Jordanian Journal of Computers and Information Technology (JJCIT), Vol. 11, No. 01, March 2025.

PRIVACY-AWARE MALARIA DETECTION: U-NET MODEL WITH K-ANONYMITY FOR CONFIDENTIAL IMAGE ANALYSIS

Ghazala Hcini and Imen Jdey

(Received: 6-Aug.-2024, Revised: 1-Oct.-2024, Accepted: 24-Oct.-2024)

ABSTRACT

Malaria detection through cell-image analysis is essential for early diagnosis and effective treatment, as timely detection can significantly reduce the risk of severe health complications. However, this process raises substantial privacy concerns due to the sensitivity of medical data. This study presents a U-Net model combined with k-anonymity to enhance data security while maintaining high accuracy. The model features a custom Spatial Attention mechanism for improved segmentation performance and incorporates advanced techniques to focus on critical image features. K-Anonymity adds controlled noise to protect data privacy by obfuscating sensitive information. The model achieved a validation accuracy of 99.60%, a Dice score of 99.61%, a precision of 99.42%, a recall of 99.96% and an F1-score of 99.69% on malaria cell images. When applied to the Cactus dataset, a real dataset, in agriculture, it achieved an accuracy of 98.58%, an F1-score of 98.44%, a Dice score of 95.08%, a Precision of 98.04% and a Recall of 98.86%, demonstrating its strong generalization capability. These results highlight the effectiveness of integrating privacy-preserving techniques with advanced neural-network architectures, improving both security and performance in diverse image-analysis applications.

KEYWORDS

Deep learning, U-net architecture, Spatial-attention mechanism, K-anonymity, Privacy preservation, Cross-domain transfer.

1. INTRODUCTION

Malaria remains a major global health challenge, causing millions of death cases every year, especially in tropical and sub-tropical areas [1]-[2]. The World Health Organization estimates that there were around 249 million malaria cases worldwide in 2022 [3], resulting in over 600,000 deaths, primarily among vulnerable populations (Figure 1). The early and accurate detection of malaria is crucial for effective treatment and disease control [4]. However, traditional diagnostic methods, like microscopy, are time-consuming and require skilled personnel, often causing delays in diagnosis and treatment [5]-[6].

Image segmentation is widely acknowledged as a crucial and fundamental task in image analysis [7]-[8]. It serves as the initial step in extracting significant information from images. The main goal of image segmentation is to divide an image into distinct segments, which allows for easier representation of objects and measurement of features. The accuracy of feature measurement is greatly affected by the quality of segmentation, emphasizing its importance in various medical imaging applications. The automation of medical-image segmentation plays a vital role in disease diagnosis, pathology localization, anatomical-structure study, treatment planning and integration with computer-assisted surgical systems [9].

Machine learning (ML) and deep learning (DL) have become integral solutions across various domains [10], particularly in healthcare, where they are leveraged for tasks, such as diagnosis, treatment planning and patient monitoring. These technologies enable the analysis of vast datasets, allowing for real-time insights that can significantly enhance healthcare outcomes. In recent years, DL techniques, specifically convolutional neural networks (CNNs) [11], have revolutionized medical-image analysis [12]-[13], providing advanced capabilities for automating disease detection and improving diagnostic accuracy [14]-[15].

Among the various architectures developed for biomedical-image segmentation, U-Net has gained prominence due to its ability to effectively capture detailed information [16]-[18]. Its encoder-decoder

G. Hcini and I. Jdey are with Department of Computer Science, ReGIM-Lab. REsearch Groups in Intelligent Machines, Sfax, Tunisia. Emails: hcinighazala@fstsbz.u-kairouan.tn and imen.jdey@fstsbz.u-kairouan.tn

structure enables precise segmentation of malaria parasites in blood smears [19], thereby facilitating rapid and accurate diagnosis. However, despite its effectiveness, the U-Net model sometimes struggles to distinguish fine details in complex images, which is crucial for accurate parasite detection. To improve the segmentation performance, this paper introduces a spatial-attention mechanism into the U-Net architecture. The spatial-attention mechanism allows the model to focus on relevant regions of the image, thereby enhancing its ability to discern subtle features and improving the overall detection accuracy [20]-[21].

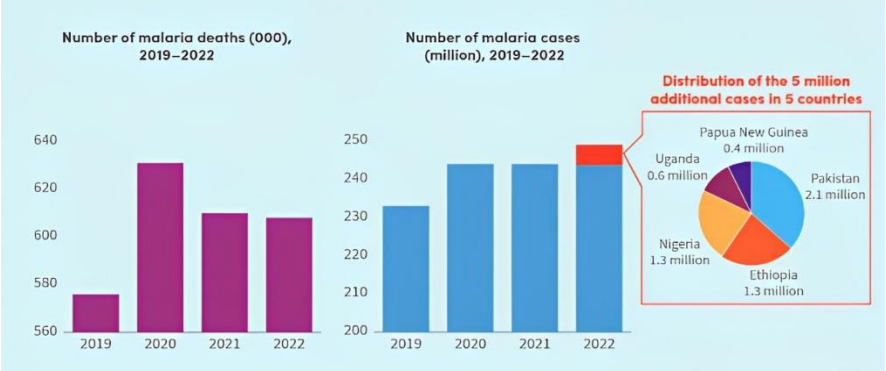

Figure 1. Malaria report: number of deaths and number of cases (2019-2022).

In addition to enhancing detection capabilities, integrating artificial intelligence in healthcare also brings up significant privacy concerns regarding handling sensitive patient data [22]. As healthcare data continues to become more digitized, it becomes crucial to maintain the confidentiality and security of patient information [23]. To address these concerns, this paper introduces a new approach that combines the enhanced U-Net model with k-anonymity techniques. This approach establishes a privacy-aware framework for malaria detection. K-anonymity is a well-established method for preserving privacy [24], as it ensures that individual data points cannot be distinguished from at least k-1 other data points [25]. This protects patient identities while allowing the model to learn from the data effectively.

K-anonymity plays a crucial role in mitigating re-identification risks, making it effective in reducing the likelihood of identifying individuals within anonymized datasets. This enhances privacy protection when sharing sensitive health information, which is increasingly demanded by researchers and regulatory bodies. The method enables the safe sharing of personal health data, facilitating advancements in medical research while striving to protect individual privacy. El Emam and Dankar [26] proposed significant improvements to traditional k-anonymity methodologies, suggesting modifications that better balance privacy protection with data utility. Their study indicates that a hypothesis-testing approach offers superior control over re- identification risks compared to baseline k-anonymity, thereby minimizing unnecessary data distortions. This advancement underscores the importance of adapting existing frameworks to meet the evolving demands of data sharing in healthcare while maintaining robust privacy safeguards.

The main contributions of our study are:

1) It developed a U-Net model combined with k-anonymity technique to enhance data privacy while maintaining high accuracy for malaria cell-image segmentation.
2) It incorporated a custom spatial-attention mechanism into the U-Net model to improve segmentation performance and focus on critical image features.
3) It demonstrated generalization capability by applying our proposed model to the Cactus dataset, a real dataset, from agriculture.

The paper is organized into four main sections: Related Works, Materials and Methods, Results and Discussion and Conclusion. The Related Works section reviews the literature on malaria detection with DL. The Materials and Methods section outlines the dataset, pre-processing steps, the architecture of the spatial attention-enhanced U-Net model and the implementation of k-anonymity. The Results and Discussion section presents experimental findings, analyzes the impact of the attention mechanism and evaluates the effectiveness of the privacy approach. Finally, the Conclusion section summarizes key findings and suggests future-research directions.

2. RELATED WORKS

Recent advancements in malaria cell-image segmentation have significantly improved diagnostic capabilities. Traditional methods laid the groundwork, but the field has evolved by adopting advanced techniques that enhance accuracy and reliability. The following review explores key recent studies that have pushed the boundaries of automated malaria detection, showcasing the progress and innovations in this critical area of medical imaging.

The proposed approach in [27] involves creating an automated system for malaria detection using a decision-tree classifier. The methodology includes pre-processing blood smear images through segmentation with the Canny edge detector and feature extraction using Hu Moments. The data is normalized to ensure consistency. The decision-tree classifier, trained and validated with 5-fold cross-validation, achieved an accuracy of 77.32%, a precision of 77.31%, a recall of 77.37% and an F1-score of 77.48%. This approach highlights the effectiveness of Hu Moments and decision-tree classification for distinguishing malaria- infected from uninfected images, offering potential improvements in diagnostic accuracy and efficiency in clinical settings. Future work should explore advanced techniques and real-time image acquisition to enhance practical applicability.

In [28], the authors proposed a hybrid model combining Capsule Neural Networks (CapsNet) with CNNs for malaria detection from blood smear microscopic images. The approach involved processing and enhancing images through rotation before feeding them into the hybrid CapsNet model. Optimized with a learning rate of 0.07 and a batch size of 20, the model demonstrated significant improvements over traditional methods. The hybrid CapsNet model achieved a detection rate of 99%, an accuracy of 99.08% and a False Acceptance Rate (FAR) of 0.97%, surpassing the DSCN-Net model, which recorded a detection rate of 98%, an accuracy of 97.2% and an FAR of 0.99%. This method underscored the enhanced efficacy of the hybrid CapsNet model in malaria detection.

The main contribution of [29] is the application of the U-Net architecture for accurate Plasmodium segmentation in thin blood smear images. The study demonstrates U-Net's effectiveness in this biomedical-imaging task and compares three loss functions—mean squared error, binary cross-entropy and Huber loss. The results reveal that Huber loss achieves the best performance metrics, with an F1-score of 92.97%, a positive predictive value (PPV) of 0.9715, a sensitivity (SE) of 89.57% and a relative segmentation accuracy (RSA) of 90.96%. These findings highlight Huber loss's ability to enhance segmentation accuracy and reliability for malaria diagnosis.

The proposed method, in [30] introduces an automated system for detecting malaria parasites in microscopic blood images. It uses bilateral filtering to enhance image quality by removing noise, followed by adaptive thresholding and morphological image processing to identify malaria parasites within individual cells. Tested on the NIH Malaria dataset, this approach achieved a detection accuracy exceeding 91%, outperforming existing methods. This algorithm provides a reliable and efficient tool for pathologists and hematologists, aiding in the accurate and timely detection of malaria.

The proposed method in [31] focuses on enhancing the analysis of malaria by automating the identification of parasitized red blood cells. It compares the performance of various models; Support Vector Machines (SVM), XG-Boost and neural networks, demonstrating that CNNs offer superior results. In experiments involving 13,750 parasitized and 13,750 non-parasitized samples, CNNs achieved an accuracy rate of 97%, outperforming SVMs (94%), XG-Boost (90%) and traditional neural networks (80%). This DL approach provides a highly accurate and robust solution for detecting malaria, significantly improving decision-making in medical diagnostics.

In [32], the proposed method involves training various object detection neural networks; YOLOv5x, Faster R-CNN, SSD and RetinaNet, on a dataset of 2,571 labeled thick blood smear images for detecting Plasmodium parasites. YOLOv5x demonstrated a high performance with a precision of 92.10%, recall of 93.50%, an F-score of 92.79% and mAP0.5 of 94.40% for detecting leukocytes, early and mature Plasmodium trophozoites. Attention modules were also tested, but showed no significant improvement over YOLOv5x. To further enhance the diagnostic process, a 3D-printed robotic system was designed for automating optical microscopy, enabling auto-focusing and slide tracking. Integrated into the iMAGING smartphone application, this system provides fully automated malaria diagnostics, including the ability to determine Plasmodium infection and parasite levels in Giemsa-stained thick blood smear samples.

In [33], the authors proposed a novel semantic segmentation neural-network architecture for rapid malaria detection. This method quickly generates classification masks that indicate the position, shape and type of detected elements in blood samples. Addressing the challenges of manual diagnosis, the approach uses light microscope imagery to classify cells into three categories: healthy, malaria-infected and background. The generated masks, which can be color-coded for better visualization, facilitate semi-automatic disease recognition while leaving the final diagnosis to specialists. The system demonstrated a high recognition accuracy of 96.65% with minimal computational demands, thus enhancing diagnostic speed and reducing misclassification rates by providing valuable additional information to healthcare providers [33].

The main contribution of [34] is the development of RBCNet, a novel pipeline for red blood-cell detection in blood smear microscopy images. RBCNet integrates a dual DL architecture: a U-Net for initial cell-cluster segmentation and a Faster R-CNN for refined detection of small cell objects. This approach, based on cell clustering rather than region proposals, enhances robustness to cell fragmentation and scalability for fine-scale structures. Tested on nearly 200,000 labeled cells from malaria smears, RBCNet achieved over 97% detection accuracy. The pipeline significantly improves detection precision and reduces false alarms, marking a crucial step toward automated malaria diagnosis.

Maqsood, A. et al. [35] proposed a custom CNN-based architecture consisting of 5 convolutional layers, 5 max-pooling layers and 2 fully connected layers. Augmentation techniques were employed to enhance the features of red blood cells before training the model. The model was evaluated using the NIH malaria benchmark dataset.

In [36], the authors modified the YOLOv4 architecture by layer pruning and backbone replacement to improve its efficiency and accuracy in detecting malaria-infected cells. By strategically removing residual blocks from layers C3 to C5 and replacing the CSP-DarkNet53 backbone with a shallower ResNet50 network, the study successfully created a lighter model that maintains a strong performance.

Chaudhry, H. et al. proposed a DL approach that not only classifies the malaria parasite type, but also identifies the life-cycle stage of the infected cell. The proposed architecture is more than twenty times lighter than the widely used Dense Convolutional Network (DenseNet) and contains less than 0.4 million parameters, making it a suitable option for mobile applications in economically disadvantaged regions for malaria detection [37].

In the context of evaluating image-segmentation models, several key metrics are commonly used to measure performance comprehensively. Accuracy is frequently used to assess the overall correctness of model predictions (Equation 1). Specificity refers to the proportion of true negative predictions among all actual negatives (Equation 2). Precision and Recall are critical for understanding the model's performance in distinguishing between classes, focusing on the accuracy of positive predictions and recall highlighting the model's ability to identify all positive instances (Equations 3, 4). The F1-score is a balanced metric by combining precision and recall, providing a single measure that considers both false positives and false negatives (Equation 5). In image segmentation, the Dice coefficient is a popular metric for evaluating the overlap between predicted and true masks, offering insights into the model's segmentation accuracy (Equation 6). These metrics collectively contribute to a robust evaluation framework, ensuring a well- rounded assessment of model performance across different tasks [38].

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

$$Specificity = \frac{(TN)}{(TN+FN)} \quad (2)$$

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

$$Precision = \frac{TP}{(TP+FP)} \quad (4)$$

$$F1-score = \frac{2\times Precision\times Recall}{Precision+Recall} \quad (5)$$

$$Dice = \frac{2.|A\cap B|}{|A|+|B|} \quad (6)$$

where:

- TP (True Positive), TN (True Negative), FP (False Positive) and FN (False Negative).
- $|A|$ is the total number of elements in the predicted segmentation.
- $|B|$ is the total number of elements in the ground-truth segmentation.
- $|A \cap B|$is the number of elements in the intersection of the predicted and ground-truth segmentations.

Table 1. Summary of recent related works in malaria segmentation.

Study	Year	Method	Dataset	Performance
[27]	2024	Decision Tree	27,558 images	Accuracy = 77.32% Precision = 77.31% Recall = 77.37% F-score = 77.48%
[28]	2024	CapsNet	27,558 images	Detection rate = 99% Accuracy = 99.08% FAR = 0.97%
[29]	2019	U-Net	30 images	F1-score = 92.97% PPV = 97.15% Sensitivity = 89.57% Accuracy= 90.9%
[30]	2020	Bilateral Filtering+Image Processing	27,558 images	Precision = 92.97% Specificity = 97.15% Recall = 89.57% Accuracy = 90.9% F1-score = 91.53%
[31]	2022	CNN	27,558 images	Accuracy = 97%
[32]	2023	YOLOv5x	2571 images	Precision = 92.10% Recall = 93.50% F-score = 92.79% mAP0.5 = 94.40%
[33]	2023	Semantic Segmentation CNN	80,000 cells	Accuracy = 99.66%
[34]	2020	RBCNet (U-Net+Faster R-CNN)	965 images	Accuracy = 97% F1-Measure = 97.76% Precision = 97.51% Recall = 98.07%
[35]	2021	CNN	27,558 images	Specificity = 97.78% Sensitivity = 96.33% Precision =96.82% Accuracy = 96.82% F1-Score = 96.82%
[36]	2024	Modifed YOLOv4	A=210 images, B=472 images	mAP=90.07%
[37]	2024	DL Approach	MP-IDB = 229 images, IML-Malaria = 345 images, MD-2019 = 883 images	Accuracy =99% Accuracy =92% Accuracy = 82%

3. MATERIALS AND METHODS

The research methodology (Figure 2) outlines the systematic approach taken in this study to address malaria detection through image segmentation, starting with a thorough problem analysis that identifies key challenges and establishes research objectives, inspired by related recent works. Following this, the methodology details the data collection and pre-processing steps, where images are sourced from Kaggle, a benchmark dataset, resized, normalized and prepared for training, alongside the generation of dummy masks for segmentation. The core of the methodology involves the design and implementation of a U- Net model enhanced with a spatial-attention mechanism and K-anonymity for privacy preservation, culminating in a rigorous evaluation phase that assesses the model's performance using metrics, such as accuracy, precision, recall and F1-score, ensuring its effectiveness in real-world applications.

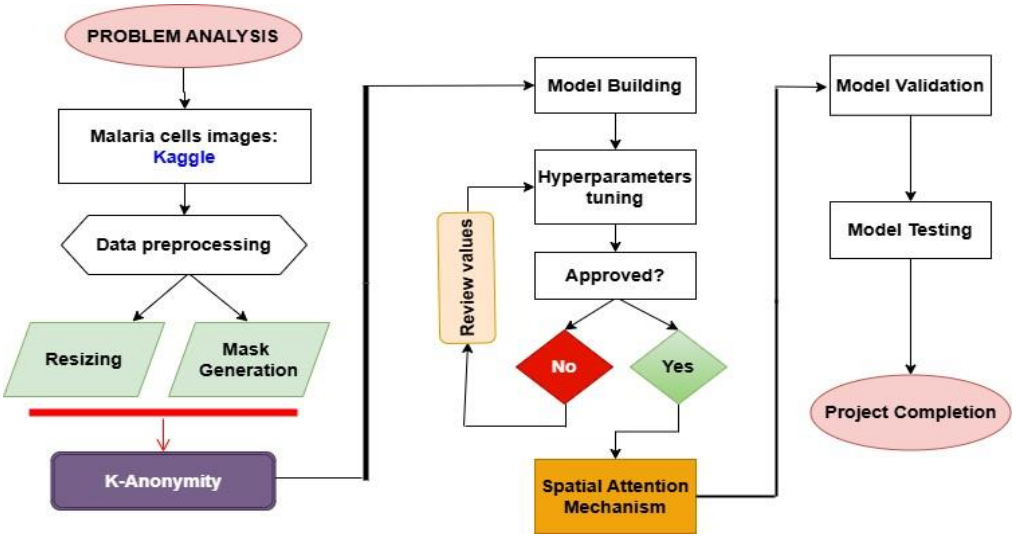

Figure 2. Research methodology overview.

3.1 Dataset

The dataset provided by the National Institutes of Health (NIH) includes publicly accessible images of peripheral blood smears from individuals, featuring both healthy subjects and those diagnosed with malaria. These images were collected at the Lister Hill National Center for Biomedical Communications, using Giemsa-stained blood samples from 150 patients infected with Plasmodium falciparum and 50 healthy individuals. The dataset comprises 27,558 images, with an equal distribution of infected and healthy cells, https://www.kaggle.com/datasets/iarunava/cell-images-for-detecting-malaria, (Figure 3).

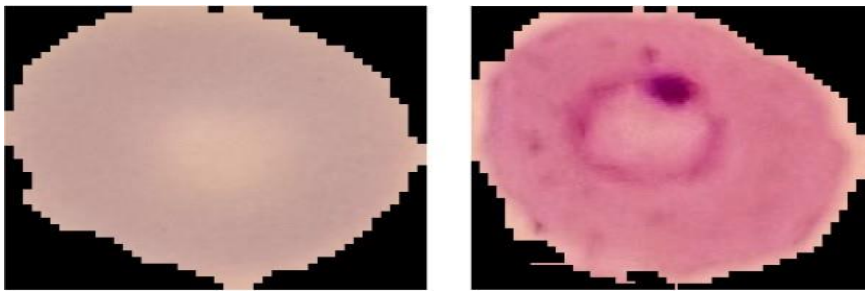

Figure 3. Dataset.

3.2 Data Pre-processing

The dataset used in our study consists of images representing both parasitized and uninfected cells. Each image is resized to a uniform dimension of 64x64 pixels and the pixel values are normalized to a range between 0 and 1, ensuring consistency and comparability in the input data. To facilitate training and evaluation, the dataset is divided into training and testing sub-sets, with 20% of the data reserved for testing to accurately assess the performance of our proposed architecture. For the segmentation task, binary masks are generated using a thresholding approach. The images are first converted into grayscale and a specific threshold is applied to create the masks, which serve as ground truth during the segmentation process.

3.3 K-Anonymity Method

Before delving into the details of the U-Net architecture, it is crucial to discuss the application of the k- anonymity method to the dataset. K-anonymity is a privacy-preserving technique used to protect sensitive information in datasets by ensuring that each record is indistinguishable from at least k-1 other records.

In this study, k-anonymity is applied to the cell images to safeguard the privacy of the individuals represented in the dataset. The function takes the dataset of cell images and a parameter k, which

determines the level of anonymity. It generates random noise with a uniform distribution between -0.1 and 0.1, with the same shape as the input images. The noise is then added to the original images and the resulting values are clipped to ensure that they remain within the valid pixel-value range of 0 to 1.

By adding random noise to the images, the k-anonymity method ensures that any identifying information related to the individuals in the dataset is obscured. This approach effectively "hides" each individual's data among at least k-1 other records, making it difficult for malicious parties to trace sensitive information back to specific individuals.

The application of k-anonymity is critical in medical and biological research, where maintaining the confidentiality of patient data is crucial. By implementing this method, researchers can conduct their analysis while adhering to ethical standards and protecting the privacy of the individuals involved in their studies. After applying k-anonymity, the noisy images are used as input to the U-Net model for the segmentation task. The model architecture is designed to maintain the utility of the data while respecting the privacy constraints imposed by the k-anonymity method.

3.4 Model Architecture

The U-Net model (Figure 4) with spatial attention is constructed to perform image-segmentation tasks effectively. It comprises three main components: the encoder, the bottleneck and the decoder. Each of these components plays a crucial role in processing the input images and generating the output masks.

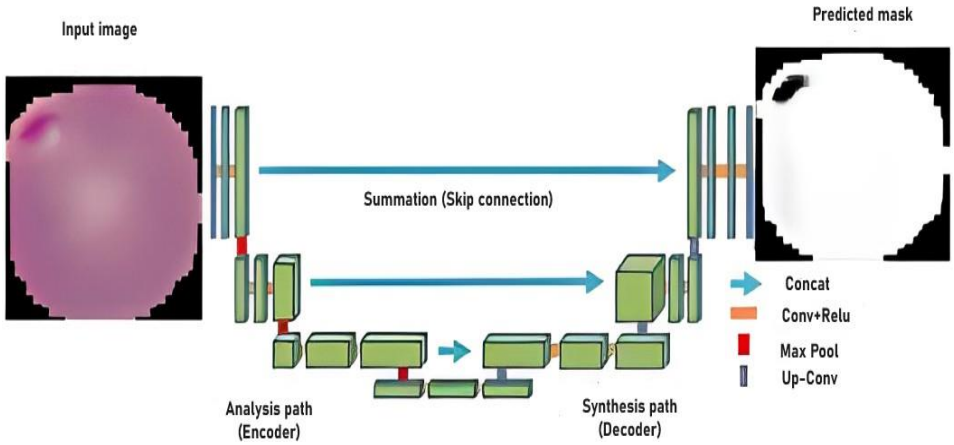

Figure 4. U-Net architecture.

3.4.1 Encoder

The encoder is responsible for capturing features from the input images through a series of convolutional and max-pooling operations. The architecture is structured as follows:

1) Convolutional Layers: The encoder begins with a series of convolutional layers that apply filters to the input images. For instance, the first block consists of two convolutional layers, each with 64 filters (3x3 kernel size) and Rectified Linear Unit (ReLU) activation. These layers help extract low-level features, such as edges and textures.
2) Max-Pooling Layers: Following the convolutional layers, a max-pooling layer (2x2 pooling size) is applied. This operation reduces the spatial dimensions of the feature maps, effectively down-sampling the input and allowing the model to focus on more abstract representations as it progresses deeper into the network.
3) Repeated Blocks: The encoder consists of multiple blocks, each progressively increasing the number of filters (128, 256 and 512) while maintaining the same structure of two convolutional layers followed by a max-pooling layer. This hierarchical structure enables the model to learn increasingly complex features at different resolutions.

3.4.2 Bottleneck

The bottleneck serves as the crucial transition between the encoder and the decoder, effectively

capturing the most salient features from the down-sampled representations. It consists of two deep convolutional layers, each equipped with 1024 filters. These layers operate on the most compressed feature maps, enabling the model to learn high-level representations that encapsulate essential information from the input images. This design allows for a more efficient encoding of the data, ensuring that vital characteristics are preserved for subsequent decoding.

3.4.3 Decoder

The decoder is designed to reconstruct the output segmentation masks from the encoded features. It mirrors the encoder's structure and includes the following components:

1) Up-sampling Layers: Each decoding block begins with an up-sampling layer that increases the spatial dimensions of the feature maps. This step effectively reverses the down-sampling performed in the encoder.
2) Skip Connections: After up-sampling, the decoder concatenates the up-sampled features with the corresponding features from the encoder. This skip connection allows the model to retain spatial information lost during down-sampling, enhancing the reconstruction accuracy.
3) Spatial Attention Layers: The primary objective of the Spatial Attention Mask (SAM) is to create an attention mask that enhances the accuracy of feature extraction from a feature map. This process involves three sequential steps. The first step is down-sampling, where the dimensions of the feature map are reduced. This is achieved by applying average-pooling and max-pooling operations along the channel axis, followed by concatenation of the results to form a compact feature descriptor. Next, this descriptor is processed through a convolutional layer with a 7×7 filter size, using padding to preserve the spatial dimensions. In the final step, the output from the convolutional layer is passed through a sigmoid activation function, which scales the values to a range between 0 and 1, resulting in the attention mask. To enhance the features further, an element-wise multiplication is performed between the original feature map and the generated attention mask, effectively emphasizing the most informative pixels while diminishing less relevant ones (Figure 5).

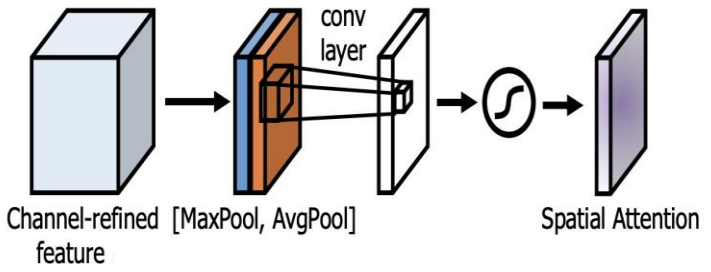

Figure 5. Spatial-attention mechanism.

The attention map highlights the most relevant spatial regions by multiplying them element-wise with the input features, effectively guiding the model to focus on important areas during the reconstruction process.

4) Repeated Blocks: The decoder continues with additional blocks, each consisting of two convolutional layers (with 512, 256 and 128 filters, respectively), followed by an up-sampling layer and a spatial-attention layer. This structure allows for a detailed reconstruction of the output mask.
5) Output Layer: Finally, a convolutional layer with a single filter and sigmoid activation is applied to the output of the last decoding block. This layer generates the final segmentation mask, providing a binary output that indicates the presence or absence of the target features.

Figure 6 illustrates the U-Net model enhanced with a spatial-attention mechanism integrated into the decoding path. The architecture includes an encoder consisting of four convolutional blocks, a central bottleneck block and a decoder with four convolutional blocks. The spatial-attention mechanism is applied after each convolutional layer in the decoder blocks to emphasize important regions of the input images. This mechanism helps in improving the segmentation accuracy by

focusing on the most relevant features in the image. The final output layer generates the segmented output based on the attention- enhanced feature maps.

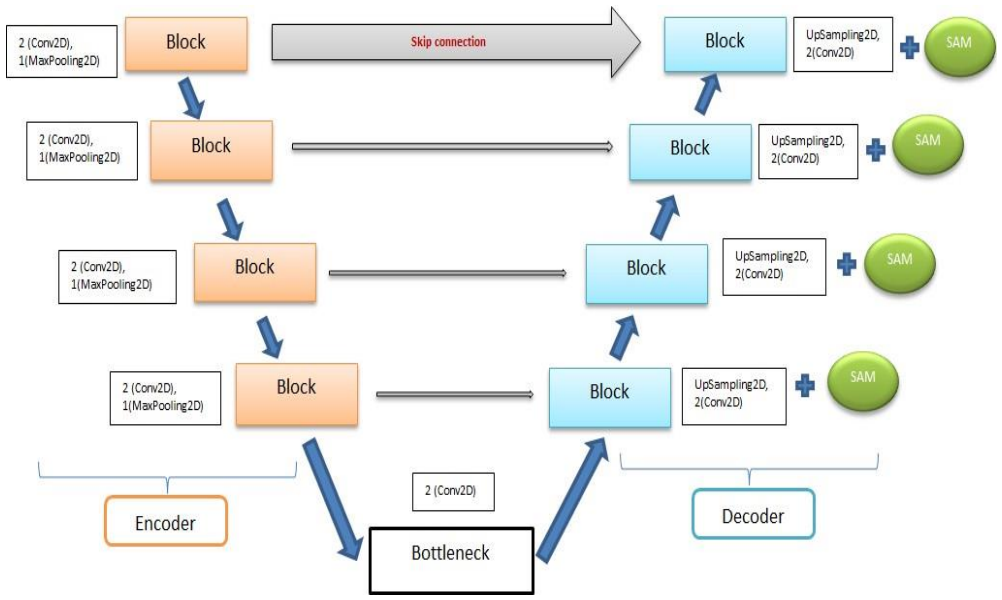

Figure 6. Proposed model: U-Net architecture with spatial-attention mechanism (SAM).

Table 2 summarizes the hyper-parameter values used in the U-Net model for malaria detection. These values were selected after extensive testing and empirical evaluation to optimize the model's performance. The careful tuning of these hyper-parameters is crucial for achieving effective segmentation and ensuring robust results across different datasets.

Table 2. Hyper-parameter summary for our proposed model.

Hyper-parameter	**Value**
Batch Size	16
Learning Rate	0.001
Number of Epochs	10
Convolutional Filter Sizes	
Layer 1	64 filters (3x3)
Layer 2	128 filters(3x3)
Layer 3	256 filters (3x3)
Layer 4	512 filters (3x3)
Bottleneck Layer	1024 filters (3x3)
Activation Function	ReLU
Pooling Dropout Rate	Max-pooling (2x2) 0.2
Spatial-attention Layer	
Convolution Kernel Size	7x7
Number of Filters	1
Activation Function	Sigmoid
K-Anonymity Parameters	
Noise Level	0.1
Number of Neighbors (k)	3

4. RESULTS AND DISCUSSION

The segmentation results demonstrate the effectiveness of the proposed approach in accurately identifying and delineating malaria-infected cells from microscopic blood smear images (Figure 7). The input image shows a representative field of view containing both infected and uninfected red blood cells. The true mask serves as the ground truth for infected cell regions. The predicted mask, generated by the segmentation model, closely matches the true mask, indicating a high degree of accuracy in identifying the infected cells. By comparing the predicted segmentation to the true mask,

the model achieves a Dice score of 99.61%, confirming its ability to locate and segment malaria-infected cells precisely. These results suggest that the proposed approach can serve as a reliable tool for automated malaria diagnosis, potentially aiding healthcare workers in resource-limited settings, where access to expert microscopy is limited.

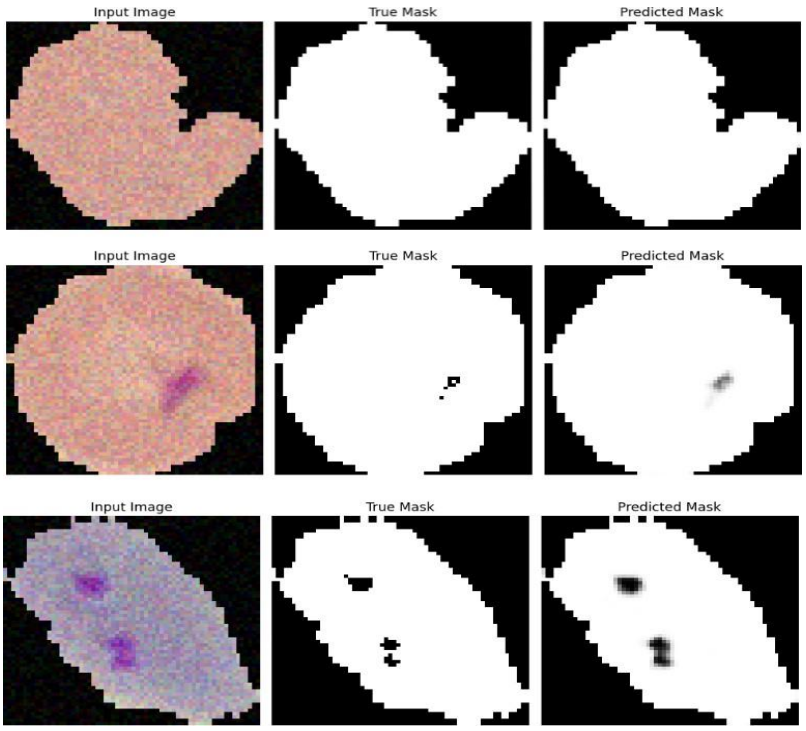

Figure 7. Segmentation results: Input image with k-anonymity, true mask and predicted mask.

The accuracy and loss curves (Figures 8, 9) demonstrate the model's performance over training epochs. The accuracy curve shows a consistent upward trend, indicating that the model is effectively learning and improving its predictions. Simultaneously, the loss curve exhibits a downward trajectory, reflecting a reduction in prediction error. Together, these curves suggest that the model is successfully optimizing its performance, achieving high accuracy while minimizing loss. This correlation between accuracy and loss indicates a well-trained model capable of generalizing well to unseen data.

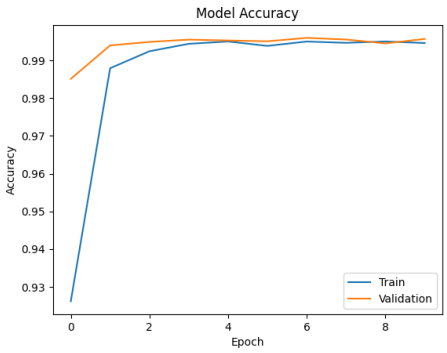

Figure 8. Accuracy curve.

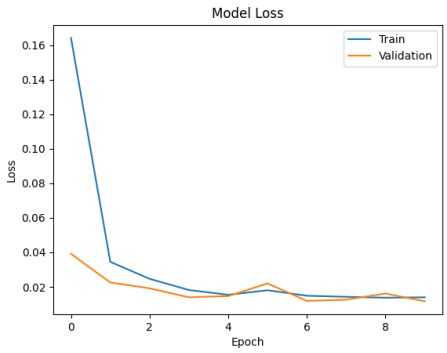

Figure 9. Loss curve.

This study introduces several significant contributions to the field of medical-image segmentation, specifically for malaria-cell detection. Our approach integrates multiple advanced techniques to enhance both the accuracy of segmentation and the privacy of sensitive data.

4.1 Enhanced U-Net Architecture with Spatial-attention Mechanism

One of the primary contributions of this study is the development of a U-Net architecture enhanced with a spatial-attention mechanism. The incorporation of this mechanism enables the model to focus on the most relevant regions of the input images, improving the extraction of critical features and

thus enhancing segmentation performance. This attention mechanism allows the network to dynamically emphasize important areas while suppressing less relevant information, leading to more precise and reliable segmentation results. The empirical performance improvements observed validate the effectiveness of this approach in addressing complex medical-imaging tasks.

4.2 Privacy Preservation through K-Anonymity

In addition to architectural improvements, we have incorporated k-anonymity to address privacy concerns associated with medical data. By adding random noise to the images, k-anonymity ensures that individual identities remain confidential, effectively protecting patient privacy while maintaining the integrity of the dataset. This technique demonstrates our commitment to ethical considerations in data handling and supports the deployment of ML models in sensitive healthcare environments without compromising data security.

4.3 Generalization Capability

In recent studies, the generalization capability of deep-learning models has been increasingly recognized as a crucial factor in their effectiveness across various domains [39]. This sub-section discusses the successful application of a model initially trained on malaria-cell images to a newly introduced real Cactus-disease dataset, which has not yet been published. The dataset comprises 343 images of healthy cacti and 285 images of diseased cacti. The results demonstrate the model's ability to generalize and perform effectively in the agricultural domain.

The model architecture originally designed for analyzing malaria cell images was adapted to address the challenges posed by the Cactus-disease dataset. The U-Net model, known for its efficacy in image-segmentation tasks, was employed to identify and classify diseases affecting cactus plants. The training process involved using the Cactus-disease dataset included a diverse set of images, depicting healthy and diseased cactus specimens.

The successful application of the model to the Cactus-disease dataset illustrates its generalization capability, showcasing how insights gained from one biological domain (malaria-cell images) can be effectively transferred to another (cactus diseases). This cross-domain application not only highlights the versatility of DL models, but also emphasizes their potential in agricultural practices, where timely and accurate disease detection is critical for crop management (Figure 10).

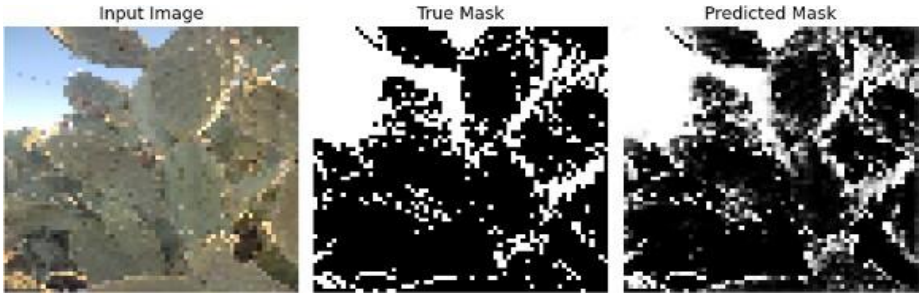

Figure 10. Segmentation results for the second dataset in agriculture domain.

The evaluation metrics for the Cactus-disease detection model are as follows: the F1-score is 98.44%, indicating a strong balance between precision and recall; the Dice score is 95.08%, reflecting the model's accuracy in segmenting the diseased areas; the Precision is 98.04%, demonstrating the model's effectiveness in minimizing false positives; and the Recall is 98.86%, highlighting the model's ability to identify diseased cacti correctly. These results underscore the model's high performance in accurately detecting cactus diseases (Figure 11).

4.4 Comprehensive Evaluation and Validation

The study includes a thorough evaluation of the model's performance using a range of metrics, such as accuracy, precision, recall and F1-score. This comprehensive assessment provides a robust understanding of the model's capabilities and potential for real-world applications. The positive results from these evaluations further strengthen the validity of our proposed method.

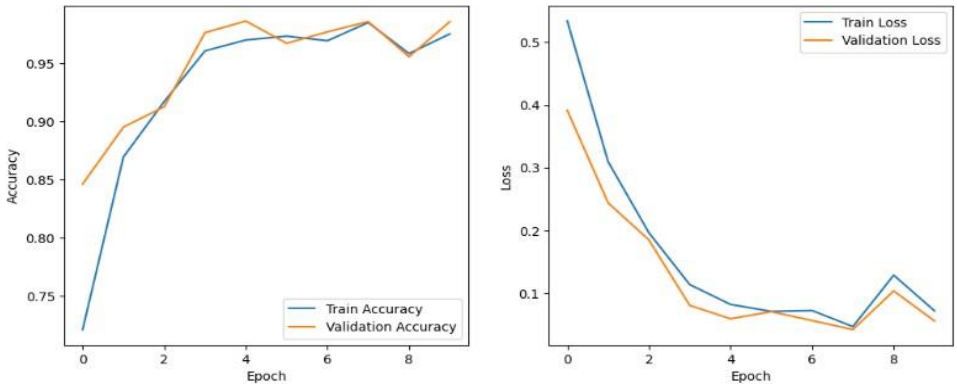

Figure 11. Accuracy and loss curves for Cactus dataset.

Table 3. Comparison of different methods based on performance, privacy and generalization.

Method	Dataset	Performance	Privacy	Generalization
Decision Tree	27,558 images	Accuracy=77.32% Precision = 77.31% Recall = 77.37% F-score = 77.48%	x	x
CapsNet	27,558 images	Detection rate = 99% Accuracy = 99.08% FAR = 0.97%	x	x
U-Net	30 images	F1-score = 92.97 PPV = 97.15% Sensitivity = 89.57% Accuracy = 90.9%	x	x
Bilateral Filtering + Image Processing	27,558 images	Precision = 92.97% Specificity = 97.15% Recall = 89.57% Accuracy = 90.9% F1-score = 91.53%	x	x
CNN	27,558 images	Accuracy = 97%	x	x
YOLOv5x	2,571 images	Precision = 92.10% Recall = 93.50% F-score = 92.79% mAP0.5 = 94.40%	x	x
Semantic Segmentation CNN	80,000 cells	Accuracy = 99.66%	x	x
U-Net + Faster R- CNN	965 images	Accuracy = 97% F1-Measure = 97.76% Precision = 97.51% Recall = 98.07%	x	x
CNN	27,558 images	Specificity = 97.78% Sensitivity = 96.33% Precision =96.82% Accuracy = 96.82% F1-Score=96.82%	x	x
Modified YOLOv4	A=210 images, B=472 images	mAP=90.07%	x	x
DL Approach	MP-IDB=229 images, IML-Malaria=345 images, MD-2019= 883 images	Accuracy =99% Accuracy =92% Accuracy=82%	x	x
Proposed Method	**27,558 images**	**Accuracy = 99.60%** **Dice Score = 99.61%** **Precision = 99.42%** **Recall = 99.96%** **F1-score = 99.69%**	√	√

4.4.1 Limitations

In our work on Kaggle, we have encountered limitations related to computational resources, particularly when using central-processing units (CPUs) for our tasks. Although Kaggle provides a robust environment with access to graphical-processing units (GPUs), reliance on CPUs can result in slower processing times, hindering our ability to efficiently test and iterate on models. The platform's current restrictions, such as the cap on GPU usage at thirty hours per week, also require us to strategically manage our computational tasks to maximize efficiency. This necessitates optimizing our code and pre-processing steps to alleviate the burden on CPU resources. Consequently, while we can leverage Kaggle's capabilities for our projects, these resource limitations demand careful planning and execution to achieve our objectives effectively.

4.4.2 Advantages and Disadvantages

The integration of our proposed approach combines advanced malaria-detection techniques, resulting in several significant advantages. First, the model achieves a high diagnostic accuracy, with a validation accuracy of 99.60% and a Dice score of 99.61%, ensuring reliable malaria detection. Furthermore, it improves data privacy by using the k-anonymity technique, which protects sensitive medical information and minimizes the risk of re-identification, thus ensuring compliance with privacy regulations. Moreover, the approach exhibits improved segmentation performance through a customized spatial-attention mechanism that focuses on critical image features, leading to better results. It also demonstrates a strong generalization ability, achieving an accuracy of 98.58% on the Cactus dataset, a real-world image dataset, indicating its adaptability beyond malaria detection. Automating diagnostic processes reduces the workload of healthcare professionals by streamlining the analysis of cellular images, enabling more efficient patient care. Finally, early and accurate diagnosis through this approach can significantly reduce the risk of serious health complications associated with malaria, contributing to improved health outcomes.

One notable disadvantage of this study is the manual selection of hyper-parameters for the U-Net model, which demands significant time and effort to identify optimal values. This process involves extensive testing and experimentation, making it time-consuming and potentially subjective. Consequently, the chosen hyper-parameters may not represent the best possible configuration for all datasets.

5. CONCLUSION

In this study, we presented a novel approach to malaria detection through cell-image segmentation using a U-Net architecture enhanced with a custom spatial-attention mechanism and K-anonymity for privacy preservation. The model demonstrated an exceptional performance on the malaria-cell image dataset, achieving a high validation accuracy, as well as high Dice score and precision. These results underscore the effectiveness of integrating advanced neural-network architectures with privacy-preserving techniques, addressing both the need for accurate disease detection and safeguarding sensitive patient data.

Furthermore, the model's generalization capability was validated through its application to a real Cactus-disease dataset, where it maintained a strong performance. This indicates the potential for cross-domain applications of the model, paving the way for its use in various agricultural and medical-imaging tasks. While the study achieved significant results, it also highlighted the challenges associated with manual hyper-parameter selection, which can be time-consuming and subjective. Future work should focus on automating this process to enhance model efficiency and adaptability.

Overall, this research contributes to the development of secure and reliable diagnostic tools in both medical and agricultural fields, promoting the integration of privacy-aware methodologies in machine-learning applications.

Future research could focus on several approaches to further enhance the effectiveness and applicability of the proposed model. For instance, employing automated hyper-parameter optimization methods, like grid search or Bayesian optimization, could refine the tuning process and boost the model performance.

REFERENCES

[1] E. O. Kolawole et al., "Malaria Endemicity in Sub-Saharan Africa: Past and Present Issues in Public Health," Microbes and Infectious Diseases, vol. 4, no. 1, pp. 242-251, 2023.

[2] J. Li et al., "Current Status of Malaria Control and Elimination in Africa: Epidemiology, Diagnosis, Treatment, Progress and Challenges," Journal of Epidemiology and Global Health, vol. 14, no. 3, pp. 561-579, DOI: 10.1007/s44197-024-00228-2, 2024.

[3] P. Venkatesan, "The 2023 WHO World Malaria Report," The Lancet Microbe, vol. 5, no. 3, p. e214, 2024.

[4] A. Mbanefo and N. Kumar, "Evaluation of Malaria Diagnostic Methods As a Key for Successful Control and Elimination Programs," Tropical Medicine and Infectious Disease, vol. 5, no. 2, p. 102, 2020.

[5] P. Gupta, "Rapid Diagnostic Tests for Malaria: Challenges and Future Prospects, a Brief Review," Challenges and Advances in Pharmaceutical Research, vol. 8, pp. 152-62, 2022.

[6] O. O. Oyegoke et al., "Malaria Diagnostic Methods with the Elimination Goal in View," Parasitology Research, vol. 121, no. 7, pp. 1867-1885, 2022.

[7] S. Minaee et al., "Image Segmentation Using Deep Learning: A Survey," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 44, no. 7, pp. 3523-3542, 2021.

[8] M. Z. Khan et al., "Deep Neural Architectures for Medical Image Semantic Segmentation," IEEE Access, vol. 9, pp. 83002-83024, DOI: 10.1109/ACCESS.2021.3086530, 2021.

[9] D. D. Patil and S. G. Deore, "Medical Image Segmentation: A Review," International Journal of Computer Science and Mobile Computing, vol. 2, no. 1, pp. 22-27, 2013.

[10] I. Jdey et al., "Fuzzy Fusion System for Radar Target Recognition," International Journal of Computer Applications & Information Technology, vol. 1, no. 3, pp. 136-142, 2012.

[11] G. Hcini et al., "HSV-Net: A Custom CNN for Malaria Detection with Enhanced Color Representation," Proc. of the 22th IEEE Int. Conf. on Cyberworlds (CW), pp. 337-340, Sousse, Tunisia, 2023.

[12] G. H Hcini, I. Jdey and H. Ltifi, "Improving Malaria Detection Using L1 Regularization Neural Network," JUCS: Journal of Universal Computer Science, vol. 28, no. 10, pp. 1087-1107, 2022.

[13] M. A. Abdou, "Literature Review: Efficient Deep Neural Networks Techniques for Medical Image Analysis," Neural Computing and Applications, vol. 34, no. 8, pp. 5791-5812, 2022.

[14] Tobias Mourier et al., "The Genome of the Zoonotic Malaria Parasite Plasmodium Simium Reveals Adaptations to Host Switching," BMC Biology, vol. 19, p. 219, pp. 1-17, 2021.

[15] D. Sukumarran et al., "Machine and Deep Learning Methods in Identifying Malaria through Microscopic Blood Smear: A Systematic Review," Engineering Applications of Artificial Intelligence, vol. 133, no. E, p. 108529, 2024.

[16] Y. Lv et al., "Attention Guided U-Net with Atrous Convolution for Accurate Retinal Vessels Segmentation," IEEE Access, no. 8, pp. 32826-32839, DOI: 10.1109/ACCESS.2020.2974027, 2020.

[17] G. Du et al., "Medical Image Segmentation Based on U-Net: A Review," Journal of Imaging Science & Technology, vol. 64, Article ID: jist0710, 2020.

[18] R. Azad et al., "Medical Image Segmentation Review: The Success of U-Net," IEEE Trans. on Pattern Analysis and Machine Intelligence, Early Access, pp. 1-20, DOI: 10.1109/TPAMI.2024.3435571, 2024.

[19] A. Ben Hamida et al., "Deep Learning for Colon Cancer Histopathological Images Analysis," Computers in Biology and Medicine, vol. 136, p. 104730, 2021.

[20] Z. Cheng, A. Qu and X. He, "Contour-aware Semantic Segmentation Network with Spatial Attention Mechanism for Medical Image," The Visual Computer, vol. 38, no. 3, pp. 749-762, 2022.

[21] Z. Chen et al., "An Object Detection Network Based on YOLOv4 and Improved Spatial Attention Mechanism," Journal of Intelligent & Fuzzy Systems, vol. 42, no. 3, pp. 2359-2368, 2022.

[22] V. D. Karalis, "The Integration of Artificial Intelligence into Clinical Practice," Applied Biosciences, vol. 3, no. 1, pp. 14-44, 2024.

[23] I. Jdey, "Trusted Smart Irrigation System Based on Fuzzy IoT and Blockchain," Proc. of the Int. Conf. on Service-oriented Computing (ICSOC 2022), pp. 154–165, Sevilla, Spain, 2022.

[24] C. N. Sowmyarani et al., "Enhanced k-Anonymity Model Based on Clustering to Overcome Temporal Attack in Privacy Preserving Data Publishing," Proc. of the 2022 IEEE Int. Conf. on Electronics, Computing and Comm. Techn. (CONECCT), DOI: 10.1109/CONECCT55679.2022.9865682, Bangalore, India, 2022.

[25] A. Majeed and S. Lee, "Anonymization Techniques for Privacy Preserving Data Publishing: A Comprehensive Survey," IEEE Access, vol. 9, pp. 8512-8545, 2020.

[26] K. El Emam and F. K. Dankar, "Protecting Privacy Using K-Anonymity," Journal of the American Medical Informatics Association, vol. 15, no. 5, pp. 627-637, 2008.

[27] N. Rismayanti, "Segmentation and Feature Extraction for Malaria Detection in Blood Smears," International Journal of Artificial Intelligence in Medical Issues, vol. 2, no. 1, pp. 18-29, 2024.

[28] S. Aanjan Kumar et al., "Application of Hybrid Capsule Network Model for Malaria Parasite Detection on Microscopic Blood Smear Images," Multimedia Tools and Applications, vol. 2024, DOI: 10.1007/s11042-024-19062-6, 2024.
[29] J. B. Abraham, "Malaria Parasite Segmentation Using U-Net: Comparative Study of Loss Functions," Communications in Science and Technology, vol. 4, no. 2, pp. 57-62, 2019.
[30] F. Tehreem and M. Shahid Farid, "Automatic Detection of Plasmodium Parasites from Microscopic Blood Images," Journal of Parasitic Diseases, vol. 44, no. 1, pp. 69-78, 2020.
[31] A. H. Alharbi et al., "Detection of Peripheral Malarial Parasites in Blood Smears Using Deep Learning Models," Computational Intelligence and Neuroscience, vol. 2022, no. 1, p. 3922763, 2022.
[32] C. R Maturana et al., "iMAGING: A Novel Automated System for Malaria Diagnosis by Using Artificial Intelligence Tools and a Universal Low-cost Robotized Microscope," Frontiers in Microbiology, vol. 14, p. 1240936, DOI: 10.3389/fmicb.2023.1240936, 2023.
[33] N. Wojtas et al., "Malaria Detection Using Custom Semantic Segmentation Neural Network Architecture," Medycyna Weterynaryjna, vol. 79, no. 8, pp. 406-412, 2023.
[34] Y. M. Kassim et al., "Clustering-based Dual Deep Learning Architecture for Detecting Red Blood Cells in Malaria Diagnostic Smears," IEEE Journal of Biomedical and Health Informatics, vol. 25, no. 5, pp. 1735-1746, 2020.
[35] A. Maqsood et al., "Deep Malaria Parasite Detection in Thin Blood Smear Microscopic Images," Applied Sciences, vol. 11, no. 5, p. 2284, 2021.
[36] D. Sukumarran et al., "An Optimised YOLOv4 Deep Learning Model for Efficient Malarial Cell Detection in Thin Blood Smear Images," Parasites & Vectors, vol. 17, no. 1, p. 188, 2024.
[37] H. A. H. Chaudhry et al., "A Lightweight Deep Learning Architecture for Malaria Parasite-type Classification and Life Cycle Stage Detection," Neural Computing and Applications, vol. 36, pp. 19795-19805, 2024.
[38] G. Hcini et al., "Investigating Deep Learning for Early Detection and Decision-making in Alzheimer's Disease: A Comprehensive Review," Neural Processing Letters, vol. 56, Article no. 153, 2024.
[39] J. Wang et al., "Generalizing to Unseen Domains: A Survey on Domain Generalization," IEEE Transactions on Knowledge and Data Engineering, vol. 35, no. 8, pp. 8052-8072, 2022.

ملخص البحث:

يُعدّ الكشْف عن الملاريا عن طريق تحليل صور الخلايا أمراً أساسياً للتّشخيص المبكّر والعلاج الفعّال؛ نظراً لأنّ الكشف في الوقت المناسب يُمكنُهُ أن يخفّض من مخاطر حُدوث مُضاعفاتٍ خطرة. إلا أنّ هذه المسألة تنطوي على تحدّياتٍ ترتبط بالخصوصية بسبب حساسية المعلومات الطبية.

تقدّم هذه الدّراسة نموذجاً مبتكراً يراعي الخُصوصية ويتجنّب الكشف عن هوية المريض؛ من أجل تحسين الأمان جنباً إلى جنبٍ مع الحفاظ على دقّة عالية. ويعمل النّموذج المقترح بآليةٍ تضْمن تحسينَ أداءِ تجْزِئة الصُّوَر، ويعتمد على تقنياتٍ متقدّمةٍ للتّركيز على السِّمات الحاسمة دون سواها. أمّا عدمُ الكشف عن الهوية فيتضمّن الحفاظَ على سِرّيّة المعلومات الحسّاسَة.

ولدى تقييم النّموذج المقترح بناءً على مجموعةٍ من مؤشّرات الأداء، أبْدى النّموذج نتائج جيّدة عند تجريبه على صُوَرِ خلايا الملاريا بدقّةٍ بلغت 99.60%. وعند تطبيقِ النّموذجِ على مجموعةِ بياناتِ نَباتِ الصّبّار، بلغت دقّته 98.58%، الأمر الّذي يعني إمكانية تعميم النّموذج لِيُطبَّق في مجالاتٍ متعدّدةٍ. وتشيرُ نتائجُ التّقييم إلى أنّ النّموذجَ المقترحَ يَجمع بين تحسينِ الأمانِ وارتفاعِ مُستوى الأداءِ في تطبيقاتٍ متنوّعةٍ لتحليلِ الصُّوَر.