Publications Template

#	Research Title	Field	Abstract	Year of Publication Publishing	Publishing Link "URL"
1	Efficient spam and phishing emails filtering based on deep learning	Deep learning, NLP, machine learning	Nowadays, spam emails represent a severe threat to security and cause a big waste in transmission time and users' time spent in browsing unsolicited bulk emails (UBE). This is in addition to a lot of bandwidth and large severs storage consumed by these spam emails, resulting in financial losses for organizations and annoying individual users. Another type of malicious emails is phishing emails, which aim to get sensitive information from users leading to credential theft. This forms a challenging threat in the cyberspace. Many machine learning (ML) approaches are used to classify emails as ham or spam emails. In this paper, a deep learning model is introduced that showed improvement in performance compared to state-of-the-art related studies. Three benchmark datasets are employed in our experiments, which include content-based features rather than text analysis techniques that may consume more time. Our classifier is used to discriminate between three classes for more general spam filtering. Different performance	2022	Efficient spam and phishing emails filtering based on deep learning - ScienceDirect

			measures are used for model validation and testing. Moreover, the time consumed in both offline training and online detection stages is reported. The proposed classifier is designed with an eye on the validation accuracy achieving fast and competitive performance promoting its use in practical applications. A comparative study is presented to show that our work outperforms recent related studies.		
2	Privacy preserving search index for image databases based on SURF and order preserving encryption	Image Processing, Cryptography	Managing large personal image databases requires efficient privacy preserving indexing methods to allow for their outsourcing to possibly curious cloud servers. To construct a secure inverted index in this paper, first, visual words are extracted from stored images based on the Speeded-Up and Robust Features (SURF). Next, Order Preserving Encryption (OPE) is used to encipher the frequencies of occurrence of the extracted visual words. Another scale and rotation invariant feature, which is the local HSV histogram, is included for comparison. From the obtained results, it is apparent that SURF achieves more precise results. Aggregation of both features is considered to further improve the accuracy. The effects of the weighting scheme of the visual words and their number on the performance are investigated. Weighted term frequency inverse document frequency (tf-idf) together with the Jaccard similarity measure yield the best	2020	Privacy preserving search index for image databases based on SURF and order preserving encryption - Magdy - 2020 - IET Image Processing - Wiley Online Library

			performance. OPE encryption is shown to have minor impact on the retrieval accuracy. To reduce encryption time, a lookup table is constructed. The inverted index reduces the search time significantly compared to a sequential search scheme as apparent from the results. A comparative study with recent related schemes demonstrates the competitiveness of the implemented system in terms of computational efficiency and accuracy.		
3	Effect of chosen features on performance of privacy preserving image retrieval systems	Image Processing, Cryptography	A huge amount of personal multimedia data is generated daily and stored on cloud servers. This data needs to be secure from curious servers, while also being searchable by them. The visual features used in a content-based image retrieval (CBIR) system are encrypted to ensure privacy of the cloud users. This paper aims to investigate several features for use in building a privacy-preserving CBIR system. These features range from simple and fast statistical bit plane distribution features to the more sophisticated local features such as Speeded-Up and Robust Features (SURF). Moreover, both series and parallel aggregation approaches of combining several features are studied to improve retrieval efficiency. Feature vectors are encrypted using distance-preserving techniques. The accuracy of the retrieval system is examined under different combinations of encrypted visual	2019	Effect of chosen features on performance of privacy preserving image retrieval systems - ScienceDirect

			features. The results are insightful offering interesting trade-offs between security, computational efficiency and accuracy.		