ISSN: 2182-2069 / E-ISSN: 2182-2077

Safety in Connected Health Network: Predicting and Detecting Hidden Information in Data Using Multilayer Perception Deep Learning Model

Dr.A.M. Adeshina[1*], S.O. Anjorin[2], and Dr. Siti Fatimah Abdul Razak[3]

[1*]Faculty of Information Science and Technology, Multimedia University, Malaysia.
am.adeshina@mmu.edu.my, codedengineer@yahoo.com, https://orcid.org/0000-0002-9919-5367

[2]High Performance Computing Research Laboratory, Nigeria. anjorin.so@hpc.com.ng,
https://orcid.org/0009-0002-9559-2899

[3]Faculty of Information Science and Technology, Multimedia University, Malaysia.
fatimah.razak@mmu.edu.my, https://orcid.org/0000-0002-6108-3183

Received: July 23, 2024; Revised: September 4, 2024; Accepted: October 3, 2024; Published: November 30, 2024

Abstract

With the tremendous growth in the use of information technology, the connected health networks are becoming more relevant, greatly improving the traditional standard of healthcare procedures from data acquisition, storage, and sharing among the medics for timely clinical diagnosis processes, therapy, and disease management. However, connected health network comes with network and cyber criminality challenges, and frequent security breach attacks on digital platforms and databases. Unfortunately, Sensitive clinical information is greatly at risk with adversaries, most clinical stakeholders find it difficult to overlook free access to the clinical records. Previously, feature aggregation networks, convolutional neural networks, residual convolutional neural networks, and machine learning models were used in different methodological approaches towards ensuring the detection of hidden information in images, unfortunately, none was able to produce optimal results. This study proposes a three-phased framework to determine the suitability of embedder networks' feature extraction for image steganalysis, predicting and detecting hidden information in images. A Multilayer Perceptron (MLP) deep learning model was trained for pattern recognition of steganography instances in acquired digital image signals. The digital image signals used for the predictive steganalysis are publicly available images contained in two circumstances highlighted regarding clean image signals (situation of cover images, but without steganography) and the embedded situation of image signals (where images (stego) with hidden data or information). Interestingly, the results of the parameter show that the Max-iter parameter of the MLP classifier hugely determines the performance of the algorithm towards detecting steganography in digital image signals. The parameter stipulates the number of times the training set will pass through the MLP network for the training process. Significantly, in our experiment, Max-iter returned the best result at 1000 netting an accuracy of 93%, precision of 57%, and recall of 100% weighted averages. Our study does not only implement a model that detects hidden information in images, but it also discovered and tuned the multilayer perceptron to determine where it will perform best.

Keywords: Deep Learning, Feature Extraction, Steganalysis, Multilayer Perceptron.

Journal of Internet Services and Information Security (JISIS), volume: 14, number: 4 (November), pp. 524-541.
DOI: *10.58346/JISIS.2024.I4.033*

*Corresponding author: Faculty of Information Science and Technology, Multimedia University, Malaysia.

1 Introduction

The data and information stored in a database may be greatly impacted by human error. Human errors are frequently the most difficult challenges in data and information security. Uninformed or ignorant workers may perhaps into the use of weak passwords, may erase data mistakenly, even be a victim of phishing schemes, have privileged account access and visit unsuitable websites. Companies need to put together a group of security specialists to conduct awareness or training campaigns, which will empower staff members and lower the possibility of data and information theft. The usage of data loss solutions can also help prevent end users from leaking sensitive data either purposefully or by mistake. These listed challenges observed in the usage of conventional data security measures has thus made it necessary to seek a more improved and better alternative to the security of data and information (Mathew & Asha, 2024; Mohandas et al., 2024). This improved alternative is the introduction of data and information hiding technique known as steganography (Krishnan et al., 2022). Following the kind of cover object being used, Steganography may be categorized into textual, imagery, audio, video and protocol steganography. Steganography aims to securely hide messages (information) so as to complicate situation for attacker. The application of a steganography and a dual layer encryption provides a more secure approach for information transmission in a cloud computing environment.

Image data that is frequently exchanging hands on the internet need to be subjected to forensics to detect the possibility of malicious messages in what is referred to as image steganalysis (Odeh & Taleb, 2023). Steganography is used to securely hide messages (information) such that the attacker does not detect the presence of any message in the cover object being used (Wan & Hu, 2024). This study investigates the extent to which parameter optimization would improve steganalysis performance using predictive analytics and the extent to which deep ensemble learning would influence steganalysis performance metrics using predictive analytics. More efforts were to investigate image embedding networks' expertise in detecting steganography in digital images. More efforts would also be on establishing embedder networks' feature extraction's stability for image steganalysis, which deviates significantly from the literature trend. This study employs a three-phased framework that aids digital forensics by predicting blind steganalysis. This study employs Multilayer Perception Deep Learning (MLP), a machine learning model to execute image steganalysis for digital forensics using feature engineering techniques, including parameter optimization and feature selection. The public datasets employed in the study were trained with deep learning algorithms in an ensemble methodological approach. The model was then tested and evaluated to ascertain its performance through benchmarking with existing state-of-the-art.

Detecting and Predicting Hidden Information in Data

Several studies attempted to create an application to detect steganography. Zou and the team in 2019 filed gaps in the literature concerning feature expression (Zou et al., 2019). They proposed a new steganalysis paradigm in which feature learning is viewed as a critical impetus for ensuring an effective steganography detector. The purpose of the submission was to innovate the steganalysis paradigm concerning the functionality of in-depth learning. The study presented a model that was planned and tuned to the characteristics of steganalysis. This was thought to make the model more effective at detecting statistical features like neighborhood correlation.

According to (Yedroudj et al., 2018), a CNN fortified with error probability in continuation of an existing study focusing on state-of-the-art techniques is more resourceful. The study employed five convolutional layers, including a Batch Normalization connected with a Scale Layer, as well as the use

of appropriately sized fully linked sections. The study used an amplified database to improve convolutional neural network training. The model was evaluated with S-UNIWARD and Wavelet Obtained Weights (WOW) embedding algorithms while subjecting its performance metrics to three methods including an ensemble classifier and two other steganalyzers. No parameter optimization is employed on the neural network is a weakness of the study.

Furthermore, Qian et al., (2018) provided a review of the steganalysis concept of feature learning using convolutional neural networks, concentrated on traditional steganalysis with handcrafted features. To enable the convolutional network on image inputs, a cropping strategy was also used. Unfortunately, no parameter optimization is employed on the neural network.

Jang et al., (2020) proposed a feature aggregation-based steganalysis network, including the use of a fixed preprocessing filter with the disadvantage of using a limited number of extracted features from the input images. As a result, the study increased the channels number in the blocks of convolutional that are close to the input data. It also aggregated feature maps of various levels and resolutions by utilizing rich information to improve the steganalysis model's performance. The study used the capped activation function to obtain better oversimplification performance on the JPEG quality factor 75 and 95 as the training set.

In 2019, Saito et al., (2019) investigated the likelihood of recognizing the locations of embedded data through steganography if the given image is allegedly suspected to be a *stego* image, to reaffirm the decision of the first level steganalysis and determine the magnitude of the embedded data. The study employed 'F5' as the steganography approach, utilizing 50% of the concealable information from the dataset to create a *stego*. For the study, three hundred and seventy images were chosen at random from the HDR Burst dataset. Each of the 370 images was arranged into sub-groups that were made up of 64 × 64 pixels, totaling 94,720 training and test sets altogether fitted on a multilayer perceptron. The strength of the study was the novelty of predicting the location of *stego* using a heat map and deployment of deep learning MLP algorithm. However, having weaknesses of non-implementation of the bias-variance tradeoff in the model and no parameter optimization employed on the neural network. Also, the study of Zhang and the team in 2018 attempted to solve existing gaps in steganalysis including working closely on the ratio of noise in the signal and as well as trying to steganalyze images of random dimensions (Zhang et al., 2018). This became expedient because some algorithms seek fixed size images as input with low precision output due to the underutilization of noise figments occasioned by feature extraction. The study therefore designed an enhanced convolutional network structure tailored towards CNN to solve the aforementioned gaps. The study used a 3 by 3 kernel in place of the traditional 5 by 5 and likewise optimized convolution kernels in the preprocessing layer. The study used smaller convolution kernels to decrease parameter numbers while modeling the features in small local regions. Spatial pyramid pooling (SPP) was implemented in the study to combine local features which enhances the demonstrative aptitude of the features. Similarly, data augmentation was employed in the study to further improve network performance with the use of feature learning as a means of feature engineering. Unfortunately, no parameter optimization employed on the neural network was a weakness.

The study of (Ye et al., 2017) presents an approach using a convolutional neural network representing an alternative approach to the concept of steganalysis relative to digital images. The approach was considered simple and resourceful in a unified framework. Moreover, the approach can learn hierarchical illustrations directly from raw images. Instead of using a random approach, weights in the first layer of the CNN were modified with the high-pass filter set used for residual map calculation in a spatial rich model. The model was strengthened by the use of a truncated linear unit and deep machine learning. The

model's neural network has no parameter optimization and has the weaknesses of an ensemble of deep learners.

The study of Zeng and the team in 2020 investigated a halftone image steganalysis as well as the influence of a Gaussian filter on image steganalysis (Zeng et al., 2020). A novel residual convolutional neural network with *stego-signal* diffusion was used. To diffuse the *stego-signal* with its neighboring pixels, the image was preprocessed with the inverse halftonic. As a result, the disparity between the cover and *stego* image was amplified on the textual, and the residual block was used to build the neural network model. This is thought to preserve the *stego-signal* better than a conventional network. Precision in the detection is improved by the magnified difference and deep learning enhances the performance of the model. Park & Cho, (2020) provided an overview of a steganography of automated image related detection system for the Kakao Talk Instant messenger. The study developed automated framework for detection of steganographic images in digital forensics, and gathered and examined image files from Social Network Service (SNS) chat rooms, which were open image steganography tools. The proposed framework was implemented on two Stegano and Cryptosteganography tools based on the KakaoTalk SNS messenger in the study. No parameter optimization is employed on the neural network, however, deep learning is expected to return a better result.

Cyber Security Issues in Connected Health Networks

Healthcare has been benefiting immensely from Connected Network paradigms being a viable alternative approach to the traditional concept of the healthcare system, although with sacrificing computational cost and a greater potential of breach of privacy (Veera Boopathy et al., 2024). Consequently, researchers' attention has been on looking into the best approaches to ensuring Connected Health Network is conveniently and affordably available to medics in facilitating reliable connectivity between hospitals and physicians thereby improving clinical collaborations. One of the outstanding contributions to resolving the challenges in Connected Health Network is the submission of (Adeshina & Hashim, 2017). The study proposed a secured framework that was evaluated as resourceful for connected health networks. The framework was outstanding in its performance when experimented with, for the diagnosis of radiological datasets. Experiments confirmed the framework fast-processing with ordinary regular hardware and software ensuring greatly lower computational cost. Though it was a notable contribution, the approach missed out on the beauty of artificial intelligence concepts thereby limiting its future usefulness.

For the fact that the concepts used in the development of connected health networks subsequently determine the possible approach for tackling observed challenges, Boudouaia et al., (2020) proposed a unidirectional hash function (cryptographic tools) for the rank-related attack which was considered one of the most challenging cyber-attack related to the routing protocol for Low Power Network (RPL). Similarly, to strengthen the network, multilayer detection for selective forwarding was proposed for the detection of network layers including the MAC pool IDs layer, rule-based layer, and anomaly detection layer (Alajmi & Elleithy, 2016). Mehetre et al., (2019) likewise presented a two-stage security solution for selective forwarding attacks and block hole attacks on connected networks using data packets in different distribution routes and Elliptic Curve Cryptography (ECC). A sinkhole attack was detected using a proposal approach from (Esiefarienrhe et al., 2022), a cross-layer design solution following the understanding fact that in order to ensure efficient transmission of packets in connected networks both the security and the Quality of Services (QoS) improvement are required. The study ensured the protection of the network from Sinkhole attacks while also improving the jitter, delay, and network throughput. The study (Chung & Park, 2019) a submission, submitted the existence of healthcare

networks in broadband communication infrastructure, and proposed a better approach to paying attention to QoS such as response time and delay.

Fingerprint mechanism-like were used (Sánchez et al., 2021) to possibly defend circumstances of value assignment in order to identify those entities requiring data in connected health networks. Cybertext-Policy ABE (CPABE) (Alshehri et al., 2012), Homomorphic Encryption in its full form, and machine learning which was based on clustering techniques were proposed in (Alabdulatif et al., 2019), CP weighted ABE was proposed, and used to secure data security with weighted attributes (Li et al., 2021) among other research works previously proposed in an attempt to tackle the security issues in connected health network. Unfortunately, despite all efforts so far, according to (Singh & Chatterjee, 2023) the following research problems remain significant challenges:

1. The lack of uniformity among connected devices reduces the accuracy of data.
2. Massive data being transferred and stored can be hacked and misused.
3. The cost in terms of communicational and computational costs is very high for constrained devices.
4. High latency and response time degrade the QoS parameter in the cloud-based healthcare system.

With this study, we have therefore proposed and implemented a three-phased framework to aid digital forensics through predictive of blind steganalysis, targeted at resolving those significant challenges in connected health networks.

2 Material and Methods

A three-phased framework was implemented for this study to aid digital forensics through the prediction of blind steganalysis. The digital image acquisition, the Feature Extraction phase, and the concluding phase, the Steganalysis Predictive Analytics with MLP.

Phase 1: Digital Image Acquisition

This study employs public image signals from two circumstances, clean image signals (situation of cover images but without steganography) and the embedded situation of image signals (where images (*stego*) with hidden data or information acquired for forensics (Corum et al., 2020). The public set contains 4319 cover images and 4013 of *stego* tagged images formatted with JPG-embedded extensions, all amounting to 8332 input signals in total, for the study. The entire 8332 public sets were used in the analysis for mining of numeric image descriptors for mining of numeric image descriptors (numeric vectors), which were then concatenated to form the labeled training set for this study's supervised learning model. In figure 1 shows the proposed framework.

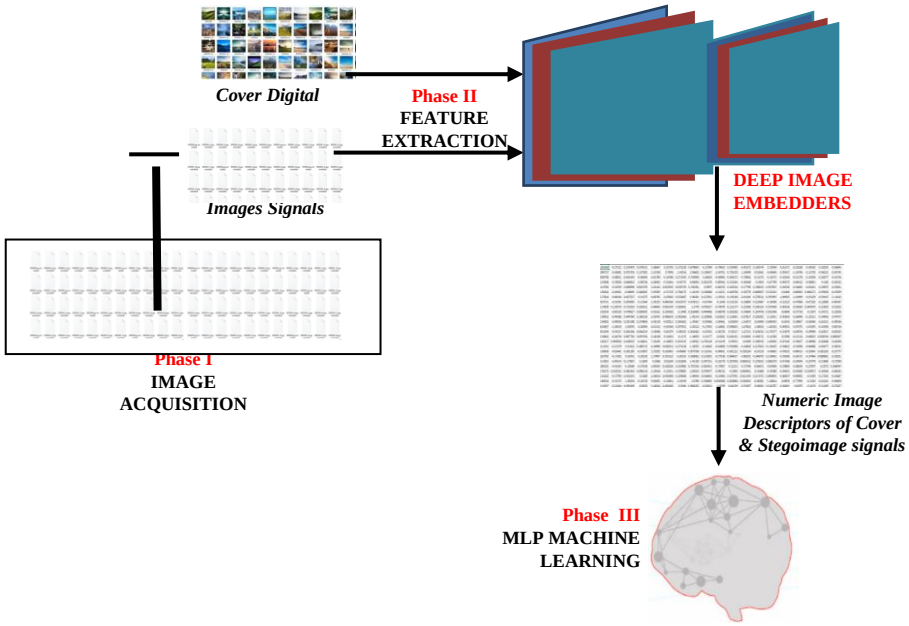


Figure 1: The Proposed Framework

Phase II: Feature Extraction

Numerical image descriptors are extracted using image embedding networks in this conceptual framework. Using image embedding to extract features entails feeding the cover and stego image signals into deep learning models that have already been trained to obtain vector representations of the actual inputs, which serve as the images' numeric descriptions. Transfer of learning is used to carry out the extraction procedure on a local server or on a dedicated digital server. After successfully extracting numeric descriptors out of the cover and stego digital images, then, numeric vectors from both versions are encapsulated and labeled as positive (stego) or negative (cover). Each deep embedder is described in detail below:

i. **SqueezeNet**: In this case, with the deep neural network vector attributes were returned on marked image instance using the deep neural network SqueezeNet 1000-no numeric, representing negative as well as positive staganography instances. SqueezeNet, when compared to other deep embedders, is fast. For image recognition, it is also a small embedder having fewer computational challenges. Following the pre-training of the model on imageNet, archiving AlexNet-level accuracy with 50X fewer parameters, swapping 3 x 3 filters for 1 x1 filters was accomplished. The remaining 3 x 3 filters, as well as the network's late down sampling, achieve input reduction.

ii. **InceptionV3:** The batch normalization layers, factoring convolutions with larger spatial filters are integrated in the architecture, which resulted in tremendous computational efficiency. The module inception is the core and significant building block of the kernel, aligned with various dimensions of 1x1 and 3x3. Targeted 2048 feature vectors of were extracted from each of the marked input image by the network.

iii. **Visual Geometry Group (VGG) (16 and 19)**: Convolutional layers and the activation function rectified linear unit (ReLU) are used by the VGG16 and VGG19 embedder families. The VGG-16 and VGG-19 embedders each have 16 and 19 layers, with a filter dimension of 3x3. The 16 and 19 variations in this study were considered due to their simplicity, moreover, they are widely

used in other studies, including. Separately, 4096 feature vectors were extracted from each signal input by the embedders.

iv. **Painters**: To predict painters, a deep convolutional network embedder referred to as *Painter*, was trained on artwork images since it has the ability to recognize patterns in artistic image signals greatly useful in describing X-ray and CT scan inputs. The activation of the network's penultimate layer is used for embedding. The deep embedder extracted 2048 feature attributes.

Phase III: Steganalysis Predictive Analytics with MLP

The framework's final phase implements the steganalysis predictive analytics. A binary classification approach employs the supervised machine learning concept, which includes cover numeric image descriptors labeled as negative, and *stego* numeric image descriptors labeled as

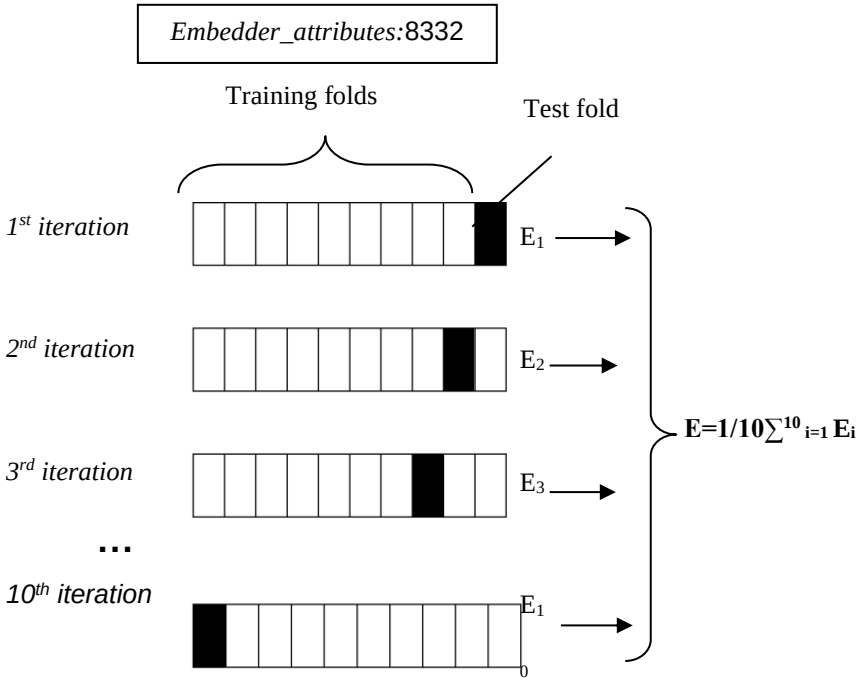


Figure 2: The Concept of Cross-validation (10-fold)

Positive. For machine learning, the deep learner algorithm Multilayer Perceptron (MLP) was used. For the simulation, the supervised machine learning approach was used, in which the MLP was first trained. The training used a significant proportion of extracted numeric image descriptors as the training dataset for pattern recognition, after which the remaining datasets were used to predict if there was the presence of a secret message in the digital images or not. For the simulation, the 10-fold cross-validation methodology was used. The dataset was randomly divided into ten equivalent sub-samples, one of which serves as the validation set for testing the model. The MLP was treated in the same manner, and the validation procedure was repeated every ten clocks. The average of the results of the ten-fold was then recoded to have a unique learner's algorithms singly estimated. This method ensures the usage of the feature vectors that was extracted for each of the 8332 image instances, the 8332, The methodology of cross-validation (10-fold) is presented in Figure 2. The parameters for training the MLP are shown in Table 1.

Table 1: Parameter Distribution Choices for Training the MLP

Hidden layer numbers	1000
Learning rate	0.001
Alpha	0.0001
Batch size	200
Batch size	1
Solver	1bfgs (Backpropagation)

The framework was implemented with object-oriented Python programming libraries and on the Orange data mining toolkit. The Orange data mining toolkit was used for feature extraction purposes where the SqueezeNet embedder was employed to extract numeric feature vectors, through image embedding, as presented in Figure 5. The feature selection of image attributes was also executed on the Orange framework. The steganalysis through machine learning was then implemented on the Jupyter notebook of the Anaconda Navigator environment presented in Figure 6, where the Python code was programmed and run to execute the framework. The Sklearn Python library was employed for the machine learning and binary classification problem of this study. During the evaluation stage, the SKlearn library was also used. The Numpy library was used for handling the multi-dimensional array and matrices due to the image embedding which requires mathematical functions for smooth operations on the arrays. Data analysis that comprises transformation, cleaning, and visualizing data points were all achieved with the Pandas library, while Scikit-learn (Sklearn) is the most useful and robust statistical machine-learning modeling tool for clustering and classification. The resulting model is then assessed using the confusion matrix generated during the machine learning phase. To determine the best parameter setting for the Multilayer perceptron in the steganalysis experiment, the performance metrics across the different parameter tuning were evaluated.

3 Result and Discussion

The acquired digital image signals with no hidden or embedded secret messages are presented in the image grid view of Figure 3, while the stego instances, with embedded secret images, are presented in the Figure 4 grid view. The addition of the two categories for the implementation of the framework is presented in the image grid view of Figure 5. The concatenated image signals in Figure 5 were subjected to feature extraction through deep learning image embedding. The numeric feature vectors extracted from each of the image signal instances are presented on the data table of Figure 6, and serves as the training set of the study for each of the five image embedders. There is a need to identify the most significant attributes in the numeric feature vectors, as determined by the Information Gain and the Chi-Square techniques, whose result is presented in the Figure 7 ranker. Additional image signals were subjected to feature extraction processes to serve as the test set of the study and the resulting numeric feature vectors, presented in Figure 8. The training of the MLP classifier with the training set produces a software solution that was tested by the test set of Figure 8 using the 10 fold-cross validation as earlier described. The result of the testing was the prediction made by the MLP after a successful training. The image signal instances contained in the test set were predicted as either a stegno image signal or cover image signal and the result of the prediction was automatically saved in a comma-separated version (CSV) file, whose result is presented in Figure 9.

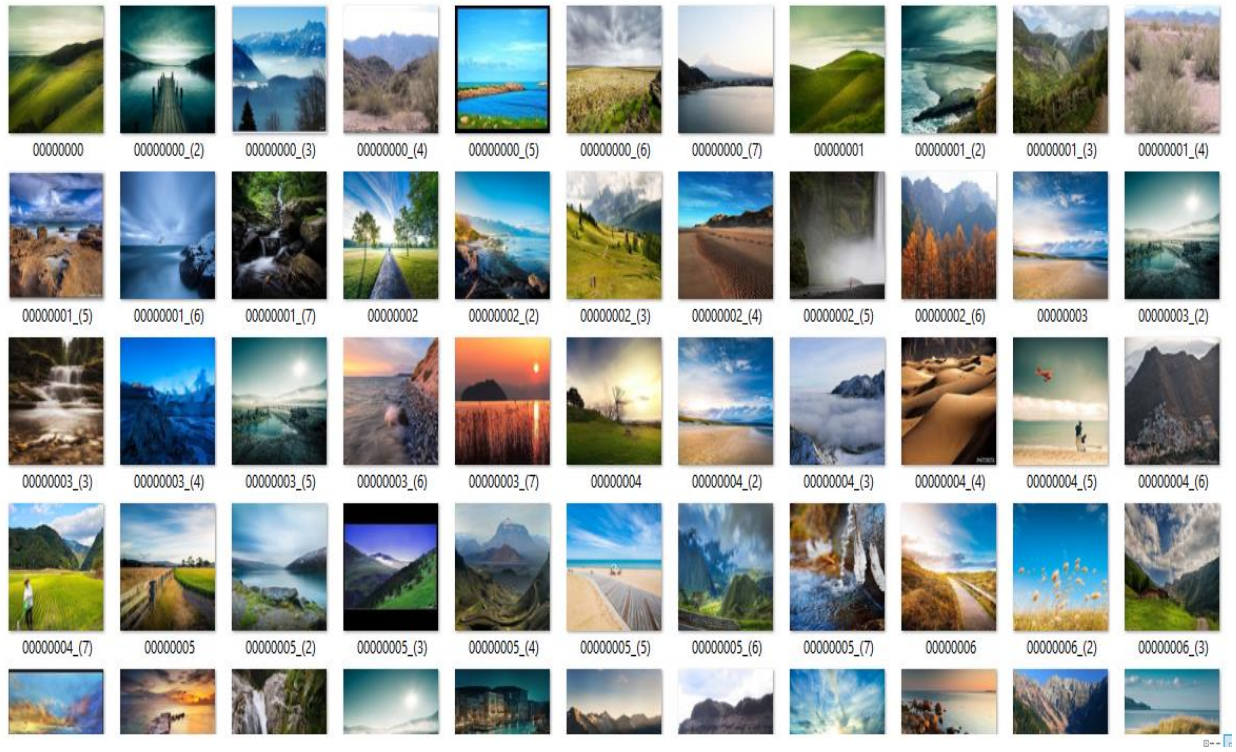


Figure 3: Screenshot of Acquired Cover Images

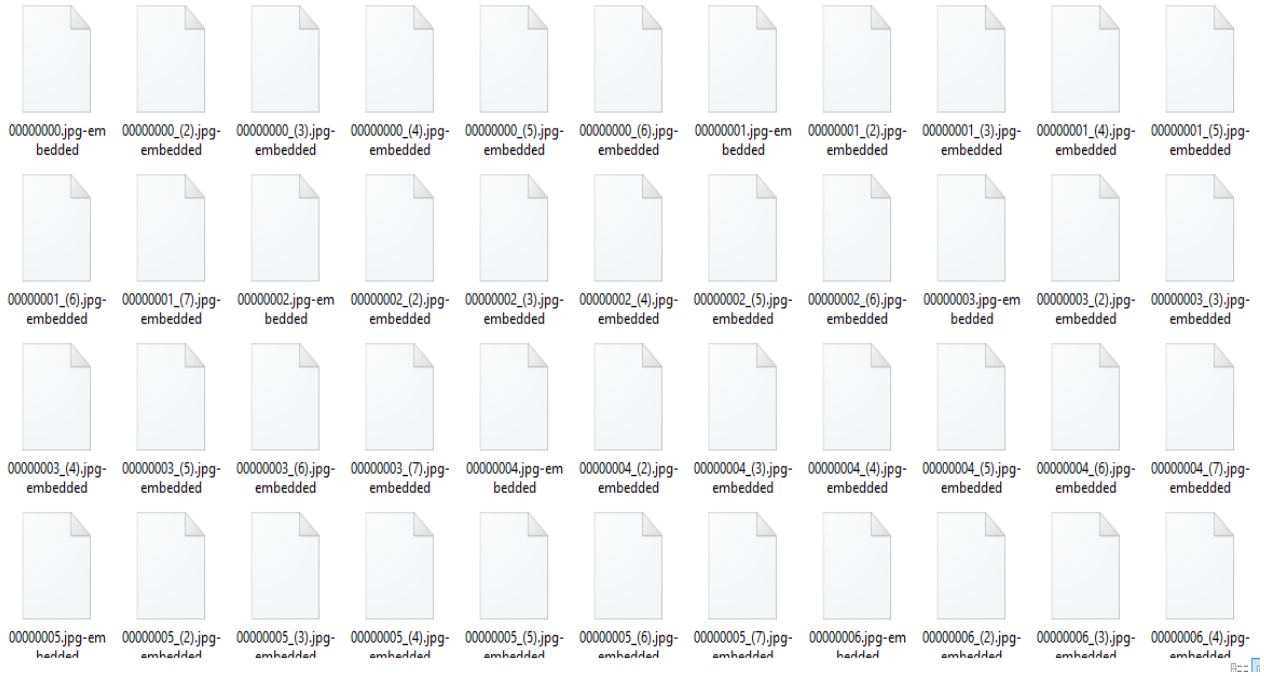


Figure 4: Screenshot of the Acquired Stego Images

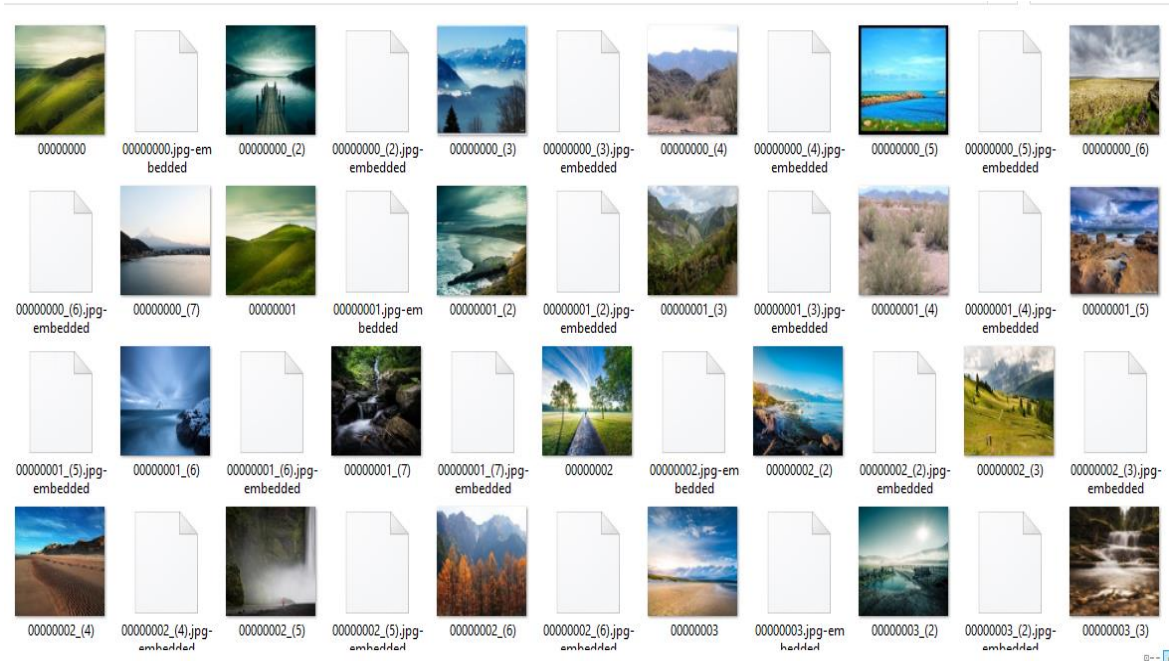
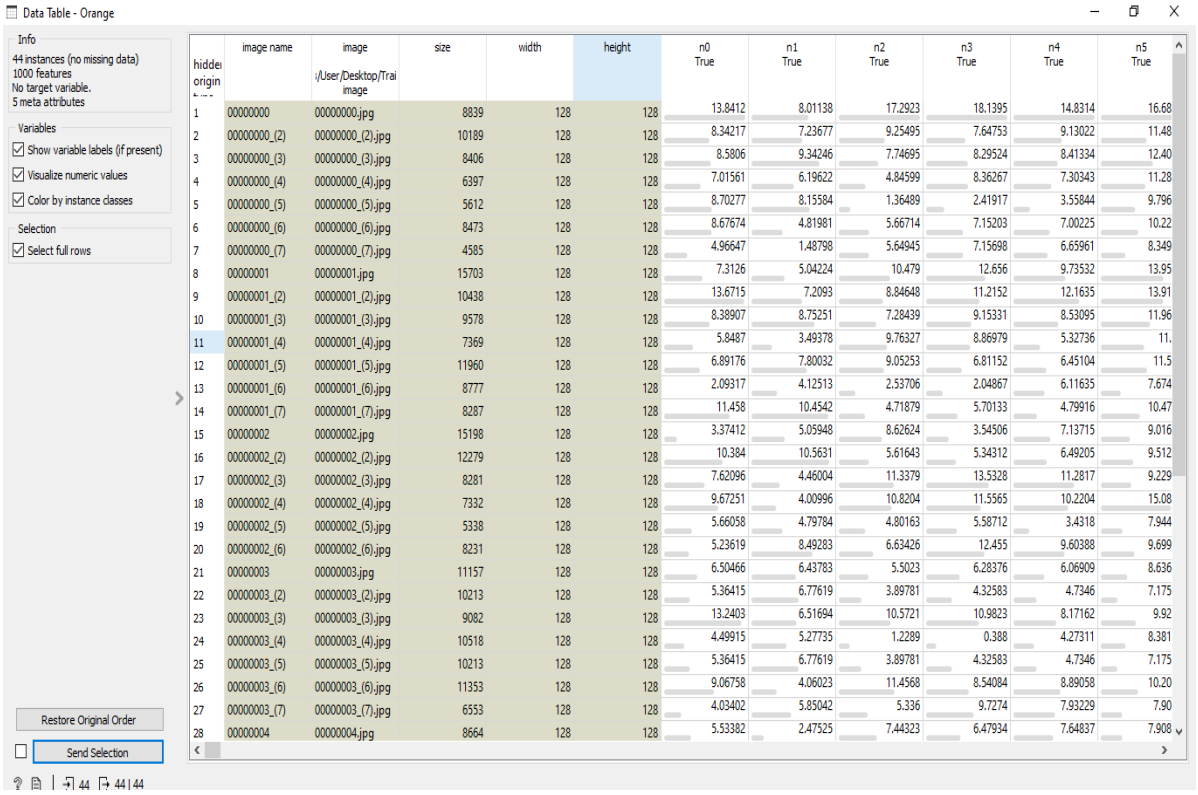
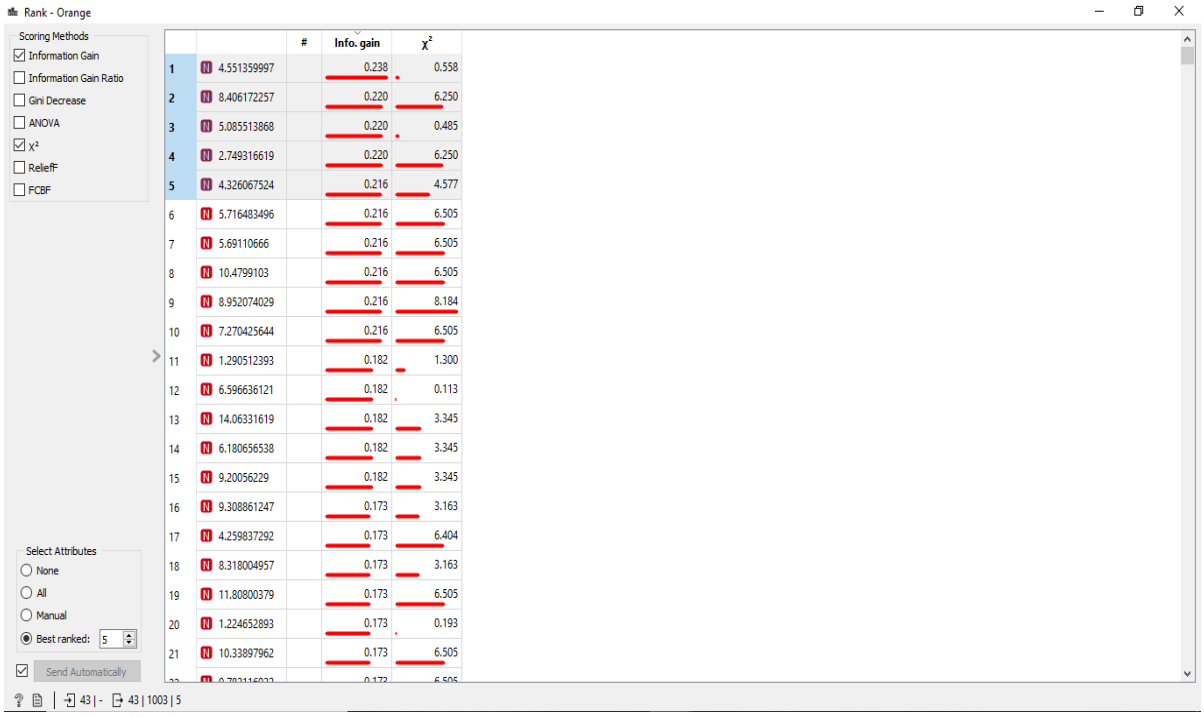


Figure 5: Screenshot of the Concatenated Acquired Cover and Stego Images



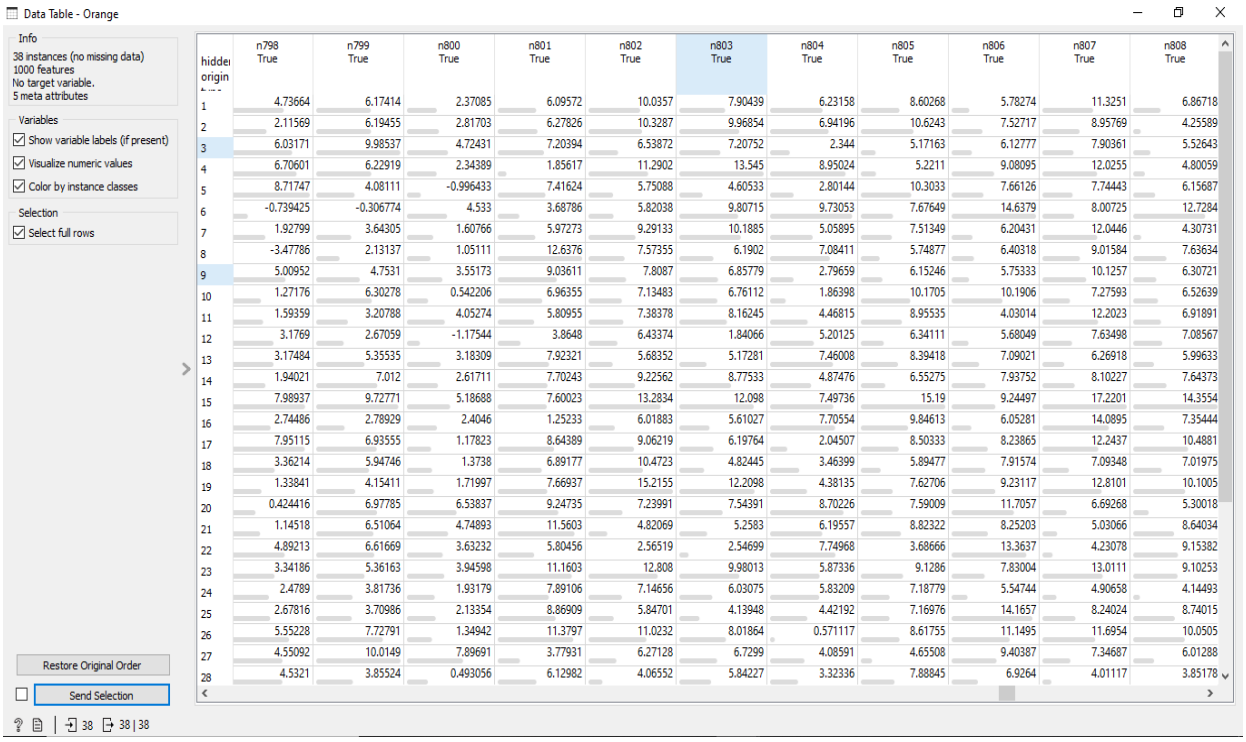
	hidden origin	image name	image /User/Desktop/Trai image	size	width	height	n0 True	n1 True	n2 True	n3 True	n4 True	n5 True
1		00000000	00000000.jpg	8839	128	128	13.8412	8.01138	17.2923	18.1395	14.8314	16.68
2		00000000_(2)	00000000_(2).jpg	10189	128	128	8.34217	7.23677	9.25495	7.64753	9.13022	11.48
3		00000000_(3)	00000000_(3).jpg	8406	128	128	8.5806	9.34246	7.74695	8.29524	8.41334	12.40
4		00000000_(4)	00000000_(4).jpg	6397	128	128	7.01561	6.19622	4.84599	8.36267	7.30343	11.28
5		00000000_(5)	00000000_(5).jpg	5612	128	128	8.70277	8.15584	1.36489	2.41917	3.55844	9.796
6		00000000_(6)	00000000_(6).jpg	8473	128	128	8.67674	4.81981	5.66714	7.15203	7.00225	10.22
7		00000000_(7)	00000000_(7).jpg	4585	128	128	4.96647	1.48798	5.64945	7.15698	6.65961	8.349
8		00000001	00000001.jpg	15703	128	128	7.3126	5.04224	10.479	12.656	9.73532	13.95
9		00000001_(2)	00000001_(2).jpg	10438	128	128	13.6715	7.2093	8.84648	11.2152	12.1635	13.91
10		00000001_(3)	00000001_(3).jpg	9578	128	128	8.38907	8.75251	7.28439	9.15331	8.53095	11.96
11		00000001_(4)	00000001_(4).jpg	7369	128	128	5.8487	3.49378	9.76327	8.86979	5.32736	11.
12		00000001_(5)	00000001_(5).jpg	11960	128	128	6.89176	7.80032	9.05253	6.81152	6.45104	11.5
13		00000001_(6)	00000001_(6).jpg	8777	128	128	2.09317	4.12513	2.53706	2.04867	6.11635	7.674
14		00000001_(7)	00000001_(7).jpg	8287	128	128	11.458	10.4542	4.71879	5.70133	4.79916	10.47
15		00000002	00000002.jpg	15198	128	128	3.37412	5.05948	8.62624	3.54506	7.13715	9.016
16		00000002_(2)	00000002_(2).jpg	12279	128	128	10.384	10.5631	5.61643	5.34312	6.49205	9.512
17		00000002_(3)	00000002_(3).jpg	8281	128	128	7.62096	4.46004	11.3379	13.5328	11.2817	9.229
18		00000002_(4)	00000002_(4).jpg	7332	128	128	9.67251	4.00996	10.8204	11.5565	10.2204	15.08
19		00000002_(5)	00000002_(5).jpg	5338	128	128	5.66058	4.79784	4.80163	5.58712	3.4318	7.944
20		00000002_(6)	00000002_(6).jpg	8231	128	128	5.23619	8.49283	6.63426	12.455	9.60388	9.699
21		00000003	00000003.jpg	11157	128	128	6.50466	6.43783	5.5023	6.28376	6.06909	8.636
22		00000003_(2)	00000003_(2).jpg	10213	128	128	5.36415	6.77619	3.89781	4.32583	4.7346	7.175
23		00000003_(3)	00000003_(3).jpg	9082	128	128	13.2403	6.51694	10.5721	10.9823	8.17162	9.92
24		00000003_(4)	00000003_(4).jpg	10518	128	128	4.49915	5.27735	1.2289	0.388	4.27311	8.381
25		00000003_(5)	00000003_(5).jpg	10213	128	128	5.36415	6.77619	3.89781	4.32583	4.7346	7.175
26		00000003_(6)	00000003_(6).jpg	11353	128	128	9.06758	4.06023	11.4568	8.54084	8.89058	10.20
27		00000003_(7)	00000003_(7).jpg	6553	128	128	4.03402	5.85042	5.336	9.7274	7.93229	7.90
28		00000004	00000004.jpg	8664	128	128	5.53382	2.47525	7.44323	6.47934	7.64837	7.908

Figure 6: Data Table Instance of Extracted Numeric Feature Vectors through Squeeze Net Image Embedding Model

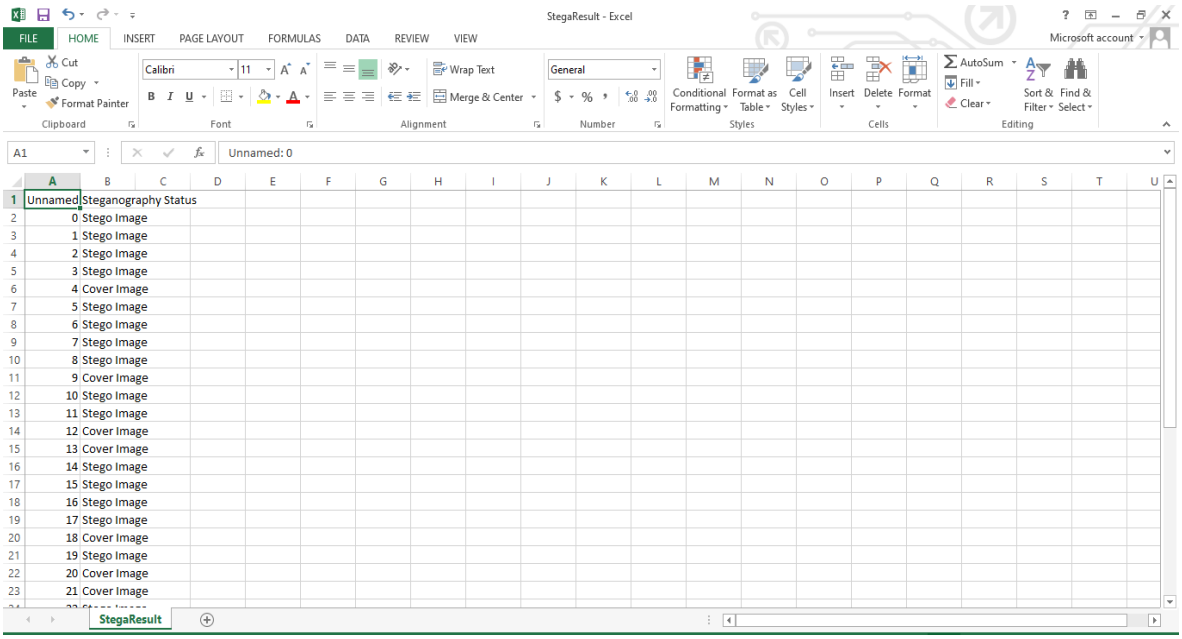


		#	Info. gain	χ²
1	4.551359997		0.238	0.558
2	8.406172257		0.220	6.250
3	5.085513868		0.220	0.485
4	2.749316619		0.220	6.250
5	4.326067524		0.216	4.577
6	5.716483496		0.216	6.505
7	5.69110666		0.216	6.505
8	10.4799103		0.216	6.505
9	8.952074029		0.216	8.184
10	7.270425644		0.216	6.505
11	1.290512393		0.182	1.300
12	6.596636121		0.182	0.113
13	14.06331619		0.182	3.345
14	6.180656538		0.182	3.345
15	9.20056229		0.182	3.345
16	9.308861247		0.173	3.163
17	4.259837292		0.173	6.404
18	8.318004957		0.173	3.163
19	11.80800379		0.173	6.505
20	1.224652893		0.173	0.193
21	10.33897962		0.173	6.505

Figure 7: Result of the Feature Selection Phase



hidde origin	n798 True	n799 True	n800 True	n801 True	n802 True	n803 True	n804 True	n805 True	n806 True	n807 True	n808 True
1	4.73664	6.17414	2.37085	6.09572	10.0357	7.90439	6.23158	8.60268	5.78274	11.3251	6.86718
2	2.11569	6.19455	2.81703	6.27826	10.3287	9.96854	6.94196	10.6243	7.52717	8.95769	4.25589
3	6.03171	9.98537	4.72431	7.20394	6.53872	7.20752	2.344	5.17163	6.12777	7.90361	5.52643
4	6.70601	6.22919	2.34389	1.85617	11.2902	13.545	8.95024	5.2211	9.08095	12.0255	4.80059
5	8.71747	4.08111	-0.996433	7.41624	5.75088	4.60533	2.80144	10.3033	7.66126	7.74443	6.15687
6	-0.739425	-0.306774	4.533	3.68786	5.82038	9.80715	9.73053	7.67649	14.6379	8.00725	12.7284
7	1.92799	3.64305	1.60766	5.97273	9.29133	10.1885	5.05895	7.51349	6.20431	12.0446	4.30731
8	-3.47786	2.13137	1.05111	12.6376	7.57355	6.1902	7.08411	5.74877	6.40318	9.01584	7.63634
9	5.00952	4.7531	3.55173	9.03611	7.8087	6.85779	2.79659	6.15246	5.75333	10.1257	6.30721
10	1.27176	6.30278	0.542206	6.96355	7.13483	6.76112	1.86398	10.1705	10.1906	7.27593	6.52639
11	1.59359	3.20788	4.05274	5.80955	7.38378	8.16245	4.46815	8.95535	4.03014	12.2023	6.91891
12	3.1769	2.67059	-1.17544	3.8648	6.43374	1.84066	5.20125	6.34111	5.68049	7.63498	7.08567
13	3.17484	5.35535	3.18309	7.92321	5.68352	5.17281	7.46008	8.39418	7.09021	6.26918	5.99633
14	1.94021	7.012	2.61711	7.70243	9.22562	8.77533	4.87476	6.55275	7.93752	8.10227	7.64373
15	7.98937	9.72771	5.18688	7.60023	13.2834	12.098	7.49736	15.19	9.24497	17.2201	14.3554
16	2.74486	2.78929	2.4046	1.25233	6.01883	5.61027	7.70554	9.84613	6.05281	14.0895	7.35444
17	7.95115	6.93555	1.17823	8.64389	9.06219	6.19764	2.04507	8.50333	8.23865	12.2437	10.4881
18	3.36214	5.94746	1.3738	6.89177	10.4723	4.82445	3.46399	5.89477	7.91574	7.09348	7.01975
19	1.33841	4.15411	1.71997	7.66937	15.2155	12.2098	4.38135	7.62706	9.23117	12.8101	10.1005
20	0.424416	6.97785	6.53837	9.24735	7.23991	7.54391	8.70226	7.59009	11.7057	6.69268	5.30018
21	1.14518	6.51064	4.74893	11.5603	4.82069	5.2583	6.19557	8.82322	8.25203	5.03066	8.64034
22	4.89213	6.61669	3.63232	5.80456	2.56519	2.54699	7.74968	3.68666	13.3637	4.23078	9.15382
23	3.34186	5.36163	3.94598	11.1603	12.808	9.98013	5.87336	9.1286	7.83004	13.0111	9.10253
24	2.4789	3.81736	1.93179	7.89106	7.14656	6.03075	5.83209	7.18779	5.54744	4.90658	4.14493
25	2.67816	3.70986	2.13354	8.86909	5.84701	4.13948	4.42192	7.16976	14.1657	8.24024	8.74015
26	5.55228	7.72791	1.34942	11.3797	11.0232	8.01864	0.571117	8.61755	11.1495	11.6954	10.0505
27	4.55092	10.0149	7.89691	3.77931	6.27128	6.7299	4.08591	4.65508	9.40387	7.34687	6.01288
28	4.5321	3.85524	0.493056	6.12982	4.06552	5.84227	3.32336	7.88845	6.9264	4.01117	3.85178



Unnamed	Steganography Status
0	Stego Image
1	Stego Image
2	Stego Image
3	Stego Image
4	Cover Image
5	Stego Image
6	Stego Image
7	Stego Image
8	Stego Image
9	Cover Image
10	Stego Image
11	Stego Image
12	Cover Image
13	Cover Image
14	Stego Image
15	Stego Image
16	Stego Image
17	Stego Image
18	Cover Image
19	Stego Image
20	Cover Image
21	Cover Image

Figure 9: Result of MLP Predictions on the Test Set

Performance Evaluation of Parameter Tuning

The performance evaluation of the Multilayer Perceptron was determined by the iteration of the testing phase of the framework through parameter tuning. Identified parameters of the MLP were tuned repeatedly to identify the optimal performing attribute set. Using the True Positive (TP), True Negative (TN), False Positive (FP) and False Negative (FN) results of each parameter tuning, the performance metrics of Accuracy, Precision, and Recall were computed. The Accuracy, precision, and Recall attributes were calculated based on the four metrics as computed below:

i. The Accuracy parameter returns the model's overall precision, which reveals the percentage of positive cases overall that the MLP accurately predicted as either *stego* or cover.

ii. Precision, however, establishes the percentage of steganography status that establishes the *stego* or cover state of each image input.

iii. The Recall is the proportion of *stego* or cover instances that are expected to be *stego* or cover. They are computed by the formula in equations 1, 2, and 3 as follows:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

$$Precision = \frac{TP}{TP+FP} \quad (2)$$

$$Recall = \frac{TP}{TP+FN} \quad (3)$$

Parameter Optimization Evaluation

Parameter optimization was implemented on the Multilayer Perceptron to ascertain the best parameter set for the steganalysis of acquired image signals. Therefore, parameter tuning is implemented on the Max-iter parameter of the MLP, which is the maximum number of hops the perceptron is allowed to find the minimum error value. It is at the minimum error value that the MLP returns its best prediction.

Therefore, the value specified as the max-iter will determine the number of epochs, which is the maximum number of times the entire dataset goes through the network. It is referred to as the batch size in Table 1 and hence, the default setting was at 200.

The parameter was then tuned from 200 to 300, 500, and 1000, therefore returning the confusion matrices presented in Figure 10, Figure 11, and Figure 12. The weighted averages of the Accuracy, Precision, and Recall, computed based on the confusion matrices are presented in Table 2, Table 3, and Table 4 respectively. The confusion matrix for the Max-iter at 500 and random rate at 5 is presented in Figure 13. As observed, the optimal performance was achieved at the Ma-iter 1000 of Table 4. Consequently, the parameter random rate set at default 1 for the earlier iterations was tuned to 5 on the optimal max-iter 1000, and the resulting weighted averages are presented in Table 4. The pair of Max-iter at 1000 and the random rate at 5 is observed to have lowered the performance metrics compared to the optimal result earlier presented in Table 6. Therefore, the optimal parameter set for the MLP, for the detection of steganography is presented in Table 4. Weighted average distribution with random rate at 5 is presented in Table 5.

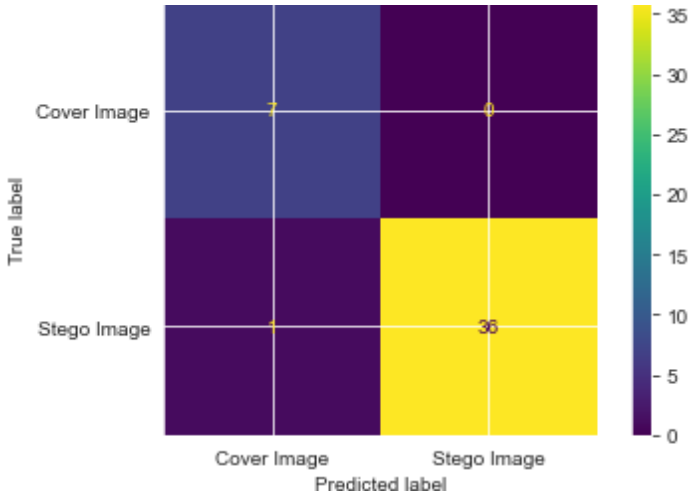


Figure 10: Confusion Matrix for Max-iter at 300

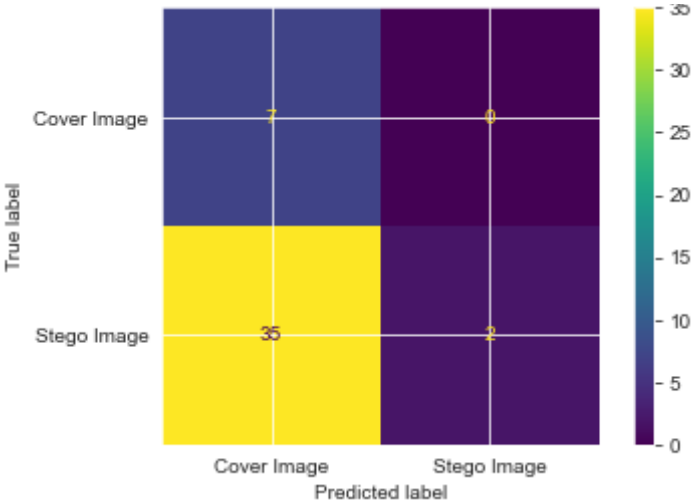


Figure 11: Confusion Matrix for Max-iter at 500

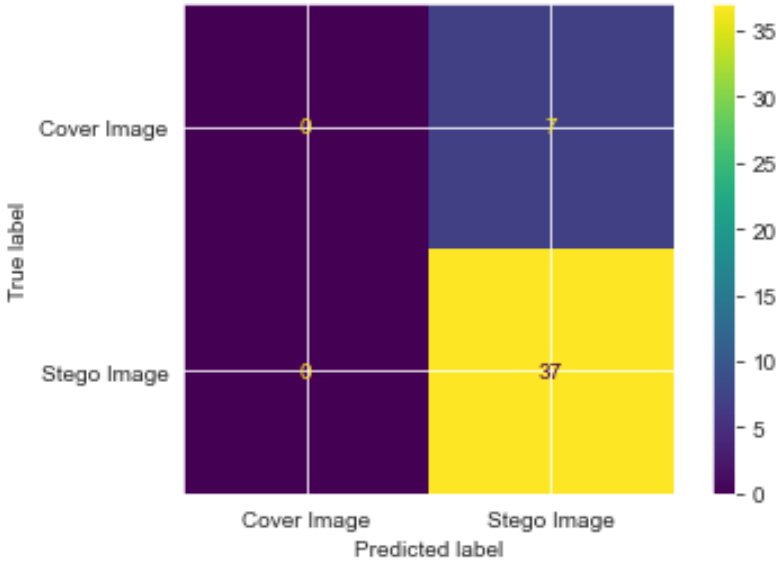


Figure 12: Confusion Matrix for Max-iter at 1000

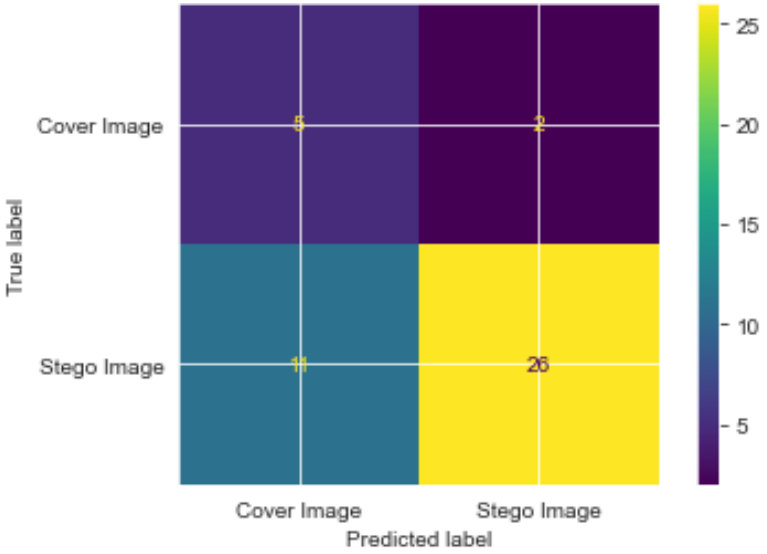


Figure 13: Confusion Matrix for Max-iter at 500 and Random Rate at 5

Table 2: Weighted Average Distribution of Max-iter at 300

Metrics	Weighted averages
Accuracy	0.973
Precision	0
Recall	0

Table 3: Weighted Average Distribution of Max-iter at 500

Metrics	Weighted averages
Accuracy	0.128
Precision	1.000
Recall	0.170

Table 4: Weighted Average Distribution of Max-iter at 1000

Metrics	Weighted averages
Accuracy	0.931
Precision	0.5714
Recall	1.000

Table 5: Weighted Average Distribution with Random Rate at 5

Metrics	Weighted averages
Accuracy	0.863
Precision	0.2857
Recall	0.666

Table 6: Weighted Average Distribution at Max-iter 1000 and Random Rate at 5

Metrics	Weighted averages (Random at 5)	Weighted averages (Random at 1)
Accuracy	0.863	0.931
Precision	0.2857	0.5714
Recall	0.666	1.000

The experimental results of the study interpret the framework earlier presented to address the objectives set for this study. Results of the parameter optimization show that the Max-iter parameter of the MLP classifier hugely determines the performance of the algorithm toward detecting steganography in digital image signals. The parameter stipulates the number of times the training set will pass through the MLP network for the training process. Model performance was observed increased over time with the iteration. As observed in Table 2 when the parameter is set at 300, the accuracy weighted average was 97% with a bad precision and recall weighted averages. The Accuracy dropped to 13% in Table 3, with the Max-iter at 500, however, the weighted averages of precision and recall improved to 100% and 17% respectively. Max-iter returned the best result at 1000 netting an accuracy of 93%, precision of 57, and recall of 100% weighted averages, as indicated in Table 4. With the optimal result achieved at 1000 max-iter, the random rate parameter is further tuned from 1 to 5 but the performance of the MLP deep classifier dropped as presented in Table 6 with 86% accuracy rate, 29% precision rate, and 67% recall weighted average. In all, the most prominent feature attributes, out of the total extracted from the image signals are presented in Figure 7. The highly rated features are the most significant in the approximation of the ground truth as to the status of an image signal as either a *stego* or cover images.

Undoubtedly, our experiments have proven the proposed methodology quite outstanding for detecting and predicting hidden information in data using the Multilayer Perception deep learning model except for the general concern that MLP uses one perceptron for each input, for instance, pixel in an image, leading to a situation where the amount of weights rapidly increases for large images thereby resulting in dealing with complexity and computational costs as it usually requires more parameters, more data and more time to converge. This could become a greater challenge in real-life situations when MLP classifiers are exclusively depended on for steganalysis.

4 Conclusion and Future Work

Using a three-phased framework, A deep learning model of Multilayer perceptron is trained for pattern recognition of steganography instances in acquired digital image signals. The image signals are acquired from the Kaggle public repository containing cover images (clean signals) and stego images (embedded

signals). The SqueezeNet network, from the acquired signals for the machine learning phase, was employed to extract numeric feature vectors. Prior to the training of the multilayer perceptron, the numeric feature vectors are subjected to a minority oversampling in order to scale up the instances of minority class of stego or cover instances contained in the training set. The parameters of the Multilayer perceptron was tuned severally to obtain the optimal parameter set determined by the accuracy, precision, and recall weighted averages. The max-iter parameter returned optimal performance at 1000, after initial iterations at 500 and 300. A Multilayer Perceptron would be able to predict a *stego* image if one of its parameters (random rate) was set to a specific value, and it would perform even better if the max-iter was set to a specific value. Unlike one of the best previously proposed methodologies which were based on deep learning residual and convolution neural networks, having recorded weaknesses of parameter optimization on the neural network, non-implementation of feature engineering technique, and even no attempt to address variance problems, our study does not only implement a model that detects hidden information in images, but it also discovered and tuned the Multilayer Perceptron to determine where it will perform best which are considered greater contributions over all the related previously proposed methodologies.

Future work is intended to critically study and propose relative solutions to the observed complexity and computational costs that are usually associated with Multilayer Perceptron, especially in steganalysis where the amount of weights rapidly increases for large images when using MLP classifiers.

References

[1] Adeshina, A. M., & Hashim, R. (2017). Computational approach for securing radiology-diagnostic data in connected health network using high-performance gpu-accelerated aes. *Interdisciplinary Sciences: Computational Life Sciences*, *9*, 140-152. https://doi.org/10.1007/s12539-015-0140-9

[2] Alabdulatif, A., Khalil, I., Yi, X., & Guizani, M. (2019). Secure edge of things for smart healthcare surveillance framework. *IEEE access*, *7*, 31010-31021. https://doi.org/10.1109/ACCESS.2019.2899323

[3] Alajmi, N. M., & Elleithy, K. (2016, April). A new approach for detecting and monitoring of selective forwarding attack in wireless sensor networks. In *2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT)* (pp. 1-6). IEEE. https://doi.org/10.1109/LISAT.2016.7494104

[4] Alshehri, S., Radziszowski, S. P., & Raj, R. K. (2012, April). Secure access for healthcare data in the cloud using ciphertext-policy attribute-based encryption. In *2012 IEEE 28th international conference on data engineering workshops* (pp. 143-146). IEEE. https://doi.org/10.1109/ICDEW.2012.68

[5] Boudouaia, M. A., Ali-Pacha, A., Abouaissa, A., & Lorenz, P. (2020). Security against rank attack in RPL protocol. *IEEE Network*, *34*(4), 133-139. https://doi.org/10.1109/MNET.011.1900651

[6] Chung, K., & Park, R. C. (2019). RETRACTED ARTICLE: Cloud based u-healthcare network with QoS guarantee for mobile health service. *Cluster Computing*, *22*(Suppl 1), 2001-2015. https://doi.org/10.1007/s10586-017-1120-0

[7] Corum, A., Coding, M., & Swag, R. (2020). Steganalysis. https://www.kaggle.com/datasets/andrewcorum/steganalysis

[8] Esiefarienrhe, B. M., Phakathi, T., & Lugayizi, F. (2022, June). Node-based QoS-aware security framework for sinkhole attacks in mobile ad-hoc networks. In *Telecom* (Vol. 3, No. 3, pp. 407-432). MDPI. https://doi.org/10.3390/telecom3030022

[9] Jang, H., Oh, T. W., & Kim, K. (2020, June). Feature aggregation networks for image steganalysis. In *Proceedings of the 2020 ACM Workshop on Information Hiding and Multimedia Security* (pp. 33-38). https://doi.org/10.1145/3369412.3395072

[10] Krishnan, H., Santhosh., Vijay., & Yasmin, S. (2022). Blockchain for Health Data Management. *International Academic Journal of Science and Engineering, 9*(2), 23–27. https://doi.org/10.9756/IAJSE/V9I2/IAJSE0910

[11] Li, H., Yu, K., Liu, B., Feng, C., Qin, Z., & Srivastava, G. (2021). An efficient ciphertext-policy weighted attribute-based encryption for the internet of health things. *IEEE journal of biomedical and health informatics*, *26*(5), 1949-1960. https://doi.org/10.1109/JBHI.2021. 3075995

[12] Mathew, C., & Asha, P. (2024). FedProx: FedSplit Algorithm based Federated Learning for Statistical and System Heterogeneity in Medical Data Communication. *Journal of Internet Services and Information Security, 14*(3), 353-370. https://doi.org/10.58346/JISIS.2024.I3.021

[13] Mehetre, D. C., Roslin, S. E., & Wagh, S. J. (2019). Detection and prevention of black hole and selective forwarding attack in clustered WSN with Active Trust. *Cluster Computing*, *22*, 1313-1328. https://doi.org/10.1007/s10586-017-1622-9

[14] Mohandas, R., Veena, S., Kirubasri, G., Thusnavis Bella Mary, I.., & Udayakumar, R. (2024). Federated Learning with Homomorphic Encryption for Ensuring Privacy in Medical Data. *Indian Journal of Information Sources and Services, 14*(2), 17–23. https://doi.org/10.51983/ijiss-2024.14.2.03

[15] Odeh, A., & Taleb, A. A. (2023). A Multi-Faceted Encryption Strategy for Securing Patient Information in Medical Imaging. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 14*(4), 164-176. https://doi.org/10.58346/JOWUA.2023.I4.012

[16] Park, J., & Cho, Y. (2020). Design and implementation of automated steganography image-detection system for the KakaoTalk instant messenger. *Computers, 9*(4), 103. https://doi.org/10.3390/computers9040103

[17] Qian, Y., Dong, J., Wang, W., & Tan, T. (2018). Feature learning for steganalysis using convolutional neural networks. *Multimedia Tools and Applications*, *77*, 19633-19657. https://doi.org/10.1007/s11042-017-5326-1

[18] Saito, T., Zhao, Q., & Naito, H. (2019, October). Second level steganalysis-embeding location detection using machine learning. In *2019 IEEE 10th International Conference on Awareness Science and Technology (iCAST)* (pp. 1-6). IEEE. https://doi.org/10.1109/ICAwST.2019.8923205

[19] Sánchez, P. M. S., Valero, J. M. J., Celdrán, A. H., Bovet, G., Pérez, M. G., & Pérez, G. M. (2021). A survey on device behavior fingerprinting: Data sources, techniques, application scenarios, and datasets. *IEEE Communications Surveys & Tutorials*, *23*(2), 1048-1077. https://doi.org/10.1109/COMST.2021.3064259

[20] Singh, A., & Chatterjee, K. (2023). Edge computing based secure health monitoring framework for electronic healthcare system. *Cluster Computing*, *26*(2), 1205-1220. https://doi.org/10.1007/s10586-022-03717-w

[21] Veera Boopathy, E., Peer Mohamed Appa, M.A.Y., Pragadeswaran, S., Karthick Raja, D., Gowtham, M., Kishore, R., Vimalraj, P., & Vissnuvardhan, K. (2024). A Data Driven Approach through IOMT based Patient Healthcare Monitoring System. *Archives for Technical Sciences, 2*(31), 9-15. https://doi.org/10.70102/afts.2024.1631.009

[22] Wan, Q., & Hu, X. (2024). Legal Framework for Security of Organ Transplant Information in the Digital Age with Biotechnology. *Natural and Engineering Sciences, 9*(2), 73-93. https://doi.org/10.28978/nesciences.1569190

[23] Ye, J., Ni, J., & Yi, Y. (2017). Deep learning hierarchical representations for image steganalysis. *IEEE Transactions on Information Forensics and Security*, *12*(11), 2545-2557. https://doi.org/10.1109/TIFS.2017.2710946

[24] Yedroudj, M., Comby, F., & Chaumont, M. (2018, April). Yedroudj-net: An efficient CNN for spatial steganalysis. In *2018 IEEE international conference on acoustics, speech and signal processing (ICASSP)* (pp. 2092-2096). IEEE. https://doi.org/10.1109/ICASSP.2018.8461438

[25] Zeng, L., Lu, W., Liu, W., & Chen, J. (2020). Deep residual network for halftone image steganalysis with stego-signal diffusion. *Signal processing*, *172*, 107576. https://doi.org/10.1016/j.sigpro.2020.107576

[26] Zhang, R., Zhu, F., Liu, J., & Liu, G. (2018). Efficient feature learning and multi-size image steganalysis based on CNN. https://doi.org/10.48550/arXiv.1807.11428

[27] Zou, Y., Zhang, G., & Liu, L. (2019). Research on image steganography analysis based on deep learning. *Journal of Visual Communication and Image Representation*, *60*, 266-275. https://doi.org/10.1016/j.jvcir.2019.02.034

Authors Biography

Dr.A.M. Adeshina, is a scholar currently with the Faculty of Information Science and Technology, Multimedia University, Malaysia. He has his core research areas in Artificial Intelligence, High-Performance Computing, GPU-based Algorithms, Neuroinformatics, Data and Cyber Security. He gained his B.Sc. (Hons.), Master's, and PhD degrees from the University of Ilorin, Nigeria, Multimedia University, Malaysia, and the University Tun Hussein Onn Malaysia respectively. He was a Postdoctoral Fellow with the Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia from 2014 to 2016. Over the years, he has been quite active in researching and applying High-Performance Computing and Artificial Intelligence approaches to the development of software solutions in medical and paramedical domains, including researching best approaches to reducing algorithmic complexities, and improving performances and bottlenecks of some of the algorithms in healthcare. Some of his findings have been presented at international conferences and his contributions are frequently being acknowledged in various capacities, published in reputable international journals, and included in most of the notable databases.

Sheriff Olanrewaju Anjorin, graduated from the University of Nigeria, Nsukka, Yaba Tech campus in 2012 for his B.Sc. in Computer Education. He is currently pursuing his Master's Degree in Computer Science at Crescent University, Ogun State, Nigeria. He is an active member of the High-Performance Computing Research Laboratory in Nigeria. Mr. Anjorin's research areas include High-Performance Computing, Artificial Intelligence, Data Science, Security, and Privacy.

Dr. Siti Fatimah Abdul Razak, received her B. Sc (Hons) in Education where she majors in Mathematics and Information Technology, and Master of Information Technology majoring in Science and System Management from Universiti Kebangsaan Malaysia in the year 2004. She completed her doctorate studies in Information Technology from Multimedia University. She is also currently an Assistant Professor at the Faculty of Information Science and Technology, Multimedia University. Apart from her administration and teaching responsibilities, she is also supervising postgraduate students and undergraduate final-year projects. Her research interests include vehicle safety applications, rule mining, machine learning, Internet-of Things, information systems development, and educational technology. She is currently a member of IEEE and the Centre for Intelligent Cloud Computing (CICC), a research centre in Multimedia University. She is also a registered Professional Technologist with the Malaysia Board of Technologists (MBOT).