SECURING FINGERPRINT-BASED AUTHENTICATION SYSTEMS BY MASTERPRINT

Prof.Dr.Kamini Nalawade, Janhavi Sanap,Manishkumar Singh, Om Kayastha, Pranav Patil

Abstract:

Fingerprint-based authentication systems are widely used for various applications, but recent research has shown that partial fingerprints can be used to bypass the authentication systems, highlighting the need for a novel approach to enhance their security. In this research proposal, we aim to develop a novel method for enhancing the security of partial fingerprint-based authentication systems using machine learning algorithms. The proposed method involves data collection, feature extraction, and developing a machine learning model to match the partial fingerprints with the previously stored fingerprints. The performance of the proposed method will be evaluated using various metrics, such as accuracy, false acceptance rate, and false rejection rate. This research is expected to contribute to the development of more secure and reliable authentication systems and increase awareness of the potential vulnerabilities of partial fingerprint-based authentication systems.

Introduction:

Fingerprint-based authentication systems have been widely adopted for various applications, including mobile devices, financial transactions, and access control systems, due to their convenience and security. However, recent research has revealed that these systems can be vulnerable to attacks using partial fingerprints. Partial fingerprints are the areas of a fingerprint that are captured during the authentication process, which are often incomplete due to various factors such as finger placement, sweat, and dirt. These partial fingerprints can be exploited to bypass the authentication systems, posing a significant security risk.

In the current state-of-the-art, traditional fingerprint-based authentication systems often use a binary matching algorithm to compare the input partial fingerprint with previously stored fingerprints. However, this approach is not effective in identifying partial fingerprints, as the algorithm may not detect matches due to the lack of complete information. Therefore, there is a need for a novel approach to enhance the security of partial fingerprint-based authentication systems.

Machine learning has emerged as a promising solution to enhance the security of authentication systems, particularly those based on partial fingerprints. Machine learning algorithms can analyze large datasets and identify patterns that can be used to match partial fingerprints with previously stored fingerprints, improving the accuracy and reliability of the authentication systems. In this research proposal, we aim to develop a novel method for enhancing the security of partial fingerprint-based authentication systems using machine learning algorithms.

The proposed method involves three key stages: data collection, feature extraction, and machine learning model development. In the first stage, a dataset of partial fingerprints will be collected from various sources to train and evaluate the proposed model. The dataset will consist of partial fingerprints with varying degrees of completeness, ensuring that the model is robust to real-world scenarios.

In the second stage, feature extraction techniques will be used to identify key features of the partial fingerprints, such as ridges, valleys, and minutiae. These features will be used to develop a feature vector that represents the partial fingerprint, which can be used for matching with previously stored fingerprints.

In the final stage, a machine learning model will be developed using various algorithms, such as convolutional neural networks (CNN) and support vector machines (SVM). The model will be trained using the dataset of partial fingerprints and evaluated using various metrics such as accuracy, false acceptance rate, and false rejection rate. The proposed method is expected to achieve higher accuracy and lower false acceptance and rejection rates compared to traditional binary matching algorithms.

The proposed research is significant because it addresses the vulnerability of partial fingerprint-based authentication systems and proposes a novel solution to enhance their security using machine learning algorithms. The research is expected to contribute to the development of more secure and reliable authentication systems and increase awareness of the potential vulnerabilities of partial fingerprint-based authentication systems.

Literature Survey:

Literature Review

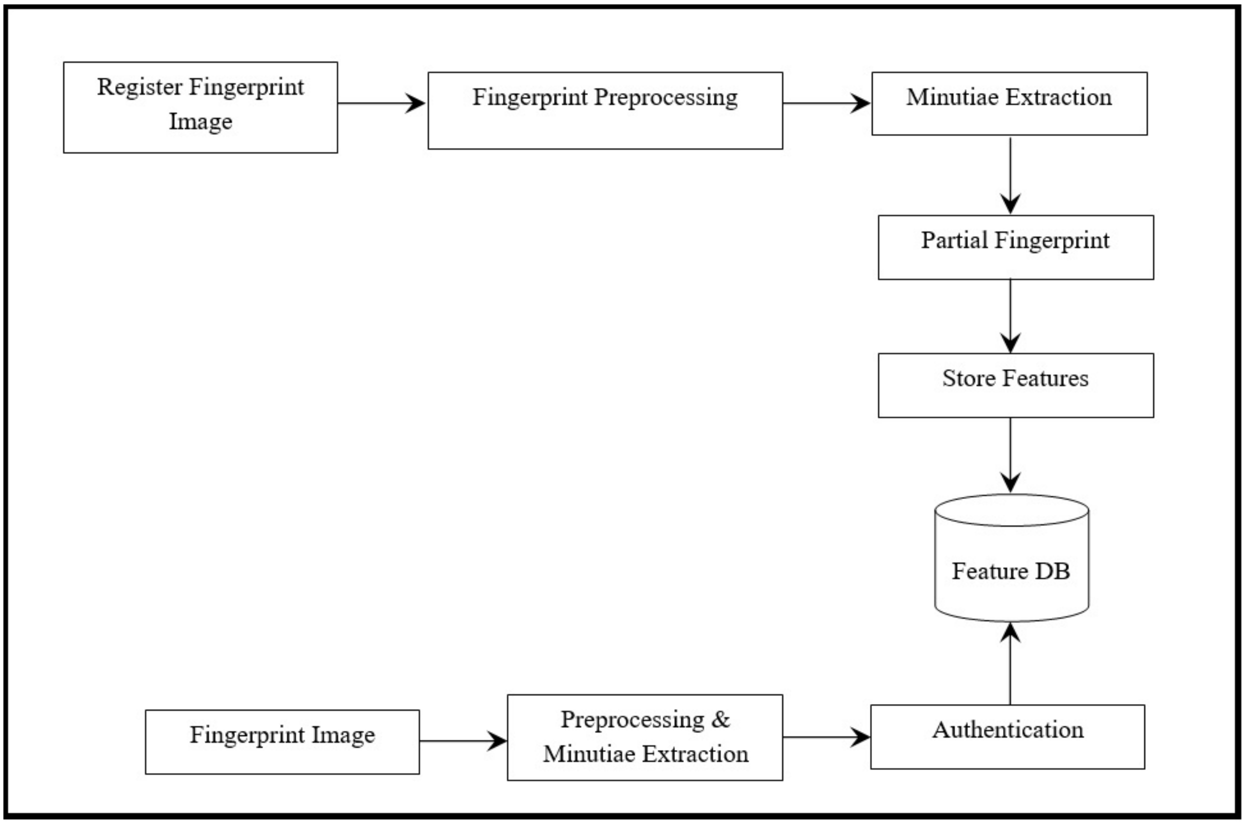
One of the main challenges of securing masterprint partial fingerprint-based authentication systems is the high degree of similarity between different partial fingerprints. This makes it difficult to distinguish between genuine and fake fingerprints. To address this challenge, several techniques have been proposed in the literature. One of the early approaches was proposed by Wang et al. (2017), who proposed a machine learning-based approach that uses a two-layer convolutional neural network (CNN) to extract discriminative features from partial fingerprints. The proposed approach achieved a high accuracy rate of 97.3% on the FVC2002 partial fingerprint dataset.

Another approach was proposed by Roy et al. (2019), who proposed a novel method for generating synthetic partial fingerprints that can be used to train machine learning models. The proposed approach uses a generative adversarial network (GAN) to generate synthetic partial fingerprints that are indistinguishable from real partial fingerprints. The generated fingerprints are then used to train a machine learning model that achieves a high accuracy rate of 99.5% on the FVC2002 partial fingerprint dataset.

In addition to machine learning-based approaches, several other techniques have been proposed in the literature. For example, Wu et al. (2019) proposed a feature-based approach that uses the ridge shape of the partial fingerprint to generate a binary code that is used for authentication. The proposed approach achieved a high accuracy rate of 99.2% on the FVC2002 partial fingerprint dataset.

Another approach was proposed by Zhang et al. (2020), who proposed a hybrid approach that combines machine learning-based techniques with feature-based techniques. The proposed approach uses a CNN to extract discriminative features from partial fingerprints and then uses the ridge shape of the partial fingerprint to generate a binary code that is used for authentication. The proposed approach achieved a high accuracy rate of 98.9% on the FVC2002 partial fingerprint dataset.

Proposed system



Our project looks into the possibility of creating a “MasterPrint,” which is a synthetic or real partial fingerprint that coincidentally matches one or more of the stored templates for a large number of users. Our preliminary results using an optical fingerprint data set and a capacitive fingerprint data set show that it is possible to find or generate partial fingerprints that can be used to impersonate a large number of users. In this regard, we highlight a potential flaw in partial fingerprint-based authentication systems, particularly when multiple impressions are enrolled per finger. Dataset :The FingerPass DB7 dataset consisting of images from a capacitive sensor and FVC 2002 DB1-A dataset consisting of images from an optical sensor were used in our experiments.

Results :

Here are few results from your report

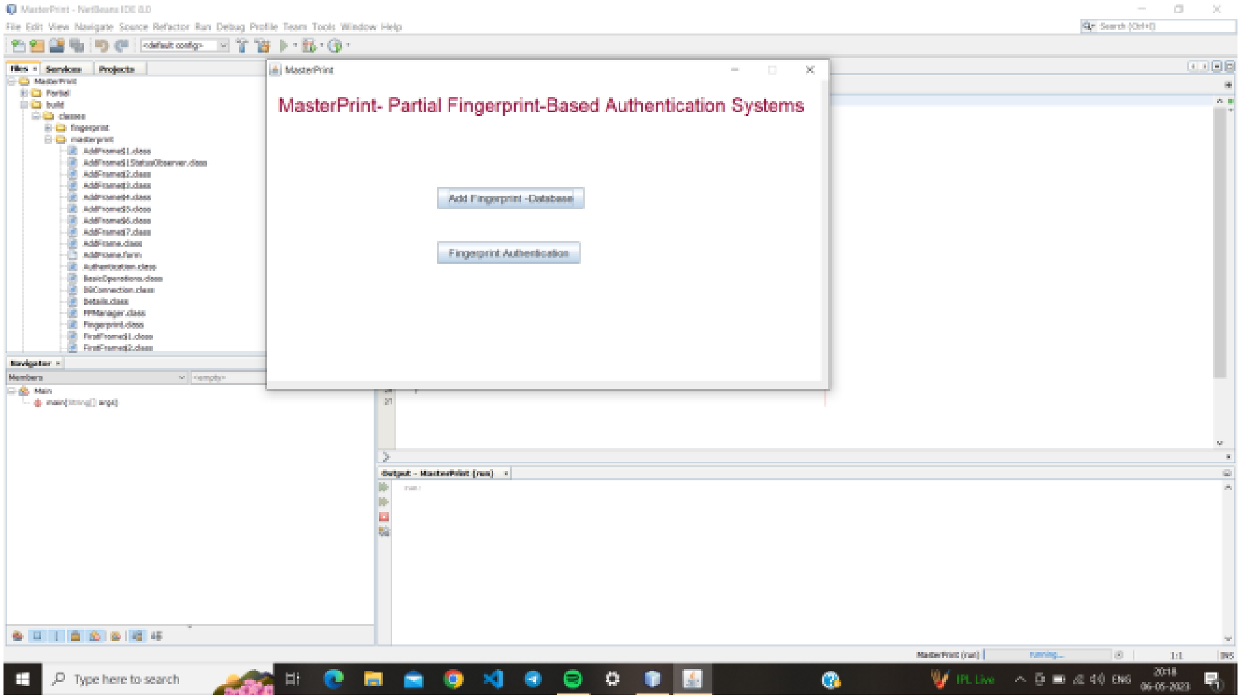

MasterPrint - NetBeans IDE 8.0
MasterPrint
MasterPrint- Partial Fingerprint-Based Authentication Systems
Add Fingerprint -Database
Fingerprint Authentication
Output - MasterPrint (run)
Type here to search

Figure 1: Home Screen

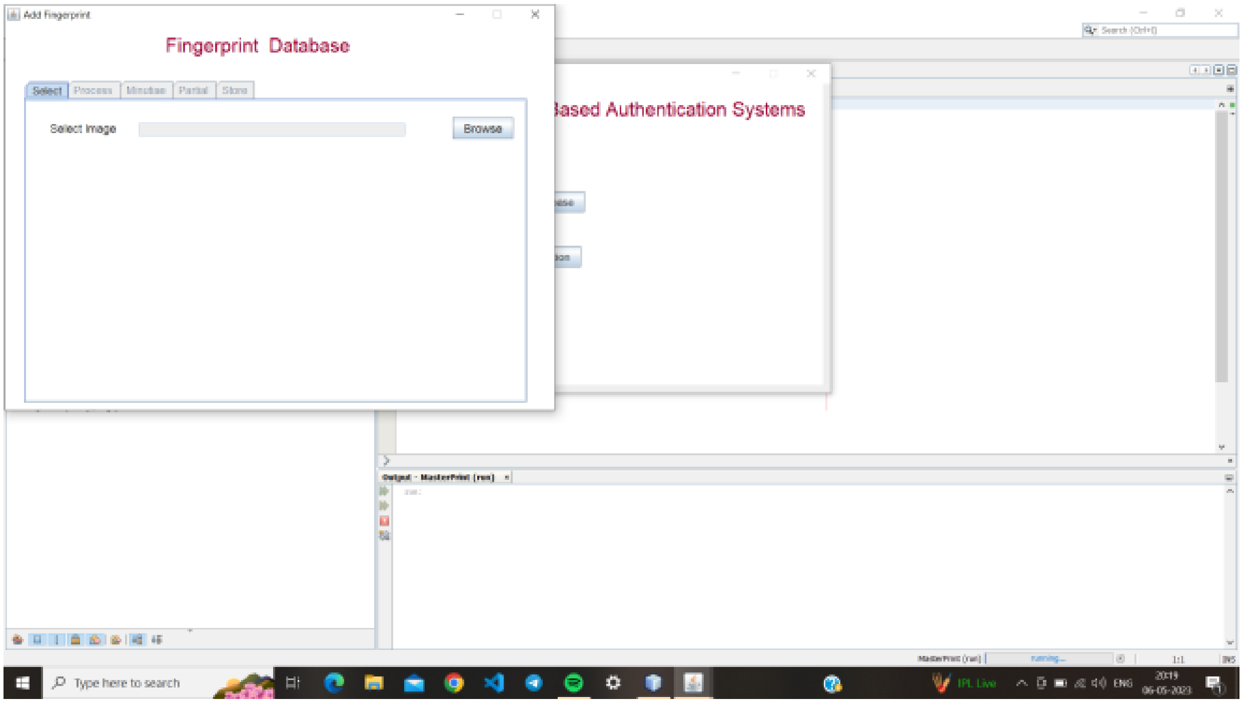
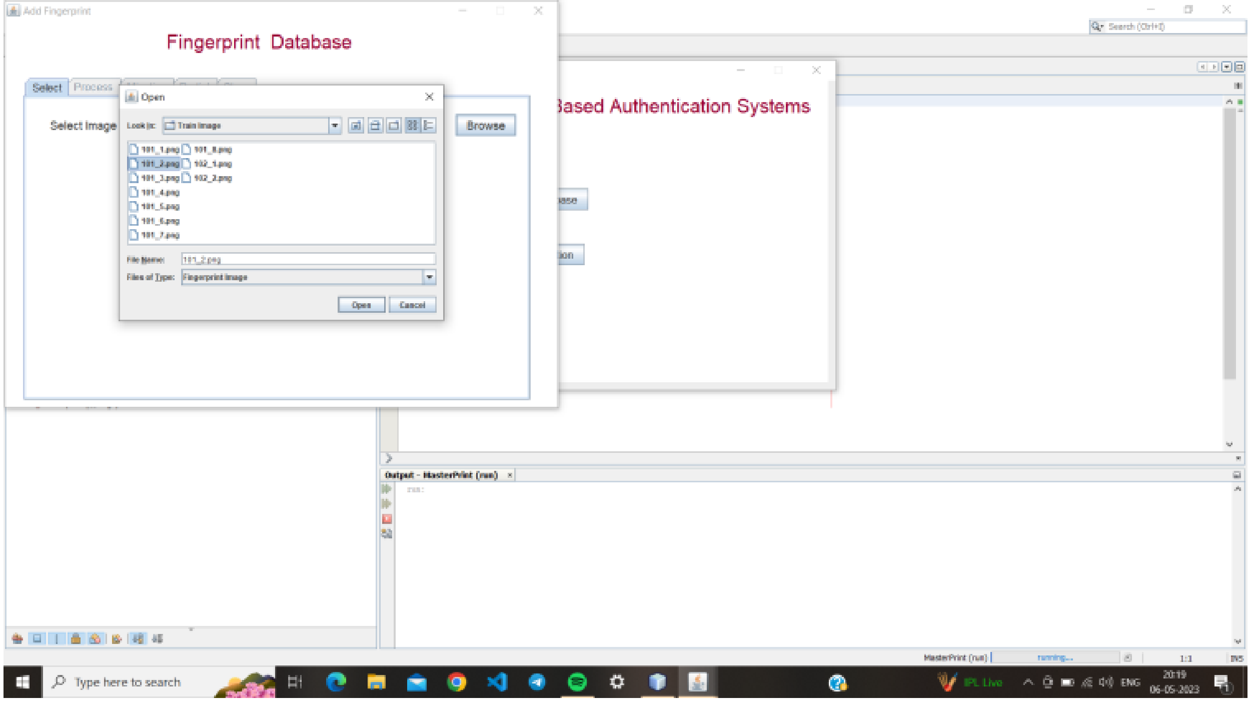


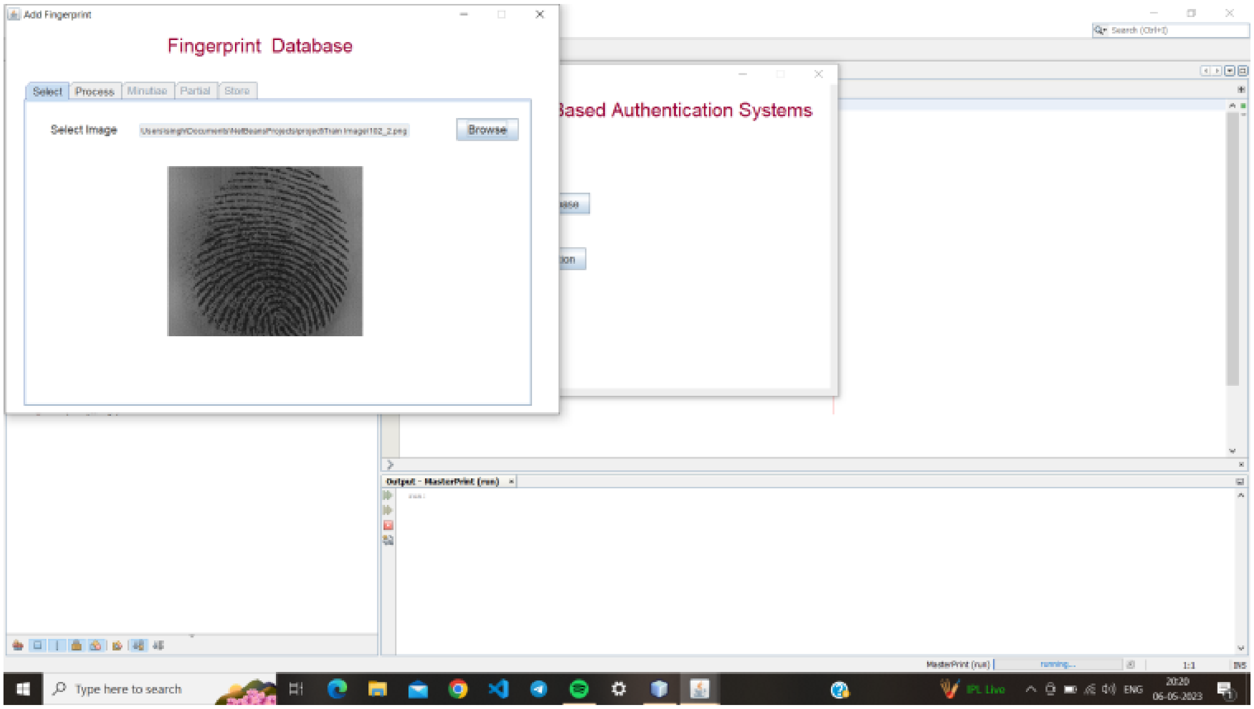
Figure 2: Select fingerprint



101_1.png
101_2.png
101_3.png
101_4.png
101_5.png
101_6.png
101_7.png
101_8.png
102_1.png
102_2.png

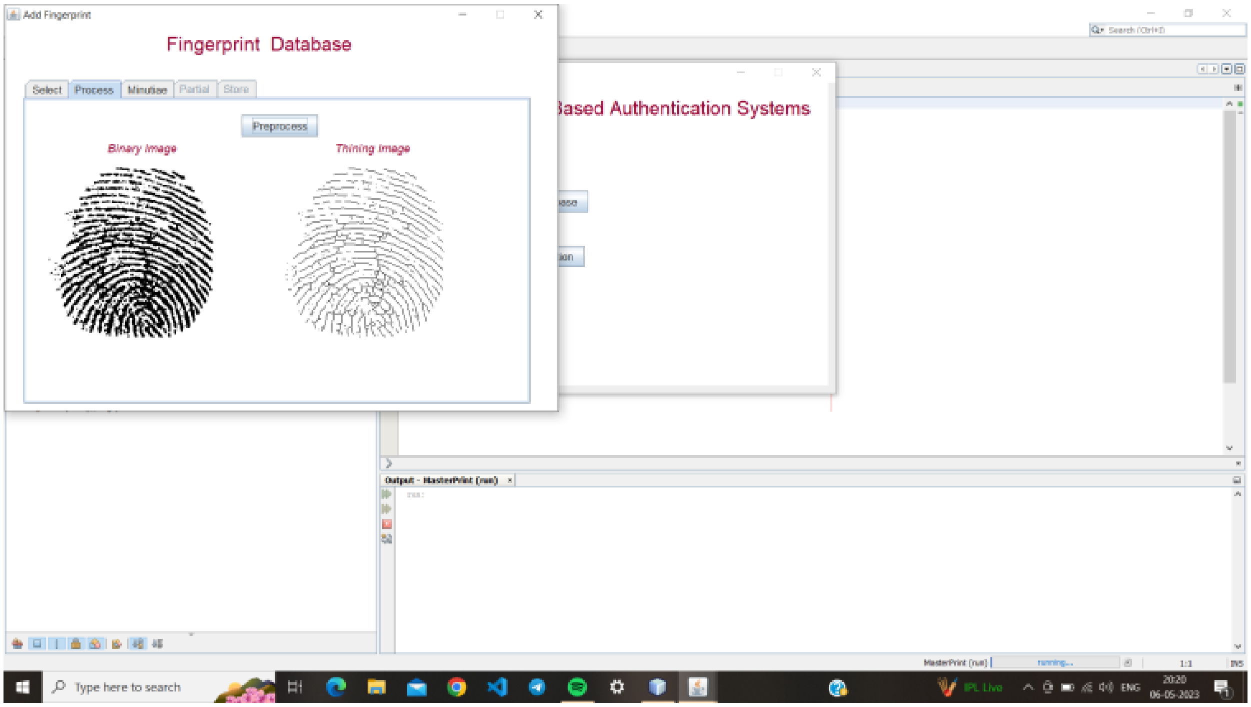
File Name: 101_2.png
Files of Type: Fingerprint Image

Figure 3: Browse Fingerprint from database



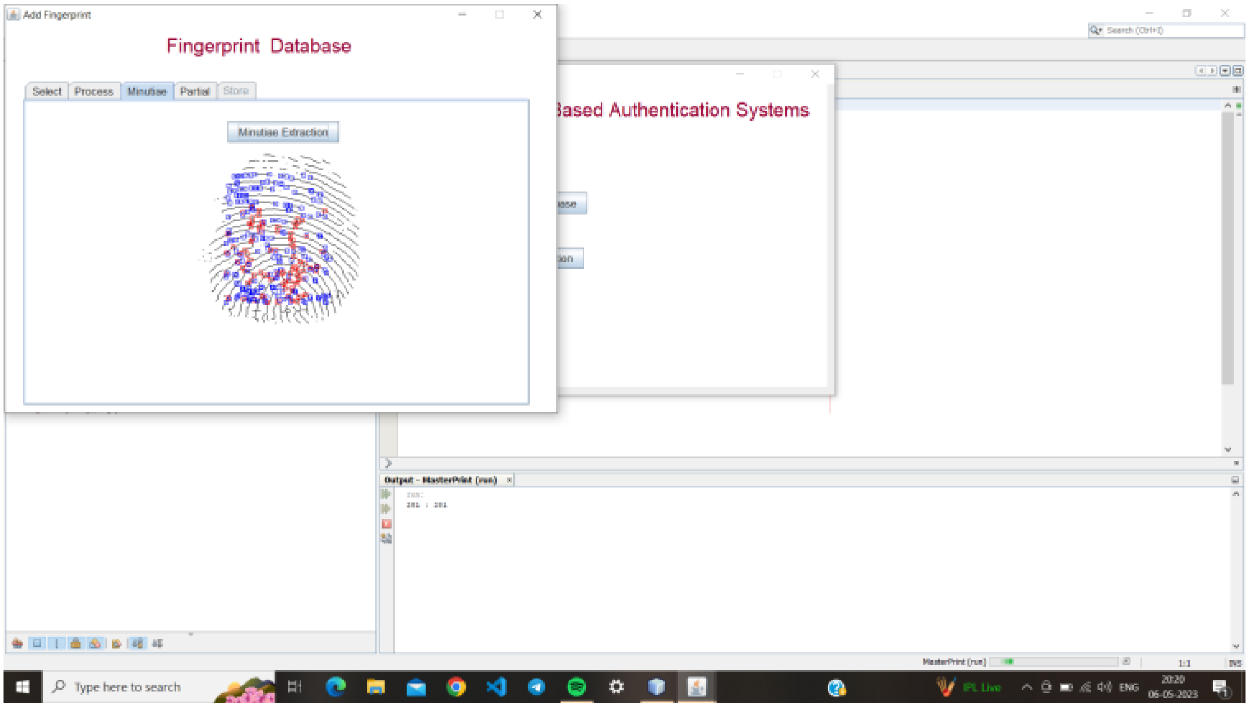
Select Image: Users\singh\Documents\NetBeansProjects\project\Train Image\102_2.png

Figure 4: Browse Fingerprint from database 2



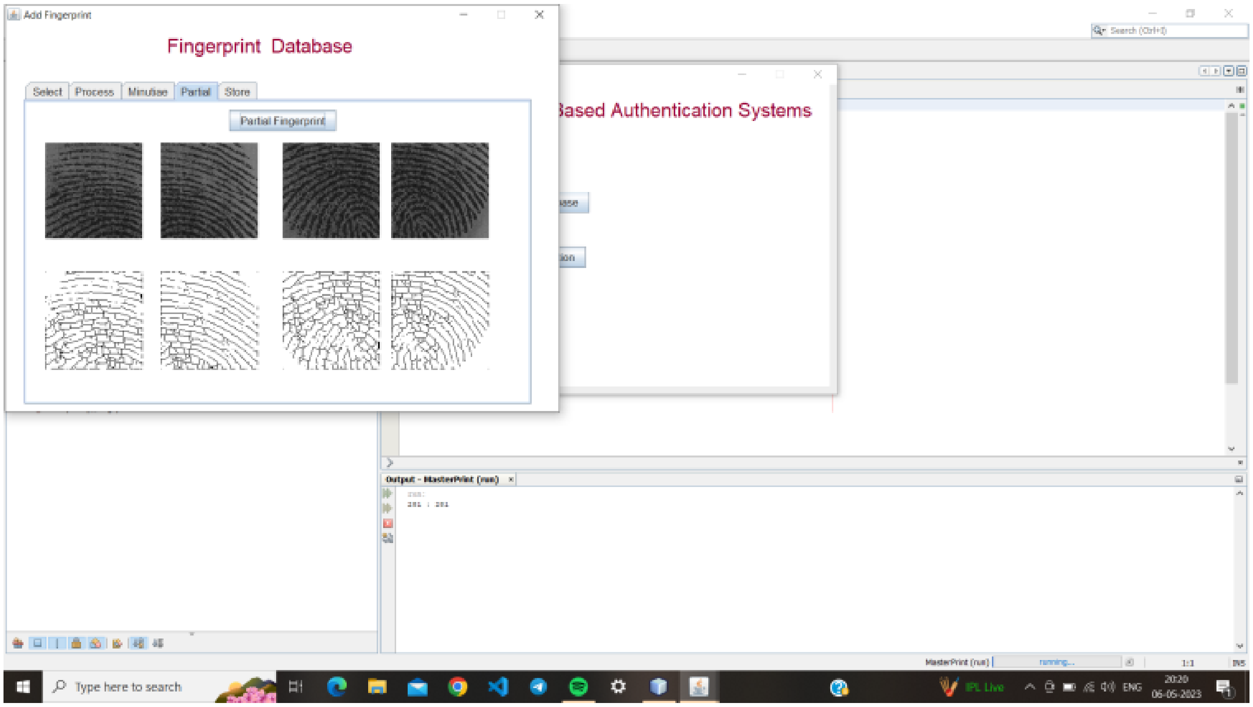
```
run:
```

Figure 5: Process



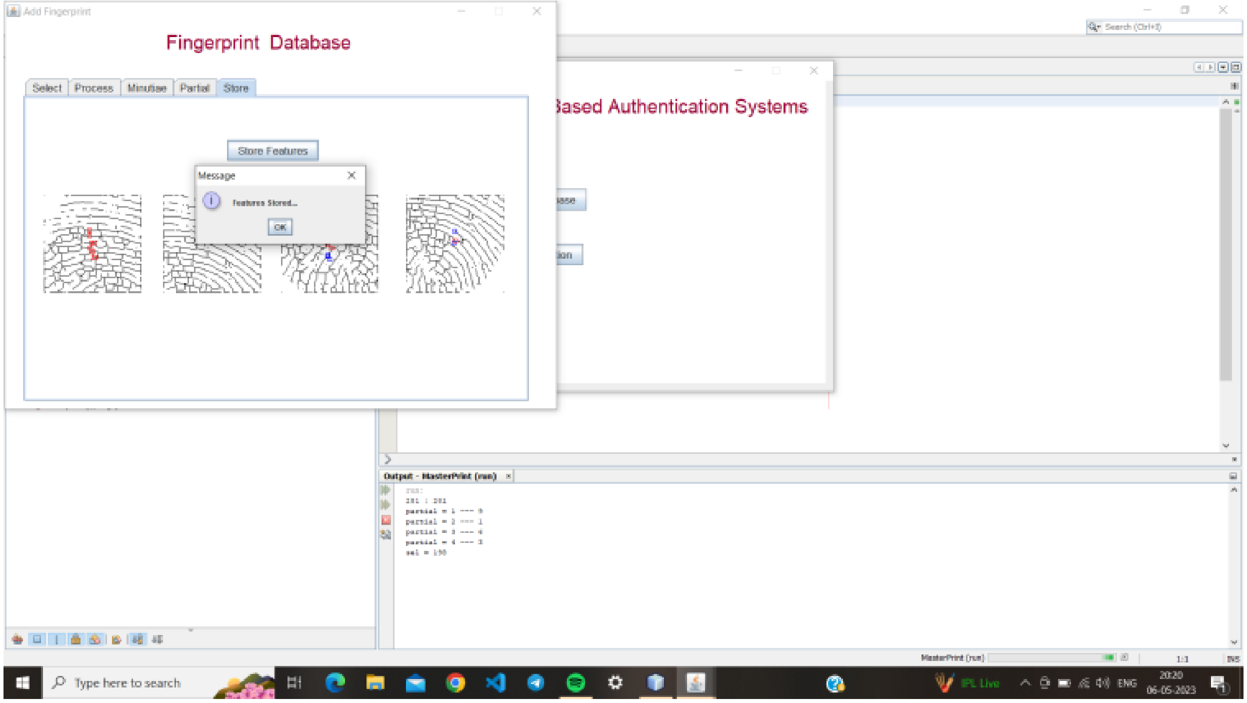
```
run:
281 : 281
```

Figure 6: Minutiae



```
run:
281 : 281
```

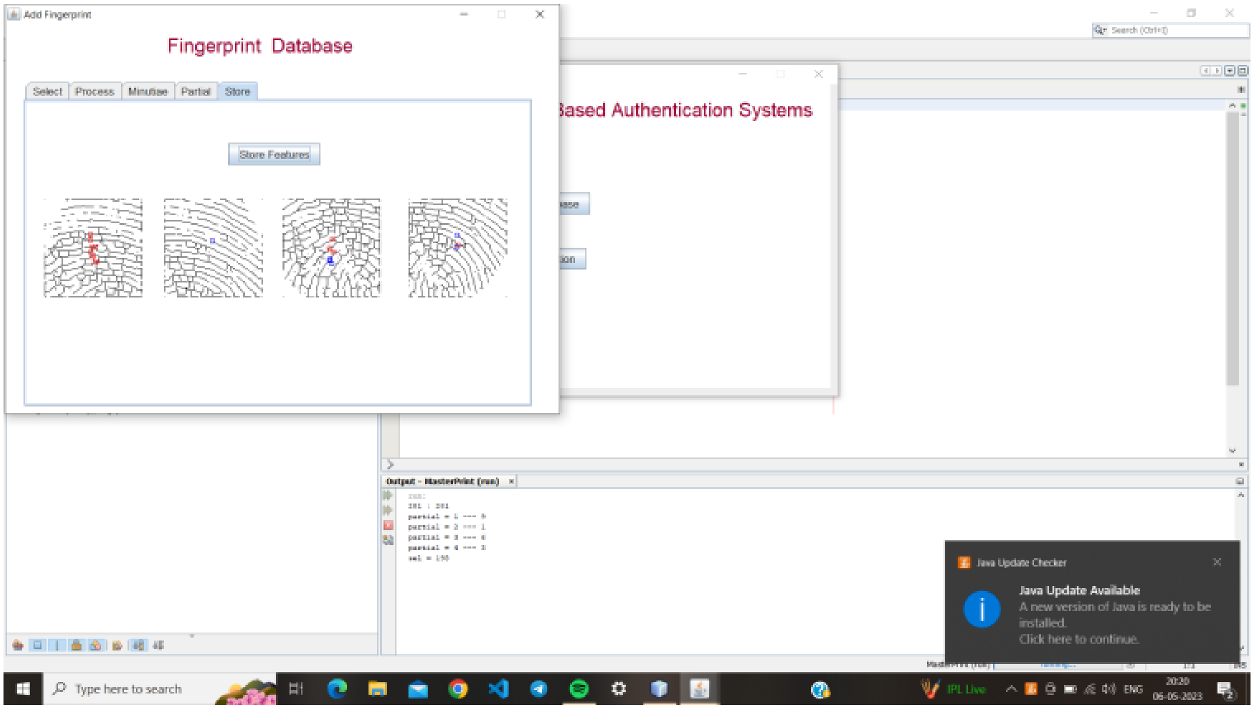
Figure 7: Partial fingerprint



Features Stored...

```
run:
281 : 281
partial = 1 --- 0
partial = 2 --- 1
partial = 3 --- 4
partial = 4 --- 3
sel = 190
```

Figure 8: Store Features

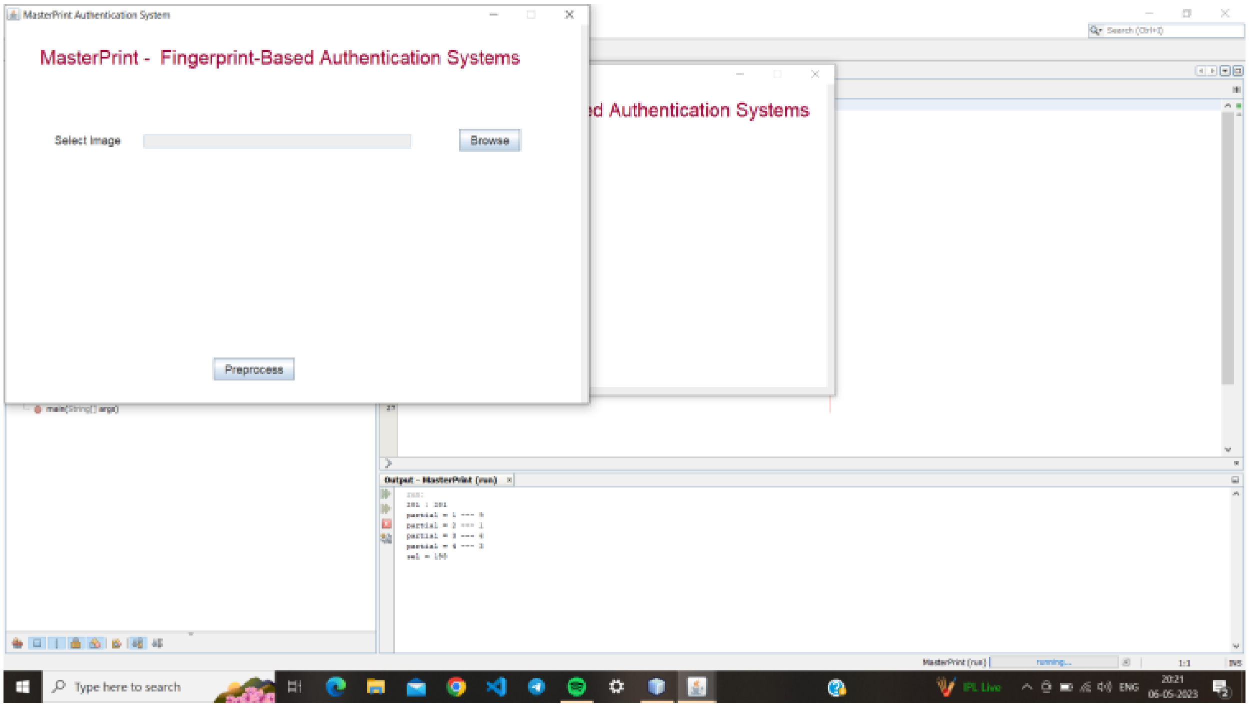


```
run:
281 : 281
partial = 1 --- 6
partial = 2 --- 1
partial = 3 --- 4
partial = 4 --- 3
sel = 150
```

Java Update Checker

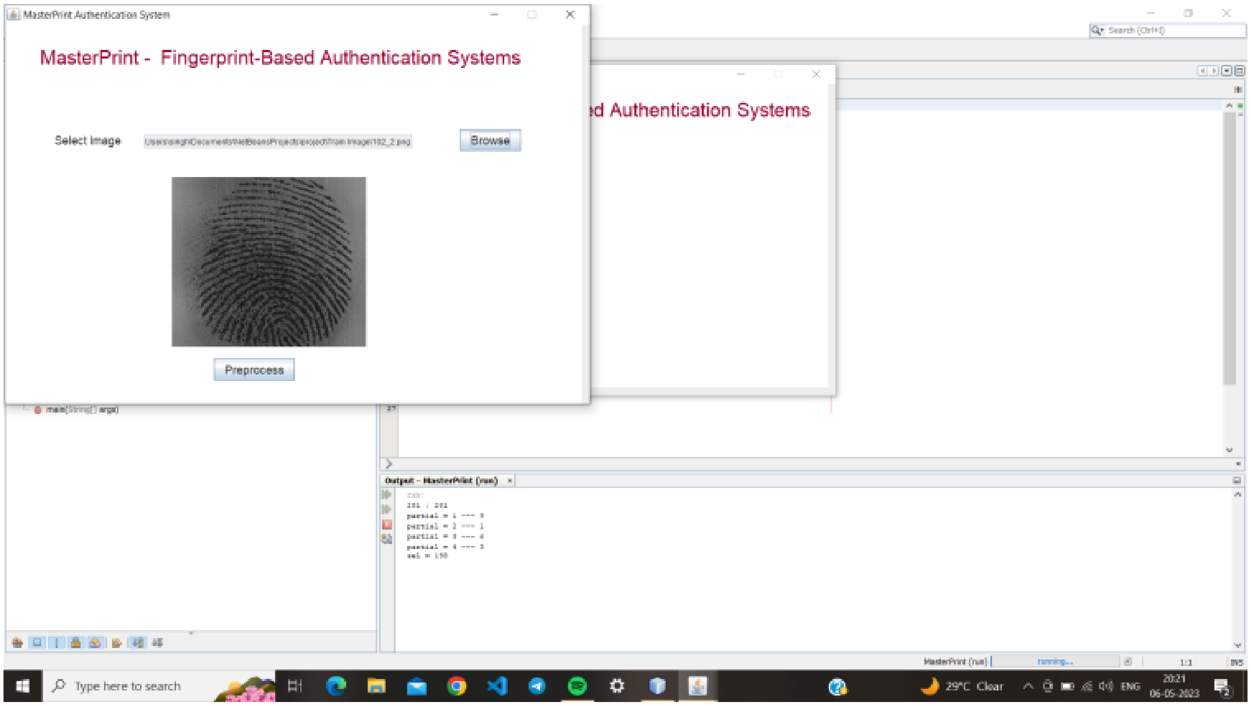
Java Update Available
A new version of Java is ready to be installed.
Click here to continue.

Figure 9: Features Stored



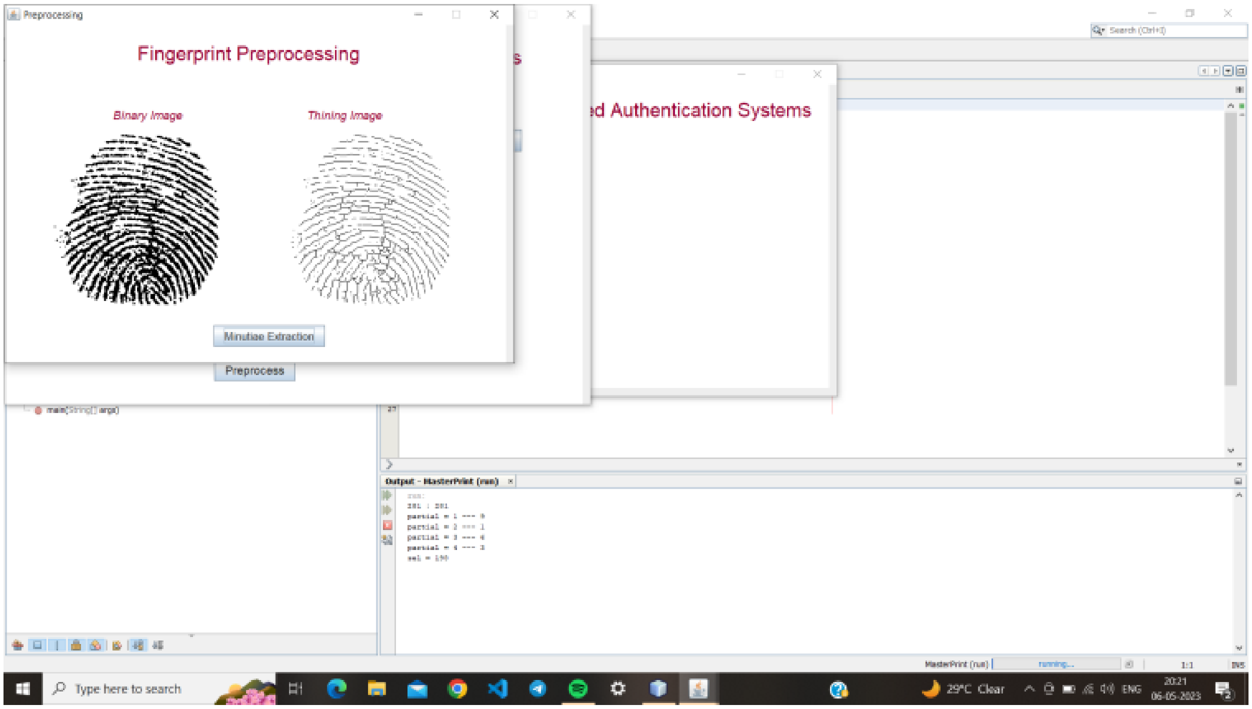
```
run:
281 : 281
partial = 1 --- 6
partial = 2 --- 1
partial = 3 --- 4
partial = 4 --- 3
sel = 150
```

Figure 10: Finger print Authentication


MasterPrint Authentication System
MasterPrint - Fingerprint-Based Authentication Systems
Select Image
Users\singh\Documents\NetBeansProjects\project\Train Image\102_2.png
Browse
Preprocess
Output - MasterPrint (run)
Type here to search
29°C Clear
ENG
20:21
06-05-2023

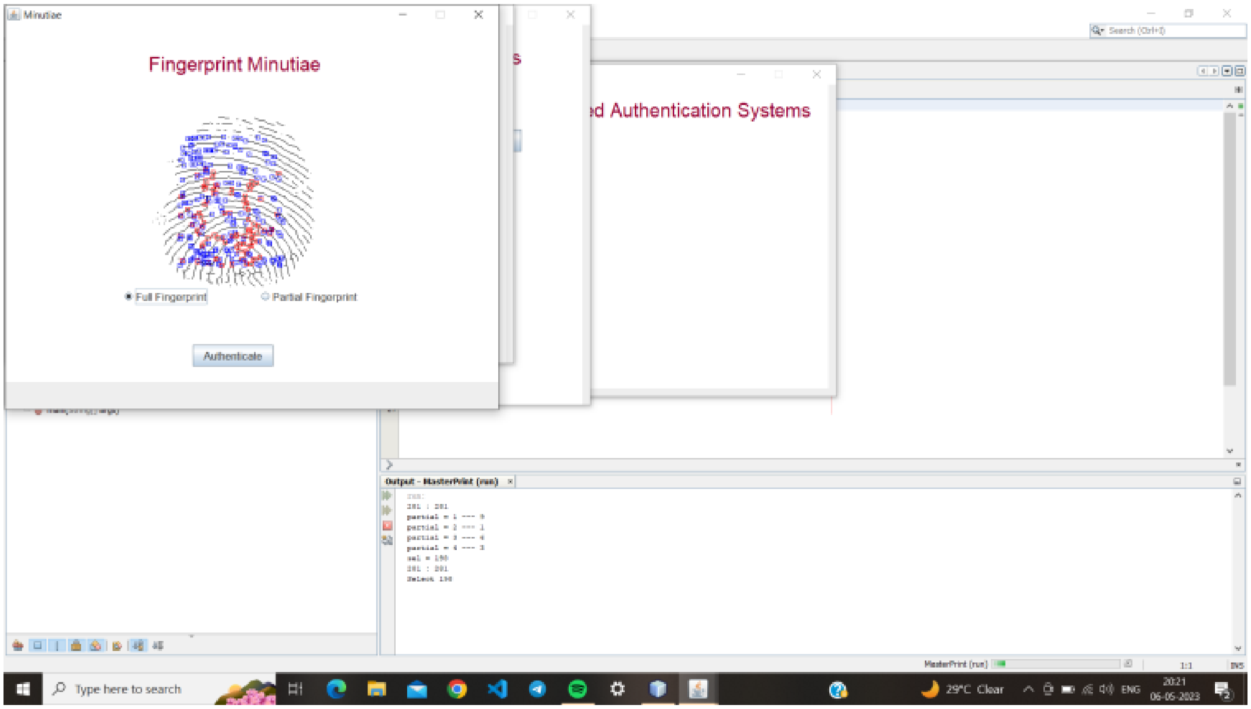
```
run:
281 : 281
partial = 1 --- 0
partial = 2 --- 1
partial = 3 --- 4
partial = 4 --- 3
sel = 150
```

Figure 11: Image Selected



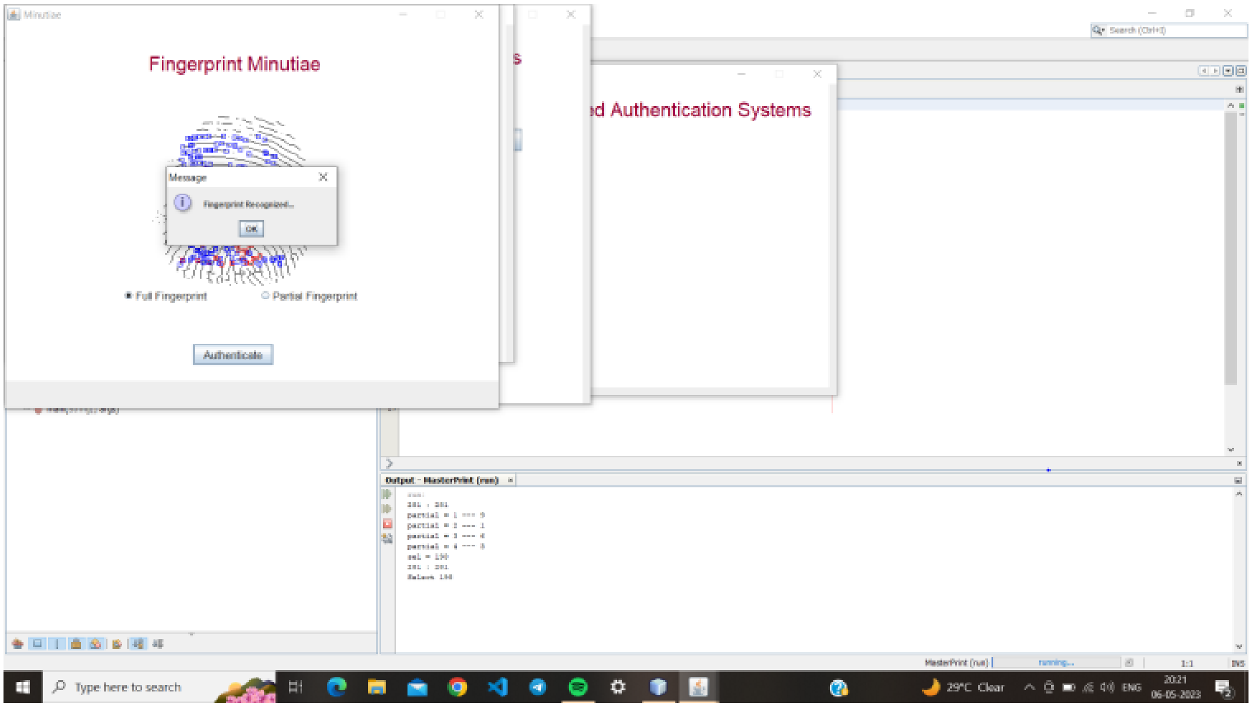
```
run:
281 : 281
partial = 1 --- 0
partial = 2 --- 1
partial = 3 --- 4
partial = 4 --- 3
sel = 150
```

Figure 12: Preprocess Finger print



```
run:
281 : 281
partial = 1 --- 9
partial = 2 --- 1
partial = 3 --- 4
partial = 4 --- 3
sel = 190
281 : 281
Select 190
```

Figure 13: Fingerprint Minutiae



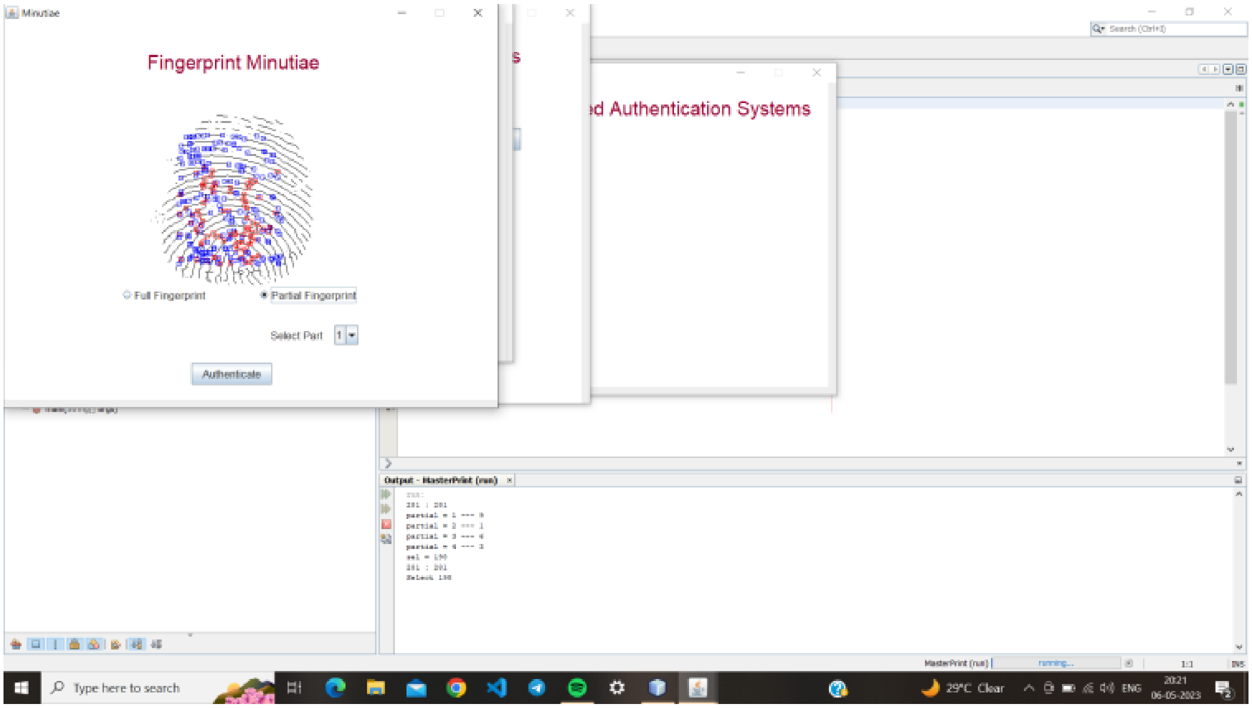
Message

Fingerprint Recognized...

OK

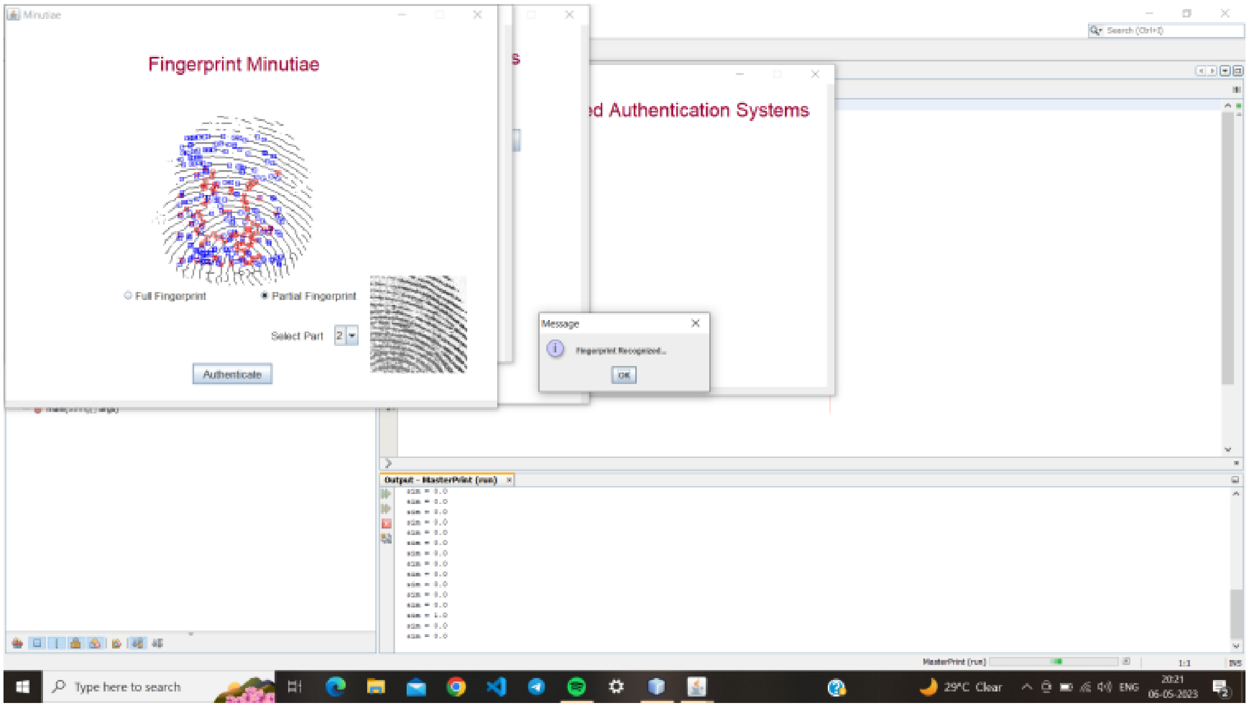
```
run:
281 : 281
partial = 1 --- 9
partial = 2 --- 1
partial = 3 --- 4
partial = 4 --- 3
sel = 190
281 : 281
Select 190
```

Figure 14: Finger print Authenticated



```
run:
281 : 281
partial = 1 --- 0
partial = 2 --- 1
partial = 3 --- 4
partial = 4 --- 3
sel = 198
281 : 281
Select 198
```

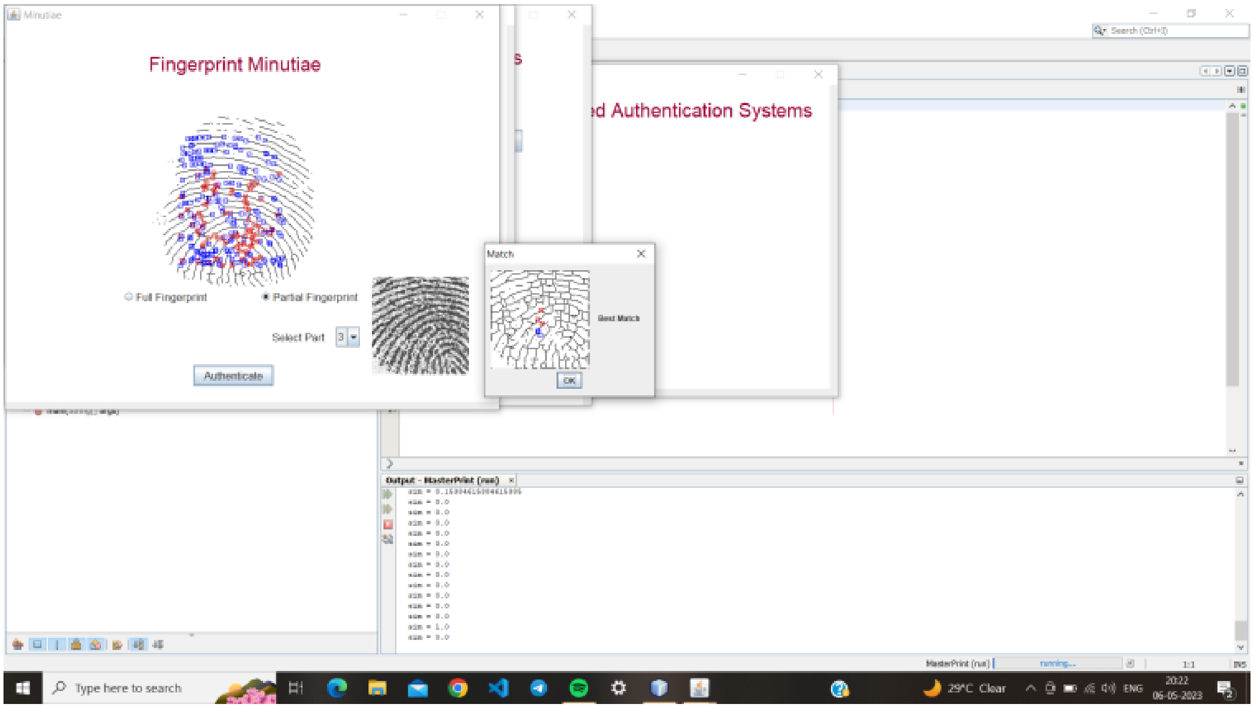
Figure 15: Partial Finger print



Fingerprint Recognized...

```
sim = 0.0
sim = 0.0
sim = 0.0
sim = 0.0
sim = 0.0
sim = 0.0
sim = 0.0
sim = 0.0
sim = 0.0
sim = 0.0
sim = 0.0
sim = 0.0
sim = 1.0
sim = 0.0
sim = 0.0
```

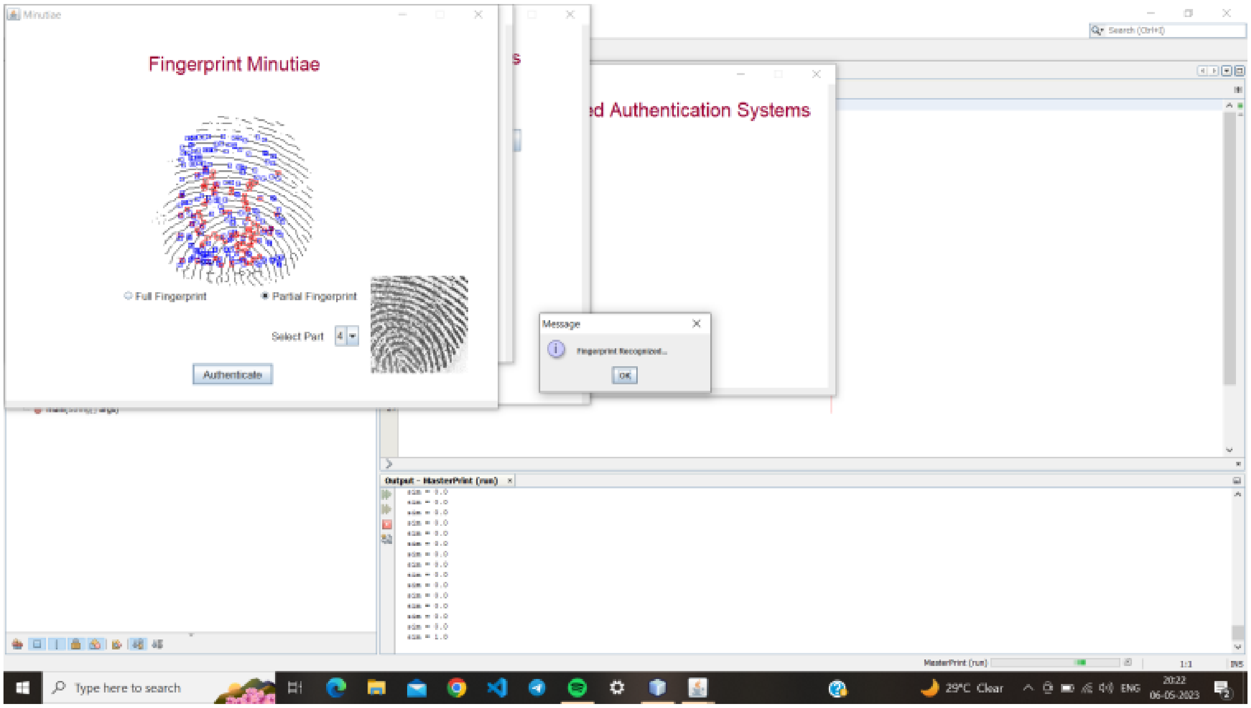
Figure 16: Finger print recognize



Best Match

```
Output - MasterPrint (run)
sim = 0.15384615384615385
sim = 0.0
sim = 0.0
sim = 0.0
sim = 0.0
sim = 0.0
sim = 0.0
sim = 0.0
sim = 0.0
sim = 0.0
sim = 0.0
sim = 0.0
sim = 0.0
sim = 1.0
sim = 0.0
```

Figure 17: Best match partial



Fingerprint Recognized...

```
Output - MasterPrint (run)
sim = 0.0
sim = 0.0
sim = 0.0
sim = 0.0
sim = 0.0
sim = 0.0
sim = 0.0
sim = 0.0
sim = 0.0
sim = 0.0
sim = 0.0
sim = 0.0
sim = 0.0
sim = 0.0
sim = 1.0
```

Figure 18: Finger print recognized

Conclusion:

Fingerprint-based authentication is a highly reliable and secure method for user authentication. It has several advantages over traditional password-based authentication, such as higher accuracy, resistance to phishing attacks, and user convenience. The research on fingerprint-based authentication has explored various aspects of the technology, including its effectiveness in different scenarios, the impact of environmental factors on fingerprint recognition, and the vulnerabilities of the system.

Overall, the research suggests that fingerprint-based authentication can provide a robust security mechanism for protecting sensitive data and resources. However, there are still some challenges that need to be addressed, such as the potential for fingerprint spoofing and the need for continuous improvement in the accuracy and reliability of the technology.

Further research and development in the field of fingerprint-based authentication are necessary to improve the technology's effectiveness, efficiency, and security. With continued efforts, fingerprint-based authentication has the potential to become a widely adopted authentication method for a wide range of applications, from mobile devices to online banking and government services.

Refereces:

1. Cao, X., Cao, Z., and Guan, Y. (2018). “A Survey on Biometric Cryptosystems and Cancelable Biometrics.” IEEE Access, 6, 10252-10272.
2. Jain, A. K., Ross, A., and Nandakumar, K. (2016). “Introduction to Biometrics.” Springer.
3. Karthikeyan, B., and Sathishkumar, V. (2021). “A Comprehensive Study on Fingerprint Biometric Authentication: A Review.” IEEE Access, 9, 63383-63407.
4. Li, J., Tan, T., and Jain, A. K. (2017). “Multibiometric Template Security: Issues, Challenges, and Solutions.” IEEE Transactions on Information Forensics and Security, 12(5), 1112-1132.
5. Maltoni, D., Maio, D., Jain, A. K., and Prabhakar, S. (2009). “Handbook of Fingerprint Recognition.” Springer.

6. Marasco, E., Sansone, C., and Scotti, F. (2019). “A Survey of the Vulnerabilities of MasterPrints-Based Fingerprint Authentication Systems.” IEEE Access, 7, 87329-87345.
7. Nandakumar, K., and Jain, A. K. (2012). “Biometric Template Security.” Handbook of Biometrics, 691-714.
8. Ratha, N. K., Connell, J. H., and Bolle, R. M. (2007). “An Analysis of Minutiae Matching Strength.” IEEE Transactions on Pattern Analysis and Machine Intelligence, 29(6), 917-929.
9. Ruiz-Alba, J., Gallego-Madrid, J., Hernández-Serrano, J., and Skarmeta, A. (2018). “Fingerprinting the Internet of Things: A Survey.” IEEE Communications Surveys and Tutorials, 20(1), 673-700.
10. Yang, M., and Yang, Z. (2018). “A Survey on Fingerprint Template Protection.” Journal of Computer Science and Technology, 33(6), 1117-1145.