Jurnal Infotel
Vol. 16, No. 1, February 2024, pp. 44–57.
doi:10.20895/infotel.v16i1.1029

Research Article

Foveal Avascular Zone Image Encryption using Pixel Scrambling Combination Technique for Medical Image Security

Dewi Purnamasari[1,*], Didin Herlinudinkhaji[2], Astrie Kusuma Dewi[3] and Muhammad Zairon Mauludin[4]

[1,2,4] Universitas Ivet, Semarang 50235, Indonesia
[3]Politeknik Energi dan Mineral Akamigas, Blora 58315, Indonesia

*Corresponding email: dewipurnamasari@ivet.ac.id

Received: August 25, 2023; Revised: November 17, 2023; Accepted: January 9, 2024.

Abstract: Data theft from year to year has increased in the era of big data and society 5.0. One area that requires data security is patient medical data. Medical image data security must be done to protect medical data security from data theft by third parties so that they cannot access the data. The development of diabetic retinopathy (DR) is also increasing every year. Determining the severity of DR is done by detecting the foveal avascular zone (FAZ). Encryption is the process of changing a plain image into a cipher image. In this study, we compared the results of image quality and encryption time between the Vigenere cipher method and a combination of pixel scrambling. The average encryption time of the tested FAZ images is 0.03 seconds. This result proves that the pixel combination method has a faster encryption time than the Vigenere cipher. Vigenere cipher encryption time is 4.96 seconds. The existence of the FAZ area with the pixel combination randomization method of the encryption process is also invisible, so third parties will not know about its existence. The combined pixel randomization method is safer because it uses a combination of calculating the mean and standard deviation.

Keywords: cipher image, diabetic retinopathy, foveal avascular zone, mean, plain image, standrad deviation

1 Introduction

Diabetic retinopathy (DR) is one of the extreme complications of diabetes mellitus, which develops over time to affect the eyes and eventually causes blindness in people [1]. In

ISSN: 2085-3688; e-ISSN: 2460-0997

countries with large populations, such as China, Bangladesh, India, and Indonesia, almost 45 % of the population suffer from diabetes DR grading from color fundus images: An autotuned deep learn [2]. According to studies conducted in America, Australia, Europe, and Asia, the number of people with DR will rise from 100.8 million in 2010 to 154.9 million in 2030, with 30 % of them at risk of going blind [3]. The FAZ is the most accurate vision zone on the retina without capillaries at the center of the macula, which is the dark zone responsible for the center of vision [4]. FAZ plays an essential role in identifying the development of DR [5]. Because FAZ is located close to blood vessels, enhancement, and blood vessel extraction steps are needed to detect it.

According to data from Cyber Patrol, data theft is increasing in Indonesia each year. During the last five years, data theft has increased by 80 % from 20 reports in 2016. The general public or hospitals reported 182 instances of data theft in 2023. This figure increased by 27.3 % compared to the previous year's 143 reports. The problem of data security is becoming more severe because the trend of data theft is increasing. In Indonesia, health data theft cases are not new [6]. In 2020, data on 30 thousand COVID-19 patients in Indonesia was allegedly stolen and sold. It causes financial and psychological losses to the victims, who may receive discriminatory treatment. In January 2022, there were allegations of patient medical record data leakage at several hospitals in Indonesia, where 720 GB of data was sold on the Raidforums online forum [7]. Digital technology currently uses data flowing in a large enough network, producing medical big data in particular, Consequently, there are worries about how it may affect data security and privacy [8].

Data security must be implemented to ensure that unauthorized parties cannot access and use the data, and is increasingly needed in the era of big data and the Internet of Things, especially for securing digital data. One area that requires data security is the world of health, especially for securing patient medical data. According to Indonesian law (UU) and applicable regulations, medical records are something doctors must keep confidential to provide health services [9]. Medical imaging is one of the digital images that are very sensitive and need to be secured to maintain their confidentiality according to the medical image code of ethics. Medical images need to be protected so that unauthorized parties cannot access the data so that manipulation or theft of valuable data or essential information does not occur. Securing medical image data needs to be done so that medical image data is not misused by unauthorized parties, as written in the Law of the Republic of Indonesia number 29 of 2004 concerning medical practice, which states that medical record data must be kept confidential.

In the explanation of Law of the Republic of Indonesia no. 29 of 2004 concerning medical practice in article 47 paragraph 2, which confirms *"Medical records as referred to in paragraph (1) must be kept and kept confidential by the doctor or dentist and the head of the health service facility,"* and also in the Regulation of the Minister of Health of the Republic of Indonesia No. 269/Menkes/Per/III/2008 concerning medical records. Article 10, paragraph 1, emphasizes that *"information regarding the patient's identity, diagnosis, disease history, examination history, and treatment history must be kept confidential by doctors, dentists, certain health workers, management officers, and leaders of health service facilities"*. Due to the sensitive nature of medical images stored in electronic health records, several security protections have been introduced through the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH). In 2022, the health services provider Eye Care Leaders data for DR suffered a ransomware attack. Each covered entity reports the violation. Therefore, it is essential to secure medical image data [10]. One method of data security is known as cryptography. Cryptography is a technique for hiding the contents of data or messages so they can no longer be understood or read [11–13].

In a previous study, Nugroho *et al.* [14] examined the FAZ detection of fundus images in the Messidor database. This study detects FAZ in four stages: a correlation test, blood vessel extraction, FAZ identification, and the pre-processing step. The blood vessels' pre-processing and extraction stages determine where the blood vessels that cover FAZ are located. The results of FAZ detection images were compared with measurements according to ophthalmology.

Nugroho *et al.* [15] researched FAZ segmentation using capillary endpoint detection. The study's results compared the Messidor and Drive retinal database tests with the correlation test. Demirtas [16] researched using the hyperchaotic 2D map method and cross-channel pixel scrambling using Lena and mandril image validation with correlation and encryption time. Al-Ali and Alkhasraji [17] researched using 2D couple chaotic maps and pseudo-random bit generation using 2D couple chaotic map dan pseudo-random bit generation. Hua *et al.* [18] examined medical images of pixel randomization combining XOR and modulo with lung and brain image research objects without going through the enhancement process. Sonbay *et al.* [19] researched CFB and CSTM validation parameters using standard deviation and variance. Shi *et al.* [20] examined HHP, zig-zag pixel scrambling, and the research objects of Lena, paper, house, and boat dollar grayscale images. Zhu *et al.* [21] analyzed the security performance of an image encryption algorithm based on a chaotic dual scrambling of pixel and bit and the research objects of paper, autumn, rice, and cameraman grayscale image while the validation using entropy.

Madono *et al.* [22] examined PIH and LPPS, looking for the mean and standard deviation of color image parameters. Purnamasari and Erwanti [6] researched with the Vigenere cipher to calculate the encryption time, the area of the method, and according to ophthalmology, with the FAZ image research object. Researchers approach cryptography, which is a method of securing data or hiding the contents of data so that it can no longer be understood or read. This research used a combination of pixel randomization with mean and standard deviation because the parameters mean and standard deviation are widely used in digital images to analyze statistics and extract features from an image. The combination method of randomizing the pixel mean and standard deviation applied to the FAZ study object has not yet been employed in any prior studies. In earlier studies, the mean and standard deviation parameters were the desired outcomes rather than technique steps. Researchers examined the image of FAZ [14, 23]. Then, for the security of the FAZ image data, it is carried out with a combination of randomization of the pixel mean and standard deviation.

In this study, we also compare previous studies with the Vigenere cipher by looking at the results of image quality and encryption time [6]. There is the enhancement stage [18,20], segmentation (directly processed). This research to obtain FAZ requires pre-processing, carried out during the enhancement stage. We used Messidor 15 retinal fundus images [6]. This research has contributed to helping Ophthalmology in terms of the security of color fundus image data, especially FAZ pathology, from the widespread theft of medical image data by unwanted third parties.

This research aims to develop and analyze cryptographic methods for the security of FAZ medical images, especially encryption, using a combination technique of randomizing the pixel mean with the standard deviation. This research also aims to evaluate image results and encryption time by comparing the Vigenere cipher method from previous research with a combination of pixel randomization methods.

2 Research Method

This study has five research stages such as pre-process stage, blood vessels extraction stage, FAZ detection stage, pixel randomization cryptographic stage, and validation stage of encryption time.

2.1 Pre-Process Stage

Pre-processing stage to carry out the pre-processing stage, the input image used is an RGB image stored in tif format. Then determine the macula points; click on the macula area, which is dark. The next stage is extracting the Green channel and converting it to grayscale. The goal is to save computation. Then the enhancement, which consists of two top-hat methods and contrast stretching. Enhancement aims to make the macular area brighter because, in retinal fundus images, FAZ is in the macular area, a dark area covered by blood vessels.

2.2 Blood Vessels Extraction Stage

At this stage, the blood vessel extraction process starts with input image input from enhancement, which is processed towards thresholding and masking. Then it is segmented using a matched filter. The next step is cropping ROI on the macula. The cropping technique determines the macula's center point (x, y). The next stage is thinning, which is thinning blood vessels. Thinning is done to make blood vessels smaller and clearer.

2.3 FAZ Detection Stage

The FAZ detection stage is to find out the area of the area obtained. The resulting image of thinning blood vessels is processed. Furthermore, the detection of FAZ with the capillary endpoint method begins by looking for the endpoint of the blood vessels. There are many endpoint blood vessels in the macula area. Endpoint blood vessels closest to the center of the macula are connected to detect the presence of FAZ. The area of the FAZ generates the area of the FAZ in pixels. This blood vessel endpoint uses 4 quadrant technique.

2.4 Pixel Randomization Cryptographic Stage

There are two stages of cryptography, namely encryption and decryption. Medical image encryption is a growing application area for cryptographic systems, and as such, should be performed using efficient algorithms that require low cost and time [24]. This research uses encryption. Encryption is changing a plain image (an image that can be read) into a cipher image (an image that cannot be read) [25]. Combining the calculation of the mean and standard deviation is how this combined pixel randomization method operates. The mean is a measure of the dispersion of an image. The average value, or mean, is the middle value of a data group. The average value is obtained from the number of data points divided by

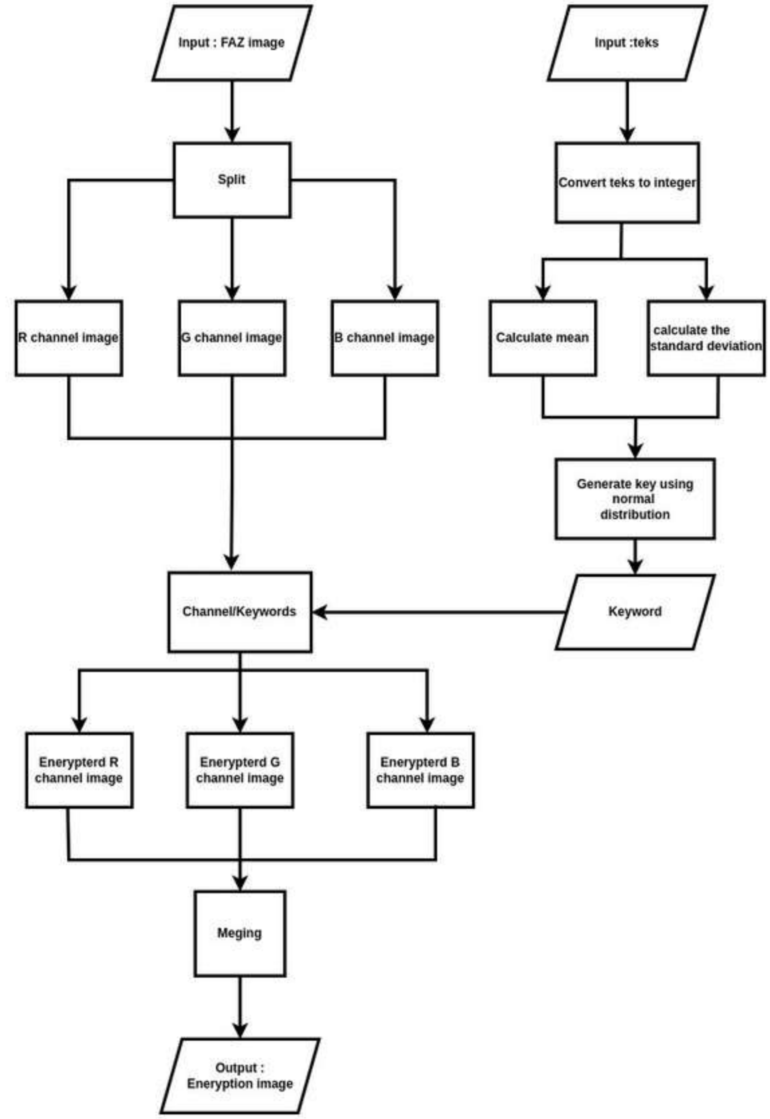

Input : FAZ image
Input :teks
Split
Convert teks to integer
R channel image
G channel image
B channel image
Calculate mean
calculate the standard deviation
Generate key using normal distribution
Channel/Keywords
Keyword
Enerypterd R channel image
Enerypterd G channel image
Enerypterd B channel image
Meging
Output : Eneryption image

Figure 1: Flowchart of the encryption.

the number of data points. The average value of the image is used as a determining value for the next process in image processing techniques. The formula for calculating the mean can be expressed in (1).

$$\text{Mean}(\bar{x}) = \frac{\sum_i^n x_i}{n} \tag{1}$$

where $\bar{x}$ is the average, n is the number of pixels, x_i is the pixel value in column i.

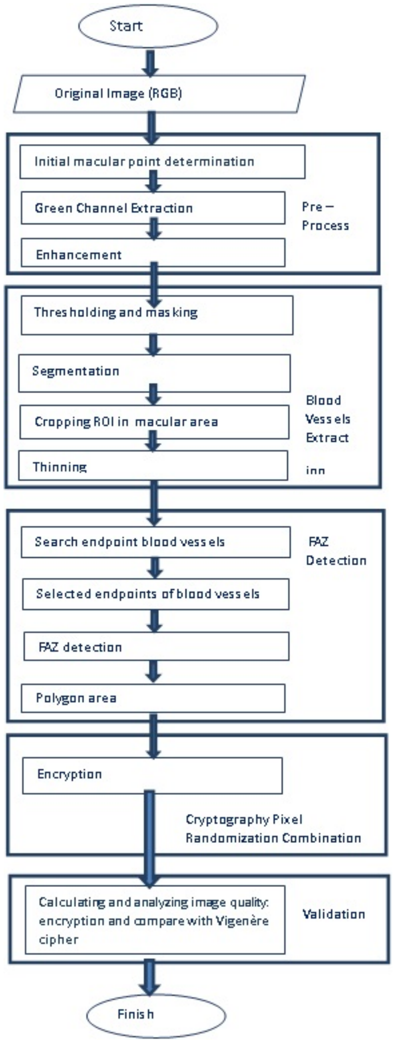

Start
Original Image (RGB)
Initial macular point determination
Green Channel Extraction
Pre – Process
Enhancement
Thresholding and masking
Segmentation
Cropping ROI in macular area
Blood Vessels Extract inn
Thinning
Search endpoint blood vessels
FAZ Detection
Selected endpoints of blood vessels
FAZ detection
Polygon area
Encryption
Cryptography Pixel Randomization Combination
Calculating and analyzing image quality: encryption and compare with Vigenère cipher
Validation
Finish

Figure 2: Flowchart of the approach.

Standard deviation is one of the basic statistical techniques used to explain group homogeneity. The formula for calculating standard deviation can be expressed in (2).

$$\sigma = \sqrt{\frac{\sum(x_i - \mu)^2}{N}} \tag{2}$$

where σ is population standard deviation, N is the size of the population, x_i is each value from the population, μ is the population mean.

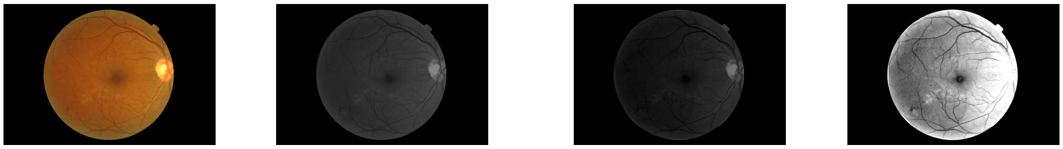
The cryptographic stages of pixel randomization combinations can be seen in Figure 1. Figure 1 shows the FAZ image encryption process. This stage includes the input image of the FAZ results as a plain image, then splits the channel into three channels, Red, Green, and Blue, then enters the key obtained from the input text and converts it into an integer. Calculate the standard deviation and the mean. Then the two fundamental techniques are combined with normal distribution to get a new key for the following essential stage. Image of FAZ channel Red, Green, and Blue (R, G, B). Then split to get the latest encrypted output image.

2.5 Validation Stage of Encryption Time

This stage is carried out using encryption time to see the results of FAZ image quality. The time needed for encryption is a measure of the complexity of the proposed algorithm, as well as its suitability for utilization in real-time applications [26]. The validation stage uses encryption time, and the results of the encryption images are compared with previous studies using the Vigenere cipher. This research used encryption time by comparing the Vigenere cipher method because one of the essential things about cryptography is the encryption time or running time. Faster running times are also required for encryption and decryption. The encryption and decryption process time will show the cryptographic process's calculation speed, which is used as a parameter for validating the cryptographic speed of a method. The validation process calculates the encryption time and FAZ image quality. This research stage as a whole can be seen in Figure 2.

3 Result

This study used the MESSIDOR retinal fundus image database with images in TIF format, which has four grades, namely grades 0, 1, 2, and 3. We used 15 retinal fundus images. Figure 3 depicts the pre-processing phase.

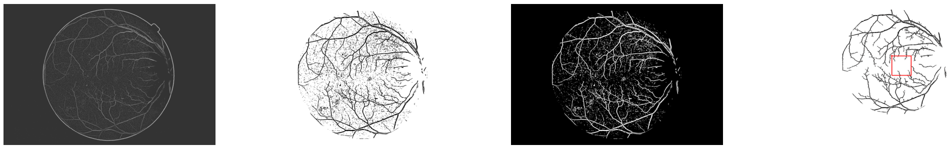


(a) Fundus image *(b) Greysacle fdari green channel =1, red dan blue =0* *(c) Top hatt transformation* *(d) Contrast stretching*

Figure 3: Enhancement result.

Figure 3 shows the grayscale obtained from the Green channel because its component is the best among the Red and Blue. The Green channel component is the brightest. A matching filter procedure is used to separate the blood vessels from the background in the results of the blood vessel extraction. Then, inverting the first white image background to a black background segmentation results in the detection of small blood vessels in the middle of the FAZ. The center of the FAZ should be an area without any veins. The blood vessel extraction stage is shown in Figure 4.

The outcomes of the matched filter image are displayed in Figure 4(a). Figure 4(b) illustrates the preliminary steps in the extraction of blood vessels following the matching filter. The image is then inverted (see Figure 4(c)). Picture inversion aims to provide an



(a) Matched filter *(b) Separating the blood vessel of the background* *(c) Invert image* *(d) Extraction of Blood vessel*

Figure 4: Vessel extraction results (blood vessels).

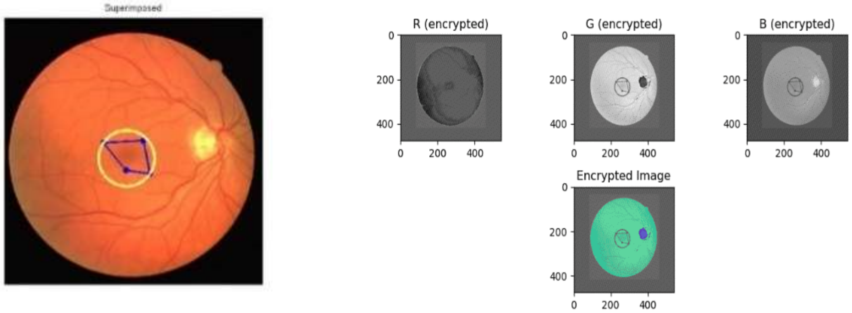
output that flips the image that was input. If the binary image is 1, the output will be 0, but if it's 0, the output will be 1 instead. In the image, it can be seen that there is still much noise in the form of small blood vessels entering. Figure 4(d) shows the results after extraction and the vascular FAZ areas marked with an ROI. The vein extraction image looks good, with no noise and a small vein is small.

(a) ROI *(b) End points blood vessel* *(c) Detection of FAZ* *(d) Extraction of FAZ*

Figure 5: Result and detection of FAZ.

FAZ detection is carried out through cropping based on an ROI measuring 256 × 256. The stages of FAZ detection can be seen in Figure 5. FAZ detection must go through the blood vessel extraction stage. Figure 5(a) is a cropping of the FAZ. Figure 5(b) shows the results of blood vessels with ends. The selection of blood vessel endpoints is taken from each quadrant. Figure 5(c) shows there are four quadrants: the first, second, third quadrant, and the fourth quadrant. After the candidate blood vessel endpoint has been selected, the blood vessel endpoint is connected. Figure 5(d) shows superimposed. The superimposed image plot results appear correct because the FAZ is located in the macular area after the area is calculated. The greater the degree of DR, the worse the degree. Because FAZ is known in the area, vessel endpoints were taken from areas close to the FAZ center point. After that, the superimposed FAZ results are used as input images for cryptography with a combination of pixel randomization.

The results of FAZ detection were obtained by changing the superimposed FAZ image, which, according to the researcher, was in the form of a polygon compared to the circular image according to ophthalmology. According to ophthalmology, the study FAZ area is smaller than that of the FAZ image. The FAZ area is in the form of a polygon, while according to the doctor, marking the FAZ by marking a circle In previous studies [6], FAZ images as input in Vigenere cipher cryptography are plain images that can be read and converted into cipher images. Based on previous research, the encrypted image of the Vigenere cipher results is shown in Figure 6.



(a) original image

(b) Encrypted image

Figure 6: Image result from encryption and Vigenere cipher [6]

Figure 6 shows the image encrypted using the Vigenere cipher. The existence of FAZ can still be seen in Red, Green, and Blue. In previous research, the data to be encrypted is an image and the key is text. The principle of the Vigenere cipher method in previous research is that the pixel image is made 1D, then each index is given an operation to change the pixel value by shifting and multiplying the modulo 256 divider (based on the concept of addition modulo 256). If the length of the key vector is shorter than the length of the original image vector, then the key vector is doubled so that both are the same length.

Previous research with the proposed method shows that the results of encryption are clearly different. The proposed method's encryption results are more secure because the existence of FAZ cannot be known. The Red and Green channels show that the location of FAZ is not found and it can also be seen that the FAZ image in the red and Green channels looks like the result of retinal image segmentation, really FAZ is not visible. The results proposed method of encryption with pixel combinations are shown in Figure 7.

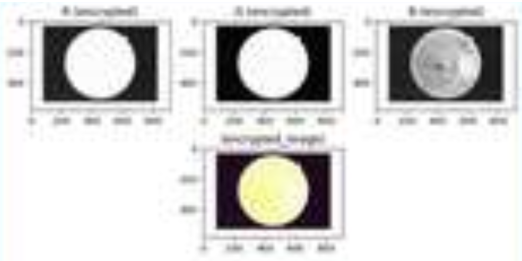


Figure 7: The resulting proposed method image from the encryption combination of pixel scrambling

Figure 7 shows the result proposed method of pixel scrambling. The proposed method uses a combination of pixel mean and standard deviation randomization. In the FAZ image results, the results look like segmentation. The existence of FAZ can still be seen in Red, Green, and Blue.

4 Discussion

There has been some research related to this topic, the image encrypted using the Vigenere cipher as shown in Figure 6. The encrypted image consists of three Red, Green, and Blue channels. The Green channel shows a brighter image since the FAZ detection process time used is the Green channel component. The encrypted image using the FAZ Vigenere cipher method is colored green. The encrypted image shows that the result differs from the original image but has the same drawbacks as the original image. The existence of the FAZ is still clearly visible. The principle of image encryption using the Vigenere cipher technique on FAZ images is plaintext in pixel intensity; if the key is shorter than the plaintext, then the key length is the same as the plaintext. If the length is the same, then the encryption process is carried out by shifting to the right, where each pixel value in the plaintext corresponds to the key corresponding to the plaintext pixel value (each index is given an operation to change the pixel value). The operation uses the concept of addition modulo 256. The disadvantage is that if the key length is shorter than the length of the plaintext, the key used to encrypt the plaintext will be repeated. Repeated keys create gaps for cryptanalysts to open by force.

The result of the proposed method is pixel scrambling. In the FAZ image results, the results look like segmentation. The encryption results are also yellow. Only the Blue component, the image results look like segmentation. Dark black results, when encrypted, will still produce black. The encrypted FAZ area does not look completely different from the Vigenere cipher. The Green channel does not appear to have any FAZ, and the image is brighter due to the enhancement process. This research was conducted by testing 15 FAZ images. This test determines the encryption time of each image by entering the INDONESIA JAYA text key. This research used one key because the processing time for encryption is relatively fast. This is due to the efficiency in crucial generation, and the number of keys can be reduced to make encryption computing accessible. The symmetric key algorithm can be used on systems in real time. Hence, using one key is faster than using asymmetric cryptography. The encryption process of combining pixel randomization is carried out by inserting a FAZ plaintext image and then separating it into three channels. The INDONESIA JAYA text key (key letters) is entered, and then the text key is processed by calculating the mean formula and the standard deviation. Then, the combination is combined with a normal distribution to obtain a new key, which is used for the next encryption process (this key is used to randomize the pixels in each channel). The new key is inserted into the separated FAZ image (R, G, B channels) to get an R, G, B FAZ encryption image. Next, the R, G, and B encryption images are combined to obtain a new FAZ image encryption. The proposed method combination pixel randomization method is safer than the Vigenere cipher method. The cryptanalyst needs time to open it by force because he has to combine the mean and standard deviation values first. The disadvantage of this research is that the retinal color fundus image has a black background, and most of the retinal color fundus images have low contrast, and the pixel intensity is uneven. FAZ image encryption time is shown in Table 1. This encryption is used to secure medical image data that is vulnerable to data theft.

Table 1 shows that the average encryption time in testing 15 FAZ images using the Vigenere cipher method was 4.96 seconds. Whereas in the proposed method, the average is 0.03 seconds. The results also show that the proposed method of pixel randomization combination has better image quality (unknown). The existence of FAZ compared to the image

Table 1: FAZ Vigenere cipher image encryption time with proposed method

2*No	2*Image	Area of FAZ	Time vigenere	Proposed method time
		(pixel)	(second)	(second)
1	Image 1. tif	3,747	4.05	0.049
2	Image 2. tif	4,133	4.67	0.037
3	Image 3.tif	2,743	4.65	0.026
4	Image 4. tif	6,579	6.59	0.026
5	Image 5. tif	4,572	4.7	0.044
6	Image 6. tif	5,070	5.2	0.028
7	Image 7. tif	5,515	4.8	0.031
8	Image 8. tif	5,672	5.02	0.031
9	Image 9. tif	3,421	5.04	0.032
10	Image 10. tif	4,332	5.49	0.031
11	Image 11. tif	4,474	5.347	0.037
12	Image 12. tif	4,902	4.85	0.025
13	Image 13. tif	5,151	4.57	0.027
14	Image 14. tif	5,340	5.06	0.025
15	Image 15. tif	3,738	4.49	0.024

results with the Vigenere cipher method. This encryption is used to secure medical image data that is vulnerable to data theft. The encryption time used in this pixel randomization combination method is faster because the process involved in calculating the mean and standard deviation is more resistant to data theft. Encryption time for the Vigenere cipher is done by calculating the initial time to enter the FAZ image minus the final FAZ image (based on the concept of addition modulo 256). Meanwhile, in this study, the encryption time was based on pixel randomization, mean, and standard deviation.

5 Conclusion and Future Work

Based on research, cryptography is necessary for medical data security. Encryption time and encryption results show that the pixel scrambling combination is faster, with an average time of 3 seconds than the Vigenere cipher and the FAZ encryption results, which are better readable by third parties. The pixel randomization combination technique is safer and different from the vigenere cipher. The cryptanalyst at Vigenere cipher finds it easier to open by force by trying to force the lock using the principle of trying and trying to shift the key. Future research can be carried out by combining the Vigenere cipher with a combination of pixel randomization and other modern cryptographic methods, adding more FAZ test image data, and adding evaluation parameters for cryptographic encryption image quality analysis.

Acknowledgments

Thank you to the Ministry of Research and Technology for the Beginner Lecturer Research Scheme, which has funded the implementation of this research.

References

[1] M. M. Islam, H.-C. Yang, T. N. Poly, W.-S. Jian, and Y.-C. (Jack) Li, "Deep learning algorithms for detection of diabetic retinopathy in retinal fundus photographs: A systematic review and meta-analysis," *Computer Methods and Programs in Biomedicine*, vol. 191, p. 105320, July 2020.

[2] T. Athira and J. J. Nair, "Diabetic retinopathy grading from color fundus images: an autotuned deep learning approach," *Procedia Computer Science*, vol. 218, pp. 1055–1066, 2023.

[3] M. Hayati, K. Muchtar, Roslidar, N. Maulina, I. Syamsuddin, G. N. Elwirehardja, and B. Pardamean, "Impact of CLAHE-based image enhancement for diabetic retinopathy classification through deep learning," *Procedia Computer Science*, vol. 216, pp. 57–66, 2023.

[4] Y. Pang, G. Zhang, H. Zhang, J. She, X. Zhang, H. Li, and G. Zhang, "Foveal avascular zone in normal human eyes by optical coherence tomography angiography," *Photodiagnosis and Photodynamic Therapy*, vol. 42, p. 103303, June 2023.

[5] Q. Li, P. Gong, P. H. Ho, B. F. Kennedy, D. A. Mackey, F. K. Chen, and J. Charng, "Evaluating distribution of foveal avascular zone parameters corrected by lateral magnification and their associations with retinal thickness," *Ophthalmology Science*, vol. 2, p. 100134, June 2022.

[6] D. Purnamasari and N. Erwanti, "Enkripsi citra fovea avascular zone (Faz) menggunakan kriptografi vigenere cipher," *Pseudocode*, vol. 9, pp. 114–121, Oct. 2022.

[7] S. Sofia, E. T. Ardianto, N. Muna, and S. Sabran, "Analisis aspek keamanan informasi data pasien pada penerapan rme di fasilitas kesehatan," *Jurnal Rekam Medik & Manajemen Informasi Kesehatan*, vol. 1, pp. 94–103, Oct. 2022.

[8] L. Taylor, "The price of certainty: How the politics of pandemic data demand an ethics of care," *Big Data & Society*, vol. 7, p. 205395172094253, July 2020.

[9] A. Ampera, "Tanggung jawab rumah sakit terhadap pasien dalam pelaksanaan pelayanan kesehatan," *Al-Ishlah: Jurnal Ilmiah Hukum*, vol. 21, pp. 59–74, Nov. 2018.

[10] G. C. M. Purba and A. Id Hadiana, "Pengamanan citra medis berbasis steganografi d an kriptografi dengan menggunakan metode end of file dan advanced encryption standard," *Informatics and Digital Expert (INDEX)*, vol. 4, pp. 1–9, July 2022.

[11] D. Purnamasari, A. K. Dewi, and A. N. Trisetiyanto, "Analisis performansi kriptografi berbasis caesar cipher untuk keamanan data menggunakan python pada tembang macapat," *Journal of Systems, Information Technology, and Electronics Engineering*, vol. 1, pp. 50–54, Dec. 2021.

[12] D. Purnamasari and H. Prasetyani, "Analisis performansi kriptografi berbasis algoritma caesar cipher dan rail fence cipher pada tembang macapat," *Joined Journal (Journal of Informatics Education)*, vol. 5, p. 1, June 2022.

[13] S. R. Bhandari and Z. B. K. Mundargi, "A review on image encryption and decryption," *International Journal of Creative Research Thoughts (IJCRT)*, vol. 6, no. 2, pp. 1314–1318, 2018.

[14] H. A. Nugroho, D. Purnamasari, I. Soesanti, K. Z. W. Oktoeberza, and D. A. Dharmawan, "Detection of foveal avascular zone in colour retinal fundus images," in *2015 International Conference on Science in Information Technology (ICSITech)*, (Yogyakarta), pp. 225–230, IEEE, Oct. 2015.

[15] H. A. Nugroho, D. Purnamasari, I. Soesanti, W. K. Z. Oktoeberza, and D. A. Dharmawan, "Segmentation of foveal avascular zone in colour fundus images based on retinal capillary endpoints detection," *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, vol. 9, pp. 107–112, Nov. 2017.

[16] M. Demirtaş, "A new RGB color image encryption scheme based on cross-channel pixel and bit scrambling using chaos," *Optik*, vol. 265, p. 169430, Sept. 2022.

[17] A. K. H. Al-Ali and J. M. D. Alkhasraji, "Colour image encryption based on hybrid bit-level scrambling, ciphering, and public key cryptography," *Bulletin of Electrical Engineering and Informatics*, vol. 12, pp. 1607–1619, June 2023.

[18] Z. Hua, S. Yi, and Y. Zhou, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Processing*, vol. 144, pp. 134–144, Mar. 2018.

[19] A. M. Sonbay, A. Fanggidae, and K. Letelay, "Penyandian data teks menggunakan algoritma cipher feed-back dan chaotic skew tent map," *Jurnal Komputer dan Informatika*, vol. 5, pp. 12–20, Oct. 2017.

[20] M. Shi, S. Guo, X. Song, Y. Zhou, and E. Wang, "Visual secure image encryption scheme based on compressed sensing and regional energy," *Entropy*, vol. 23, p. 570, May 2021.

[21] S. Zhu, C. Zhu, and H. Yan, "Cryptanalyzing and improving an image encryption algorithm based on chaotic dual scrambling of pixel position and bit," *Entropy*, vol. 25, p. 400, Feb. 2023.

[22] K. Madono, M. Tanaka, M. Onishi, and T. Ogawa, "Scrambling parameter generation to improve perceptual information hiding," *Electronic Imaging*, vol. 33, pp. 155–1–155–8, Jan. 2021.

[23] H. A. Nugroho, D. Purnamasari, I. Soesanti, K. Z. W. Oktoeberza, and D. A. Dharmawan, "Detection of foveal avascular zone in colour retinal fundus images," in *2015 International Conference on Science in Information Technology (ICSITech)*, (Yogyakarta), pp. 225–230, IEEE, Oct. 2015.

[24] S. T. Ahmed, D. A. Hammood, R. F. Chisab, A. Al-Naji, and J. Chahl, "Medical image encryption: a comprehensive review," *Computers*, vol. 12, p. 160, Aug. 2023.

[25] M. Kaur, S. Singh, and M. Kaur, "Computational image encryption techniques: a comprehensive review," *Mathematical Problems in Engineering*, vol. 2021, pp. 1–17, July 2021.

[26] W. Alexan, M. Elkandoz, M. Mashaly, E. Azab, and A. Aboshousha, "Color image encryption through chaos and kaa map," *IEEE Access*, vol. 11, pp. 11541–11554, 2023.