तमसो मा ज्योतिर्गमय
LEAD ME FROM DARKNESS TO LIGHT
NATIONAL INSTITUTE OF TECHNOLOGY
SRINAGAR KASHMIR

Effective Feature Extraction from Encrypted Images

Project Supervisor
Dr. Ranjeet Kumar Rout

Momin Aftab (2020BCSE001)
Muneeb Ahmad (2020BCSE002)

Why do we need security?

Introduction

In the era of cybersecurity and privacy-preserving technologies, the need for secure image processing has gained significant importance. This presentation will focus on the effective extraction of features from encrypted images which is a critical aspect of maintaining data confidentiality while still enabling useful analysis.

Problem Statement

Developing a model for the effective classification of encrypted facial data, while maintaining minimal computational cost and ensuring secure data handling and decryption processes.

Literature Review

[2019] HOG feature extraction from encrypted images for privacy-preserving machine learning
Masaki Kitayama, Hitoshi Kiya

The paper describes the process of extracting HOG features from encrypted images, which are then used as input for machine learning algorithms. The paper also discusses the use of a secure decryption process to ensure the confidentiality of the data.

[2023] An Image Feature Extraction to Generate a Key for Encryption in Cyber Security Medical Environments
Salim Jamil, Abeer & Azeez, Raghad & Hassan, Nidaa

The paper focuses on a encryption method for securing medical images, it begins with edge detection, then uses the resulting image features to create an encryption key.

[2023] Fine-Grained Encrypted Image Retrieval in Cloud Environment
Yi-Hui Chen & Min-Chun Huang

Challenges

- The trade-off between data confidentiality and classification performance.

- The need for efficient and scalable methods to handle large datasets.

- Previous method limitations:

1. It requires specific conditions to be effective, which limits its broader application.

2. It was primarily tested under specific datasets. Its performance across a wider range of datasets and contexts remains under-explored.

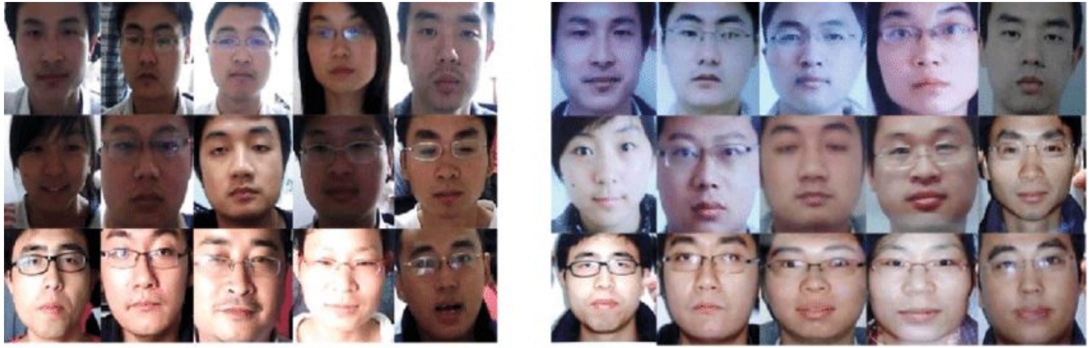
DATASET

Dataset

For this project, we utilized the **NUAA Imposter Database**, specifically designed to explore spoofing attacks against facial recognition systems. This database categorizes face photographs into two groups: genuine clients and impostors.

Dataset

Our analysis involves applying texture analysis techniques to these images to enhance detection and security measures.



Real access images

Attack photo images

Work Done

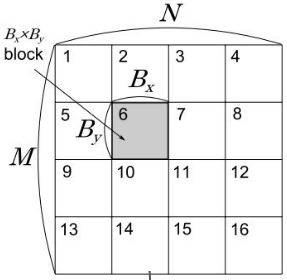
Image Preprocessing:

Given an image I of dimensions M×N,

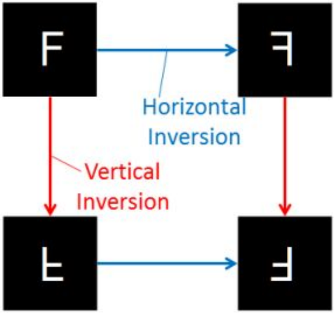
1. We divide the image into blocks B_m, of dimensions $B_x \times B_y$ where m = 1, 2 ,... M
2. We use a secret key K_1 to randomly rotate and permute the blocks
3. We use a secret key K_2 to randomly rotate and invert the blocks
4. We use a secret key K_3 to randomly apply negative-positive transformations to each block

This set of operations gives us an encrypted image I'.

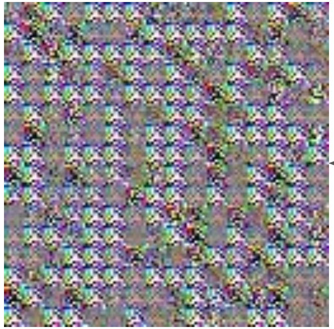
Original Image



Block Permutation



Block Inversion

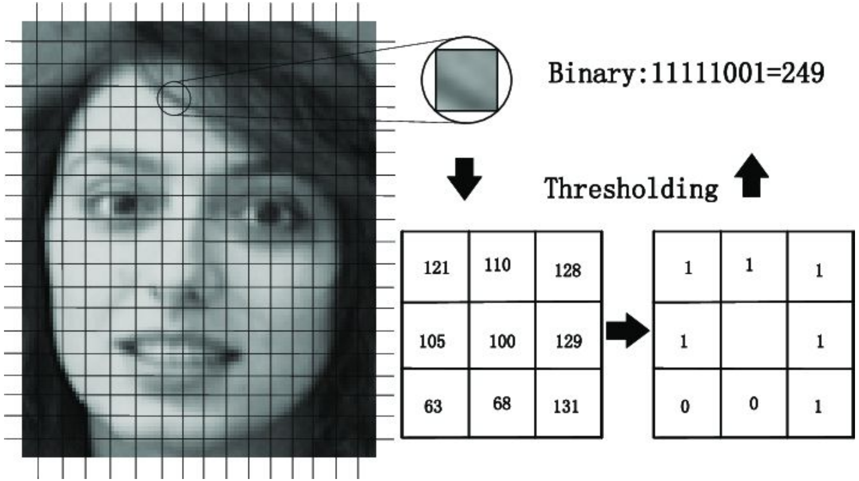


Block Transformation

Using a feature extractor

Upon processing the encrypted image I′, we can apply the Local Binary Patterns (LBP) feature extraction technique.

LBP examines the local texture patterns around each pixel by comparing it to its neighboring pixels, creating a binary pattern that represents the texture features of the image.



121	110	128
105	100	129
63	68	131

1	1	1
1		1
0	0	1

This feature set derived from the LBP extractor can be employed to predict and classify the output, enabling the analysis and interpretation of encrypted image data while maintaining data confidentiality.

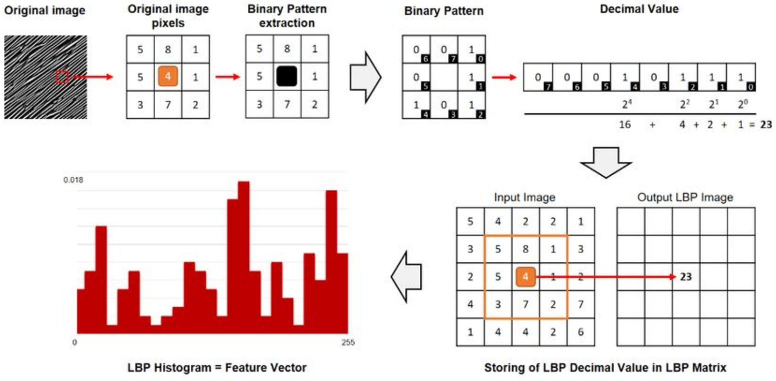
LBP as a feature extractor

Cell Division: The image is divided into smaller, fixed-size cells (e.g., 16x16 pixels).

LBP Operation: For each cell, the LBP operation is performed pixel by pixel. Each pixel is compared with its neighbors in a circular pattern, encoding the result as a binary number based on whether neighboring pixels are greater than or equal to the center pixel.

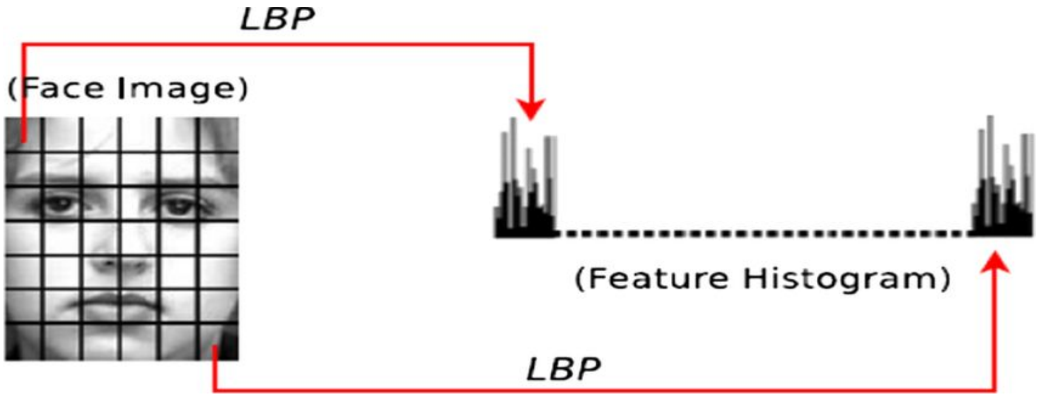
Histogram Computation: For each cell, a histogram of the LBP codes is computed, reflecting the texture patterns within that cell.

Optional Uniform Pattern Extension: To reduce feature dimensionality and achieve rotation invariance, uniform LBP patterns may be used, where histograms only account for patterns with two or fewer bitwise transitions.



Feature Vector Construction:

The histograms from all cells are concatenated to form a comprehensive feature vector representing the entire image. This vector captures the texture information distributed across the image.



Normalization (Optional):

The feature vector can be normalized to ensure that the magnitude of the vector does not bias the subsequent classification.

Classification:

The feature vector is fed into a classifier such as a Support Vector Machine (SVM).

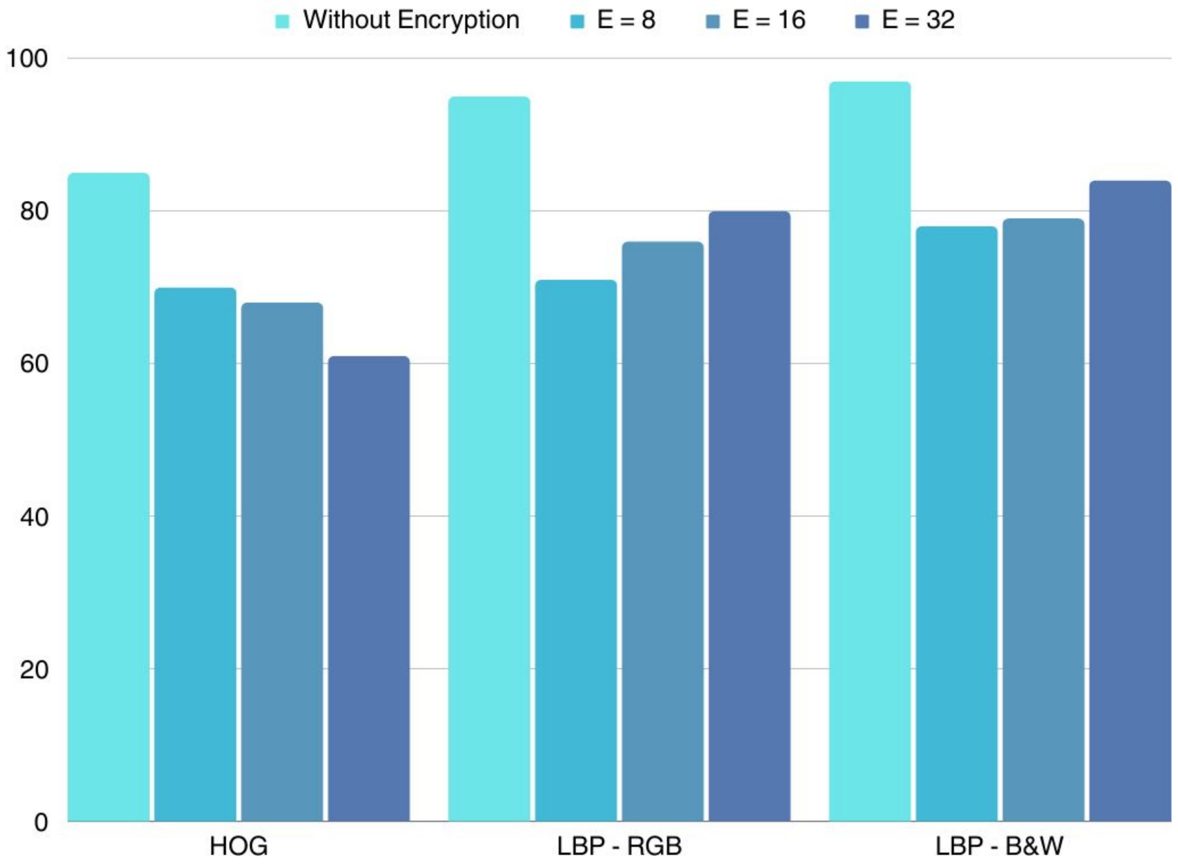
The classifier is trained on feature vectors from a labeled dataset, learning to associate specific patterns of features with particular classes or outcomes.

Results (so far)

	Without Encryption	Block Size = 8	Block Size = 16	Block Size = 32
HOG	85%	70%	68%	61%
LBP (RGB)	95%	71%	76%	80%
LBP (Grayscale)	97%	78%	79%	84%

All values have been rounded off to the nearest integer

Results (so far)



TIMELINE
FOR PROJECT

TASKS	MARCH				APRIL				MAY				JUNE			
DATA COLLECTION	●	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○
PREPROCESSING & ANALYSIS	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○
LITERATURE SURVEY	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○
ENCRYPTION METHODS	○	○	○	●	●	●	●	●	●	●	○	○	○	○	○	○
MODEL EXPERIMENTATION	○	○	○	●	●	●	●	●	●	●	○	○	○	○	○	○
FINAL RESULTS	○	○	○	○	○	○	○	○	●	●	●	●	○	○	○	○
PAPER WRITING	○	○	○	○	○	○	○	○	●	●	●	●	●	●	●	●

CONCLUSION

Conclusion

In this project, we proposed a method of recognition of visually protected images, which allow us to directly use them for purposes of computer vision.

In the case of facial recognition, our method proved to be effective at recognizing protected faces.

Thank you!