

# ENKRIPSI CITRA FOVEA AVASCULAR ZONE (FAZ) MENGGUNAKAN KRIPTOGRAFI *VIGENERE CIPHER*

Dewi Purnamasari<sup>1</sup>, Nindita Erwanti<sup>2</sup>,

<sup>1</sup> Prodi Sistem dan Teknologi Informasi, Fakultas Saintek, Universitas Ivet, Jl.Pawiyatan Luhur IV No.16 Semarang

<sup>2</sup> Prodi Bisnis Digital, Fakultas Saintek, Universitas Ivet, Jl.Pawiyatan Luhur IV No.16 Semarang

<sup>1</sup>dewipurnamasari@ivet.ac.id

<sup>2</sup>nindita.erwanti@ivet.ac.id

**Abstrak:** Kemajuan teknologi yang berkembang pesat sekali sangat memengaruhi atas keamanan data baik data teks maupun data citra digital. Pencurian data dari tahun ke tahun mengalami peningkatan. Salah satu area yang memerlukan keamanan data yaitu keamanan data medis pasien. Keamanan data citra medis sangat perlu dilakukan untuk melindungi keamanan data medis dari pencurian data oleh pihak ketiga supaya tidak bisa mengakses data tersebut. Perkembangan *Diabetic Retinopathy* (DR) setiap tahunnya juga meningkat. Menentukan tingkat keparahan DR dilakukan dengan mendeteksi Fovea Avascular Zone (FAZ). Pada penelitian ini mengenkripsi *plainimage* FAZ menjadi *cipherimage* menggunakan metode *Vigenere Cipher*. Waktu enkripsi rata rata dari citra FAZ yang diujikan adalah 4.96 detik. Pada pengujian didapatkan semakin luas area FAZ maka waktu enkripsinya juga semakin lama.

**Kata Kunci:** *Diabetic Retinopathy, Fovea Avascular Zone, plainimage, cipher image, Vigenere cipher*

**Abstract:** *Technological advances are growing rapidly, greatly affecting the security of data, both text data and digital image data. Data theft from year to year has increased. One area that requires data security is the security of patient medical data. Medical image data security is very necessary to protect the security of medical data from data theft by third parties so that they cannot access the data. The development of Diabetic Retinopathy (DR) every year is also increasing. Determining the severity of DR is done by detecting the Fovea Avascular Zone (FAZ). In this study, encrypt the FAZ plain image into a cipher image using the Vigenere Cipher method. The average encryption time of the FAZ image tested is 4.96 seconds. In the test, it is found that the wider the FAZ area, the longer the encryption time.*

**Keywords:** *Diabetic Retinopathy, Fovea Avascular Zone, plain image, cipher image, vigenere cipher*

## I. PENDAHULUAN

Diabetes *Retinopathy* (DR) adalah salah satu komplikasi mikrovaskular *Diabetes Melitus* (DM) merupakan penyebab utama kebutaan pada orang dewasa di seluruh dunia [1] [2]. Penelitian

di Amerika, Australia, Eropa dan Asia melaporkan bahwa jumlah penderita DR meningkat dari 100.8 juta pada tahun 2010 menjadi 154.9 juta pada tahun 2030 dengan 30% terancam kebutaan [3]. FAZ adalah zona visi yang paling akurat pada retina tanpa kapiler di pusat macula yang merupakan zona gelap [4]. FAZ memegang peranan penting dalam mengidentifikasi perkembangan DR. Karena letaknya tertutup pembuluh darah maka untuk mendeteksi FAZ diperlukan tahap *enhancement* dan ekstraksi *blood vessels*.

Pencurian data menurut data dari Patroli Siber menyatakan bahwa dari tahun ke tahun semakin meningkat di Indonesia. Selama lima tahun terakhir peningkatan pencurian data meningkat 80% dari 20 laporan pada 2016. Pada tahun 2022 terdapat 182 kasus pencurian data yang dilaporkan masyarakat ataupun rumah

sakit. Angka ini meningkat 27.3% dibandingkan dengan tahun sebelumnya sebanyak 143 laporan.

Keamanan data adalah sesuatu yang sangat penting dan perlu dilakukan yang mempunyai tujuan memastikan data tidak dapat diakses dan digunakan oleh pihak ke tiga yang merupakan orang yang tidak berhak menerima informasi. Di era *Society 5.0* memberikan kemudahan bagi kita bertukar informasi maupun data. Tetapi disisi lain pengamanan data menjadi hal utama dan semakin diperlukan, terlebih lagi untuk pengamanan data digital. Salah satu area yang memerlukan pengamanan data adalah dunia kesehatan, khususnya untuk pengamanan data medis pasien. Karena sesuai dengan Undang-Undang (UU) dan peraturan yang berlaku, rekam medis adalah sesuatu yang wajib dijaga kerahasiaannya oleh dokter atau penyelenggara pelayanan kesehatan [5].

Salah satu metode pengamanan data dikenal dengan kriptografi. Kriptografi adalah teknik untuk menyembunyikan isi data atau pesan sehingga tidak dapat lagi dimengerti atau dibaca [6][7][8]. Algoritma kriptografi *vigenere* adalah salah satu algoritma kriptografi klasik. Algoritma *Vigenere* yang juga dikenal dengan *Vigenere Cipher* merupakan pengembangan dari *Caesar Cipher* yang termasuk dalam kategori metode kriptografi substitusi. *Vigenere cipher* yang digunakan masih sebatas untuk mengenkripsi data teks, karena memang pada awalnya kriptografi klasik hanya diperuntukkan untuk mengenkripsi pesan teks. Pada perkembangannya, *Vigenere Cipher* juga dapat digunakan untuk mengenkripsi data citra digital. Pada [4], dilakukan enkripsi citra dengan kunci berupa teks menggunakan *Vigenere Cipher*.

Pada penelitian sebelumnya Abduh Riski dkk meneliti implementasi *Vigenere Cipher* pada citra medis pasien kanker payudara dan citra berupa citra asli yang langsung diuji tanpa ada proses enhancement citra [9]. Pada penelitian Dewi Purnamasari dkk meneliti tentang deteksi FAZ dan evaluasi yang diukur adalah korelasi dari luas area FAZ dengan membandingkan luas area FAZ metode peneliti dengan dan luas area FAZ menurut ophtamology [10] [11]. Jadi penelitian sebelumnya hanya membahas deteksi FAZ saja, tidak membahas kriptografi. Pada penelitian ini melanjutkan penelitian sebelumnya dan menerapkan metode kriptografi *Vigenere cipher*. Peneliti menggunakan *Vigenere cipher* untuk mengenkripsi data citra *medis Fovea Avascular Zone* (FAZ) berupa citra pasien penderita *Diabetes Retinopathy* dengan menggunakan kunci yang berupa kunci teks dan parameter yang digunakan untuk mengevaluasi adalah waktu enkripsi.

## II. LANDASAN TEORI

### A. Citra Digital

Citra adalah salah satu bentuk informasi yang diperlukan manusia selain teks, suara dan video. Informasi yang terkandung dalam sebuah citra dapat diinterpretasikan berbeda-beda oleh manusia satu dengan yang lain. Citra juga dapat direpresentasikan dari intensitas cahaya pada bidang dimensi dua. Citra dapat dibedakan menjadi dua, yaitu citra analog dan citra digital. Citra analog adalah citra yang terbentuk dari sinyal kontinu dan dihasilkan dari alat akuisisi citra analog, Nilai intensitas cahaya pada citra analog terletak pada interval  $[0, \infty)$ . Contoh citra analog adalah seperti gambar pada televisi, foto sinar X, foto CT scan, foto hasil kamera analog.

Sedangkan citra digital adalah citra yang terbentuk dari sinyal diskrit. Citra digital dapat diproses/dimanipulasi menggunakan komputer. Dalam komputer, citra digital diproses berdasarkan nilai intensitas cahayanya atau disebut juga sebagai piksel (picture element/pixel). Piksel ini memiliki koordinat (x,y) dan amplitudo f(x,y). Koordinat (x,y) menunjukkan letak/posisi piksel dalam suatu citra, sedangkan amplitudo f(x,y) menunjukkan nilai intensitas warna citra.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Gambar 1 Tabel Pemetaan *Vigenere Cipher*

### B. *Vigenere Cipher*

*Vigenere Cipher* adalah modifikasi dari *caesar cipher*, dari yang awalnya *caesar cipher* adalah metode kriptografi substitusi abjad-tunggal, kemudian dimodifikasi menjadi metode kriptografi substitusi abjad-majemuk. Proses enkripsi *Vigenere cipher* menggunakan tabel *Vigenere* terdapat pada Gambar 1. Plainteks diubah menjadi abjad lainnya dengan menggeser sesuai dengan nilai numerik kunci, yaitu A = 0, B = 1, C = 2, ..., Z = 25. Jika panjang kunci lebih pendek dari panjang plainteks, maka kunci digandakan hingga panjangnya sama dengan plainteks [9].

Algoritma ini akan meminimalkan kemungkinan dipecahkannya cipherteks jika satu huruf plainteks diketahui. Model matematika dari enkripsi pada algoritma *Vigenere cipher* ini adalah seperti berikut:

$$C_i = E_k(M_i) = (M_i + K_i) \bmod 26$$

Dan model matematika untuk deskripsinya adalah:  $M_i = D_k(C_i) = (C_i - K_i) \bmod 26$

$$C_i = E_k(M_i) = (M_i + K_i) \bmod 26$$

Dan model matematika untuk deskripsinya adalah:

$$M_i = D_k(C_i) = (C_i - K_i) \bmod 26$$

Dengan C memodelkan cipherteks, M memodelkan Plainteks, dan K memodelkan kunci. Contoh dari penerapan algoritma *Vigenere cipher* adalah jika kita memiliki sebuah plainteks yang ingin dienkrpsi: UNIVERSITAS IVET Dan kita menggunakan kunci: RAHASIA Maka plainteks akan dienkrpsi dengan cara:

Plaintext: UNIVERSITAS IVET

Kunci : RAHASIARAHASIA

Ciphertext : KNPVWZSZTHSRQVVT

### III. METODOLOGI PENELITIAN

Penelitian ini mempunyai lima tahap penelitian ditunjukkan pada Gambar 2 yaitu:

#### A. Tahap Pra-proses

Untuk melakukan tahap pra proses, citra masukan yang digunakan berupa citra RGB tersimpan dalam format tif. Kemudian determinasi poin *macula*, dapat mengklik area *macula* yang merupakan area gelap selanjutnya

ekstraksi *green channel* kemudian ubah ke *grayscale*, kemudian di *enhancement* yang terdiri dari dua metode *top hat* dan *contrast stretching*.

#### B. Tahap Ekstraksi Blood Vessels

Pada tahap ini dilakukan proses ekstraksi *blood vessels* dimulai dengan input citra masukan dari *enhancement* di proses menuju *thresholding* dan *masking*. Kemudian di segmentasi menggunakan *matched filter*. Langkah selanjutnya *Cropping ROI* di *macula*. Teknik *cropping* digunakan dengan menentukan titik pusat (x,y) pada *macula*. Tahap selanjutnya adalah *thinning* merupakan tahap penipisan *blood vessels*.

#### C. Tahap Deteksi FAZ

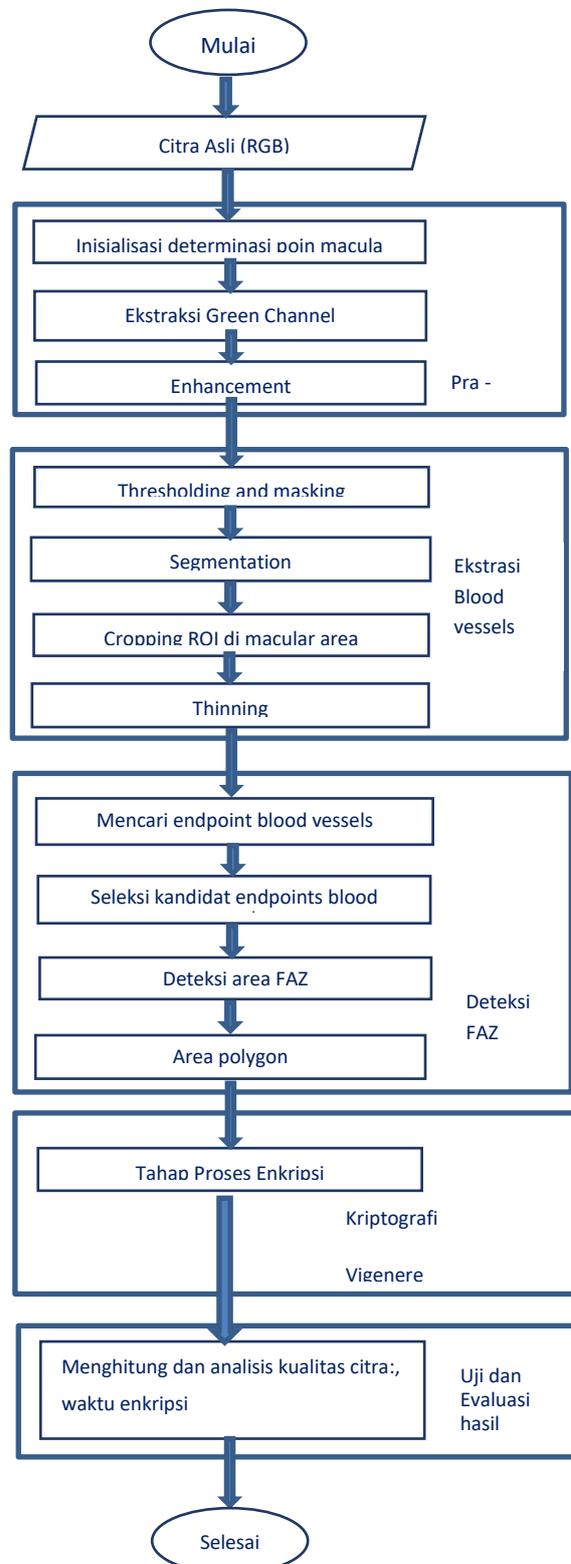
Tahap deteksi FAZ digunakan untuk mengetahui luas area yang didapat. Citra hasil *thinning blood vessels* diolah. Selanjutnya deteksi FAZ dengan metode titik ujung kapiler dimulai dengan mencari *endpoint blood vessels*. Didapatkan banyak *endpoint blood vessels* di area makula, kemudian area FAZ dideteksi menghasilkan area FAZ dalam satuan pixel

#### D. Tahap Kriptografi Vigenere Cipher

Tahap ini terdiri dari dua tahap adalah enkripsi dan tahap deskripsi. Penelitian menggunakan tahap enkripsi. Tahap ini memasukan input citra hasil FAZ sebagai plain citra kemudian masukkan kunci berbentuk teks dengan panjang karakter 256. Dengan metode *vigenere cipher* citra FAZ diubah menjadi citra yang tidak bisa dibaca (*ciph*)

#### E. Tahap Uji dan Evaluasi

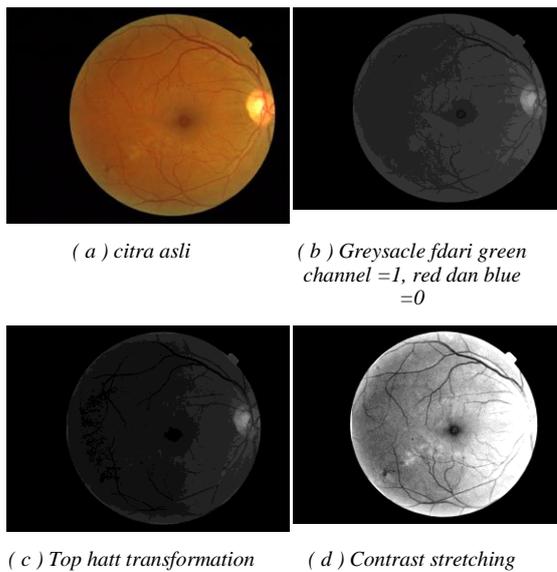
Menghitung waktu enkripsi



Gambar 2 Tahapan Peneliti

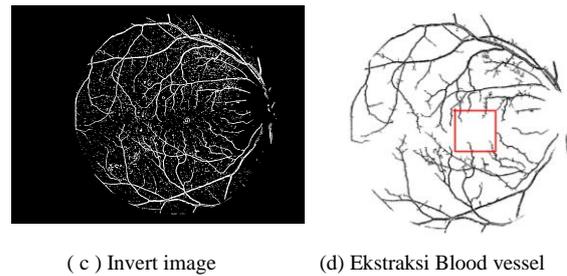
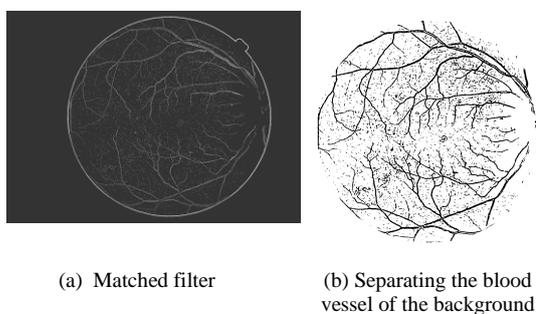
#### IV. HASIL DAN PEMBAHASAN

Penelitian ini menggunakan database MESSIDOR citra fundus retina dengan citra berbentuk format TIF yang mempunyai 4 grade yaitu grade 0,1,2 dan 3. Peneliti menggunakan citra fundus retina berjumlah 15. Gambar 3 menunjukkan deteksi FAZ melalui proses *enhancement*.



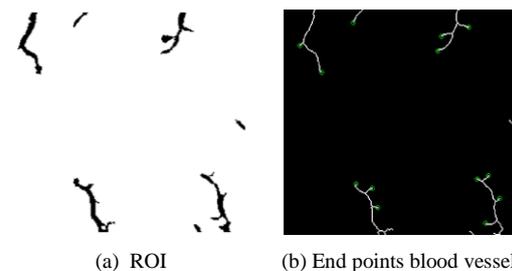
Gambar 3 Hasil dari enhancement

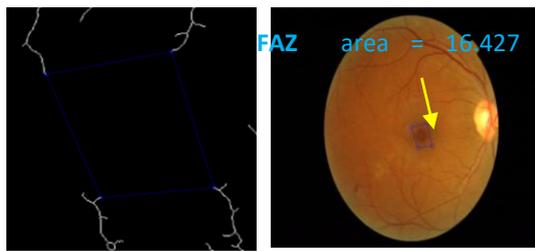
Pada Gambar 3 menunjukkan bahwa grayscale yang didapat dari greenchannel karena komponen greenchannel paling bagus diantara komponen red dan komponen blue. Sedangkan pada Gambar 4 menunjukkan hasil dari ekstraksi blood vessels.



Gambar 4 Hasil ekstraksi pembuluh darah (blood vessels)

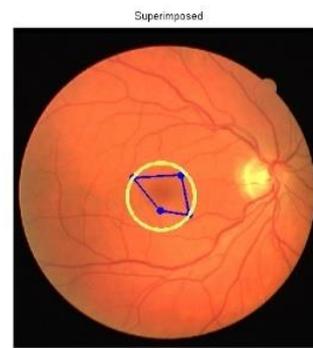
Hasil segmentasi di tengah FAZ terdeteksi pembuluh darah kecil. Seharusnya di tengah FAZ adalah daerah tanpa pembuluh darah. Gambar 4 (a) menunjukkan hasil gambar *matched filter*. Sedangkan Gambar 4 (b) menunjukkan proses awal ekstraksi pembuluh darah setelah *matched filter*. Gambar 4 (c) Hal ini diikuti dengan membalikkan citra. Tujuan dari inversi citra adalah memberikan keluaran yang menghasilkan pembalikan dari citra masukan. Jika citra biner adalah 1 maka outputnya akan menjadi 0, sebaliknya nilai inputnya adalah 0 akan menghasilkan output bernilai 1. Pada gambar terlihat masih banyak noise berupa pembuluh darah kecil yang masuk. Gambar 4 (d) menunjukkan hasil setelah proses ekstraksi dan area FAZ pembuluh darahnya yang ditandai dengan ROI. Gambar ekstraksi pembuluh darah terlihat bagus, tidak ada noise dan pembuluh darah kecil. Gambar 5 menunjukkan hasil deteksi FAZ.



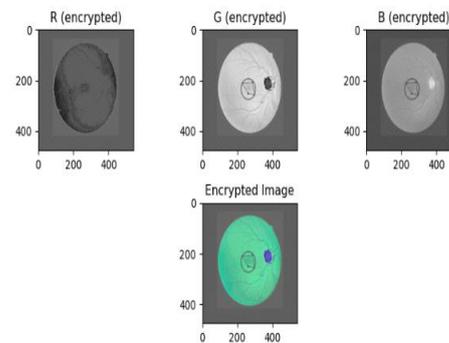


(c) Deteksi FAZ (d) Ekstraksi FAZ

Gambar 5 Hasil dari deteksi FAZ



(a) citra asli



(b) Citra enkripsi

Gambar 6 Citra hasil dari enkripsi

Deteksi FAZ harus melewati tahap ekstraksi b. Karena FAZ mencari dari titik akhir penentuan pembuluh darah. Pemilihan titik akhir pembuluh darah diambil dari masing-masing kuadran. Ada empat kuadran. Kuadran pertama, Kuadran kedua, Kuadran ketiga, dan Kuadran empat. Setelah terpilih calon titik akhir pembuluh darah maka titik akhir pembuluh darah dihubungkan. Setelah selesai citra di *superimposed*. Tampak bahwa hasil plot citra *superimposed* dengan benar karena FAZ terletak di area makula. Setelah luas dihitung. Semakin besar derajat *Diabetic Retinopathy* maka derajatnya semakin buruk. Karena FAZ dikenal di daerah tersebut. Titik akhir pembuluh darah diambil dari area yang dekat dengan titik pusat FAZ. Setelah itu hasil *superimposed* FAZ dijadikan citra masukan untuk kriptografi dengan *Vigenere cipher*.

Citra hasil dari proses enkripsi dapat ditunjukkan pada Gambar 6. Hasil tersebut didapatkan dari mengubah citra *superimposed* FAZ yang berbentuk *polygon* menurut peneliti dan berbentuk lingkaran menurut *ophthamology*. Area FAZ lebih kecil dibandingkan dari citra FAZ menurut *ophthamology*.

Citra FAZ sebagai input di kriptografi *vigenere cipher* merupakan citra yang dapat dibaca yang merupakan citra plain kemudian diubah menjadi citra cipher. Pada Gambar 6 menunjukkan bahwa citra enkripsi terdiri dari 3 channel red green dan blue. Pada *green channel* terlihat gambar lebih terang hal ini disebabkan karena waktu proses deteksi FAZ yang digunakan adalah komponen *greenchannel*. Citra enkripsi terlihat bahwa hasilnya berbeda dengan citra asli.

Pada penelitian ini dilakukan dengan mengujikan 15 citra FAZ. Pengujian ini digunakan untuk mengetahui waktu enkripsi dari masing masing citra dengan memasukkan kunci teks INDONESIA JAYA. Pada Tabel 1 menunjukkan waktu enkripsi citra FAZ. Enkripsi

ini digunakan untuk mengamankan data citra medis yang rentan terhadap pencurian data.

Tabel 1. Tabel Waktu enkripsi citra FAZ Grade 0

No.	Tabel Waktu Enkripsi FAZ		
	Image	Waktu Enkripsi (detik)	Luas area (pixel)
1	Image 1. tif	4.05	3747
2	Image 2. tif	4,67	4133
3	Image 3.tif	4.65	2743
4	Image 4. tif	6,59	6579
5	Image 5. tif	4.7	4572
6	Image 6. tif	5.2	5070
7	Image 7. tif	4,8	5515
8	Image 8. tif	5.02	5672
9	Image 9. tif	5.04	3421
10	Image 10. tif	5.49	4332
11	Image 11. tif	5.347	4474
12	Image 12. tif	4.85	4902
13	Image 13. tif	4.57	5151
14	Image 14. tif	5.06	5340
15	Image 15. tif	4.49	3738

Pada Tabel 1 menunjukkan bahwa waktu rata-rata enkripsi dalam pengujian 15 citra FAZ adalah 4.96 detik. Pada Image 4.tif luas area FAZ paling besar maka waktu komputasi enkripsi juga semakin lama dapat dilihat untuk waktu enkripsi hampir sebanding dengan ukuran citra asli dari database Messidor

## V. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan peneliti maka dapat ditarik kesimpulan bahwa enkripsi adalah mengubah plainimage (citra yang dapat dibaca menjadi cipher image (citra yang tidak dapat dibaca). Waktu enkripsi untuk penelitian ini adalah 4,96 detik. Semakin luas area maka waktu enkripsi juga semakin lama.

## REFERENSI

- [1] C. V. Noble J, "Diabetic retinopathy," *CMAJ*, vol. 182, no. 15, p. 1646, 2010.
- [2] D. S. Fong *et al.*, "Retinopathy in Diabetes," *Diabetes Care*, vol. 27, 2004, doi: 10.2337/diacare.27.2007.S84.
- [3] J. W. Y. Yau *et al.*, "Global prevalence and major risk factors of diabetic retinopathy," *Diabetes Care*, vol. 35, pp. 556–564, 2012, doi: 10.2337/dc11-1909.
- [4] M. H. Ahmad Fadzil, L. I. Izhar, H. Nugroho, and H. A. Nugroho, "Analysis of retinal fundus images for grading of diabetic retinopathy severity," *Med. Biol. Eng. Comput.*, vol. 49, pp. 693–700, 2011, doi: 10.1007/s11517-011-0734-2.
- [5] A. Ampera, "Tanggung jawab rumah sakit terhadap pasien dalam pelaksanaan pelayanan ke," *J. Al-Ishlah*, vol. 19, no. 2, pp. 197–212, 2017.
- [6] D. Purnamasari, A. K. Dewi, and A. N. Trisetiyanto, "Analisis Performansi Kriptografi Berbasis Caesar Cipher Untuk Keamanan Data Menggunakan Python Pada Tembang Macapat," vol. 1, no. 2, pp. 50–54, 2022.
- [7] D. Purnamasari and H. Prasetyani, "Analisis Performansi Kriptografi Berbasis Algoritma Caesar Cipher dan Rail Fence Cipher pada Tembang Macapat," pp. 1–8.
- [8] D. Purnamasari, "Implementasi Algoritma Kriptografi Caesar Cipher dan Rail Fence Cipher untuk Keamanan Data Teks Menggunakan Python," *E-Journal.Ivet.Ac.Id*, vol. 4, pp. 1–7, 2021, [Online]. Available: <http://e-journal.ivet.ac.id/index.php/jiptika/article/view/1697>
- [9] D. Medis and S. Jari, "IMPLEMENTASI VIGENERE CIPHER PADA Pendahuluan Citra

- Digital,” vol. 02, no. 01, pp. 23–30, 2018.
- [10] H. A. Nugroho, D. Purnamasari, I. Soesanti, W. KZ, and D. Dharmawan, *Detection of foveal avascular zone in colour retinal fundus images*. 2015. doi: 10.1109/ICSITech.2015.7407808.
- [11] H. Adi Nugroho, D. Purnamasari, I. Soesanti, W. K. Z. Oktoeberza, and D. Arief Dharmawan, “Segmentation of foveal avascular zone in colour fundus images based on retinal capillary endpoints detection,” *J. Telecommun. Electron. Comput. Eng.*, vol. 9, no. 3–8, pp. 107–112, 2017.