

Classification and Detection of retinal hemorrhages by Using Moment Invariants and Gray-Level Based Features

Godlin Atlas L¹, Kumar Parasuraman²

*¹Research Scholar, Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli, Tamilnadu, India

²Assistant Professor, Centre for Information Technology and Engineering, Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli, Tamilnadu, India

ABSTRACT

Diabetes happens when the pancreas fails to release enough insulin, step by step affecting the retina of the human eye. As it propels, the vision of a patient starts separating, inciting diabetic retinopathy. In such way, retinal pictures acquired through fundal camera help in analyzing the outcomes, nature, and status of the effect of diabetes on the eye. The objectives of this examination are to (I) perceive vein, (ii) recognize hemorrhages and (iii) describe various periods of diabetic retinopathy into commonplace, coordinate and no proliferative diabetic retinopathy (NPDR). The commence of the gathering of different periods of diabetic retinopathy is the ID and estimation of veins and hemorrhages present in the retinal picture. Its ask for to this record (despite when the NN was set up on the DRIVE database) outmaneuvers all analyzed division approaches. Its ampleness and power with different picture conditions, together with its ease and speedy execution, influence this vein division to recommendation fitting for retinal picture PC examinations, for instance, robotized screening for early diabetic retinopathy area.

Keywords : Diabetic Retinopathy, Exudates, Image Processing, Classification, Diabetic Retinopathy

I. INTRODUCTION

Diabetes is an illness which happens when the pancreas does not release enough insulin or the body can't process it fittingly. As diabetes progresses, the disease bit by bit impacts the circulatory structure including the retina and happens in light of whole deal collected mischief to the veins, declining the vision of the patient inciting diabetic retinopathy. Following 15 long stretches of diabetes around 10% of people twist up stupor and about 2% make genuine visual impedance. According to a measure by WHO, more than 220 million people worldwide have diabetes [1]. It is the sixth most compelling motivation for visual disability among the all-inclusive community of working age in India, making it the world's diabetic capital. Retinal pictures increased through fundal camera with back mounted

propelled camera [2] give important information about the result, nature, and status of the effect of diabetes on the eye. These photos assist ophthalmologist with assessing patients with a particular true objective to plan different kinds of organization and screen the propel more capably [3]. The retinal microvasculature is exceptional in that it is the primary bit of human course that can be particularly imagined non-rudely in vivo and can be easily caught for mechanized picture examination [2]. In [4] showed a nonparametric and unsupervised strategy for customized edge assurance for picture division. This uses only the zeroth-and the principle ask for add up to previews of the dull level histogram. In [5] watched out for the issue of distinguishing veins which have ordinarily poor neighborhood separate and stresses that present edge acknowledgment figuring yield unacceptable results.

They proposed a head for incorporate extraction in perspective of optical and spatial properties of the inquiry be seen. In [2] plot the division of retinal developments whereupon retinal automated picture examination is based. In [6] portrayed an improved methodology for recognizing hemorrhages in fundus pictures. The general recognizable proof plot included six stages - picture digitization, picture institutionalization, extraction of optic nerve head, area of hemorrhages candidates, end of false positives (FP) in veins, and transfer of FPs by feature examination. In any case, the strategy for end of the veins for the successful area of deplete candidates was not overseen here. In [3] proposed modified gathering of different periods of diabetic retinopathy - smooth non-proliferative retinopathy, coordinate no proliferative retinopathy, genuine non-proliferative retinopathy and proliferative retinopathy using neural framework from six features removed from the retinal pictures.

confusion and basically, PR proliferative and proliferative DR. Expansive hemorrhages are asymptomatic beside when they are arranged in the point of convergence of the macula. Two instances of far reaching retinal deplete shared month to month cycle Figure.1. Differentiated and anatomical structures, for instance, optic circle, fovea and veins, the shape and appearance of hemorrhages demonstrate broad fluctuation.

The straggling leftovers of the paper is dealt with as takes after. Next region studies other conveyed vessels division courses of action. Zone III depicts them at serial used as a piece of this examination. Zone IV clears up and depicts the proposed technique for retinal vessel division, while Section V demonstrates its results and contrasts them to those got and other existing methodology. At long last, the creators' decisions and talk finish this paper.

II. RELATED WORK

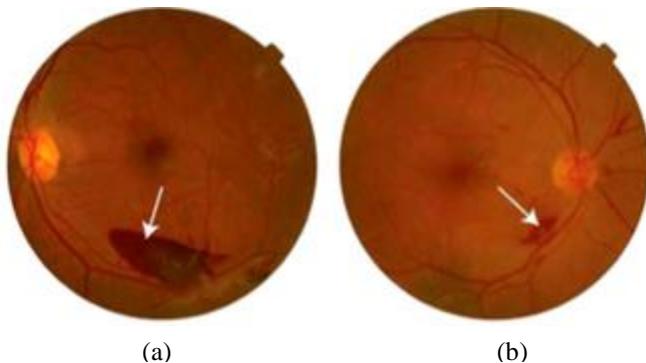


Figure. 1. Cases of retinal hemorrhages with various shapes and appearances.

The most by and large saw indications of DR are microaneurysms, little hemorrhages, exudates, drusen, and cotton wool spots. In light of the difference in appearance of these injuries, changed systems have been wanted to perceive every sort of these wounds openly in DR recognizing confirmation structures. Retinal hemorrhages are caused by retinal is substance and on a very basic level caused by unusually delicate veins in hypertension, intestinal

In [1], the optic circle is restricted abusing its high dim level assortment. This approach has been seemed to work commendably if there are no or only several pathologies like exudates that moreover appear to be awe inspiring and are furthermore especially separated. No system is proposed for the disclosure of the structures. In [15], a zone edge is used to restrict the optic plate. The shapes are recognized by strategies for the Hough change, i.e., the point of the photo is figured, and the best fitting circle is settled. This approach is extremely repetitive and it relies upon conditions about the condition of the optic circle that are not for the most part met. Once in a while, the optic plate is even no detectable absolutely in the photo plane, hence the shape is far from being round or even elliptic. Also, in [17], the Hough change is used to perceive the types of the optic hover in infrared and argon-blue pictures. Regardless of a couple of upgrades, issues have been

communicated if the optic circle does not meet the shape conditions (e.g., in case it lies on the edge of the photo) or if the distinction is low. In [14], the optic circle is limited by backtracking the vessels to their beginning stage. This is doubtlessly a standout amongst the most secure ways to deal with constrain the optic circle, yet it needs to rely upon vessel disclosure. It is alluring to detach division errands in order to avoid a conglomeration of division botches and to save computational time (the area of the vascular tree is particularly repetitive). In [20], morphological isolating systems and dynamic structures are used to find the breaking point of the optic plate, in [19] a district edge is used to limit the optic circle and the watershed change to find its shapes.

Crafted by cutting edge pictures for eye infections conclusion could be abused for electronic early acknowledgment of DR. A structure that could be used by no experts to filtrate occasions of patients not impacted by the disease, would diminish the masters' workload, and augmentation the sufficiency of preventive conventions and early the paretic medicines. Moreover, it would likewise bring about money related benefits for general Health Systems, since fiscally insightful meds identified with early illness distinguishing proof provoke uncommon cost speculation reserves [8]. Since vascular irregularities are one of DR signs, modified evaluation of eye-fundus veins is essential for motorized acknowledgment of DR. As a past propel, vessel assessment demands vascular tree division from the establishment for also getting ready. Data on vein territory can be used to reduce the amount of false promising focuses in micro aneurysm and deplete revelation [9]– [12]. Other than these applications propelled by means of motorized early acknowledgment of DR, vascular tree division shows supportive for other clinical purposes: evaluation of the retinopathy of thoughtlessness [15], arteriolar narrowing [16], [17], vessel tortuosity to depict

hypertensive retinopathy [18], vessel broadness estimation to investigate hypertension and cardiovascular contaminations [19]– [21], and PC helped laser medical procedure [22], [23], among others. On the other hand, the vascular tree can in like manner be useful as critical information to discover diverse fundus features, for instance, the optic plate [24] and the fovea [25]. Also, it may fill in as a mean for the enlistment of multimodal pictures [13], [14].

Notwithstanding its straightforwardness, the high precision accomplished by this technique in vein revelation is relative to that point by point by the most exact methodologies in creating. Furthermore, it offers a prevalent lead against pictures of various conditions. This the fact of the matter is particularly fitting on the off chance that we recall that the significant reason for understanding a vessel division calculation is its blend in frameworks for robotized disclosure of eye illnesses. This sort of structures ought to require no client composed exertion and, subsequently, be sufficiently beneficial to look at changed sorts of pictures. Inside the field of retinal imaging, this consolidates a beast test, since clearing variability is found in the photograph anchoring process and a trademark grouping is spoken to inside seeing the retina.

III. THEORETICAL DEPLOYMENT PROCESS

65 retinal images of normal, moderate NPDR, and severe NPDR cases used in this work were downloaded from STARE (Structured Analysis of the Retina) Project database (<http://www.parl.clemson.edu/stare/>) as detailed in Table I. They were acquired in 24-bits per pixel with a dimension of 576 x 768. all possible orientations, 25 kernels of the matched filter are generated each oriented at an angle of 7.5° . The rotation matrix is given by (2) $\begin{bmatrix} \cos \theta & \theta \\ \theta & -\sin \theta \end{bmatrix}$ (2) $\begin{bmatrix} r_i & -\theta \\ \theta & r_i \cos \theta \end{bmatrix}$

lsin. The filter is supposed to be centered at [0, 0]. A set of kernels are applied to fundus image and at each pixel only the maximum of their responses is retained. The corresponding weights in the kernels are given by

Table -1: Details of Retinal Diabetic Images

Type	Number of cases
Normal	30
SevereNPDR	12
ModerateNPDR	23

3.1 Blood Vessel Detection

Blood vessels can act as landmarks for localizing the optic nerve, the fovea and lesions. As a result of systemic or local ocular disease, the blood vessels can have measurable abnormalities in diameter, color and tortuosity. There are three interesting properties of the blood vessels in retinal images that help in differentiating them from other features:

1) The anti-parallel pairs can be approximated by piecewise linear segments due to small curvatures present in the blood vessels.

2) Vessels have lower reflectance compared to other retinal surfaces, so they appear darker relative to the background. It was observed that these vessels almost never have ideal step edges. Although the intensity profile varies by a small amount from vessel to vessel, it may be approximated by an inverted Gaussian curve as given by (1)

$$f(x,y) = -A \exp\left(-\frac{d^2}{2\sigma^2}\right) + B \quad (1)$$

where, d = perpendicular distance between the point (x, y) and the straight line passing through the center of the of the blood vessel in a direction along its

length, σ = spread of the intensity profile, A = gray level intensity of the local background, and k = measure of reflectance of the blood vessel relative to its neighborhood.

3) Although the width of a vessel decreases as it travels radially outward from the optic disk, such a change in vessel caliber is a gradual one. The widths of the vessels are found to lie within a range of 2-10 pixels (36-180 μ m).

The matched filter has the same inverted Gaussian response as the gray level profile of the blood vessel. The design of the matched filter is as follows: assuming that all blood vessels are of equal width, the Gaussian curve is truncated at $u = 3\pm\sigma$, u is a point in the rotated coordinate system, the length of piecewise linear segment $L=17$, an angular resolution of 7.5° to span u^2

$$k(x,y) = \exp\left(-\frac{d^2}{2\sigma^2}\right) \quad (2)$$

Therefore,

$$N = \left\{ (u, v) \mid |u| \leq 3\sigma, |v| \leq \dots \right\} \quad (3)$$

If A denotes the total number of points in N, then the mean is given by (5):

$$\mu = \frac{1}{N} \sum_{i=1}^N k(x,y)_i \quad (4)$$

where μ_i is the mean value of the kernel and i is the kernel number. The convolutional mask of the kernel is given by (6):

$$K(x,y)(a,b,c,d) = \sum_{i=1}^N k(x,y)_i \delta(x-x_i, y-y_i) \quad (5)$$

Now, template matching can be employed to detect the blood vessel for applying the entire algorithm of the matched filter, the G-plane of the image is considered (since it yields better results). After enhancing the contrast of the image, median filter is used to remove the noise. The designed matched filter is applied on the image to detect the blood

vessels. Finally, a binaries image is obtained by thresholding. However, a major shortcoming of the whole process is the presence of discontinuous lines in the detections. To improve on this, perception based banalization was carried out using a new binary detection method. A matrix was generated to store the number of matched filter which was responsible for detecting that particular pixel of the blood vessel. The gray level value of the pixels in a particular direction of detection was multiplied by a factor. The value was then checked to be above threshold level. For 0°, 15° and 180°, pixels in the horizontal direction were checked; for 30°, 45° and 60°, pixels in the 45 degree and 225 degree directions were checked; for 75°, 90° and 105°, pixels in vertical direction and for 120°, 135° and 150°, pixels in 135 degrees and 315 degree directions were checked. If gray value multiplied by a factor (say 1.2) was greater than the threshold, then that pixel was counted as blood vessel. Finally, the blood vessels are extracted pixel by pixel.

3.2. Hemorrhage Detection

The location conspires for discharge competitors comprised of four phases: 1) picture digitization, 2) identification of drain hopefuls, 3) disposal of FPs (false positive) in veins, and 4) end of FPs by include examination.

Because of blaze light utilized as a part of the fundus photography, there is a run of the mill change in the shade of the fundus pictures. The brilliance estimations of the fundus picture were changed by a nonlinear bend in the tint immersion esteem (HSV) space. With a specific end goal to underscore dark colored districts, the shine rectified shading fundus pictures were then subjected to gamma remedy on every red, green, and blue (R, G and B) picture. The gamma esteem was exactly set to 1.5. In this manner, the histograms of every R, G and B picture were broadened. At last, the drain hopefuls were

distinguished utilizing thickness examination. The distinction in the pixel esteems between two smoothed pictures identified the veins and discharge hopefuls. The FPs veins were dispensed with utilizing jumping box method The proportion of significant hub length and the minor hub length of each portion was ascertained as given by (7) and those with higher qualities were wiped out.

$$\text{ratio} = \frac{\text{Significant pivot length}}{\text{Minor hub length}} \quad (6)$$

Proportions over 1.57 were dispensed with and those beneath 1.57 were considered as hemorrhages. This idea is legitimate when hemorrhages are thought to be close to round shape and the veins show is straight shape. 2.3 Classification.

This includes three phases – (1) preparing stage: recognizing delegate preparing zones and building up a numerical depiction of the traits of each class write through preparing set, (2) grouping stage: informational index is arranged into the class it most nearly looks like, and (3) yield organize: the procedure comprises of a lattice of deciphered classification composes. In this work, a propelled a non-parametric Tree-type classifier – Random Forests (RF) is utilized for characterization. RF are outfit techniques utilizing tree-type classifiers $\{h(x, \Theta_k), k=1, \dots, K\}$ where the $\{\Theta_k\}$ are i.e. irregular vectors and x is the information design. They are a mix of tree indicators to such an extent that each tree relies upon the estimations of an irregular vector tested autonomously and with a similar conveyance for all trees in the backwoods. It utilizes sacking to shape a troupe of order tree [7-8]. RF is recognized from other sacking approaches in that at each part hub in the basic characterization trees, an arbitrary subset of the indicator factors is utilized as potential factors to characterize split. In preparing, it makes numerous Classification and Regression Tree prepared on a bootstrapped test of the first preparing

information, and inquiries just crosswise over haphazardly chose subset of the info factors to decide a split for every hub. RF uses Gini record of hub contamination to decide parts in the indicator factors. For order, each tree makes a unit choice for the most prominent class at input x . The yield of the classifier is dictated by a dominant part vote of the trees that outcome in the best characterization precision. It is better than numerous tree based calculations, since it needs affectability to clamor and does not over fit. The trees in RF are not pruned; in this manner, the computational many-sided quality is decreased. Subsequently, RF can deal with high dimensional information, utilizing an expansive number of trees in the gathering. This joined with the way that irregular determination of factors for a split try to limit the relationship between the trees in the group, brings about mistake rates that have been contrasted with those of Ad boost, in the meantime being considerably lighter in usage. recommends RF "unexcelled in exactness among current calculations". RF has likewise outflanked CART and comparative boosting and stowing based calculation [8]. In the present work, RF has been executed utilizing a Linux based irregular timberland bundle, accessible in R interface.

3.3. Accuracy Assessment

The exactness of the characterization was finished utilizing affectability, specificity, positive forecast esteem (PPV), negative expectation esteem (NPV) as given by conditions (8-11) in view of the four conceivable results - genuine positive (TP); false positive (FP), genuine negative (TN) and false negative (FN).

$$\text{Sensitivity} = \text{TP}/(\text{TP} + \text{FN}) \quad (7)$$

$$\text{Specificity} = \text{TN}/(\text{FP} + \text{TN}) \quad (8)$$

$$\text{PPV} = \text{TP}/(\text{TP} + \text{FP}) \quad (9)$$

$$\text{NPV} = \text{TN}/(\text{TN} + \text{FN}) \quad (10)$$

The affectability measures the extent of genuine positives which are effectively distinguished. The specificity measures the extent of negatives which are accurately recognized. PPV is the accuracy of positives that were effectively distinguished. NPV is the accuracy of negatives effectively distinguished.

IV. RESULTS AND DISCUSSION

sin a RGB retinal image, contrast is greater when the green channel alone is utilized in fundal image feature extraction. Adaptive histogram equalization was used to enhance the contrast of the features of interest against the background.

4.1 Blood Vessel Extraction

A 3 x 3 median filter was used to remove the random noise as displayed in Fig. 1. Blood vessels were detected (as shown in white pixels against black background in Fig. 2) after applying the designed matched filter. The matched filtered image was converted to binary equivalent with a global threshold value of 0.1490 determined empirically (Fig. 3), where presence of discontinuous lines was observed. Perception based binarization was carried out by generating a matrix, to store the matched filter number, and then the pixel gray level in that particular direction, multiplied by a factor, was checked for a threshold level.



Figure 2. Retinal image after removing the noise.

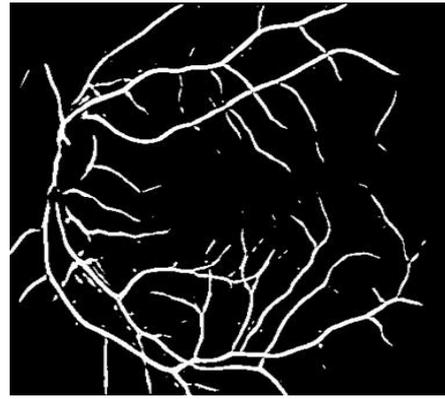


Figure 5. Picture after recognition based binarization.

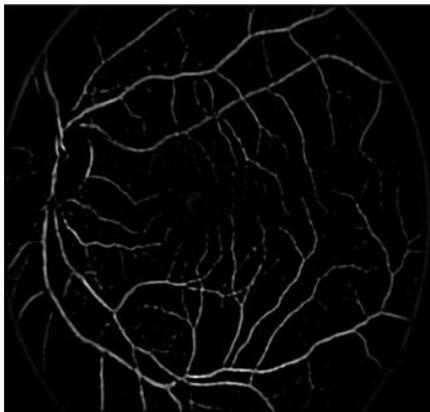


Figure 3. Image obtained after passing through the matched filter.



Figure 4: Double Image after thresholding.

The pixels were investigated level way, 45° , 225° , vertical course, 135° and 315° . If the diminish regard copied by the factor was more imperative than the edge, the pixel was thought about vein. Removed veins are showed up as white pixels in Fig. 4. In the midst of the conditions of diabetes, the thickness of these vessels augments exorbitantly various wrinkle, rendering a sensible indication of the change of diabetic retinopathy in the patient. The thickness can be evaluated by finding the total area of the veins i.e., the total number of white pixels in the photo.

4.2 Hemorrhage Detection

Two smoothened pictures of different window sizes were gotten using smoothening channel and differenced to isolate veins and recognize deplete contenders. The photo was threshold using an overall threshold regard as showed up in the Fig. 5. The false positive veins were discarded using hopping box framework. The extent of noteworthy center point length and the minor center length of each part were found out and those with higher regards (>1.57) were abstained from. The hemorrhages were distinguished and their thickness was registered by finding the amount of white pixels in the photo (Fig. 6).

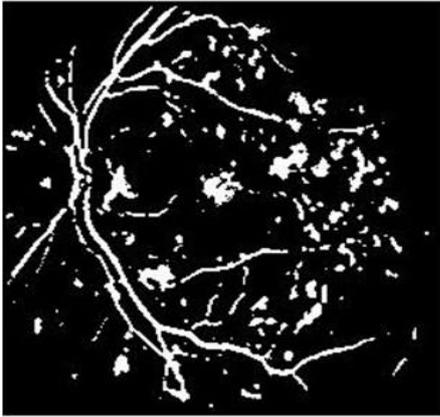


Figure 6. Thresholded image.

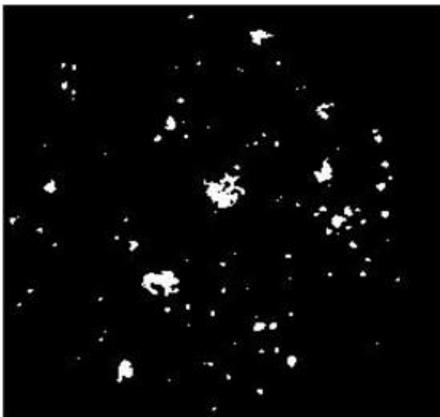


Figure 7. Hemorrhages in the retinal image.

4.3. Classification of different stages of Diabetic Retinopathy

Six features – area and perimeter in each of the R, G, B components of the blood vessels and hemorrhages were extracted. Area is the number of white pixels (blood vessel and hemorrhage candidates) present within the vessels and perimeter the periphery of the vessels. These extracted features were used as inputs to the RF classifier for categorizing the three stages of retinal images. The range of the area and perimeter values of blood vessels and hemorrhages for each stage of the diabetic retinopathy with the different RGB layers are shown in Table 2 and 3

TABLE 2. Range of Input Area Features to Classification Algorithms

Classes	Area in R layer ($\mu \pm \sigma$)	Area in G layer ($\mu \pm \sigma$)	Area in B layer ($\mu \pm \sigma$)
Normal	9169 \pm 1529	8184 \pm 1384	8093 \pm 1467
Moderate NPDR	1269 \pm 1548	12903 \pm 1687	13365 \pm 1992
Severe NPDR	16075 \pm 1596	14879 \pm 1380	16156 \pm 1760

TABLE 3. Range of Input Perimeter Features to Classification Algorithms

Classes	Perimeter in R layer ($\mu \pm \sigma$)	Perimeter in G layer ($\mu \pm \sigma$)	Perimeter in B layer ($\mu \pm \sigma$)
Normal	5640 \pm 901	5348 \pm 840	5603 \pm 861
Moderate NPDR	7568 \pm 847	7630 \pm 725	8875 \pm 1126
Severe NPDR	9475 \pm 878	9004 \pm 552	11258 \pm 984

The examination uncovered that TP=14, FP=0, TN=9, FN=2, sensitivity=0.875, specificity=1, positive anticipated esteem (PPV)=1, and negative anticipated esteem (NPV)=0.8181. The obscure experiments were ordered accurately by 88.46%.

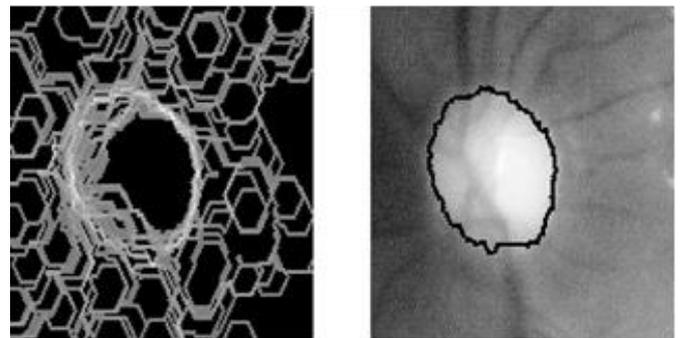


Figure 8. Zone estimations of veins and hemorrhages in RGB layers.

This exhibits the proposed system for arrange in perspective of district and edge of veins and

hemorrhages make impelling comes to fruition [22] reported affectability of 80.21% and specificity of 70.66% while isolating diabetic retinopathy from normal pictures. Here, the retinal pictures we preprocessed using flexible, neighborhood, and separation change. They grasped a neural framework based portrayal

- Erosion: $[\varepsilon^{(sB)}(f)](x) = \min_{b \in sB} f(x + b)$.
- Dilation: $[\delta^{(sB)}(f)](x) = \max_{b \in sB} f(x + b)$.
- Opening: $\gamma^{(sB)}(f) = \delta^{(sB)}[\varepsilon^{(sB)}(f)]$.
- Closing: $\phi^{(sB)}(f) = \varepsilon^{(sB)}[\delta^{(sB)}(f)]$.

We call sB structuring element B of size s . Furthermore, we define the geodesic transformations of an image f (marker) and a second image g (mask)

$$\begin{aligned} \varepsilon_g^{(n)}(f) &= \varepsilon_g^{(1)} \varepsilon_g^{(n-1)}(f) \text{ with } \varepsilon_g^{(1)}(f) = \varepsilon^{(B)}(f) \vee g \\ \delta_g^{(n)}(f) &= \delta_g^{(1)} \delta_g^{(n-1)}(f) \text{ with } \delta_g^{(1)}(f) = \delta^{(B)}(f) \wedge g \\ R_g(f) &= \delta_g^{(i)}(f) \text{ with } \delta_g^{(i)}(f) = \delta_g^{(i+1)}(f); \\ R_g^*(f) &= \varepsilon_g^{(i)}(f) \text{ with } \varepsilon_g^{(i)}(f) = \varepsilon_g^{(i+1)}(f); \end{aligned}$$

$\varepsilon_g^{(n)}(f), \delta_g^{(n)}(f), R_g(f)$ and $R_g^*(f)$ are called geodesic

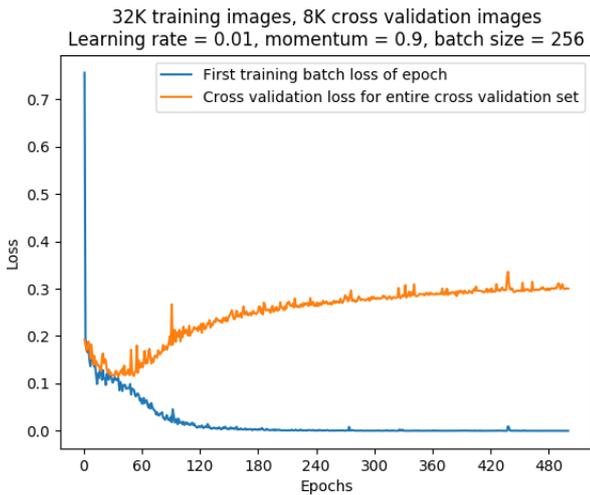


Figure 9. Graphical portrayal of preparing and testing informational collection for RF classifiers.

The carton plots of the zone and edge extents of the isolated features for different kinds of pictures are showed up in Fig. 7 and 8. The case plot work in R quantifiable programming gave connections between's each period of diabetic retinopathy. To prepare and testing the classifiers, the 65 retinal pictures were separated into two sets – an arrangement set of 39 optional illustrations and a test set of 26 tests. A graphical depiction of getting ready and testing instructive record, and the amount of

testing. Near results have been represented by [20], where hemorrhages and micro aneurysms were distinguished to examine diabetes. Their strategy had 71.4% specificity and 96.7% affectability in recognizing diabetic retinopathy. The results got from our method for feature extraction and request contrive revealed that ordinary cases were gathered with 90% accuracy.

V. CONCLUSION AND FUTURE WORK

Our proposed vessel extraction strategy does not require any client mediation, and has predictable execution in both typical and strange pictures. Higher precision than that of other beforehand can be accounted for vessel division strategies. The outcomes showed thus demonstrate that robotized distinguishing proof of retinal veins in light of Gabor channel reactions and NN classifiers can be extremely effective. Henceforth, eye mind pros can conceivably screen bigger populaces utilizing this technique. Moreover, perceptions in view of such a device would be deliberately reproducible. The examination revealed that TP=14, FP=0, TN=9, FN=2, sensitivity=0.875, specificity=1, positive foreseen regard (PPV)=1, and negative foreseen regard (NPV)=0.8181. The dark analyses were requested viably by 88.46%. This shows the proposed method for arrange in perspective of domain and fringe of veins and hemorrhages make impelling results.

VI. REFERENCES

- [1] Heer, T., Garcia-Morchon, O., Hummen, R., Keoh, S.L., Kumar, S.S. and Wehrle, K., 2011. Security Challenges in the IP-based Internet of Things. *Wireless Personal Communications*, 61(3), pp.527-542.
- [2] Liu, Jing, Yang Xiao, and CL Philip Chen. "Authentication and access control in the internet of things." In *Distributed Computing*

- Systems Workshops (ICDCSW), 2012 32nd International Conference on, pp. 588-592. IEEE, 2012.
- [3] Zhao, Kai, and Lina Ge. "A survey on the internet of things security." In *Computational Intelligence and Security (CIS)*, 2013 9th International Conference on, pp. 663-667. IEEE, 2013.
- [4] Zolanvari, Maede, and R. Jain. "IoT Security: A Survey." (2015).
- [5] Zhang, Z.K., Cho, M.C.Y., Wang, C.W., Hsu, C.W., Chen, C.K. and Shieh, S., 2014, November. IoT security: ongoing challenges and research opportunities. In *Service-Oriented Computing and Applications (SOCA)*, 2014 IEEE 7th International Conference on (pp. 230-234). IEEE.
- [6] I. Blake, G. Seroussi, and N. Smart. *Elliptic Curves in Cryptography*. Cambridge University Press, 1999.
- [7] A. K. Ranjan, V. Kumar, and M. Hussain. Security analysis of TLS authentication. In *Proc. of Int. Conf. on Contemporary Computing and Informatics (IC3I)*, pages 1356–1360, Nov. 2014.
- [8] Matharu, Gurpreet Singh, Priyanka Upadhyay, and Lalita Chaudhary. "The Internet of Things: challenges & security issues." In *Emerging Technologies (ICET)*, 2014 International Conference on, pp. 54-59. IEEE, 2014.
- [9] Park, Chang-Seop. "A Secure and Efficient ECQV Implicit Certificate Issuance Protocol for the Internet of Things Applications." *IEEE Sensors Journal* 17, no. 7 (2017): 2215-2223.
- [10] Borgohain, Tuhin, AmardeepBorgohain, Uday Kumar, and SugataSanyal. "Authentication systems in Internet of Things." *arXiv preprint arXiv:1502.00870* (2015).
- [11] Alrawais, Arwa, Abdulrahman Alhothaily, and Xiuzhen Cheng. "X. 509 Check: A Tool to Check the Safety and Security of Digital Certificates." In *Identification, Information, and Knowledge in the Internet of Things (IIKI)*, 2015 International Conference on, pp. 130-133. IEEE, 2015.
- [12] Chau, Sze Yiu, Omar Chowdhury, Endadul Hoque, Huangyi Ge, Aniket Kate, Cristina Nita-Rotaru, and Ninghui Li. "SymCerts: Practical Symbolic Execution For Exposing Noncompliance in X. 509 Certificate Validation Implementations." In *Security and Privacy (SP)*, 2017 IEEE Symposium on, pp. 503-520. IEEE, 2017.
- [13] S. Acharya, A. Polawar, P. Pawar, "Two factor authentication using smartphone generated one time password", *IOSR Journal of Computer Engineering (IOSR-JCE)*, Vol. 11(2), (May-Jun. 2013), pp. 85-90.
- [14] Schukat, Michael, and Pablo Cortijo. "Public key infrastructures and digital certificates for the Internet of things." In *Signals and Systems Conference (ISSC)*, 2015 26th Irish, pp. 1-5. IEEE, 2015.
- [15] R. Roman, P. Najera, J. Lopez, "Securing the Internet of Things," *Computer*, vol.44, no.9, pp.51,58, Sept. 2011
- [16] Hui Suo Jiafu Wan Caifeng Zou Jianqi Liu,"Security in the Internet of Things: A Review"2012 International Conference on Computer Science and Electronics Engineering
- [17] X. Xu, "Study on Security Problems and Key Technologies of the Internet of Things," *Computational and Information Sciences (ICCIS)*, 2013 Fifth International Conference on, vol., no., pp.407,410, 21-23 June 2013 doi: 10.1109/ICCIS.2013.114
- [18] Kim, E., Kaspar, D., Chevrollier, N., &Vasseur, J. P. (2011). Design and application spaces for 6LoWPANs draft-ietf-6lowpan-usecases-09. Design and application spaces for 6LoWPANs draft-ietf-6lowpan-usecases-09, January 2011
- [19] Perrig, A., Szewczyk, R., Wen, V., Culler, D., &Tygar, J. D. (2002). Spins: Security protocols

- for sensor networks. In *Wireless Networks Journal*, September 2002.
- [20] D Suresh K., Rizwan P. and M. Rajasekhara Babu (2016). *EEIoT: Energy Efficient Mechanism to Leverage the Internet of Things (IoT)*, IEEE Int. Con. on Emerging Technological Trends, Kollam, pp-14-22, India.
- [21] D. Granlund, C. Åhlund, and P. Holmlund, "EAP-Swift: An Efficient Authentication and Key Generation Mechanism for Resource Constrained WSNs," *Int. Journal of Distributed Sensor Networks* Vol. 2015 (2015), Article ID 460914
- [22] <https://aws.amazon.com/documentation/>
- [23] Savio Sciancalepore, Student Member, IEEE, Giuseppe Piro, Member, IEEE, Gennaro Boggia, Senior Member, IEEE, and Giuseppe Bianchi, *Public Key Authentication and Key agreement in IoT devices with minimal airtime consumption*
- [24] <https://www.ipa.go.jp/security/rfc/RFC3280-04EN.html>
- [25] Sugata Sanyal, Ayu Tiwari, Sudip Sanyal, "A Multifactor Secure Authentication System for Wireless Payment", *Emergent Web Intelligence: Advanced Information Retrieval*, Ed: Chbeir Richard et al, First Edition, 2010, Chapter 13, pp. 341-369, XVI, Springer Verlag London Limited, 2010, DOI: 10.1007/978-1-84996-074-8_13.