International Information and Engineering Technology Association
Advancing the World of Information and Engineering

International Journal of Safety and Security Engineering
Vol. 14, No. 3, June, 2024, pp. 941-952
Journal homepage: http://iieta.org/journals/ijsse

Using Crossover Area of the Retinal Eye to Generate a Secret Key Based on Deep Learning-YOLO-v5 Object Detection Algorithm

Zainab Sahib Dhahir*, Israa Ali Alshabeeb, Khamael Raqim Raheem, Wafaa Mohammed Ridha Shakir

Department of Technical Computer Systems, Technical Institute of Babylon, Al-Furat Al-Awsat Technical University, Babil 51015, Iraq

Corresponding Author Email: zainab.dhahir@atu.edu.iq

https://doi.org/10.18280/ijsse.140325

Received: 17 March 2024
Revised: 20 May 2024
Accepted: 4 June 2024
Available online: 24 June 2024

Keywords:
security key, retinal image, crossover detection, deep learning, YOLO-v5, block chain

ABSTRACT

Traditional security keys based on passwords are vulnerable to attacks. Recent developments in biometric security systems offer a solution. This study presents a novel approach for generating security keys using the YOLO-v5 deep learning model to detect crossover points in retinal images. We extract RGB hash values from these points and use blockchain to create secure keys. This method enhances security and reduces processing delays. Our approach achieved an F1-score of 69% to 76% on the DRIVE, IOSTAR, and Ibn Al-Haytham datasets, demonstrating promising results compared to existing biometric security technologies.

1. INTRODUCTION

Ensuring the security of data, whether stored or transmitted, is crucial to prevent unauthorized access. Traditional cryptosystems rely on secret keys, which can be compromised. This study addresses the need for secure key generation by leveraging biometric data, specifically the unique patterns in retinal images. We aim to develop a robust method using deep learning (YOLO-v5) and blockchain technology to generate security keys from retinal crossover points.

It is crucial to ensure the security of data, whether it is stored or transmitted across networks. Without proper security measures, unauthorized parties can access sensitive information, leading to serious consequences. Therefore, it is important to implement strong encryption and authentication methods to protect data from being compromised [1]. The basis for user authentication in conventional cryptosystems is holding secret keys; this mechanism breaks down if the secrets are shared with unauthorized users. Furthermore, keys cannot offer non-repudiation because they might be misplaced, stolen, or forgotten [2]. The degree of security of a symmetric or asymmetric encryption system depends on how secret the cryptographic key or private key is [1, 2]. The information is secure when using different cryptographic techniques, including Rivest-Shamir-Adleman (RSA), Data Encryption Standard (DES), Triple DES (3DES), and Advanced Encryption Standard [1, 3]. Regardless of their strength, all algorithms have problems with keys that need to be longer, making them vulnerable to guessing and hacking. Message authentication is also based on the key, rather than biometrics, as in traditional encryption techniques. An unauthorized user or attacker is likely to assume the correct key because key generation can be guessed or cracked. The difficulty of remembering keys and the lack of confidence in the database's ability to store them securely are two other significant barriers to achieving network security caused by key generation. Recent developments have made the crypto-biometrics system an essential remedy for the issues that plague traditional cryptography systems [4]. Crypto-biometrics system goal is to obtain the key by using the user's biometric data to address the problems currently faced by alteration, discrimination, and structure. It is called distortion to account for the biometric variance [3, 5]. Due to the uniqueness of biometric data, this method ensures the security of digital data and makes it almost impossible to produce duplicates [3]. Regarding accuracy, the retinal biometric features recognition approach is more precise than any other biometric technology. During life, the blood vessel structure of the retina hardly changes (except in case of disease or accident). Retinal identification is most commonly used in conjunction with surveillance systems in high-security organizations due to the unique biological properties of the retina described above [4]. The system shall generate the same key for the same person, even if the biometric record is subject to different conditions. The system's security ensures that the user's biometric data is unique and that neither the key nor the biometric original can be traced or guessed [2, 3]. Therefore, the ability of biometric-based security to provide security in sophisticated technologies is quite high [3]. The retinal vascular tree is a complicated region of arteries and veins that constantly cross and split throughout the eye fundus [5]. Bifurcation makes it difficult to quantify the aspects associated with the crossings [6]. Because of the importance of vessel crossings, advances in their detection have the potential to be used for a variety of applications. In this regard, important topics such as vascular system segmentation [7] or microaneurysm identification have benefited from the application of deep neural networks (DNNs) [8]. In contrast to conventional methods, deep learning-based approaches often provide better performance because they do not need to create complicated algorithms ad hoc [6, 7]. Learning in-depth approaches and supervised learning techniques that extract invisible characteristics from un-processed picture data are widely employed for object recognition today. Deep learning (DL) has become a popular and effective approach for machine learning algorithms in the computer and information science field in areas like pattern identification, object recognition, and classification [9]. Convolutional Neural Network (CNN) is one of the various frameworks of DL and provides excellent results for classification, segmentation, and detection tasks in digital image research [10, 11]. CNN-based architectures are widely used to achieve more accurate and faster recognition in image processing [12, 13]. Based on a Region-based Convolutional Neural Network (RCNN), a junction network is used to find probable bifurcation and crossover locations on retinal color images [14]. The YOLO-v5 (You Only Look Once) algorithm approximates one of the various DL frameworks and provides excellent performance for classification, segmentation, and detection tasks in digital image analysis. YOLO–v5 performs the recognition task (localization and classification) more precisely than earlier recognition algorithms because it analyses an input image by testing the entire image [13]. The YOLO–v5 object detection algorithm developed the intersection identification and classification system. The YOLO–v5 algorithm is used for object recognition and classification. The following are the paper's primary contributions and findings:

1. Identifying vessel crossings is done by detecting two close bifurcations in recorded skeletons. This approach does not rely on geometric criteria such as connectivity, vessel angles, and vessel widths, commonly used to differentiate between crossings and bifurcations.
2. The proposed approach is designed to be independent of the accuracy of the segmentation of the blood vessel tree.
3. The approach successfully identified the retina's closely spaced and unclear intersection areas. This is a noteworthy achievement, as accurately identifying these areas can be challenging even for experienced human observers.

This paper has the following structure: in section 1, the introduction; in section 2, related works; an overview of the YOLO–v5 method and blockchain technique implemented in this paper. In section 3, the background; the methodology in section 4, experimental results and discussion in section 5, and in section 6 the conclusion and future works.

2. RELATED WORKS

Key generation technique is one of the most important factors for improving network security [8, 15]. Public-key schemes are asymmetric and require two keys, unlike typical one-key encryption based on mathematical functions [2]. Passwords can be lost, stolen, or compromised, which is the main drawback of using a key generation approach to ensure security. This part of the paper reviews the current state-of-the-art enhanced detection and classification of biometric data utilizing various techniques. Table 1 contains a summary of these associated studies.

Table 1. The summary of related biometric security systems works

Reference	Description	Performance
Tajuddin and Nandini [15]	Retina biometric parameter used for cryptographic key generation Algorithm directly generates key from retinal blood vessels information	Limits to key generation using grey scale images focus on thick blood vessels in retina for key generation.
Mazher and Waleed [16]	Retina features extracted using glowworm swarm optimization algorithm Chaotic map used for high-quality random cryptographic key generation	GSO algorithm extracts retina features for random key generation.
Salih and Mahdawi [17]	Proposed RC4-Retina algorithm based on user's retina. Introduced retina key scheduling algorithm (RKSA) for key generation.	Weaknesses in key creation and utilization Standard RC4 algorithm vulnerabilities.
Alrifaee and Ismaeel [18]	Three types of keys generated from retina vessel's	Keys based on DCE, RCE, and DRCE distances in retina.

Table 2. The summary of related detection technology

Reference	Description	Performance
Hervella et al. [5]	It takes longer to forecast bifurcation and crossover using a deep neural network that has been trained on full images.	They used DRIVE and IOSTAR datasets of reference with detailed annotations of vessel crossings and bifurcations. The proposed method achieves 74.23% and 70.90% F-scores to detect crossings and bifurcations.
Hao et al. [6]	OCTA images of the retina suggest a novel multi-task network (VAFF-Net) for joint segmentation, detection, and classification of retinal vascular junctions. The network uses a voting-based adaptive feature fusion algorithm.	Used OCTA image of DRIVE dataset for vessel segmentation, namely ROSE (Retinal OCTA segmentation) the proposed HR-Net method achieves (68.93%) F-score and (55.88%) with RB-Net method for the detection of the junctions on colored images.
Zhao et al. [14]	The RCNN-based Junction Proposal Network directly searches the potential bifurcation and crossover locations on retinal color images.	They used the DRIVE and IOSTAR datasets, with training time for the detection stage at 187 minutes and for the classification stage at 12 minutes, which achieved 70% and 60% F1 scores, respectively.
Pampana and Rayudu [19]	A method of deep learning involving a region-based convolutional neural network (RCNN) has been suggested.	Using DRIVE and IOSTAR datasets, the proposed method achieves 75% and 62% F-score for detecting the junctions.

Recent advancements in biometric security systems leverage unique human traits to enhance security. Studies have explored various biometric modalities, including fingerprints, facial recognition, and retinal scans. Retinal biometric features offer high precision due to their stability over a lifetime [20]. Previous work, such as Tajuddin and Nandini [15], Mazher and Waleed [16], Salih and Mahdawi [17], Alrifaee and Ismaeel [18], has demonstrated the use of retinal biometric data for cryptographic key generation and key management, leveraging the uniqueness and stability of the retinal blood vessel patterns. The proposed algorithms and techniques aim to enhance the security and reliability of cryptographic systems by utilizing the retinal biometric modality.

Previous studies, such as Hervella et al. [5], Hao et al. [6], and Zhao et al. [14], has demonstrated the effectiveness of deep learning models in detecting retinal features. Our study builds on these findings by employing YOLO-v5 for crossover point detection and integrating blockchain for secure key generation. As a result, research has made progress in using biometric data to generate the key by creating a distinctive key using human biometric data, such as blood vessels in the retina [9]. To ensure the security of networks, several researchers have been investigating cryptobiometric techniques for some time [10].

Tables 1 and 2 present related research on the generation of secret keys based on the major features of the eye as well as research on the detection of these features.

3. BACKGROUND

This section briefly explains deep learning, blockchain and hash function techniques used in research.

3.1 YOLO–v5 architecture

Modern real-time object detection technology is called YOLO–v5. YOLO–v5 is well known for its speed and precision, and it has been used in various fields, including healthcare, security monitoring, and self-driving cars. YOLO uses a Convolutional Neural Network (CNN) foundation–v5 to create picture features. The model's neck combines these attributes before sending them to the head. The model head then evaluates the sum of the characteristics to forecast an image [6]. Important regions (for the localization role) were found using the YOLO–v5 general-purpose object identification algorithm and the detected areas were graded (for the classification task). As illustrated in Figure 1, the YOLO-v5 model processes input retinal images through a convolutional neural network to identify crossover points. The architecture includes a backbone for feature extraction, a neck for combining features, and a head for bounding box prediction. This figure illustrates the step-by-step process from input image analysis to crossover point detection.

The YOLO–v5 model is built with an architecture that analyses all image features, followed by two fully connected layers that provide bounding box prediction for objects [21].

3.2 Overview of blockchain

In an open environment, blockchain provides a new way to store data, conduct transactions and operations, and establish trust. Blockchain is a breakthrough technology for cryptography and cybersecurity. It has many use cases, including Bitcoin, smart contracts, and the IoT smart grid. Many people view blockchain as a technological breakthrough for cryptography and cybersecurity, with use cases spanning from widely used cryptocurrency systems like Bitcoin to smart contracts, smart grids via the Internet of Things, and other applications. The security and privacy of blockchains remain at the forefront of the discussion when using blockchain in various applications, even though blockchain has seen significant attention in academia and business in recent years [22].

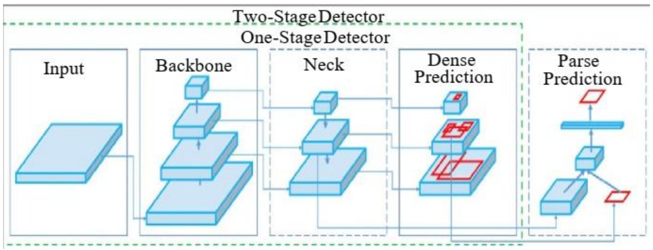


Figure 1. YOLO–v5 architecture [14]

3.3 The structure of blockchain

The block typically includes the primary data, the hash of the previous and current blocks, the timestamp, and other metadata.

Main data: Depending on the service, a blockchain may be applied to transaction records, bank clearing records, contract recordings, or the Internet of Things (IoT) data records.

Hash: A transaction was hashed to a code and disseminated to every node when it was performed. Blockchain uses the Merkle tree function to create a final hash value that is also the Merkle tree root since each node's block might include thousands of transaction data. Data transmission and computation requirements can be significantly decreased by employing the Merkle tree function, which will record the final hash value in the block header (hash of the current block).

Timestamp: Block generation time [23].

3.4 The hash function

It is a mathematical function that takes an input (often a string of arbitrary length) and produces a fixed-size output (usually a sequence of bytes or a string of a fixed length). The output is often called the "hash" or "message digest" of the input. Hash functions are commonly used in computer science for various purposes, such as indexing data in hash tables, verifying data integrity, and encrypting passwords. One of the key properties of a good hash function is that it should be easy to compute the hash value for any given input, but it should be difficult to generate the same hash value from different inputs. This property is known as "collision resistance." Hash or one–way functions are also commonly used in cryptographic applications, such as digital signatures and message authentication codes. In these applications, the hash function is used to create a compact and unique representation of a message, which can then be used to verify the integrity of the message or to prove the authenticity of the sender [24].

4. METHODOLOGY

The first step of the proposed secret key generation process is to capture the required biometric template and extract the components from the biometric retinal image that can be used in the proposed security approach. When two vessels (an artery and a vein) cross, it is called a crossover.

The crossing points are identified using the YOLO–v5 algorithm after initializing the data acquisition and making the annotations.

Figure 2 provides a visual representation of the proposed approach, viewing the flow of the entire process. It highlights the sequential steps involved, from data acquisition to the final generation of a secure key. This visual aid is crucial for grasping the complexity and precision of the methodology used in the study.

4.1 Dataset preparation

The dataset used in this study comprises 160 images from the DRIVE [25], IOSTAR [26], and Ibn Al-Haytham Teaching Eye Hospital datasets. The images, originally 2376×1584 pixels, were resized to 416×416 pixels for pre-processing. Data augmentation techniques, including flips, rotations, and brightness adjustments, were applied to enhance the training dataset. The dataset was annotated using the Roboflow labeling model, resulting in 384 images for training, validation, and testing.

•Total images: 384 (augmented from original 160)

•Image dimensions: 416×416 pixels

•Data split: 70% training, 20% validation, 10% testing

Figure 3 visually represents the various data augmentation techniques applied to the retinal images. By demonstrating these techniques, the figure shows how the dataset was prepared to train the YOLO-v5 model effectively. It highlights the importance of data augmentation in enhancing the model's robustness and accuracy. After completing this process, we had a data collection of about 384 images prepared for the main module (object detection) as training, validation, and test set.

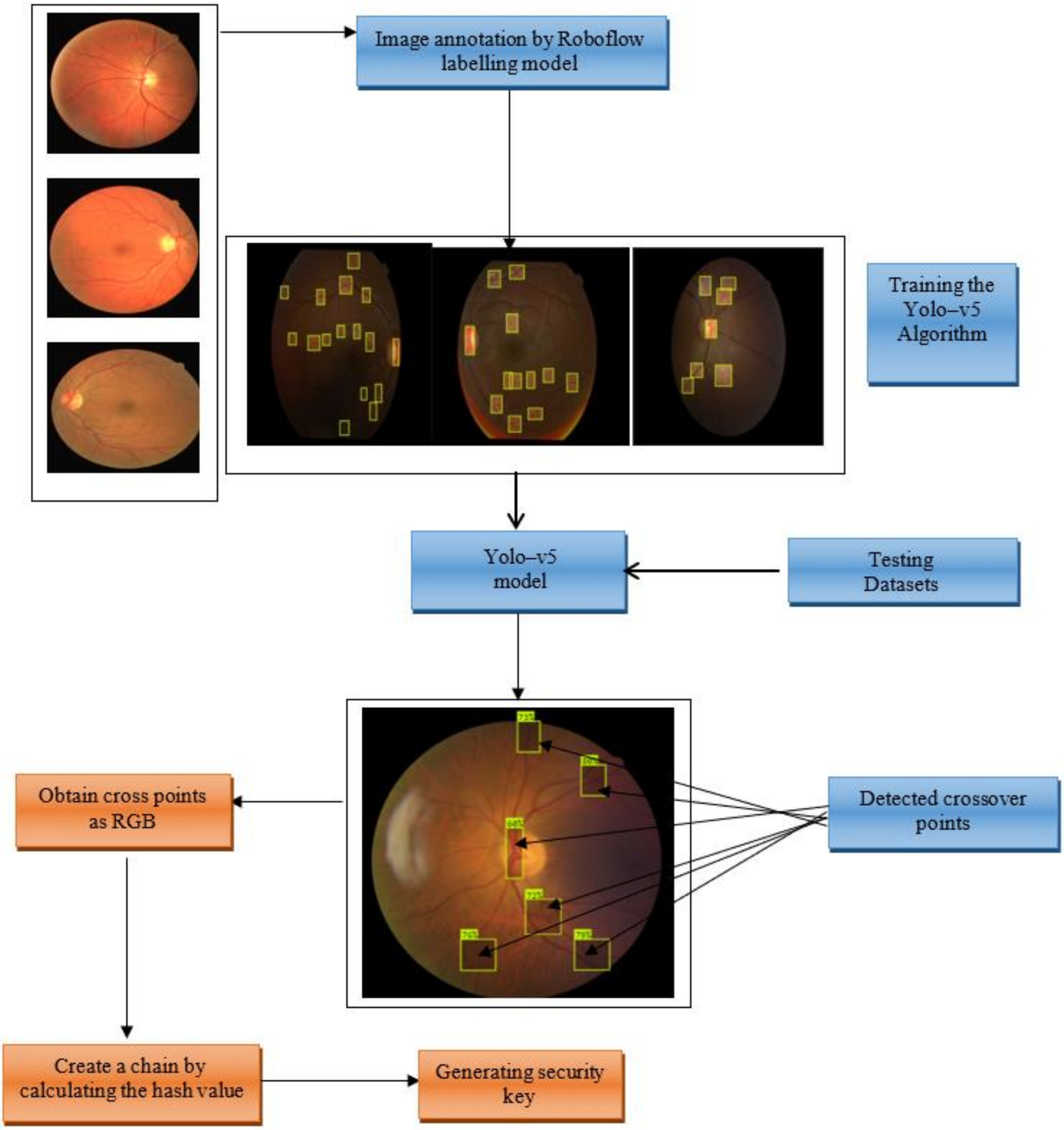
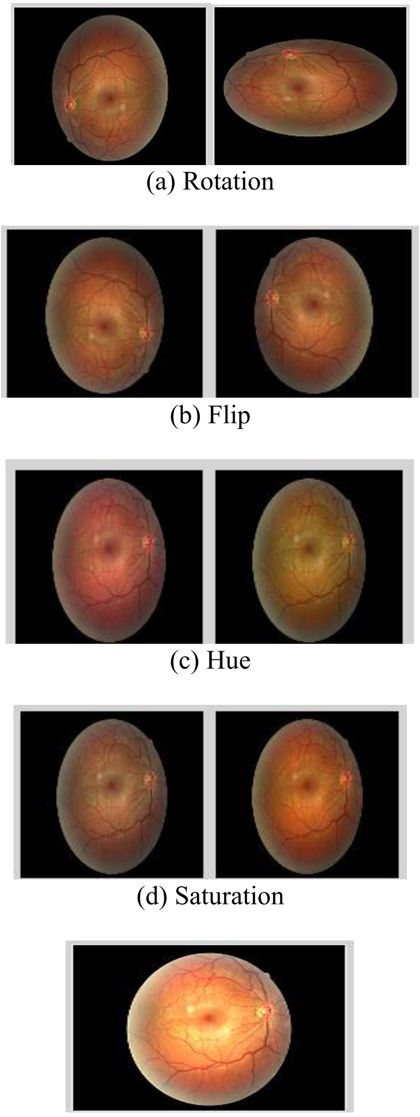


Image annotation by Roboflow labelling model
Training the Yolo–v5 Algorithm
Yolo–v5 model
Testing Datasets
Detected crossover points
Obtain cross points as RGB
Create a chain by calculating the hash value
Generating security key

Figure 2. Proposed security key generation approach


(a) Rotation

(b) Flip

(c) Hue

(d) Saturation

(e) Brightness

Figure 3. Augmentation process using (a) upside-down/counter clockwise, (b) vertical/horizontal, (c) 15°/-15°, (d) 21%/-21% and (e) 44%

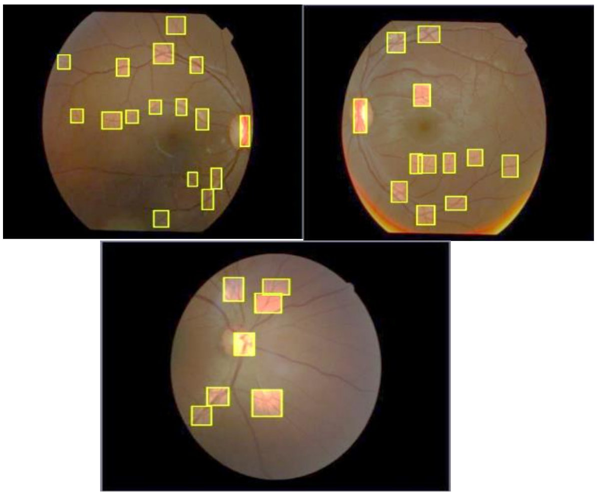


Figure 4. Annotated examples of crossover points in retinal images

Once the dataset was ready, we annotated each image to a category crossover point as shown in Figure 4. The dataset's crossover area images have been annotated with the image annotation tool using the Roboflow labeling model; annotations highlight the specific areas within the retinal images that are identified as crossover points, which are crucial for the training and validation of the YOLO-v5 object detection algorithm. The visual representation demonstrates the accuracy of the data annotation process, supporting the methodology and validating the data preparation phase for generating biometric security keys.

Training Details:

- Framework: YOLO-v5 with PyTorch
- Environment: Google Colab with TPU and GPU support
- Training epochs: 150
- Batch size: 32
- Data augmentation techniques: Flips, rotations, brightness adjustments

4.2 Key generation

A security key is a string of letters selected or created randomly to prevent detection or easy guessing. The goal of all security key generation procedures and methodologies, from direct to hybrid, are to make the key difficult to guess. The crossover points of the retina, which are biometric features of human eyes, were used in this paper to introduce a new method of generating security keys. This method capitalizes on the fact that each person's retina eye is unique and has a different tissue that distinguishes it from the other. Following the identification and detection of crossover points using the YOLO–v5 supervised learning algorithm, the coordinates (x, y) are stored using the blockchain structure as a link list format, where the color value of the point (RGB) is stored along with the hash value (H) of the point being formed to be an indicator of the next point in the list, and so on until all points are stored. Each image from the training model has its expected crossover point (x, y) coordinates values set aside, and the subsequent procedure uses these values to build the security key according to the proposed Algorithm 1.

Algorithm: Generating security key

1. Input: Get a crossing point's x and y coordinates to start.
2. Identify each point's RGB information, RGB(x,y).
3. Create a chain by calculating the hash value (H) of the RGB and saving the data as a link list [x, y, hash] for each point in the image.

Hash
Data
Hash

4. The security key of this series is then configured mathematically, as indicated by the following equation:

For rounds I=0 To n-1: (all points)

$$sum = sum + \sum_{I=0}^{n-1} (x_1 * y_1) * H_I \bmod P$$

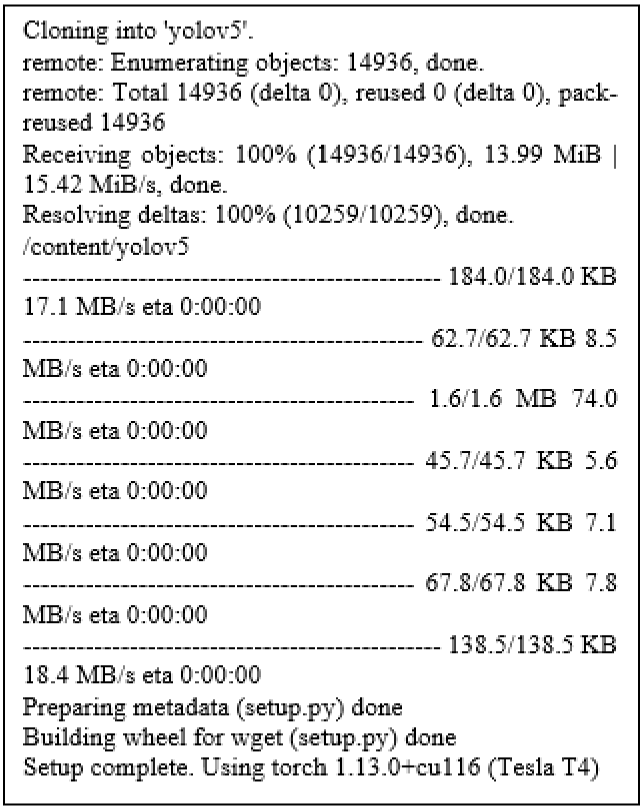
H_I: The hash value of (RGB).

P: The prime number chosen for user I.

5. Output: Security key= Binary (sum).

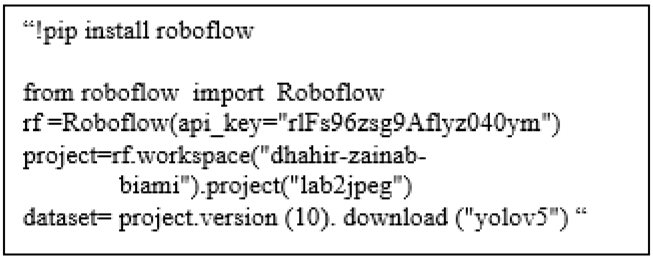
5. EXPERIMENTAL RESULTS AND DISCUSSIONS

The proposed method employs the YOLO-v5 algorithm for detecting crossover points in retinal images, which are then used to generate security keys. The dataset used comprises images from the DRIVE, IOSTAR, and Ibn Al-Haytham Teaching Eye Hospital datasets. The images were pre-processed and augmented to enhance the robustness and accuracy of the model. The YOLO–v5 repository is cloned, and the requirements are installed.



```
Cloning into 'yolov5'.
remote: Enumerating objects: 14936, done.
remote: Total 14936 (delta 0), reused 0 (delta 0), pack-
reused 14936
Receiving objects: 100% (14936/14936), 13.99 MiB |
15.42 MiB/s, done.
Resolving deltas: 100% (10259/10259), done.
/content/yolov5
---------------------------------------------- 184.0/184.0 KB
17.1 MB/s eta 0:00:00
-------------------------------------------- 62.7/62.7 KB 8.5
MB/s eta 0:00:00
-------------------------------------------  1.6/1.6  MB  74.0
MB/s eta 0:00:00
-------------------------------------------- 45.7/45.7  KB  5.6
MB/s eta 0:00:00
-------------------------------------------- 54.5/54.5  KB  7.1
MB/s eta 0:00:00
-------------------------------------------- 67.8/67.8  KB  7.8
MB/s eta 0:00:00
---------------------------------------------- 138.5/138.5 KB
18.4 MB/s eta 0:00:00
Preparing metadata (setup.py) done
Building wheel for wget (setup.py) done
Setup complete. Using torch 1.13.0+cu116 (Tesla T4)
```

Figure 5. Cloning and installing the YOLO–v5 repository



```
“!pip install roboflow

from roboflow  import  Roboflow
rf =Roboflow(api_key="rlFs96zsg9Aflyz040ym")
project=rf.workspace("dhahir-zainab-
            biami").project("lab2jpeg")
dataset= project.version (10). download ("yolov5") “
```

Figure 6. Data set linking

Figure 5 illustrates the steps involved in cloning and installing the YOLO-v5 repository. This figure is crucial for understanding the technical setup required to implement the proposed security key generation approach. It provides a visual guide for replicating the environment used in the study.

Linking the dataset to Google Colab ensures that the annotated images are easily accessible for training. This step is crucial for streamlining the data pipeline and ensuring that the training process is efficient and reproducible. Proper preparation of the dataset is vital for training a robust model. Dividing the dataset into training, validation, and testing sets allows for accurate evaluation of the model's performance and generalization capabilities. Figure 6 ensures that these steps are well-documented and easy to follow, setting the stage for successful model training and evaluation.

5.1 Performance metrics

The evaluation metrics that were used to train the proposed approach are:

Mean Average Precision (mAP):

Mean Average Precision (mAP) is used to evaluate object detection algorithms such as Fast R-CNN, Yolo–v5, Mask R-CNN, etc. Recall values between 0 and 1 determine the average precision (AP) [21]. The following submatrices form the basis of the mAP formula:

- Confusion Matrix,
- Intersection over Union (IoU),
- Recall, Precision

Confusion matrix

We need four characteristics to create a confusion matrix:

True Positives (TP): The label was successfully predicted by the model and matched to the data.

True Negatives (TN): The model neither predicts the label nor includes the ground truth.

False Positives (FP): The model predicted a label but is not part of reality (Type I error).

False Negatives (FN): Although the model does not predict a label, it is part of reality. (Error of type II).

Intersection over Union (IoU):

Intersection over Union indicates the predicted bounding box coordinates overlap with the ground truth box, as shown in Figure 7. A higher (IoU) value indicates that the predicted bounding box coordinates closely resemble the ground truth box coordinates [6].

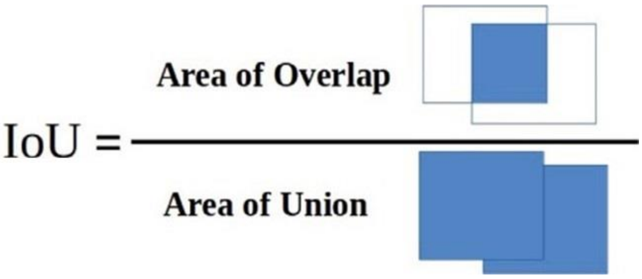


Figure 7. Computing IoU [6]

Using Eq. (1) as illustrated in [6], we can determine the precision, recall, and F1-score from the scales above.

$$\begin{aligned} Precision &= (TP+FP) \\ Recall &= (TP+FN) \\ F1Score &= \frac{2(Precision * Recall)}{(Precision + Recall)} \end{aligned} \tag{1}$$

Table 3. The detection of crossover points in training data

Data Set	Train Arguments	Precision	Recall	F1-Score	Map
147 images Without Augmentation	150 epochs, batch size 16	0.74	0.64	0.69	0.67
384 images	150 epochs, batch size 32	0.72	0.69	0.70	0.70
With Augmentation	150 epochs, batch size 16	0.73	0.67	0.70	0.72
448 images With Augmentation	150 epochs, batch size 16	0.78	0.73	0.76	0.77

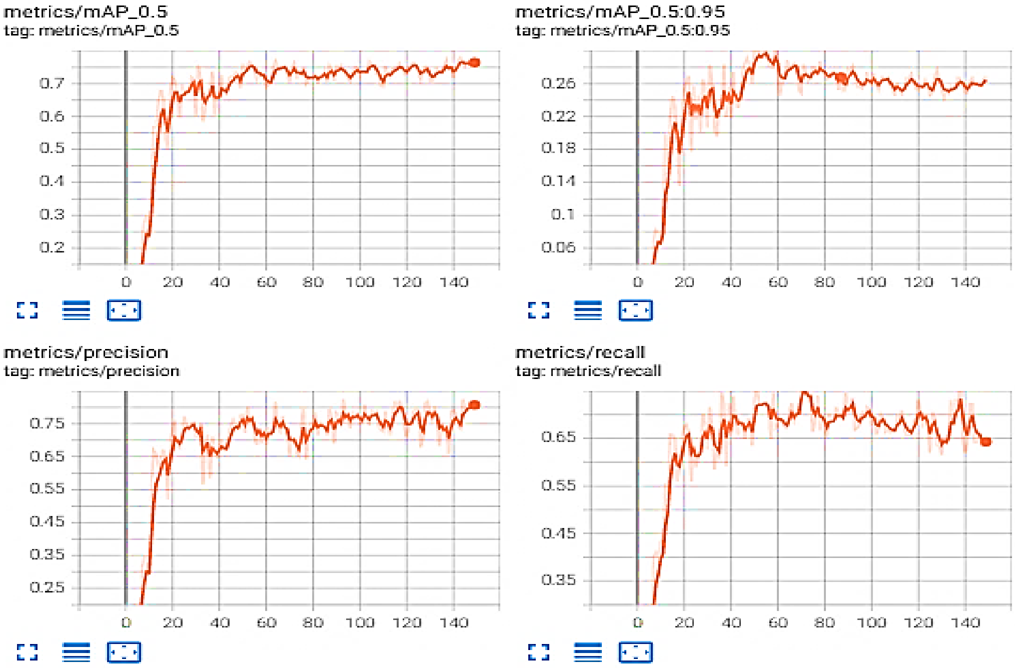


Figure 8. The evaluation metrics of the entire 150 epochs

The YOLO-v5 model was trained using the PyTorch framework on Google Colab, leveraging TPU and GPU support. Training parameters included 150 epochs, a batch size of 32, and data augmentation. The model's performance was evaluated using metrics such as precision, recall, and F1-score. Detailed training logs and hyperparameter settings are provided in Table 3. The total execution time was 21 m and 11 sec for 150 epochs. This demonstrates that the model is fast and accurate when using the original YOLO–v5 architecture.

As shown in Table 3 quantitative results the precision, recall, and F1-score achieved by the YOLO-v5 model on the testing set are (0.78, 0.73 and 0.76) with the mean Average Precision (mAP) yielding a value of 0.77. This metric indicates the model's ability to balance precision and recall across different thresholds.

The confusion matrix provides a detailed breakdown of true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN) for the testing set as shown in Table 4.

Table 4. Confusion matrix for testing set

	Predicted Positive	Predicted Negative
Actual Positive	TP (116)	FN (43)
Actual Negative	FP (32)	TN (309)

IoU measures the overlap between the predicted bounding boxes and the ground truth bounding boxes. Higher IoU values indicate better performance in object detection. Table 5 shows the results of confusion matrix that indicate a reasonably good performance of the model.

Table 5. IoU-based performance metrics

IoU Threshold	Precision	Recall	F1-Score
0.5	0.81	0.78	0.79
0.75	0.72	0.69	0.70

Figure 8 provides a visual representation of the evaluation metrics over the course of 150 training epochs for the YOLO-v5 model. This figure is crucial as it demonstrates the performance and learning progress of the model, highlighting key aspects such as precision, recall, and mean Average Precision (mAP) throughout the training process.

The loss function for the training model, shown in Eq. (2), is calculated by summing the loss functions for all bounding box parameters (x, y, w, h, confidence score, and class probability).

$$\begin{aligned}
&\lambda_{\text{coord}}\sum_{i=0}^{S^2}\sum_{j=0}^{B}1_{ij}^{\text{obj}}\left[\left(x_i-\hat{x}_i\right)^2+\left(y_i-\hat{y}_i\right)^2\right]\\
&+\lambda_{\text{coord}}\sum_{i=0}^{S^2}\sum_{j=0}^{B}1_{ij}^{\text{obj}}\left[\left(\sqrt{w_i}-\sqrt{\hat{w}_i}\right)^2+\left(\sqrt{h_i}-\sqrt{\hat{h}_i}\right)^2\right]\\
&+\sum_{i=0}^{S^2}\sum_{j=0}^{B}1_{ij}^{\text{obj}}\left(C_i-\hat{C}_i\right)^2\\
&+\lambda_{\text{noobj}}\sum_{i=0}^{S^2}\sum_{j=0}^{B}1_{ij}^{\text{noobj}}\left(C_i-\hat{C}_i\right)^2\\
&+\sum_{i=0}^{S^2}1_{i}^{\text{obj}}\sum_{c\in\text{classes}}\left(\left(c\right)-\hat{p}_i\left(c\right)\right)^2
\end{aligned} \qquad (2)$$

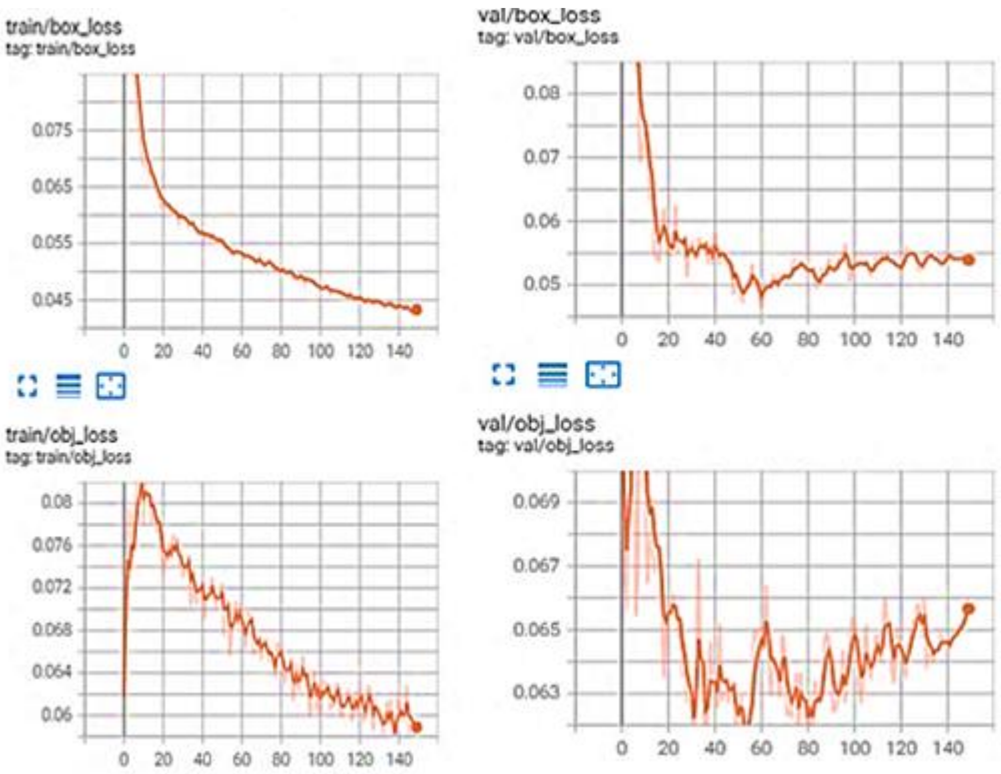


Figure 9. Loss metric for training data and validation data

The loss function for the training and validation datasets is illustrated in Figure 9. This figure demonstrates the convergence of the training process, indicating that the model is learning effectively.

- Training Loss: The loss decreases steadily, showing the model's ability to learn from the training data.
- Validation Loss: The validation loss remains low, indicating good generalization to unseen.

Some of the grid cells in the image have a confidence score of 0 because they contain no object, which affects the remaining object-containing regions.

The model saves separate files for the most recent epoch weighting and maximum accuracy weighting after training to avoid overfitting. The trained weights can locate the crossover spots on any image. When a crossing point is found, a bounding box is drawn to enclose the object and indicate the likelihood that it is the crossover point. Leading to training divergence and model instability, YOLO–v5 applies the largest penalty for predictions from bounding boxes with objects (λcoord = 5) and the lowest penalty for predictions without objects (λnoobj=0.5).

After detecting all the items, if their probability is below a specific threshold (0.4 in this case), some of the crossing points in the image's lower left and upper left are not projected as crossing points, even though their presence is evident. The overall hit rate for the detection method ranged from 0.64% to 0.73%. With additional data sets, we can achieve higher accuracy.

Figure 9 presents the loss metrics for both the training and validation datasets over the course of 150 epochs. A decreasing training loss indicates that the model is effectively learning the patterns in the training data. Monitoring validation loss is crucial for detecting overfitting.

The overall hit rate for the detection method ranged from 0.69% to 0.76%. With additional data sets, we can achieve higher accuracy. Figure 10 visually corroborates the quantitative metrics reported in the study, providing a clear and tangible example of the model's capability to accurately detect retinal crossover points, which are essential for generating secure keys.

The labels of recognized crossover points are displayed in Figure 11, providing a visual representation of the detected features and their corresponding labels.

Figure 11 illustrates the labels of the detected crossover points, each marked with a bounding box. These points represent the intersections of blood vessels in the retinal images. Each bounding box is labeled with a unique identifier and a confidence score ranging from 0 to 1. This figure demonstrates the precision of the YOLO-v5 model in identifying crossover points by showing that the bounding boxes are accurately placed over the correct features in the retinal images. Additionally, the figure highlights the robustness of the YOLO-v5 model by displaying consistent detection across various images, regardless of variations in image quality or retinal structure. This indicates that the model has effectively generalized from the training data to handle different types of retinal images, confirming the practical applicability of the detected points for generating secure keys.

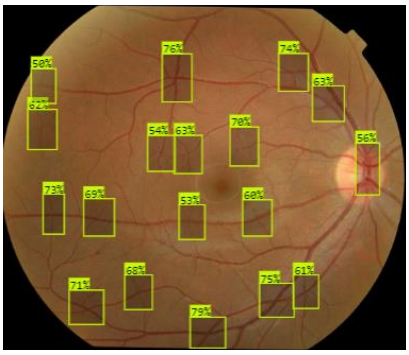


Figure 10. Best-trained weight anticipated image

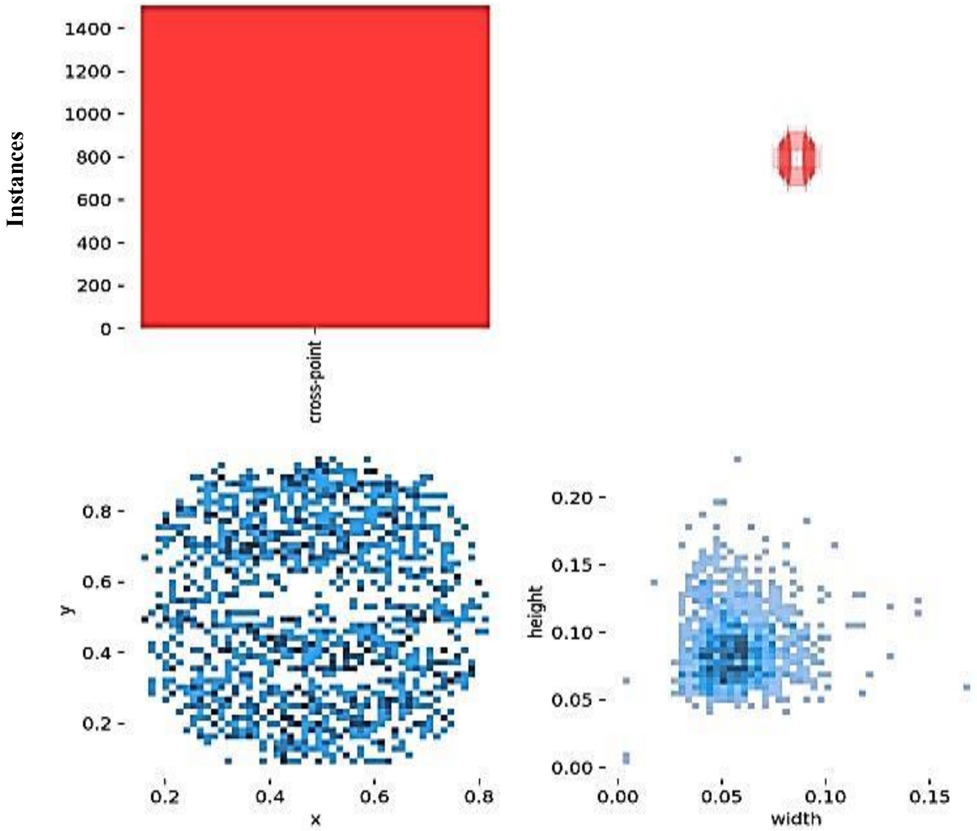


Figure 11. Cross-points labels

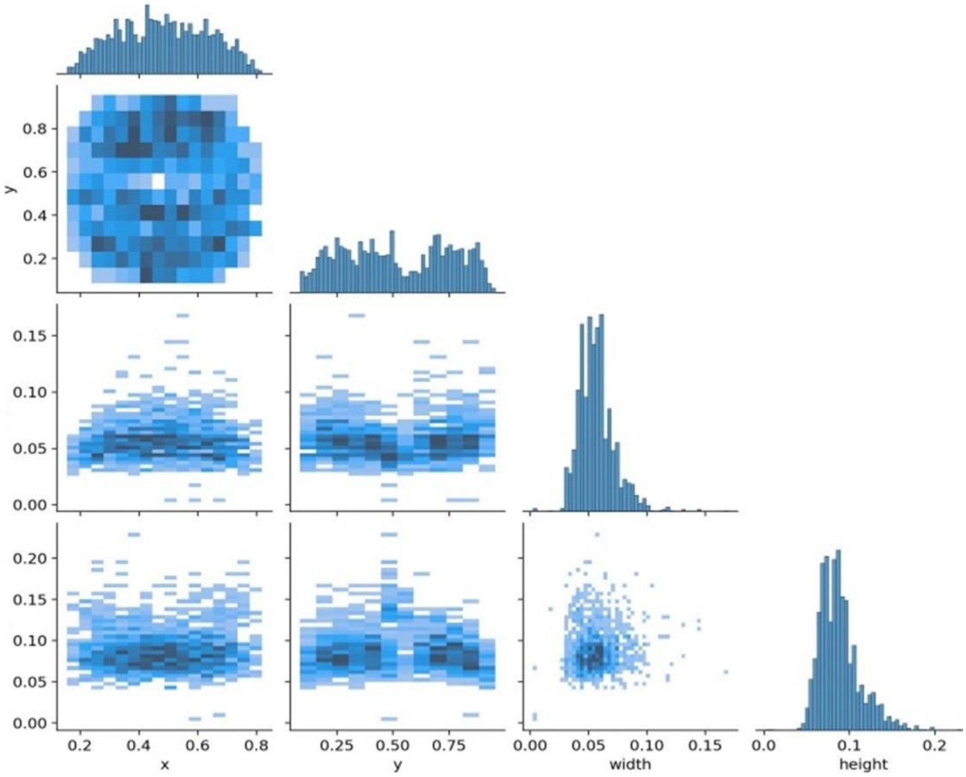


Figure 12. Labels_correlogram

Figure 12 illustrates the correlogram of the labels, providing a comprehensive visual representation of the relationships and correlations among the detected crossover points in the retinal images. The correlation coefficients range from -1 to 1, indicating the strength and direction of the relationships between variables. Positive correlations are typically shown in shades of blue, indicating that as one variable increases, the other tends to increase. The intensity of the color represents the strength of the correlation, with darker colors indicating stronger correlations. The correlogram presented in Figure 12 offers a comprehensive visual examination of the connections among the identified crossover points within the retinal images. It emphasizes the magnitude and orientation of the correlations, verifies the efficacy of the model, and the accuracy of the annotations, while also providing valuable perspectives that can enhance the operational execution of the security key generation process. This manuscript presents a novel methodology for the generation of security keys.

5.2 Security key generation

To generate a security key, we use the predicted crossover points for the retina image. Table 6 shows the detected points in one of the images.

The detected crossover points are used to generate security keys for different retinal images. Table 7 shows the generated keys and the number of crossover points used.

To demonstrate the effectiveness of our approach, we compared the YOLO-v5 model's performance with other existing methods in the literature. Table 8 provides a comparison of the proposed method with the related biometric security systems listed in Table 1, focusing on the techniques used. The comparison metrics include precision, recall, and F1-score as shown in Table 9.

The proposed approach demonstrates high precision, recall, and F1-score compared to existing methods. The integration of YOLO-v5 with blockchain technology for security key generation proves to be effective and robust. The results indicate that the model can accurately detect crossover points and generate unique security keys, making it a promising approach in the field of biometric security systems.

Table 6. Crossover point values of one retina image

X	Y	(RGB) -Value
180	252	216
197	438	171
200	184	144
221	94	192
230	452	184
243	265	189
257	115	120
273	134	153
277	114	153
225	224	176
246	222	185
412	245	302
213	369	194
295	351	208
358	416	208
357	402	186

Table 7. Generated security key

Images	Crossover Points Number	Generated Security Key
Image1	16	10000111110011
Image2	18	10100111010011
Image3	27	11000111010111
Image 4	17	11110111010000
Image 5	11	11100111100001
Image 6	23	10000000110010
Image 7	30	00000000110101
Image 8	15	00010100000100
Image 9	22	00010010011101
Image 10	10	00001111111100

Table 8. Comparison of the proposed method with the related biometric security systems

Reference	Techniques Used	Comparison with Proposed Method
Tajuddin and Nandini [15]	Uses retina biometric parameters for cryptographic key generation. Utilizes thick blood vessels in greyscale images for key generation.	Proposed Method: Utilizes YOLO-v5 deep learning model to detect crossover points in RGB images, providing a more detailed and accurate approach for key generation.
Mazher and Waleed [16]	Retina features extracted using glowworm swarm optimization (GSO) algorithm and chaotic map for key generation.	Proposed Method: Employs YOLO-v5, a state-of-the-art object detection algorithm, offering higher accuracy and reliability in detecting crossover points compared to GSO.
Salih and Mahdawi [17]	Proposed RC4-Retina algorithm with retina key scheduling algorithm (RKSA) for key generation.	Proposed Method: Utilizes blockchain technology for secure key generation, addressing vulnerabilities in traditional algorithms like RC4.
Alrifaee and Ismaeel [18]	Generates keys based on three types of retinal vessel distances (DCE, RCE, DRCE).	Proposed Method: Uses YOLO-v5 to detect specific crossover points for generating keys, providing a more precise and potentially more secure method.

Table 9. The Proposed approach comparison with other methods

Papers	Techniques	Dataset	Precision (%)	Recall (%)	F-Score Value (%)
Hervella et al. [5]	Deep Neural Network	Used DRIVE and IOSTAR datasets (50% training, 50% testing dataset).	0.61	0.62	74.23
Hao et al. [6]	VAFF-Net	Used DRIVE datasets (50% training, 50% testing dataset).	60.64	68.98	55.88
Zhao et al. [14]	RCNN	Used DRIVE and IOSTAR datasets (50% training, 50% testing dataset).	0.78	0.71	0.55
Mazher and Waleed [16]	RCNN	Used DRIVE and IOSTAR datasets (75% training, 25% testing dataset).	0.75	0.62	0.59
Proposed approach	YOLO–v5	Used (DRIVE, IOSTAR and Ibn Al-Haytham Teaching Eye Hospital) datasets (70% training, 20% validation and 10% testing dataset).	0.78	0.73	0.76

6. CONCLUSIONS

In the past, cryptography was used to achieve security. Today, one of the biggest concerns is data security on a network. Thanks to technological improvements, security keys can now be generated using biometrics. Since the retina is unique and reduces the probability of duplicates, this study aims to provide a secure method to create the key. The technique presented in this paper generates a unique key directly from the crossing points of human biometric information and does not store it in a database. The proposed security key generation method has significant implications for network security and data protection. By leveraging unique retinal patterns, this approach enhances security in biometric authentication systems. Potential applications include secure access control in high-security facilities, encryption key generation for sensitive data, and integration with blockchain for secure transactions. This approach does not provide redundant crossing points and makes the cryptographic secret harder to decode or guess. Although a larger sample size of the dataset might be necessary to achieve higher accuracy, the main findings of this study with different datasets range from 0.69% to 0.76% and are considered acceptable. Each retina generates a unique security key that can be used for various applications, including network security and encryption keys. Future research could explore hybrid deep learning models combining YOLO-v5 with other architectures to enhance accuracy. Additionally, addressing retinal distortions due to diseases or injuries could improve the robustness of the security key generation method.

Integrating this approach with real-time security systems and expanding the dataset with diverse retinal images are other potential areas for further study.

REFERENCES

[1] Lakshmi, A.J., Babu, I.R. (2012). Design of secured key generation algorithm using fingerprint based biometric modality. IOSR Journal of Engineering, 2(2): 325-330. https://doi.org/10.9790/3021-0202325330

[2] Hussein, S.N., Obaid, A.H., Jabbar, A. (2022). Encryption symmetric secret key in wireless sensor network using AES algorithm. Iraqi Journal of Science, 63(11): 5037-5045. https://doi.org/10.24996/ijs.2022.63.11.38

[3] Wang, Y.Z., Li, B., Zhang, Y., Wu, J.X., Ma, Q.Y. (2021). A secure biometric key generation mechanism via deep learning and its application. Applied Sciences, 11(18): 8497. https://doi.org/10.3390/app11188497

[4] Trivedi, T.R., Seshadri, D.R. (2011). Efficient cryptographic key generation using biometrics. International Journal of Computer Technology and Applications, 2(1): 183-187. https://www.researchgate.net/publication/49612789_Efficient_Cryptographic_Key_Generation_using_Biometrics.

[5] Hervella, A.S., Rouco, J., Novo, J., Penedo, M.G., Ortega, M. (2020). Deep multi-instance heatmap regression for the detection of retinal vessel crossings and bifurcations in eye fundus images. Computer Methods and Programs in Biomedicine, 186: 105201. https://doi.org/10.1016/j.cmpb.2019.105201

[6] Hao, J.K., Shen, T., Zhu, X.L., Liu, Y.H., Behera, A., Zhang, D., Chen, B., Liu, J., Zhang, J., Zhao, Y.T. (2022). Retinal structure detection in OCTA image via voting-based multitask learning. IEEE Transactions on Medical Imaging, 41(12): 3969-3980. https://doi.org/10.1109/tmi.2022.3202183

[7] Maninis, K.K., Pont-Tuset, J., Arbeláez, P.A., Gool, L.V. (2016). Deep retinal image understanding. Medical Image Computing and Computer-Assisted Intervention – MICCAI 2016, Springer, Cham, pp. 140-148. https://doi.org/10.1007/978-3-319-46723-8_17

[8] Chudzik, P., Majumdar, S., Calivá, F., Al-Diri, B., Hunter, A. (2018). Microaneurysm detection using fully convolutional neural networks. Computer Methods and Programs in Biomedicine, 158: 185-192. https://doi.org/10.1016/j.cmpb.2018.02.016

[9] Lee, H., Chen, Y.P.P. (2015). Image based computer aided diagnosis system for cancer detection. Expert Systems with Applications, 42(12): 5356-5365. https://doi.org/10.1016/j.eswa.2015.02.005

[10] Alom, M.Z., Aspiras, T.H., Taha, T.M., Asari, V.K., Bowen, T.J., Billiter, D., Arkell, S. (2019). Advanced deep convolutional neural network approaches for digital pathology image analysis: A comprehensive evaluation with different use cases. arXiv, 1904, 09075. https://doi.org/10.48550/arXiv.1904.09075

[11] Bochkovskiy, A., Wang, C.Y., Liao, H.Y. (2020). YOLOv4: Optimal speed and accuracy of object detection. ArXiv, 2004, 10934. https://doi.org/10.48550/arXiv.2004.10934

[12] Xu, R.J., Lin, H.F., Lu, K.J., Cao, L., Liu, Y.F. (2021). A forest fire detection system based on ensemble learning. Forests, 12(2): 217. https://doi.org/10.3390/f12020217

[13] Salman, M.E., Çakar, G.Ç., Azimjonov, J., Kösem, M., CediMoğlu, İ.H. (2022). Automated prostate cancer grading and diagnosis system using deep learning-based YOLO object detection algorithm. Expert Systems with Applications, 201: 117148. https://doi.org/10.1016/j.eswa.2022.117148

[14] Zhao, H., Sun, Y., Li, H.Q. (2020). Retinal vascular junction detection and classification via deep neural networks. Computer Methods and Programs in Biomedicine, 183: 105096. https://doi.org/10.1016/j.cmpb.2019.105096

[15] Tajuddin M., Nandini, C. (2013). Cryptographic Key Generation using Retina Biometric Parameter. International Journal of Engineering and Innovative Technology (IJEIT), 3(1): 53-56. https://typeset.io/papers/cryptographic-key-generation-using-retina-biometric-4qslbm4a1d.

[16] Mazher, A.N., Waleed, J. (2022). Retina based Glowworm swarm optimization for random cryptographic key generation. Baghdad Science Journal, 19(1): 0179. https://doi.org/10.21123/bsj.2022.19.1.0179

[17] Salih, H.M., Mahdawi, R.S.A. (2021). The security of RC4 algorithm using keys generation depending on user's retina. Indonesian Journal of Electrical Engineering and Computer Science, 24(1): 452. https://doi.org/10.11591/ijeecs.v24.i1.pp452-463

[18] Alrifaee, Z.I.A., Ismaeel, T.Z. (2022). Cryptography based on retina information. Indonesian Journal of Electrical Engineering and Computer Science, 28(3): 169. https://doi.org/10.11591/ijeecs.v28.i3.pp1697-1708

[19] Pampana, L.K., Rayudu, M.S. (2022). Detection and

classification of multi-scale retinal junctions using region-based CNN. Signal, Image and Video Processing, 16: 265-272. https://doi.org/10.1007/s11760-021-01986-3

[20] Litjens, G., Kooi, T., Bejnordi, B.E., Setio, A.A.A., Ciompi, F., Ghafoorian, M., Laak, J.A.W.MV.D., Ginneken, B.V., Sánchez, C.I. (2017). A survey on deep learning in medical image analysis. Medical Image Analysis, 42: 60-88. https://doi.org/10.1016/j.media.2017.07.005

[21] Yang, R.J., Li, W.F., Shang, X.N., Zhu, D.P., Man, X.Y. (2023). KPE-YOLOV5: An improved small target detection algorithm based on YOLOV5. Electronics, 12(4): 817. https://doi.org/10.3390/electronics12040817

[22] Chaurasia, J., Kumari, S., Singh, V., Dehraj, P. (2023). A survey on blockchain security issues using Two-Factor Authentication approach. Intelligent Communication Technologies and Virtual Mobile Networks, Springer, Singapore, 591-601. https://doi.org/10.1007/978-981-19-1844-5_46

[23] Lin, I.C., Liao, T.C. (2017). A survey of blockchain security issues and challenges. International Journal of Network Security, 19(5): 653-659. https://doi.org/10.6633/IJNS.201709.19(5).01

[24] Abdoun, N., Assad, S.E., Hoang, T.M., Deforges, O., Assaf, R., Khalil, M. (2020). Designing two secure keyed hash functions based on sponge construction and the chaotic neural network. Entropy, 22(9): 1012. https://doi.org/10.3390/e22091012

[25] Staal, J., Abramoff, M.D., Niemeijer, M., Viergever, M.A., Ginneken, B.V. (2004). Ridge-based vessel segmentation in color images of the retina. IEEE Transactions on Medical Imaging, 23(4): 501-509. https://doi.org/10.1109/tmi.2004.825627

[26] Abbasi-Sureshjani, S., Smit-Ockeloen, I., Bekkers, E., Dashtbozorg, B., Romeny, B.T.H. (2016). Automatic detection of vascular bifurcations and crossings in retinal images using orientation scores. In 2016 IEEE 13th International Symposium on Biomedical Imaging (ISBI), Prague, Czech Republic, pp. 189-192. https://doi.org/10.1109/isbi.2016.7493241

NOMENCLATURE

YOLO-v5	You Only Look Once, version 5 – a deep learning object detection algorithm
RGB	Red, Green, Blue – color channels used in image processing
F1-Score	Harmonic mean of precision and recall
TP	True Positive – correctly identified positive cases
TN	True Negative – correctly identified negative cases
FP	False Positive – incorrectly identified positive cases
FN	False Negative – incorrectly identified negative cases
mAP	Mean Average Precision – metric for evaluating object detection models
IoU	Intersection over Union – metric for evaluating overlap of bounding boxes
DCE	Distance-based Cryptographic Extraction
RCE	Random Cryptographic Extraction
DRCE	Double Random Cryptographic Extraction
CNN	Convolutional Neural Network
RCNN	Region-based Convolutional Neural Network
GSO	Glowworm Swarm Optimization
VAFF-Net	Voting-based Adaptive Feature Fusion Network
TPU	Tensor Processing Unit
GPU	Graphics Processing Unit
DRIVE	Digital Retinal Images for Vessel Extraction – dataset
IOSTAR	Intraoperative OCT Study and Analysis Resource – dataset
RKSA	Retina Key Scheduling Algorithm
TP	Tensor Processing Unit
DRCE	Double Random Cryptographic Extraction
H	Hash value
RSA	Rivest-Shamir-Adleman – a public-key cryptosystem
DES	Data Encryption Standard – a symmetric-key algorithm
3DES	Triple Data Encryption Algorithm – a symmetric-key block cipher
AES	Advanced Encryption Standard – a symmetric-key algorithm