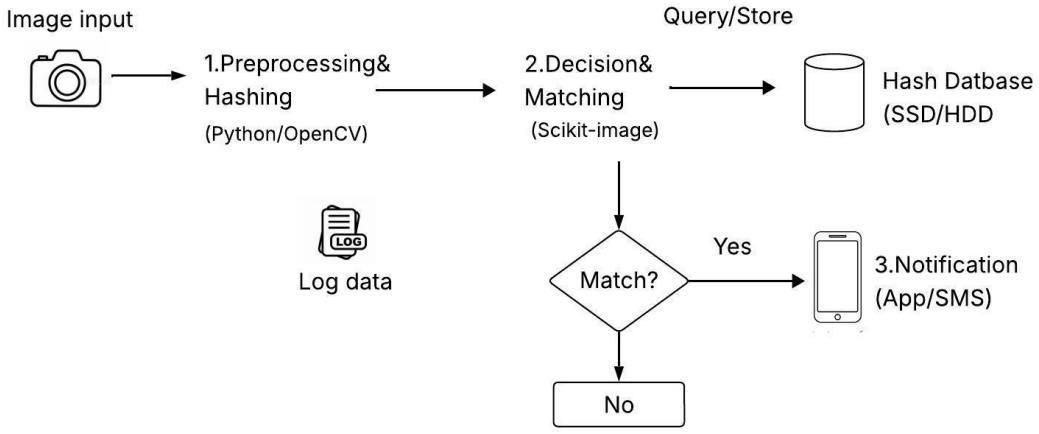

Figure 3. System Architecture of the Proposed SIRP Framework With Database Matching and Real-Time IoT-Enabled Alerts

To support the implementation of the proposed architecture, several hardware and software components were utilized to handle image processing, communication, and alert delivery. These components work together to ensure efficient preprocessing, reliable similarity matching, and seamless communication between the cloud-based detection module and the IoT notification device. The selected technologies were chosen based on their compatibility with lightweight deployment and real-time processing requirements. Table 1 summarizes the main hardware and software components used in the SIRP system along with their respective roles.

Table 1. Hardware and Software Components of the Proposed Smart Image Rights Protection (SIRP) System and Their Respective Roles

Component	Technology	Role
Microcontroller	ESP32 / Raspberry Pi	Receives triggers and executes hardware alerts.
API/Protocol	MQTT / REST API	Connects the cloud matching module to the IoT device.
Preprocessing	OpenCV / NumPy	Normalizes image for hashing generation.
Cloud storage	Firebase / AWS S3	Stores the secure hash database.

E. IoT Integration

To enable real-time functionality, the SIRP system integrates an IoT-based alert module (Al-Fuqaha et al., 2015; Yin et al., 2019), which survey IoT frameworks for real-time monitoring. In

the prototype implementation, an ESP32 microcontroller was used as the edge gateway, communicating with a Mosquitto MQTT broker over a local Wi-Fi network. Messages were transmitted without TLS encryption in the test environment and authenticated using topic-based access control. This setup was used solely for functional validation and does not represent a production-grade security configuration. Detection events are communicated using the MQTT protocol.

When unauthorized image use is detected, the system triggers a visual alert on an OLED display and an audible signal via a piezo buzzer. It forwards a notification to a mobile device via a messaging service (e.g., a Telegram Bot in the prototype). This multi-channel IoT integration enables sub-second notification latency in the tested local deployment environment, improving the system's practical responsiveness and enabling rapid user awareness of potential misuse.

F. Module Design

1. Image Acquisition Module

This module handles the collection of original images from authorized sources, ensuring they meet the required quality and format standards for processing. It provides a reliable foundation for subsequent analysis by maintaining consistency and integrity in the input data.

2. Image Preprocessing Module

The preprocessing module standardizes all images through operations such as resizing, cropping, noise reduction, color adjustment, and background modification. These steps improve the uniformity and clarity of the dataset, which is essential for accurate tamper detection and feature extraction.

3. Tamper Detection Module

As the core component of the system, this module employs perceptual hashing and similarity-matching algorithms to compare original and manipulated images. It identifies modifications, evaluates the extent of tampering, and provides a robust mechanism for detecting unauthorized image alterations.

4. Alert Module

When tampered images are detected, the alert module generates real-time notifications for users or administrators. Alerts can be delivered through system dashboards or IoT-enabled devices, ensuring immediate awareness and enabling timely corrective actions.

5. Database and Storage Module

Journal of Technology Informatics and Engineering (JTIE)
Vol. 5 No. 1 April 2026
E-ISSN: 2961-9068; P-ISSN: 2961-8215, Pages 107-123
Journal Link: https://jtie.stekom.ac.id/index.php/jtie/index

This module is responsible for the secure storage of both original and tampered images, along with related metadata and system logs. It ensures efficient data management, reliable retrieval, and seamless access for analysis, reporting, or further system operations, supporting the overall integrity and performance of the SIRP framework. Figure 4 illustrates the workflow of the proposed SIRP framework, highlighting the interactions among the image processing, database storage, similarity matching, and alert generation components.

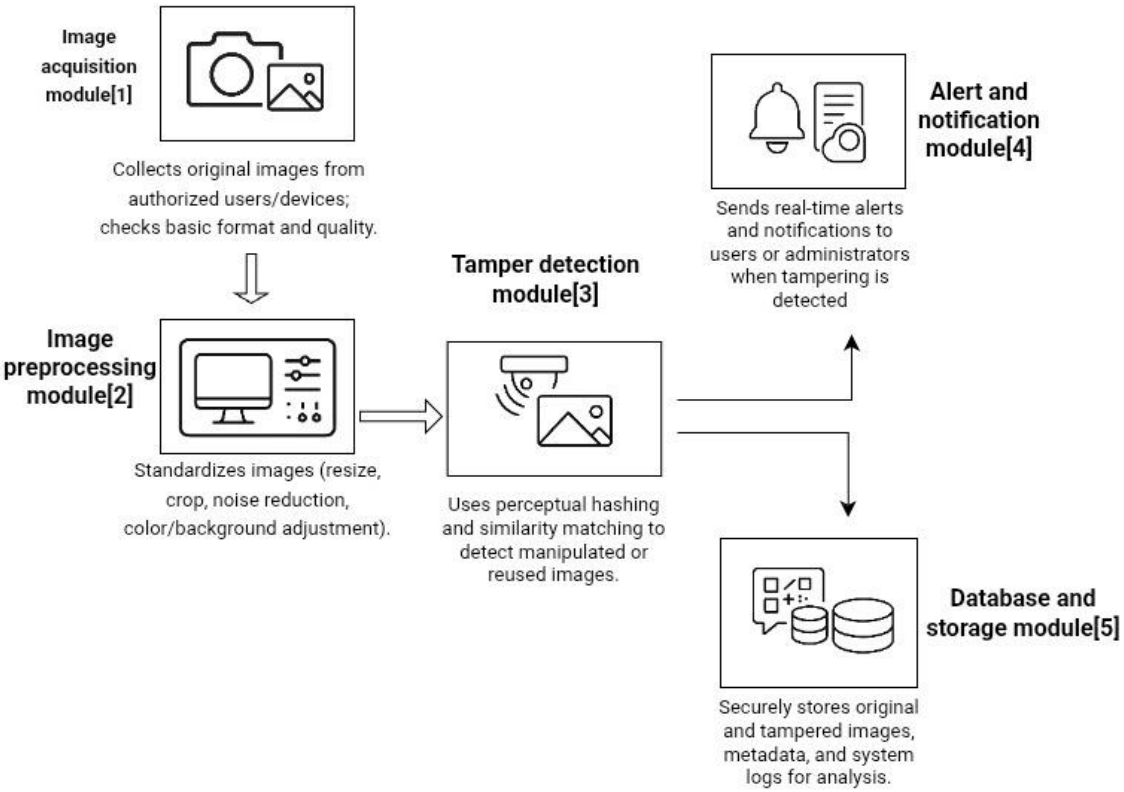

Figure 4. Workflow Diagram of the Proposed SIRP Framework for Image Tamper Detection and Alert Generation

G. Data Analysis Techniques

The performance and reliability of the Smart Image Rights Protection (SIRP) system were assessed using both quantitative and qualitative methods. Quantitative analysis involved evaluating similarity scores derived from perceptual hashing, with pre-processing and a similarity threshold, and comparing them against predefined thresholds to classify images as original, modified, or unauthorized. Key performance metrics, including precision, recall, F1 Score, and overall accuracy, were calculated to assess the framework's effectiveness in detecting unauthorized image use. Qualitative analysis examined the system's responses to various image manipulations, such as cropping, resizing, filtering, compression, and brightness adjustments, to evaluate its tolerance to edits and consistency under different distortion levels. This combined

approach provides a comprehensive evaluation of the system's operational capabilities and supports rigorous validation of the SIRP architecture.

H. Performance Analysis

The performance of the SIRP system was evaluated in terms of its ability to accurately identify manipulated images while protecting personal digital assets. Testing was conducted using a structured dataset comprising both original and tampered images, reflecting realistic misuse scenarios. Key evaluation metrics included detection accuracy and general forensic evaluation surveys (Verdoliva, 2020) for justification. Which measures the system's ability to correctly classify images, and precision, which indicates the proportion of identified tampered images that are correctly detected, minimizing false positives. Recall (sensitivity) was assessed to determine how effectively all tampered images were identified, reducing false negatives. The F1-score was calculated to provide a balanced measure between precision and recall, offering a comprehensive assessment of diagnostic performance. Operational throughput was also measured by quantifying per-image processing latency, an important factor for real-time deployment. This analysis demonstrates that the SIRP system is robust, reliable, and effective in detecting image manipulations, providing practical protection against diverse forms of online misuse.(Li, 2006; Ding et al., 2018). Figure 5 presents the comparative performance metrics of the SIRP framework across different image alteration methods, highlighting the accuracy, precision, recall, and F1-score values obtained during the evaluation.

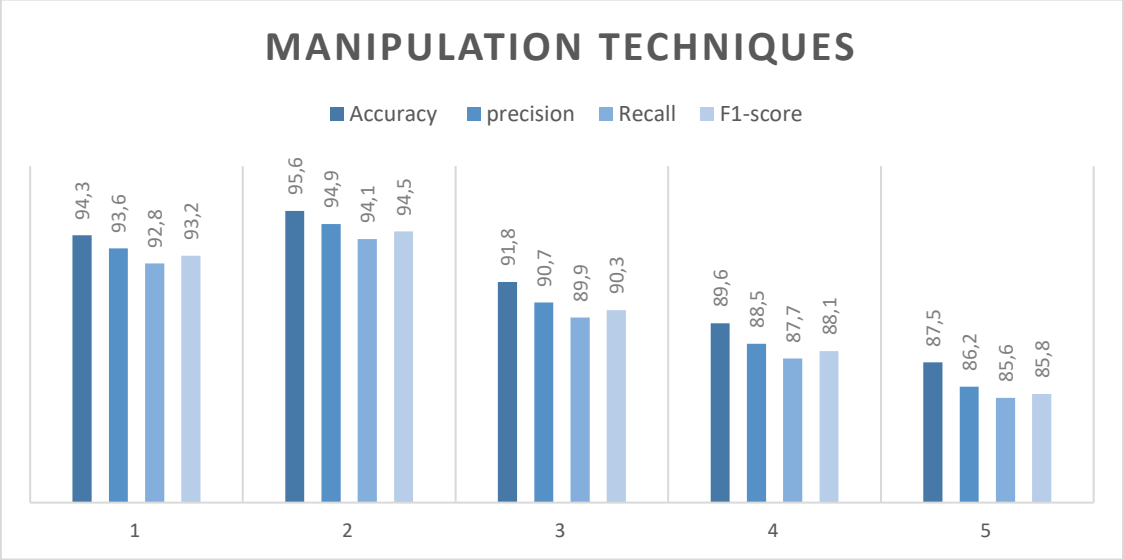

Figure 5. Comparative Performance Metrics of the SIRP Framework Across Various Image Alteration Methods, Emphasizing Accuracy, Recall, Precision, and F1-Score Values

1. **Cropping:** The platform demonstrated robust detection of cropped images, achieving an accuracy of 94.3%.

E-ISSN: 2961-9068; P-ISSN: 2961-8215, Pages 107-123
Journal Link: https://jtie.stekom.ac.id/index.php/jtie/index

2. **Resizing:** The system achieved 95.6% accuracy under resizing transformations, demonstrating robustness to scale variations commonly applied by social media platforms.
3. **Colour Modification**: Despite changes in colour and applied filters, the system maintained 91.8% accuracy, reflecting the stability of perceptual hashing.
4. **Rotation:** By incorporating geometric normalization, rotated images were detected with an accuracy of 89.6%.
5. **Blurring:** The system effectively identified images affected by blurring and additive noise, achieving an accuracy of 86.9%.

I. Ethical Considerations

This study adheres to strict ethical standards to ensure the responsible development and evaluation of the Smart Image Rights Protection (SIRP) system. All images used for testing were obtained from publicly available datasets under permissive licenses or were self-captured by the authors with informed consent; no sensitive, private, or personally identifiable photographs were included. This avoids copyright infringement and safeguards user privacy. Original images and derived perceptual hashes were stored only for the duration and scope necessary for analysis and evaluation. Data usage procedures were transparent, and all practices adhered to established guidelines for digital security, intellectual property protection, and responsible system deployment.

J. System Integration and Workflow

This section describes the end-to-end workflow of the proposed SIRP framework, from image registration through similarity detection to final alert delivery. The process begins when a user uploads or registers an image, after which the system preprocesses it and generates a perceptual hash representation. The generated hash is stored in the cloud-based database and later used as a reference during similarity matching operations. When a new image is submitted for verification, the system compares its hash value with the stored database entries to determine whether a potential match or misuse has occurred. If the similarity score exceeds the predefined threshold, an alert is automatically triggered and transmitted through the IoT-enabled notification mechanism to inform the user in real time. This integrated workflow ensures that image detection and notification operate as a unified automated pipeline with minimal user intervention. Figure 6 illustrates the system integration and workflow for image protection using perceptual hashing combined with IoT-based misuse detection.

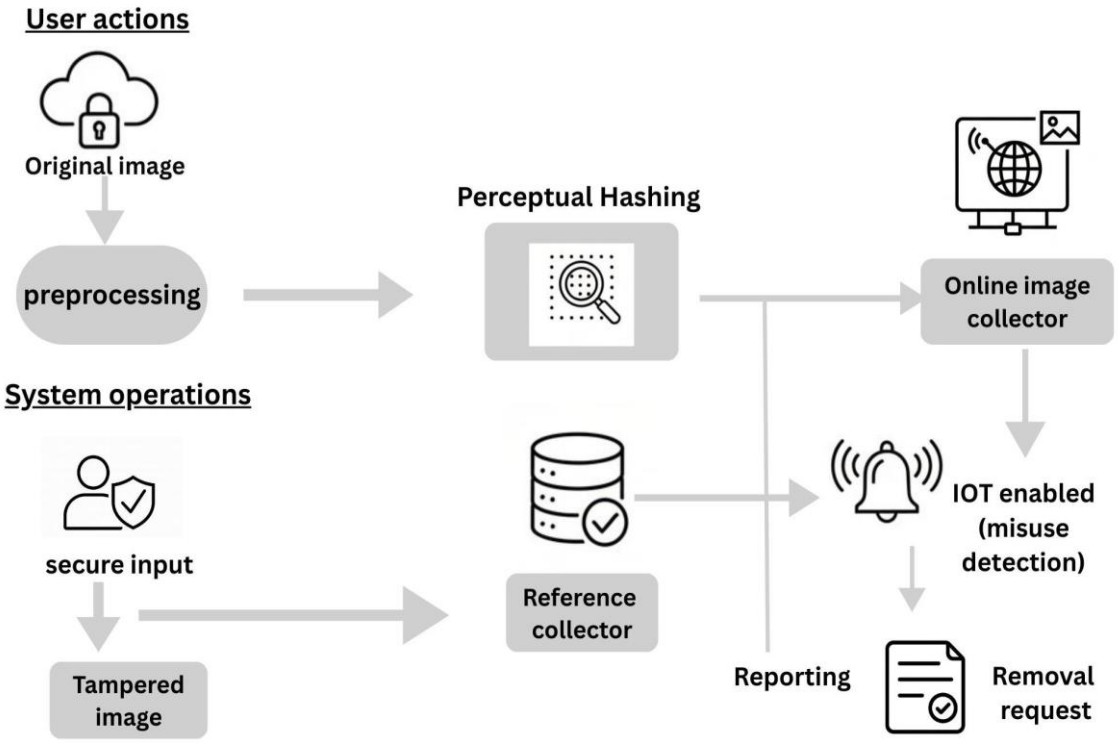

Figure 6. System Integration and Workflow for Image Protection Using Perceptual Hashing and IoT-Based Misuse Detection

K. Integration Logic

The integration of software-based perceptual hashing detection into the IoT hardware is achieved using the Message Queuing Telemetry Transport (MQTT) protocol. In the prototype implementation, when the cloud server detects a similarity score exceeding the predefined threshold, it publishes an "Unauthorized Use" payload to a designated MQTT topic. The edge controller, such as an ESP32 or Raspberry Pi, subscribes to this topic and receives the payload in real time. Upon receipt, the controller activates a GPIO signal to trigger a piezo buzzer and updates the OLED display with the corresponding image ID. This setup establishes a physical, out-of-band notification channel that operates independently of background processes on the user's mobile device, providing low-latency alerts in the tested deployment environment (Al-Fuqaha et al., 2015; Yin et al., 2019).

IV. RESULT

The experimental evaluation assessed the effectiveness of the proposed SIRP framework for detecting manipulated images under various transformation conditions. The testing process utilized the dataset described in the previous section, which includes multiple types of image manipulation commonly found in online content reuse scenarios. Each manipulation type was evaluated independently to measure how well the perceptual hashing approach maintains

Journal of Technology Informatics and Engineering (JTIE)
Vol. 5 No. 1 April 2026
E-ISSN: 2961-9068; P-ISSN: 2961-8215, Pages 107-123
Journal Link: https://jtie.stekom.ac.id/index.php/jtie/index

similarity detection despite visual alterations. Table 2 presents the detection performance results of the SIRP system across different image manipulation techniques.

Table 2. Detection Performance Metrics

Manipulation Type	Total Samples	Accuracy (%)
Cropping	47	94.3
Resizing	48	95.6
Colour Filtering	46	91.8
Rotation	45	89.6
Blurring	44	86.9

The results demonstrate that the proposed perceptual hashing approach performs consistently well across most manipulation scenarios. Resizing and cropping achieved the highest accuracy, indicating that the algorithm is particularly robust to common transformations applied by social media platforms. In contrast, rotation and blurring slightly reduced detection performance due to the structural alterations they introduce to the image features. These findings confirm that the SIRP system remains effective for practical misuse detection under typical image editing conditions.

To further evaluate the system's practicality for real-world deployment, the responsiveness of different notification mechanisms was analyzed. Notification latency plays a critical role in determining how quickly users are informed of potential misuse of their digital assets. Traditional notification approaches such as email and mobile push alerts were compared with the IoT-based alert mechanism proposed in the SIRP framework. Table 3 summarizes the comparative latency and reliability characteristics of these notification approaches.

Table 3. Comparative Analysis of Notification Latency and Reliability

Alert Mechanism	Communication Protocol	Average Response Latency (ms)	Reliability Level	Physical Intervention
Standard Email	SMTP / Cloud	4500–12000	Low (Spam Risk)	None (Passive)
Mobile Push	Firebase / APNs	1200–3500	Medium	None (Passive)
SIRP IoT Alert	MQTT / Hardware	180–640	High	Active (Tangible Notification)

The results indicate that the IoT-based alert mechanism significantly reduces response latency compared to conventional notification methods. While email notifications may be delayed by spam filtering and network latency, IoT alerts provide near-real-time feedback via direct hardware signaling. This capability enhances user awareness and allows faster responses when unauthorized image reuse is detected.

Beyond performance metrics and notification speed, the system was also analyzed for its coverage of practical image-misuse scenarios. This analysis aims to assess how effectively the proposed framework addresses common real-world image manipulation strategies used in unauthorized

content reuse. The evaluation considers multiple forms of image transformation frequently observed on social media and digital platforms. Table 4 summarizes the effectiveness of the SIRP framework across different misuse scenarios.

Table 4. Practical Misuse Coverage Table

Misuse Scenario	Detection Effectiveness
Social media resizing and compression	**High**
Partial image reuse (cropping misuse)	**Moderate -High**
Color and filter-based editing	**Moderate-High**
Image rotation and orientation change	**Moderate**
Background modification	**Moderate**
Blurring and noise addition	**Moderate-High**
Combined manipulation attacks	**Acceptable**

V. DISCUSSION

The experimental results indicate that perceptual hashing is effective for detecting common, low-level transformations such as resizing and cropping in the evaluated controlled dataset, where global image structure is largely preserved. Performance degradation under blurring and combined manipulation attacks highlights a known limitation of hash-based approaches, which rely on low-frequency structural similarity and become less discriminative as visual content is increasingly distorted (Li, 2006; Ding et al., 2018; Verdoliva & Cozzolino, 2018)

The integration of IoT-based hardware alerts addresses the time-to-action limitation in conventional digital rights protection workflows (Al-Fuqaha et al., 2015; Yin et al., 2019). While hash-based matching provides evidence of potential misuse, the physical and mobile alerts reduced response latency from seconds or minutes to sub-second notification in the tested prototype deployment over a local Wi-Fi network using an MQTT broker. This design shifts the system from passive detection toward more immediate user awareness, which is important in scenarios where unauthorized content spreads rapidly after upload.

However, the reported performance reflects controlled manipulation scenarios. More aggressive adversarial edits, composite image reuse, and large-scale cross-platform monitoring were not evaluated and remain open challenges (Masood et al., 2021; Lu & Lin, 2024; Verdoliva, 2020). These limitations motivate future extensions involving stronger feature representations and broader deployment settings.

VI. CONCLUSION

This work demonstrates that perceptual hashing, combined with prototype MQTT-based alerts, can detect unauthorized image reuse under common transformations, such as resizing and cropping, with up to 95.6% accuracy in controlled settings. The system reduced alert latency in the tested environment, enabling faster user awareness of potential misuse. These results indicate

that SIRP is a lightweight prototype framework for real-time notification of suspected image reuse under typical platform-induced manipulations, rather than a complete solution for large-scale or adversarial misuse scenarios.

Although SIRP effectively detects common forms of image reuse, several extensions are required for broader real-world deployment. Incorporating deep learning-based feature representations could improve robustness to adversarial manipulations and AI-generated imagery. Large-scale cross-platform monitoring remains future work and would require platform API integration or web-crawling mechanisms, combined with scalable indexing. To support higher throughput and continuous monitoring, hybrid cloud edge deployment strategies could be explored. Additionally, secure evidence management mechanisms, such as tamper-resistant audit logs, could strengthen legal usability. Extending the framework to video-based misuse detection represents a further research direction for deep learning-based detection.

REFERENCE

Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., & Serra, G. (2011). A SIFT-Based Forensic Method for Copy–Move Attack Detection and Transformation Recovery. *IEEE Transactions on Information Forensics and Security*, *6*(3), 1099–1110. https://doi.org/10.1109/tifs.2011.2129512

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys & Tutorials*, *17*(4), 2347–2376. https://doi.org/10.1109/comst.2015.2444095

Asmaraloka, A. M., Hermansyah, M. A., Nisa, K., Saputra, F. H. D., & Setiawan, A. (2025). Implementation of the K-Nearest Neighbor (KNN) Algorithm in Handwritten Digit Pattern Recognition Using the Zoning Method. *Jurnal Ilmiah Sistem Informasi*, *4*(2), 175–185. https://doi.org/10.51903/kf6s5f56

Bandyopadhyay, D., & Sen, J. (2011). Internet of Things: Applications and Challenges in Technology and Standardization. *Wireless Personal Communications*, *58*, 49–69. https://doi.org/10.1007/s11277-011-0288-5

Bayram, S., Sencar, H. T., & Memon, N. (2009). An Efficient and Robust Method for Detecting Copy–Move Forgery. In *Proceedings of the 2009 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 1053–1056. https://doi.org/10.1109/icassp.2009.4960267

Buyya, R., Yeo, C. S., & Venugopal, S. (2008). Market-Oriented Cloud Computing: Vision, Architecture, and Challenges. In *Proceedings of the 2008 IEEE International Symposium on Cluster Computing and the Grid (CCGRID)*, 5–13. https://doi.org/10.1109/ccgrid.2008.18

Ding, K., Meng, F., Liu, Y., Xu, N., & Chen, W. (2018). Perceptual Hashing Based Forensics Scheme for the Integrity Authentication of High Resolution Remote Sensing Image. *Information*, *9*(9), 229. https://doi.org/10.3390/info9090229

Farid, H. (2009). Image Forgery Detection. *IEEE Signal Processing Magazine*, *26*(2), 16–25. https://doi.org/10.1109/msp.2008.931079

Guo, Y., Dang, H., Fu, C., & Zhang, L. (2021). Deepfake Detection With Semantic Inconsistencies. In *Proceedings of the 16th European Conference on Computer Vision (ECCV 2020)*, 445–461. https://doi.org/10.1007/978-3-030-58577-8_29

Kaur, P., & Singh, J. P. (2017). Image Copy-Move Forgery Detection Using SURF and DCT Features. In *Proceedings of the 2017 IEEE International Conference on Advanced Computing and Communication Systems (ICACCI)*, 1–6. https://doi.org/10.1109/icacci

Li, C.-T. (2006). Identification of Bitmap Images Using Perceptual Hash. *Journal of Systems and Software*, *81*(6), 971–980. https://doi.org/10.1016/j.jss.2007.01.018

Lu, C.-S., & Lin, C.-H. (2024). Robust Image Deepfake Detection With Perceptual Hashing. In *Proceedings of the 10th International Conference on Information Systems Security and Privacy (ICISSP 2024)*, 220–229. https://doi.org/10.5220/0012317800003648

Masood, M., Nawaz, M., Malik, K. M., & Javed, A. (2021). Deepfakes Generation and Detection: A Survey. *IEEE Access*, *9*, 98795–98817. https://doi.org/10.1109/access.2021.3099369

Mirsky, Y., & Lee, W. (2021). The Creation and Detection of Deepfakes: A Survey. *ACM Computing Surveys*, *54*(1), 1–41. https://doi.org/10.1145/3425780

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of Things: Vision, Applications and Research Challenges. *Ad Hoc Networks*, *10*(7), 1497–1516. https://doi.org/10.1016/j.adhoc.2012.02.016

Nguyen, T. T., Nguyen, C. M., Nguyen, D. T., & Nahavandi, S. (2022). Deep Learning for Deepfakes Creation and Detection. *Computer Vision and Image Understanding*, *223*, 103525. https://doi.org/10.1016/j.cviu.2022.103525

Pebadja, G., & Kholifah, S. (2023). The Impact of Brand Image, Pricing Strategies, and Product Quality on Consumer Loyalty in the Coffee Industry: An Empirical Study Using Structural Equation Modeling. *Journal of Management and Informatics*, *2*(2), 1–20. https://doi.org/10.51903/jmi.v2i2.134

Popescu, A. C., & Farid, H. (2005). Exposing Digital Forgeries by Detecting Duplicated Image Regions. *Dartmouth College Technical Report*. https://farid.berkeley.edu/downloads/publications/cvpr05.pdf

Rössler, A., Cozzolino, D., Verdoliva, L., Riess, C., Thies, J., & Nießner, M. (2020). FaceForensics++: Learning to Detect Manipulated Facial Images. *International Journal of Computer Vision*, *128*, 260–275. https://doi.org/10.1007/s11263-019-01281-8

Shahri, E., Pedreiras, P., & Almeida, L. (2022). Extending MQTT With Real-Time Communication Services Based on SDN. *Sensors*, *22*(9), 3162. https://doi.org/10.3390/s22093162

Tolosana, R., Vera-Rodriguez, R., Fierrez, J., Morales, A., & Ortega-Garcia, J. (2020). Deepfakes and Beyond: A Survey of Face Manipulation. *Information Fusion*, *64*, 131–148. https://doi.org/10.1016/j.inffus.2020.06.014

Verdoliva, L. (2020). Media Forensics and Deepfakes: An Overview. *IEEE Journal of Selected Topics in Signal Processing*, *14*(5), 910–932. https://doi.org/10.1109/jstsp.2020.3002101

Verdoliva, L., & Cozzolino, D. (2018). Image Forgery Detection: A Survey. *IEEE Access*, *6*, 13745–13759. https://doi.org/10.1109/access.2018.2816030

Wang, S. Y., Wang, O., Zhang, R., Owens, A., & Efros, A. A. (2020). CNN-Generated Images Are Surprisingly Easy to Spot. In *Proceedings of the 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 869–878. https://doi.org/10.1109/cvpr42600.2020.00871

Yin, C., Liu, J., & Zhou, C. (2019). Real-Time Monitoring System Design for IoT Devices. *IEEE Internet of Things Journal*, *6*(2), 3198–3207. https://doi.org/10.1109/jiot.2018.2872701

Zauner, C. (2010). *Implementation and Benchmarking of Perceptual Image Hash Functions*. Upper Austria University of Applied Sciences. https://www.phash.org/docs/pubs/thesis_zauner.pdf

Zhou, F., Qiao, Y., & Li, Q. (2024). Real-Time Enhancement of Low-Light Images Using Generative Adversarial Networks (GANs). *Journal of Technology Informatics and Engineering*, *4*(1), 1–10. https://doi.org/10.51903/jtie.v4i1.279

Zhao, G., & Cao, Z. (2016). Robust Image Perceptual Hashing With Local and Global Features. *IEEE Transactions on Information Forensics and Security*, *11*(8), 1803–1814. https://doi.org/10.1109/tifs.2016.2561905