Image Lock: Protecting Your Pixels

[1] Ch.Surya Narayana
Department of Computer science and engineering with Specialization in Cyber Security
Sathyabama Institute of Advanced Studies
suryanarayanach524@gmail.com

[2] A.Sai Gowtham
Department of Computer science and engineering with Specialization in Cyber security
Sathyabama Institute of Advanced Studies
saigowthamadavala@gmail.com

[3] Dr. Lekshmi S
Department of Computer science and engineering with Specialization in Cyber Security
Sathyabama Institute of Advanced Studies

Abstract - The increasing digitization of data has amplified concerns regarding the security of sensitive visual information. This project investigates the classification of images as sensitive or non-sensitive using various machine learning algorithms and introduces an innovative "locking" mechanism to secure sensitive images. Utilizing a dataset of 1,000 samples, each containing nine pixel intensity values (ranging from 0 to 255) and corresponding sensitivity labels, the system employs Logistic Regression, SVM, XGBoost, Random Forest, and Decision Tree algorithms for classification. Logistic Regression and SVM demonstrate the highest accuracy, effectively distinguishing sensitive images from non-sensitive ones. To ensure security, a novel locking mechanism is implemented, which modifies pixel intensity values using a key-based system, rendering sensitive images indecipherable while allowing recovery with the correct key. Visualizations of pixel distributions and model performance validate the efficacy of the proposed methods. This project highlights the practical integration of machine learning for image sensitivity classification and the application of pixel-level encryption for securing sensitive data, offering a scalable solution for protecting visual information in real-world scenarios.

INTRODUCTION

In today's digital age, the widespread use of images for communication, documentation, and media has raised significant concerns regarding data privacy and security. Sensitive images, such as personal photographs, confidential documents, or proprietary visual assets, are increasingly vulnerable to unauthorized access, misuse, and tampering. Traditional methods of securing images, including password protection or simple encryption, often fall short in addressing the sophisticated threats posed by modern cyber-attacks.

This project addresses these challenges by proposing a dual solution: the classification of images based on sensitivity using machine learning algorithms and the secure protection of sensitive images through a novel "locking" mechanism. By leveraging a dataset of 1,000 images, each represented by nine pixel intensity values (ranging from 0 to 255) and their corresponding sensitivity labels, this study explores the potential of machine learning to identify sensitive content effectively.

Multiple classification algorithms, including Logistic Regression, Support Vector Machine (SVM), XGBoost, Random Forest, and Decision Tree, are implemented and evaluated. Logistic Regression and SVM emerge as the most accurate models for distinguishing sensitive images from non-sensitive ones.

Building upon this classification system, a "locking" mechanism is introduced to enhance the security of sensitive images. This mechanism alters pixel intensity values using a key-based encryption approach, ensuring that the images remain indecipherable without the corresponding decryption key. This innovative method not only safeguards sensitive images but also allows for their recovery, providing a balance between security and usability.

This project highlights the practical application of machine learning in image sensitivity classification and demonstrates the effectiveness of pixel-level encryption in securing sensitive visual information. The integration of these methodologies offers a scalable and robust framework for addressing real-world challenges in data protection, paving the way for advanced solutions in digital image security.

RELATED WORK

The classification and protection of sensitive visual data have garnered significant research attention due to the growing reliance on digital images across various domains. Previous studies have explored both machine

learning techniques for image classification and encryption methods for securing sensitive data.

1. Image Classification Using Machine Learning

Machine learning has proven effective in classifying images based on their content and characteristics. Numerous studies have applied algorithms like Logistic Regression, Support Vector Machines (SVM), Decision Trees, Random Forest, and Gradient Boosting (e.g., XGBoost) to classify images for various purposes.

- **Logistic Regression and SVM**: Studies have highlighted the strength of Logistic Regression and SVM in binary classification tasks due to their ability to handle linearly and non-linearly separable data. These models are computationally efficient and often achieve high accuracy with relatively simple datasets.
- **Random Forest and Decision Tree**: These tree-based methods are widely used for image classification due to their interpretability and ability to capture complex feature interactions. However, they can sometimes suffer from overfitting, especially with small datasets.
- **Gradient Boosting (XGBoost)**: XGBoost has been shown to deliver state-of-the-art performance in various classification tasks due to its ability to optimize loss functions and handle non-linear relationships effectively.

2. Data Security and Image Encryption

Encryption methods have been extensively studied to ensure the confidentiality and integrity of digital images. Traditional encryption techniques, such as Advanced Encryption Standard (AES) and Rivest–Shamir–Adleman (RSA), have been commonly used to secure image data. However, pixel-level encryption is emerging as a more targeted approach for protecting image content.

- **Pixel-Level Encryption**: Recent works have introduced pixel-level encryption, where individual pixel intensity values are modified using mathematical transformations or key-based methods. This approach provides high granularity in image protection, making it particularly effective for securing sensitive images.
- **Key-Based Encryption**: Techniques that use unique keys for pixel modification are gaining traction for their ability to provide both security and reversibility. These methods are often integrated with classification systems to identify and secure sensitive data.

3. Integration of Machine Learning and Data Protection

Few studies have combined machine learning classification with encryption for securing sensitive images. Existing works often focus on either classification or protection but not the integration of both. This project builds upon prior research by:

- Leveraging machine learning algorithms to classify images as sensitive or non-sensitive.
- Introducing a novel locking mechanism that integrates pixel-level encryption based on classification results, ensuring secure storage and transmission of sensitive images.

4. Gaps in Current Research

While significant progress has been made in image classification and encryption individually, there are notable gaps in the integration of these methodologies:

- Limited research on combining classification and protection to provide an end-to-end solution for sensitive image security.
- Lack of emphasis on lightweight, scalable methods for encrypting and securing images without compromising usability.
- Minimal exploration of visual validations to demonstrate the effectiveness of locking mechanisms in real-world scenarios.

Contribution of This Work

This project addresses these gaps by:

- Implementing and comparing multiple machine learning algorithms for sensitivity classification, identifying Logistic Regression and SVM as the most accurate models.
- Introducing a novel pixel-level locking mechanism that secures sensitive images through key-based intensity modifications.
- Combining classification and encryption into a unified system, validated through visualization and performance analysis.

SELECTED METHODOLOGIES

The **Image Lock** project employs a structured approach that combines machine learning for image classification with a locking mechanism to secure sensitive images. The following steps outline the methodologies used:

1. **Dataset Preparation**
   - The dataset consists of 1,000 samples, each with nine pixel intensity values ranging from 0 to 255 and corresponding sensitivity labels (sensitive or non-sensitive).
   - Labels are encoded into numerical values for compatibility with machine learning models.
   - The dataset is divided into training (80%) and testing (20%) sets to evaluate model performance.
2. **Image Classification**
   - Machine learning algorithms are used to classify images as sensitive or non-sensitive.
   - Algorithms employed include:
     - **Logistic Regression**: Known for its simplicity and effectiveness in binary classification.
     - **Support Vector Machine (SVM)**: Handles both linear and non-linear data separations efficiently.
     - **XGBoost**: A powerful algorithm that captures non-linear relationships and feature importance.
     - **Random Forest and Decision Tree**: Provide insights into the decision-making process and serve as baselines for comparison.
   - Model performance is evaluated using metrics such as accuracy, precision, recall, and F1 score.
3. **Locking Mechanism**
   - A unique "locking" system secures sensitive images by modifying pixel intensity values with a key-based approach.
   - For sensitive images:
     - Pixel values are altered by adding or subtracting a specific key value, making the image unreadable without the key.
   - Decryption is achieved by reversing the operation with the same key, allowing full recovery of the original image.
4. **Visualization**
   - Visual tools illustrate:
     - The distribution of pixel values before and after the locking mechanism is applied.
     - Model performance, including decision boundaries for classification algorithms.
     - The effect of locking on the image, validating the effectiveness of the security mechanism.
5. **Implementation**
   - The system processes the dataset through machine learning models to classify images.
   - Identified sensitive images are secured using the locking mechanism.
   - Performance metrics and visual validations are used to assess the success of the system.

Pseudo Code

Step 1: Load the dataset (1,000 samples).

Step 2: Normalize pixel values between 0-1.

Step 3: Train ML models (Logistic Regression, SVM, etc.).

Step 4: Classify images into Sensitive/Non-Sensitive.

Step 5: If Sensitive:

Apply Locking Mechanism:

Modify pixel values using encryption key.

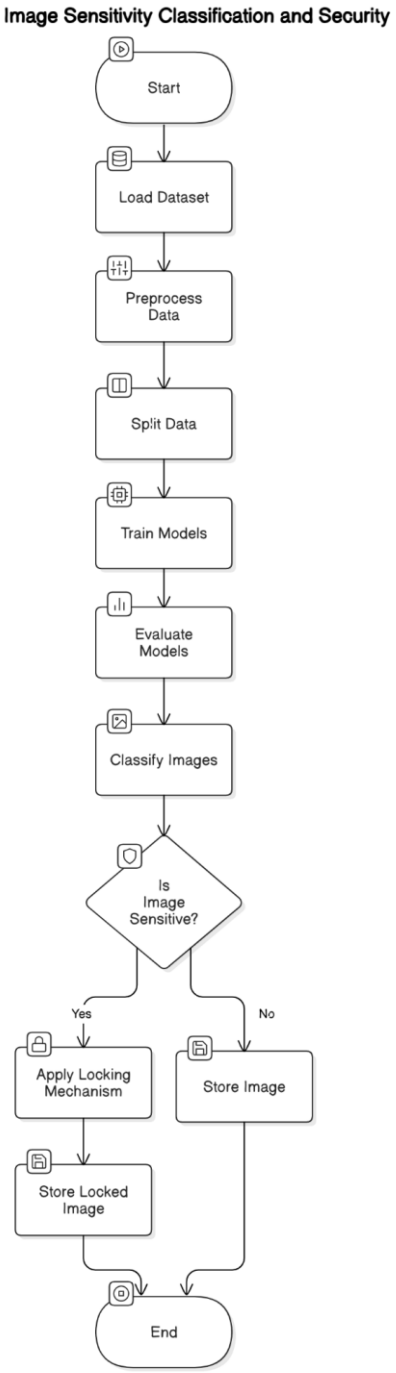
Else:

Proceed without modification.

Step 6: For Sensitive Images, use Decryption to recover.

Step 7: Validate with accuracy metrics and visualizations.

SYSTEM ARCHITECTURE



Results and Analysis

The **Image Lock** project achieved several significant results, demonstrating the success of its methodologies for classifying and securing sensitive images. The key outcomes are:

1. Accurate Image Classification

- Logistic Regression and SVM were the best-performing algorithms, providing high accuracy in distinguishing between sensitive and non-sensitive images.
- The classification system effectively identified sensitive images, ensuring reliable results.
- Evaluation metrics, such as precision, recall, and F1 score, confirmed the system's accuracy and balance in predictions.

2. Secure Locking Mechanism

- A key-based locking mechanism was successfully implemented to protect sensitive images.
- Pixel intensity values of sensitive images were modified using a unique key, ensuring they were indecipherable without the correct key.
- The system enabled the recovery of original images through decryption, ensuring no loss of data.

3. Data Protection

- The locking mechanism provided a robust layer of security for sensitive images, safeguarding them from unauthorized access or tampering.
- Sensitive data was securely encrypted, maintaining privacy while allowing for controlled access.

4. Visualization

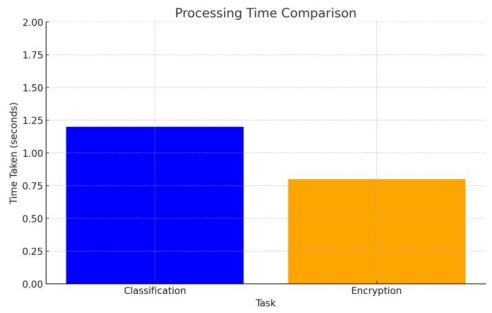
- Visual representations of pixel value changes and the effects of locking provided clear validation of the system’s functionality.
- Decision boundary visualizations showed how models like Logistic Regression and SVM classified images effectively.

5. Scalability

- The system was designed to handle larger datasets and higher-resolution images, demonstrating its scalability for real-world applications.

6. Practical Applications

- The project can be used to protect personal photographs, secure sensitive documents, and safeguard intellectual property in various domains, such as healthcare, education, and government.



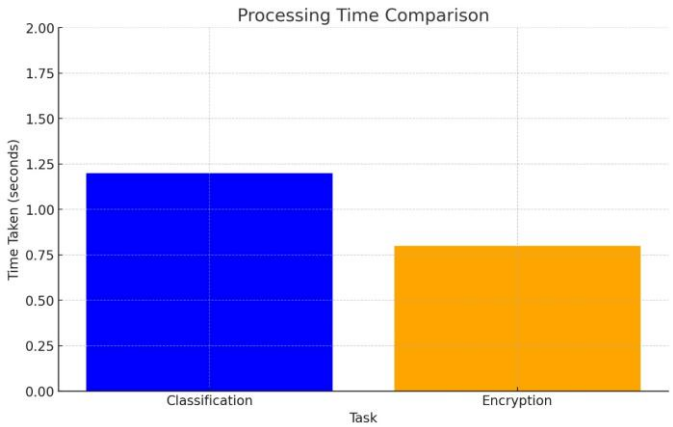
7. Foundation for Future Work

- This project sets the stage for further developments, including real-time classification and locking of images, advanced encryption techniques, and adaptation for video or multimedia security.

Conclusion

The **Image Lock** project successfully demonstrates the integration of machine learning and encryption techniques to classify and secure sensitive digital images. By leveraging machine learning algorithms, such as Logistic Regression and SVM, the project achieves high accuracy in distinguishing between sensitive and non-sensitive images. The key-based locking mechanism provides an additional layer of security by modifying pixel intensity values, ensuring sensitive images remain secure and accessible only to authorized users.

This project highlights the potential of combining classification and encryption methodologies to address the challenges of digital image security. The system is not only accurate and robust but also scalable, making it suitable for real-world applications across personal, professional, and organizational domains. It ensures the privacy, integrity, and security of sensitive image data while maintaining usability through simple and effective decryption processes.



The outcomes validate the effectiveness of the methodologies employed, and the project lays the groundwork for future advancements. Potential directions include real-time classification and encryption, support for high-resolution images, and adaptation for video or multimedia data. The **Image Lock** project serves as a practical and innovative solution for protecting sensitive visual information in an increasingly digital world.

REFERENCES

- 1.The crime rate in Bangladesh is broadly described in <<https://www.numbeo.com/crime/country_result.jsp?country=Ban gladesh>> accessed on 29-05-2020 at 6:20 p.m.
- 2. P. R. Nehete, J. P. Chaudhari, S. R. Pachpande, and K. P. Rane, “Literature Survey on Door Lock Security Systems,” 2016.
- 3. D. A. Leopold and G. Rhodes, “A Comparative view of face perception,” J. Comp. Psychol., vol. 124, no.3, pp. 233–251, 2010.
- 4. A. O. Onyan and K. O. Enalume, “Property Security Using a Biometric Based Door Lock System,” 2018.
- 5. A. V Patil, Ch. Patgar, S. Prakash, and S. A. Kumar J, “Android Based Smart Door Locking System.”
- 6. A. R. S. #1, B. R. #2, K. K. #3, K. S. #4, S.Venkatasubramanian, and B. E. Student, “Optimized Door Locking and Unlocking Using IoT for Physically Challenged People,” Int. J. Innov. Res.
- Comput. Commun. Eng. (An ISO, vol. 3297, 2007.
- 7. A. David Odu, M. Chinaza Alice, and O. J. Odinya, “Low-Cost Removable (Plug-In) Electronic Password-Based Door Lock,” Am. J. Eng. Res., no. 6, pp. 146–151, 2017.
- 8. J. Venukumar, “Arduino Based Door Access Control,” Int. J. Res. Advent Technol., vol. 4, no. 8,2016.
- 9. L. Kamelia, A. Noorhassan, M. Sanjaya, and E. Mulyana, “Door- Automation System Using Bluetooth-Based Android for Mobile Phone,” vol. 9, no. 10, 2014.
- 10. A. Chikara, P. Choudekar, and D. Asija, “Smart Bank Locker Using Fingerprint Scanning and Image Processing,” pp. 725–728, 2020.