Asymmetric Encryption Techniques for Data Embedding and Authentication in Fingerprints Using Eigen Space-Based Modelling

M.Sc. Thesis

Ravi Prakash (31320026)

Guided by: **Dr. Sinnu Susan Thomas**

About Myself

- **Ravi Prakash** - B.Sc. (Hons), and M.Sc. in *Computer Science*
- **Academic Interest, and Experience:**
  - Insight building for real-world problems like COVID-19 using AI/ML
  - Pen-testing & applied cryptography
  - Natural language processing (NLP) for problems like mental health analysis
- **Professional Experience:**
  - Penetration Testing Intern - *Virtually Testing Lab*
  - Blockchain Intern (Security Research) - *Kerala Blockchain Academy*
  - Co-Founder - *Jijeevisha Trust (NGO)*

Areas of Interest

- Cyber Security
  - Application of cryptography in real-world situations
  - Offensive solutions to defend the malware attacks
  - Vulnerability assessment, and source code analysis
- Machine Learning
  - Exploring the scope of explainable AI (XAI)
  - Fuzzy logic for predictive analytics
- Biometrics (fingerprints)
- Security in Metaverse & XR

Publications

- Sharma, A., Dutta, M., **Prakash, R.** *(2023)* ***"Comparative Performance Analysis of ML Algorithms for COVID-19 in India,"*** International Conference on Artificial Intelligence of Things (ICAIoT). ***(accepted)***

- **Prakash, R.,** Anoop, V.S., Ashraf S. *(2022)* ***"Blockchain technology for cybersecurity: A text mining literature analysis,"*** International Journal of Information Management Data Insights. Volume 2, Issue 2.

- Vashisht G., **Prakash, R.** *(2020)* ***"Predicting the Rate of Growth of the Novel Corona Virus 2020,"*** International Journal on Emerging Technologies (IJET). Volume 11, Issue 2.

Prakash, R., Thomas, S.S. (2023) “Asymmetric Encryption Techniques for Data Embedding and Authentication in Fingerprints Using Eigen Space Based Modelling,”

- Applications of fingerprints for biometric data protaction, and information security
- Visual hash for secure data embedding *(Hybrid Fingerprint Orientation Map)*
- Dynamic key-pair generation for identical inputs:
  - to overcome *frequent password updates*
  - for *dynamic data encryption*
- Enhanced authenticity at co-working spaces, and educational institutes
- A better *machine learning classifier* based on *fuzzy logic*

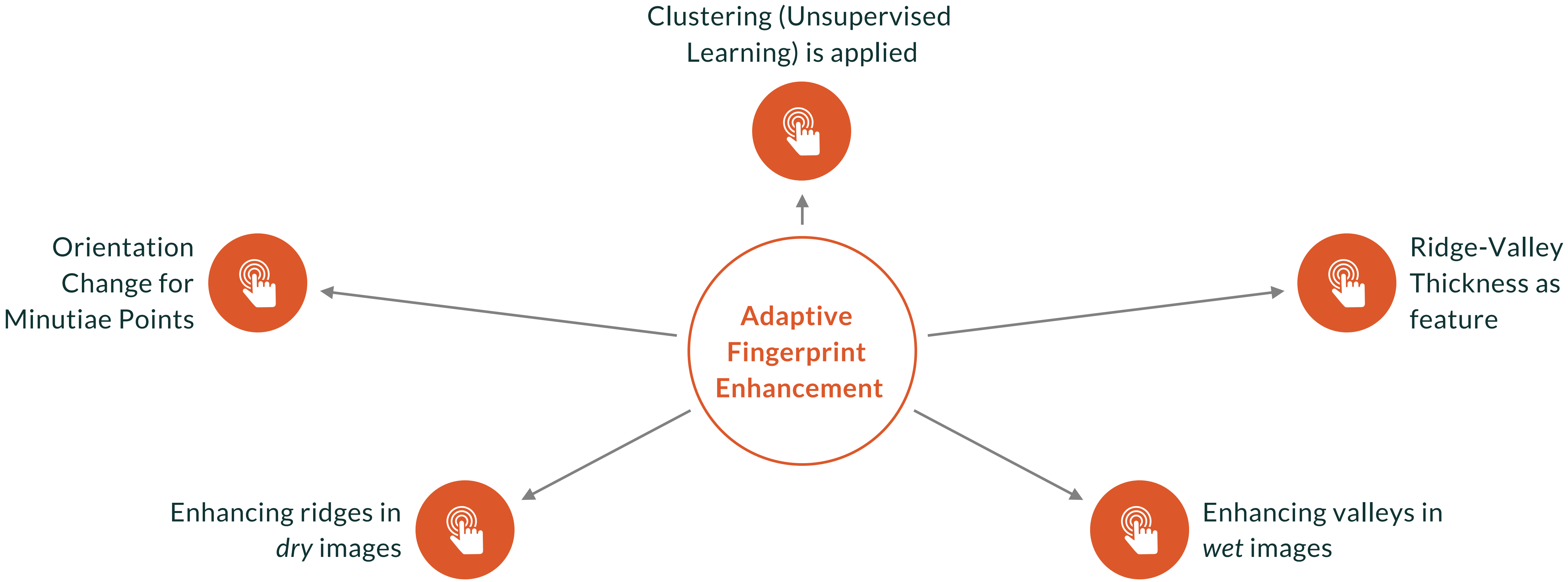
  Overcomes multi-class data imbalance

State of the Art

- **FVC 2000 database** [1] for data security [2] and individual identification [3].
- The **ensemble learners** like Random Forest [4] and Gradient Boost [5]
- Dataset balancing with Synthetic Minority Oversampling Technique (**SMOTE**) [6]
- **Min-cut Max-flow** [7] optimization
- Asymmetric and symmetric ciphers like **DES-L** [8]
- Data embedding matrices like **QR Code** [9]
- Adaptive fingerprint detection based on the **image intensity** & **gradients** [10]

Adaptive fingerprint image enhancementwith fingerprint image quality analysis [10]

Key takeaways



Adaptive Fingerprint Enhancement

Clustering (Unsupervised Learning) is applied

Orientation Change for Minutiae Points

Ridge-Valley Thickness as feature

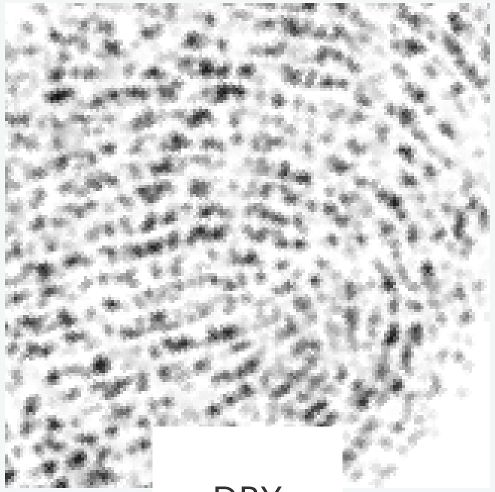
Enhancing ridges in *dry* images

Enhancing valleys in *wet* images

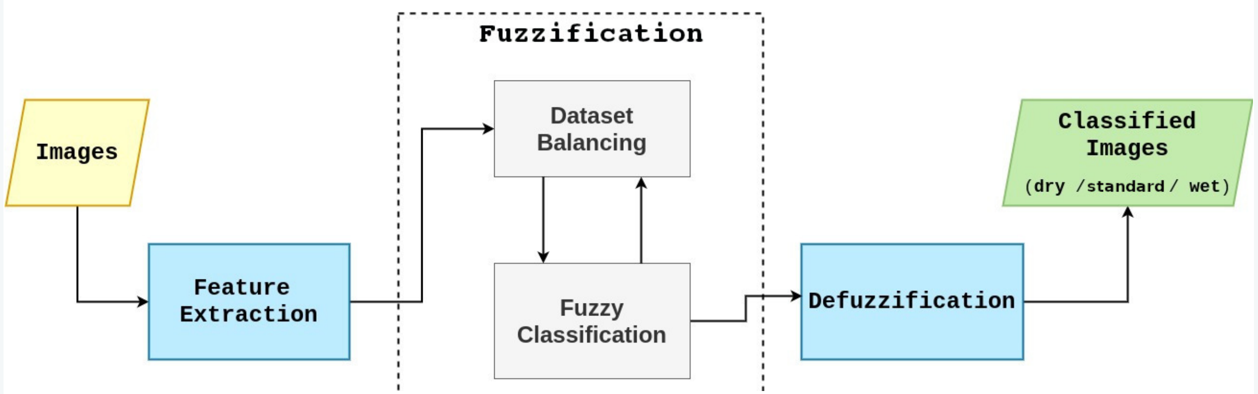
Proposed Methodology

Data Balancing & UC-FLEM

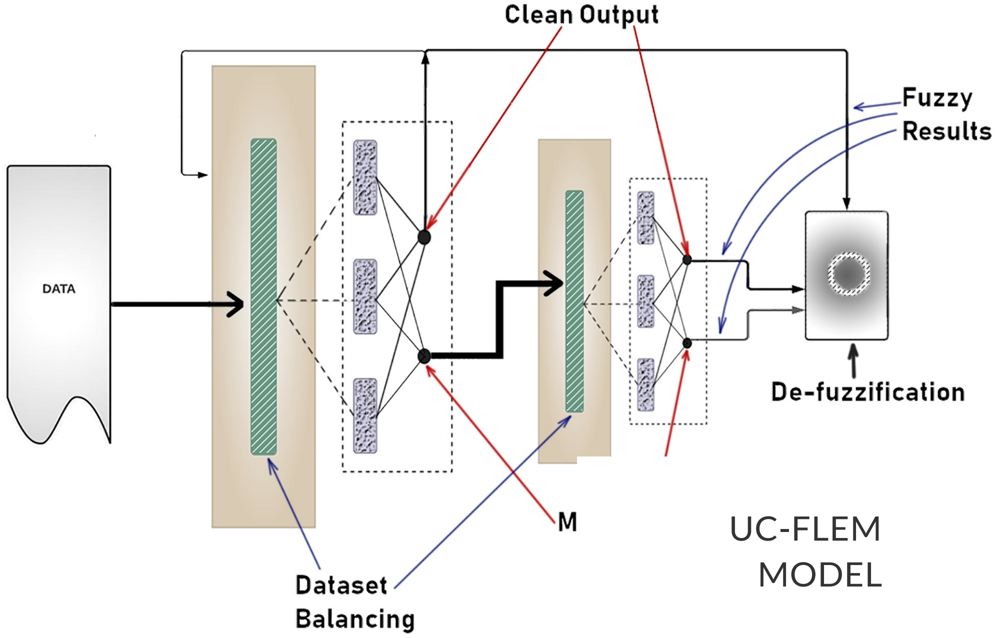
STANDARD



DRY



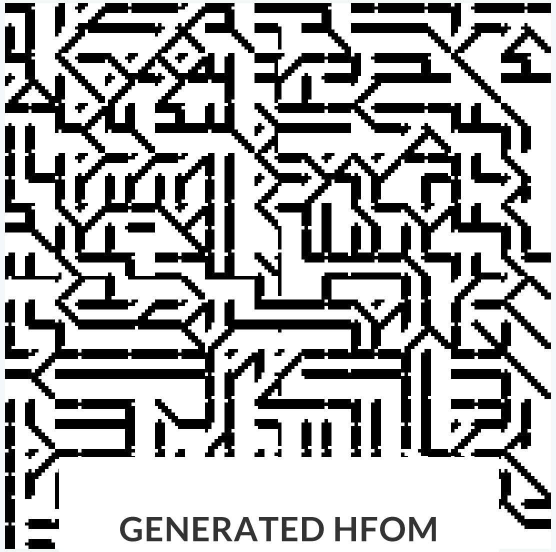
CLASSIFICATION



UC-FLEM MODEL

Methodology cont..

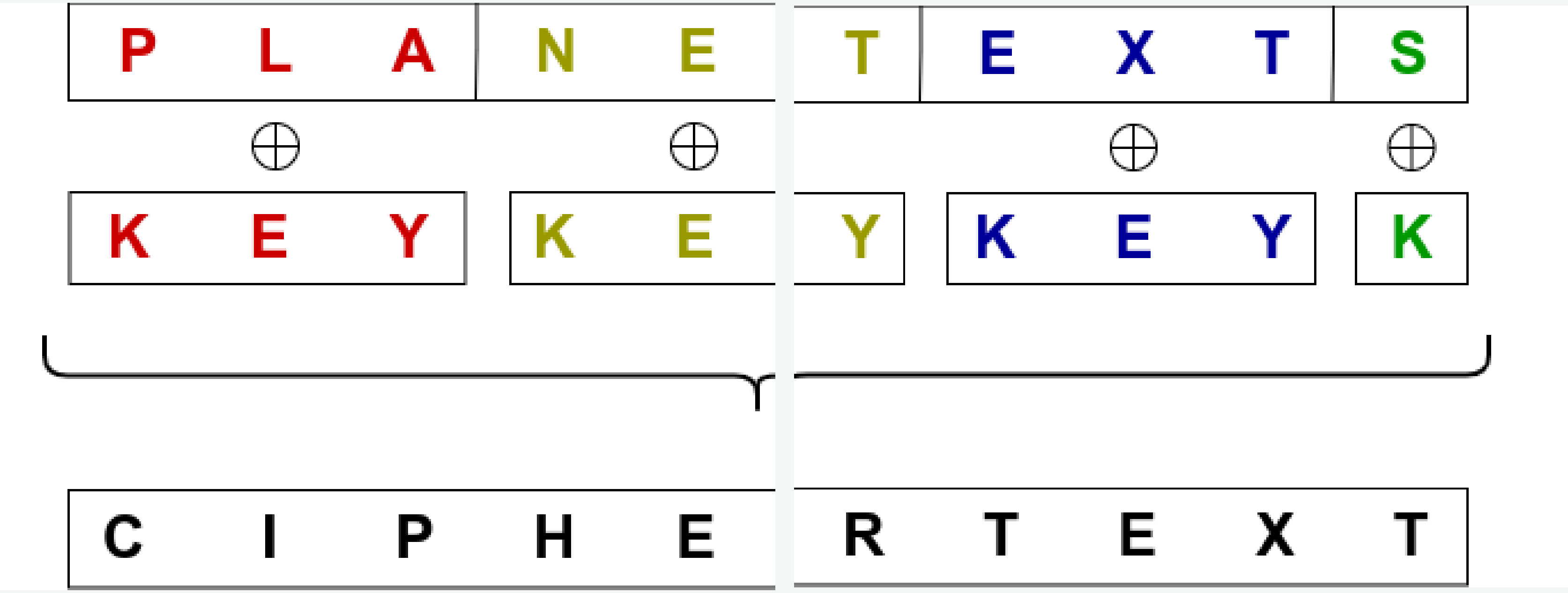
HFOM Generation



GENERATED HFOM

Methodology cont..

Data Security

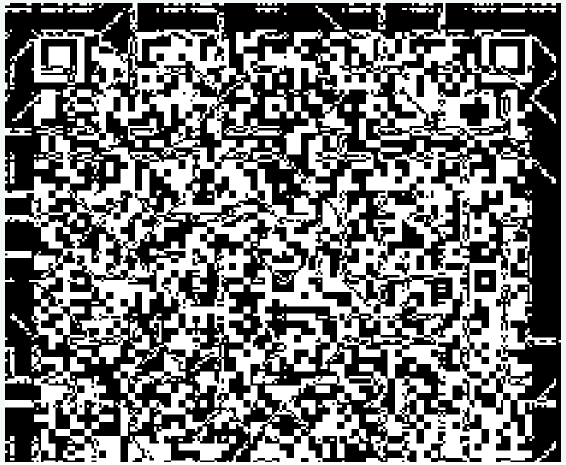


P L A N E T E X T S

⊕ ⊕ ⊕ ⊕

K E Y K E Y K E Y K

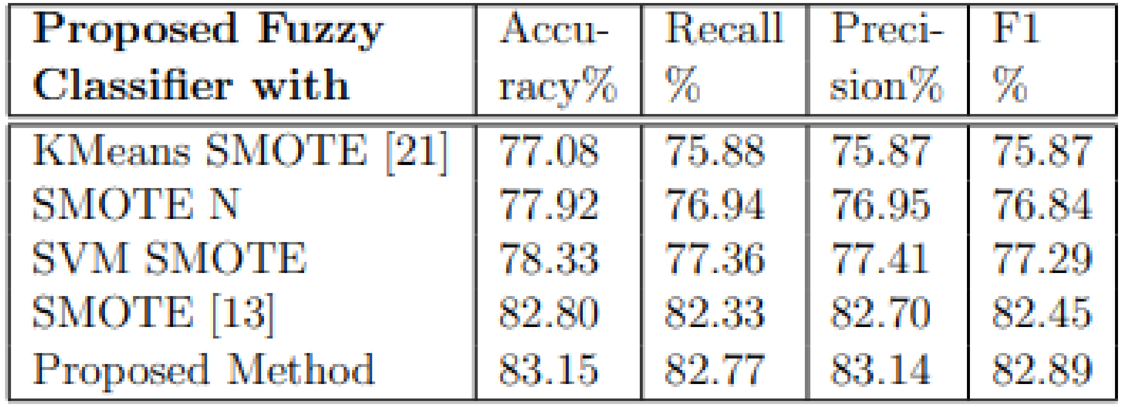
C I P H E R T E X T



ENCRYPTED INFORMATION

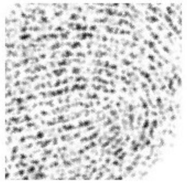
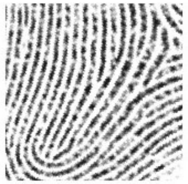
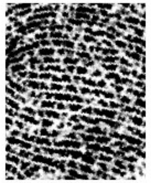
Experimental Results

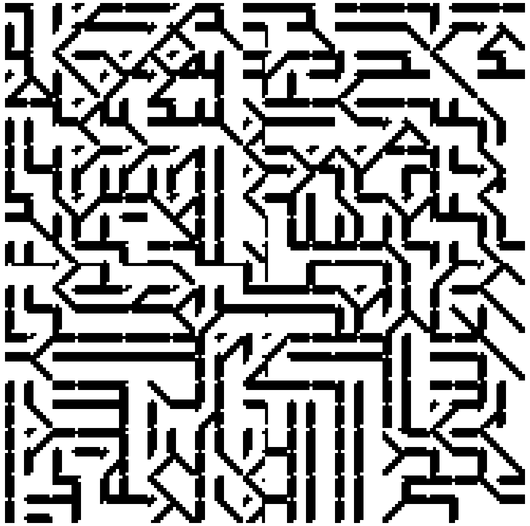
UC-FLEM & HFOM



Proposed Fuzzy Classifier with	Accuracy%	Recall %	Precision%	F1 %
KMeans SMOTE [21]	77.08	75.88	75.87	75.87
SMOTE N	77.92	76.94	76.95	76.84
SVM SMOTE	78.33	77.36	77.41	77.29
SMOTE [13]	82.80	82.33	82.70	82.45
Proposed Method	83.15	82.77	83.14	82.89

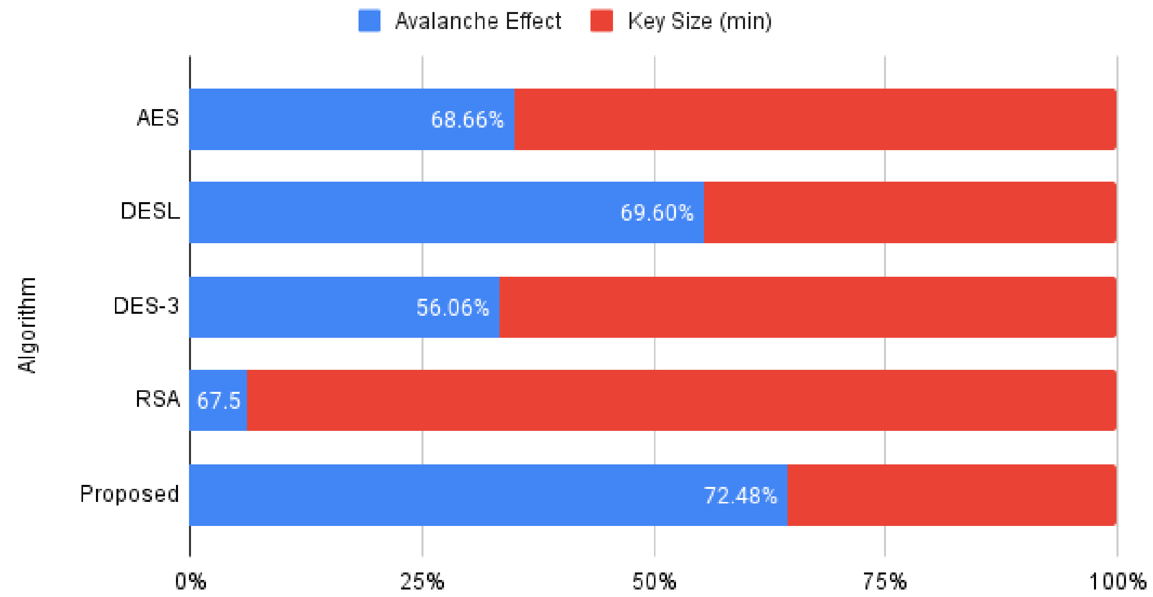
Table 4.3: Performance with different oversampling methods.

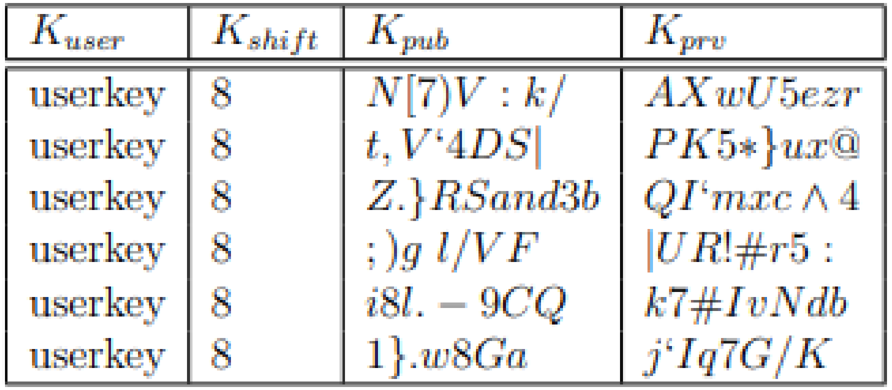
Input Images			
Classified As	DRY	NORMAL	WET



Results cont..

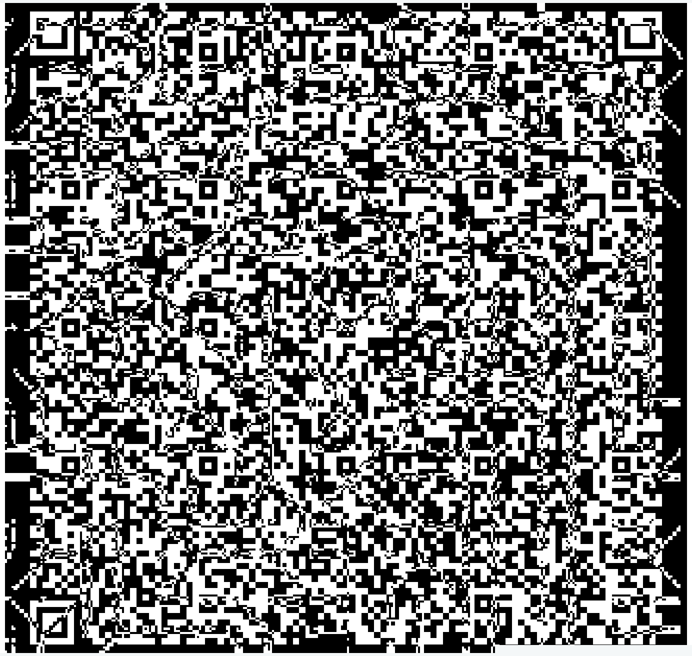
Data Security





K_{user}	K_{shift}	K_{pub}	K_{prv}
userkey	8	$N[7)V:k/$	$AXwU5ezr$
userkey	8	$t,V`4DS\vert$	$PK5*\}ux@$
userkey	8	$Z.\}RSand3b$	$QI`mxc\wedge4$
userkey	8	$;)g\ l/VF$	$\vert UR!\#r5:$
userkey	8	$i8l.-9CQ$	$k7\#IvNdb$
userkey	8	$1\}.w8Ga$	$j`Iq7G/K$

Table 4.7: Samples of public-private key-pairs generated dynamically.



Conclusion

Novel model for **multi-class imbalanced** dataset **Classification** using **Fuzzy-logic** and **Eigen-space Modeling** i.e. **UC-FLEM**.

Enhanced the Orientation Change using **Laplacian filter.**

New feature for fingerprints - *Squared Sum of Ridge to Valley Ratio*, and *Average of Orientation Change*

Embedded data security using **non-reversible HFOM** generation.

Multiple key-pairs for same pass-phrase and new Asymmetric encryption.

Future Scope

Adaptive binarization of threshold can be introduced.

Dynamic password updating and **hot-line** connection establishment.

Using HFOM with RFID cards for attendance systems.

References

[1] University, B. B. (2000). Fvc2000 fingerprint verification competition.http://bias.csr.unibo.it/fvc2000/db4.asp

[2] Ivanov, V. I., & Baras, J. S. (2017). Authentication of swipe fingerprint scanners. IEEE Transactions on Information Forensics and Security (TIFS)

[3] Kumar, A., & Zhou, Y. (2012). Human identification using finger images. IEEE Transactions on Image Processing (TIP)

[4] Breiman, L. (2001). Random forests. Machine Learning

[5] Friedman, J. H. (2001). Greedy function approximation: A gradient boosting machine. The Annals of Statistics, 29 .

[6] Chawla, N., Bowyer, K., & Hall, W., L.O. Kege lmeyer (2002). Smote: Synthetic minority over-sampling technique. Journal of Artificial Intelligence Research

[7] Shi, J., & Malik, J. (2000). Normalized cuts and image segmentation. IEEE Transactions on Pattern Analysis and Machine Intelligence

[8] Bansod, G., Raval, N., & Pisharoty, N. (2015). Implementation of a new lightweight encryption design for embedded security. IEEE TIFS

[9] Yuan, T., Wang, Y., Xu, K., Martin, R. R., & Hu, S.-M. (2019). Two layer qr codes. IEEE TIP

[10] E.-K. Yun, S.-B. Cho, "Adaptive fingerprint image enhancement with fingerprint image quality analysis," Image and Vision Computing, vol. 24, 2006.

Thank You!