



IMPLEMENTASI VIGENERE CIPHER PADA PENGAMANAN DATA MEDIS

ABDUH RISKI¹, AHMAD KAMSYAKAWUNI, DAN M. ZIAUL ARIF

¹Jurusan Matematika FMIPA Universitas Jember, riski.fmipa@unej.ac.id

Abstrak

Fokus dari penelitian ini adalah melakukan pengamanan data medis berupa citra menggunakan teknik kriptografi vigenere cipher. Data medis berupa rekam medis adalah sesuatu yang harus dijaga kerahasiaannya. Kemudian, di era yang serba digital, sangat dibutuhkan suatu metode penyimpanan citra rekam medis yang bersifat digital agar terjaga kerahasiaannya. Vigenere cipher adalah metode kriptografi klasik substitusi abjad-majemuk. Biasanya vigenere cipher digunakan untuk mengenkripsi pesan berbasis teks. Pada penelitian ini vigenere digunakan untuk menyandikan citra dan kunci yang digunakan juga berupa citra. Langkah pertama, citra asli dan citra kunci ditransformasi menjadi matriks piksel dengan kedalaman 8 bit. Kemudian langkah selanjutnya dilakukan enkripsi menggunakan vigenere cipher. Hasil penelitian menunjukkan metode yang diusulkan dapat digunakan untuk mengamankan citra data medis. Diperoleh NPCR sebesar 100% dengan rata-rata UACI 20% untuk citra RGB dan 43% untuk citra biner.

Kata kunci: Vigenere, Citra, Data Medis, Sidik Jari, UACI

1 Pendahuluan

Keamanan data adalah sesuatu yang perlu dilakukan untuk memastikan data tidak diakses dan digunakan oleh yang tidak berhak. Di era *big data* dan *internet of things*, pengamanan data menjadi semakin diperlukan, terlebih lagi untuk pengamanan data digital. Salah satu area yang memerlukan pengamanan data adalah dunia kesehatan, khususnya untuk pengamanan data rekam 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 [1].

Salah satu metode pengamanan data dikenal dengan kriptografi. Kriptografi adalah teknik untuk menyembunyikan isi data atau pesan sehingga tidak dapat lagi dimengerti atau dibaca. Algoritma kriptografi vigenere [2] 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. Meskipun metode vigenere sederhana dan termasuk dalam kriptografi klasik, tetapi vigenere cipher masih layak untuk digunakan. Salah satunya adalah penerapan vigenere cipher pada pengamanan data rekam medis pasien seperti pada [3]. 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 juga dapat digunakan untuk mengenkripsi data citra digital. Pada [4], dilakukan enkripsi citra dengan kunci berupa teks menggunakan vigenere cipher.

Pada penelitian ini vigenere cipher akan digunakan untuk mengenkripsi data medis berupa citra hispatologi pasien penderita kanker payudara, dengan menggunakan kunci yang juga berupa citra yaitu citra sidik jari.

2 Data dan Metode Penelitian

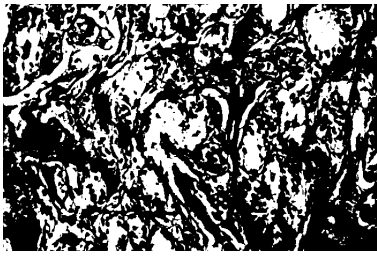
Penelitian ini menggunakan metode penelitian studi simulasi untuk mengukur tingkat keberhasilan metode yang diusulkan. Data yang digunakan dalam simulasi adalah data citra asli berupa 10 citra hispatologi pasien penderita kanker payudara yang diperoleh dari [5]. Pada penelitian ini juga digunakan data sekunder dari [6] yaitu 10 citra kunci berupa citra sidik jari.

Tahapan-tahapan penelitian yang dilakukan adalah pembuatan perangkat lunak implementasi vigenere cipher pada penyandian citra hispatologi menggunakan kunci citra sidik jari. Kemudian dilakukan simulasi penyandian terhadap data-data yang ada, dan menguji hasilnya menggunakan NPCR dan UACI. Simulasi juga dilakukan dengan membandingkan metode yang diusulkan dengan metode pada [4]. Selanjutnya, metode enkripsi vigenere yang diusulkan disebut dengan vigenere baru dan metode enkripsi vigenere pada [4] disebut dengan vigenere lama.

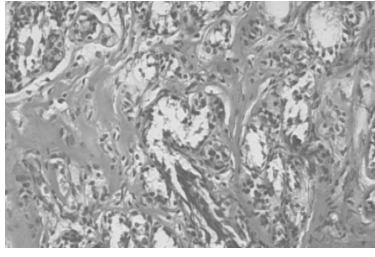
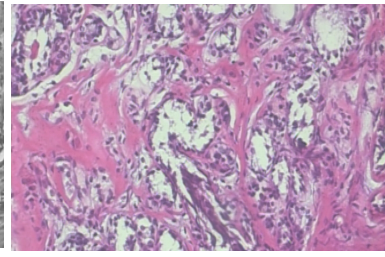
3 Citra Digital

Citra adalah representasi 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. 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*). Nilai piksel citra digital tergantung pada kedalaman bit penyusunnya. Citra dengan kedalaman 8 bit memiliki nilai piksel $I(x, y) = 0, 1, 2, 3, \dots, 255$, yaitu sebanyak $2^8 = 256$ piksel. Dimana $I(x, y)$ adalah nilai piksel pada baris ke- x dan kolom ke- y , $x = 1, 2, 3, \dots, m$, $y = 1, 2, 3, \dots, n$. Pada penelitian ini hanya digunakan citra digital, sehingga selanjutnya citra digital hanya disebutkan dengan citra.

Berdasarkan warna penyusunnya, citra dapat dibagi menjadi tiga jenis, yaitu citra biner, citra *grayscale*, dan citra RGB (*red, green, blue*). Citra biner seperti pada Gambar 1, merupakan citra dengan kedalaman 1 bit. Nilai $I(x, y)$ hanya sama dengan 0 (hitam) atau 1 (putih). Gambar 2 merupakan citra *grayscale* 8 bit. Warna abu-abu pada citra tersebut berkisar dari 0 hingga 255, $I(x, y) = 0, 1, 2, \dots, 255$. Sedangkan citra RGB (Gambar 3) adalah citra yang tersusun dari 3 warna dasar yaitu, merah, hijau dan biru. Sehingga citra RGB terdiri dari tiga kanal yaitu kanal warna merah, kanal warna hijau dan kanal warna biru. Nilai piksel citra RGB adalah $I(x, y, z) = 0, 1, 2, \dots, 255$, dimana z adalah posisi dari kanal, $z = 1, 2, \dots, o$, dengan $o = 3$ untuk citra RGB sedangkan $o = 1$ untuk citra biner dan *grayscale*.



Gambar 1: Citra Biner

Gambar 2: Citra *Grayscale*

Gambar 3: Citra RGB

4 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 seperti pada Gambar 4. Plainteks dirubah menjadi abjad lainnya dengan menggeser sesuai dengan nilai numerik kunci, yaitu $A = 0, B = 1, C = 2, \dots, Z = 25$. Jika panjang kunci lebih pendek dari panjang plaintexts, maka kunci digandakan hingga panjangnya sama dengan plaintexts, [2], [3], [4].

		Plainteks																									
		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
Kunci	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 4: Tabel Vigenere

Misal plaintexts atau pesan yang akan disandikan adalah PESANRAHASIA dan kuncinya adalah APEL. Hasil enkripsinya seperti berikut ini.

Teks Asli	P	E	S	A	N	R	A	H	A	S	I	A
Kunci	A	P	E	L	A	P	E	L	A	P	E	L
Teks Cipher	P	T	W	L	N	G	E	S	A	H	M	L

Cipher yang diperoleh adalah PTWLN GESAHML. Proses enkripsi vigenere klasik dapat dituliskan dengan Persamaan 1, sedangkan proses dekripsinya dengan Persamaan 2.

$$c_i = (p_i + k_i) \mod 26 \quad (1)$$

$$p_i = (c_i - k_i) \mod 26 \quad (2)$$

Pada penelitian ini, data yang akan dienkripsi adalah citra dan kunci juga berupa citra. Warna dari masing-masing citra dirubah menjadi nilai piksel dengan kedalaman 8 bit. Kemudian masing-masing matriks piksel ditransformasi menjadi vektor piksel dengan panjang $m \times n$. Jika panjang

vektor kunci lebih pendek dari panjang vektor citra asli, maka vektor kunci digandakan sehingga panjang keduanya sama. Formula enkripsi dan dekripsinya adalah

$$I_i^c = (I_i^p + I_i^k) \mod 256$$

$$I_i^p = (I_i^c - I_i^k) \mod 256$$

dimana $i = 1, 2, \dots, m \times n$ adalah panjang vektor. Untuk menghindari sebuah piksel dienkripsi menjadi piksel yang sama, pada saat nilai $I_i^k = 0$, maka diganti menjadi $I_i^k = 1$.

5 NPCR dan UACI

Number of changing pixel rate (NPCR) dan *unified averaged changed intensity* (UACI) adalah formula untuk melakukan analisis diferensial dari dua buah citra. NPCR digunakan untuk mengetahui berapa banyak piksel yang berbeda dari dua buah citra. Sedangkan UACI untuk mengetahui seberapa besar interval perbedaan nilai piksel dari kedua citra [7]. Misal I dan I' adalah dua citra yang berbeda, sehingga formula NPCR dan UACI dapat dinyatakan sebagai berikut.

$$D(x, y, z) = \begin{cases} 0 & \text{jika } I(x, y, z) = I'(x, y, z) \\ 1 & \text{jika } I(x, y, z) \neq I'(x, y, z) \end{cases}$$

$$\text{NPCR} = \sum_{x,y,z}^{m,n,o} \frac{D(x,y,z)}{m \times n \times o} \times 100\%$$

$$\text{UACI} = \sum_{x,y,z}^{m,n,o} \frac{|I(x,y,z) - I'(x,y,z)|}{255 \times m \times n \times o} \times 100\%$$

Citra cipher dikatakan baik atau aman jika nilai NPCR nya dan UACI nya minimal 49.9% untuk citra biner. Sedangkan untuk citra *grayscale* atau RGB, batas bawah nilai NPCR=99.6% dan UACI=33.4% untuk dapat dikatakan citra cipher yang dihasilkan adalah baik [7]. Secara visual, citra cipher yang baik adalah yang sangat "berbeda" dengan citra aslinya. Sehingga citra asli tidak dapat langsung dikenali dengan mudah secara visual dari citra cipher.

6 Hasil dan Pembahasan

Simulasi dilakukan dengan mengenkripsi 10 citra asli menggunakan 10 citra kunci. Citra asli adalah citra data rekam medis berupa citra hispatologi pasien penderita kanker payudara dari 10 pasien berbeda, sedangkan citra kunci adalah citra sidik jari tangan kanan dan kiri dari 5 orang berbeda. Citra cipher hasil enkripsi mempunyai nilai NPCR 100% untuk keseluruhan citra. Artinya setiap nilai piksel citra cipher tidak sama dengan nilai piksel citra asli. Hal ini karena kunci yang digunakan tidak memuat kunci 0, karena ketika nilai piksel citra kunci 0 diganti dengan 1. Sedangkan nilai UACI dari citra cipher dan citra asli seperti pada Tabel 1.

Rata-rata nilai UACI pada Tabel 1 adalah sekitar 20%. Tentu nilai tersebut berada di bawah ambang batas bawah UACI agar citra cipher dikatakan aman. Hal tersebut terjadi karena penggunaan citra kunci yang berupa citra sidik jari. Pada gambar 5, dapat dilihat bahwa pada citra sidik jari didominasi oleh warna hitam dan putih, sedangkan hanya sebagian kecil citra terdiri dari warna abu-abu. Hal ini menyebabkan nilai piksel citra kunci terdiri dari banyak nilai 0 dan 255. Sebanyak 14% nilai piksel citra sidik jari sama dengan 0 dan 255. Ketika kunci bernilai 0, piksel citra image tidak digeser sehingga hasil enkripsinya tidak berubah. Oleh karena itu pada metode vigenere baru kunci 0 diganti dengan 1. Sehingga nilai piksel hasil enkripsinya berbeda dengan nilai piksel

Tabel 1: Nilai UACI Vigenere Baru

Citra Kunci	Citra Asli									
	1	2	3	4	5	6	7	8	9	10
1	18.47	25.54	24.70	19.42	24.22	20.83	28.83	16.31	21.63	22.90
2	18.57	22.51	22.09	19.63	21.59	20.14	24.58	16.59	20.35	20.92
3	18.62	23.57	23.00	19.75	22.43	20.54	26.00	16.55	20.80	21.58
4	15.96	22.83	22.12	16.53	22.13	17.76	27.69	14.17	19.24	21.15
5	16.80	22.56	21.87	17.38	21.58	18.69	25.82	14.94	19.38	20.62
6	16.57	20.19	19.70	17.10	19.57	17.72	23.02	14.91	18.39	19.13
7	20.64	24.13	23.76	21.61	23.13	22.00	26.32	18.34	22.30	22.81
8	14.54	17.18	16.89	14.77	16.75	15.45	19.09	13.14	15.85	16.32
9	15.96	19.76	19.32	16.51	19.35	17.06	22.88	14.36	17.83	18.82
10	13.92	19.26	18.69	14.34	19.25	15.09	24.82	12.42	16.72	18.64



Gambar 5: Citra Kunci

citra asli, yaitu mengalami pergeseran ke kanan sebanyak 1. Sedangkan ketika kunci bernilai 255, maka proses enkripsi dilakukan dengan menggeser nilai piksel citra asli ke kiri sebanyak 1. Karena $255 \cong -1 \pmod{256}$.

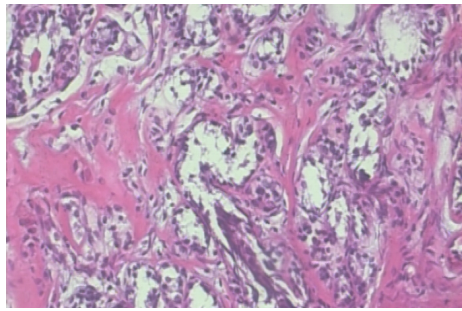
Simulasi juga dilakukan dengan melakukan enkripsi menggunakan metode dan kunci seperti pada [4]. NPCR yang dihasilkan dari metode vigenere lama juga 100%. Sedangkan UACI dari vigenere lama adalah seperti pada Tabel 2.

Tabel 2: Nilai UACI Vigenere Lama

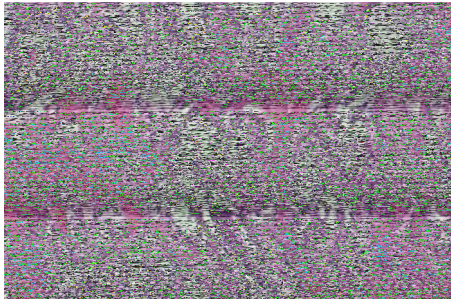
Citra Asli									
1	2	3	4	5	6	7	8	9	10
38.78	54.86	53.24	47.43	48.87	49.37	56.00	33.74	45.48	44.10

Nilai UACI dari citra cipher yang dihasilkan vigenere lama lebih tinggi dari UACI vigenere baru, serta nilai UACI vigenere lama berada di atas ambang batas bawah nilai UACI. Secara Uji numerik, metode vigenere lama lebih baik dari pada metode vigenere baru. Tetapi jika dilihat secara visual pada citra cipher yang dihasilkan, pola citra asli terlihat jelas pada citra cipher vigenere lama. Gambar 7 merupakan citra cipher hasil metode vigenere baru. Sedangkan Gambar 8 adalah citra cipher hasil metode vigenere lama seperti pada [4]. Warna pada Gambar 7 tidak jauh berbeda jika dibandingkan dengan citra asli pada Gambar 6, sesuai dengan nilai UACI-nya yang tidak terlalu besar. Sedangkan citra cipher vigenere lama memiliki warna yang jauh berbeda dibandingkan dengan warna pada citra asli. Tetapi pola citra asli (Gambar 6) terlihat jelas pada citra cipher vigenere lama (Gambar 8). Hasilnya tidak sama dengan UACI yang dihasilkan, UACI vigenere lama lebih besar dari UACI vigenere baru. Tetapi citra cipher vigenere baru lebih baik dari pada citra cipher vigenere lama karena pola citra asli tidak lagi terlihat jelas pada citra cipher vigenere baru. Tidak berkorelasinya UACI dengan tampilan visual karena memang belum ada formula yang dapat menggantikan penilaian "mata manusia".

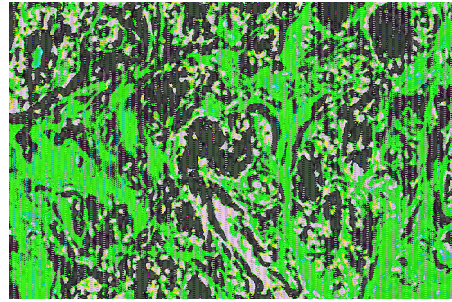
Untuk dapat menguji bahwa pola citra asli terlihat jelas pada citra cipher vigenere lama



Gambar 6: Citra Asli

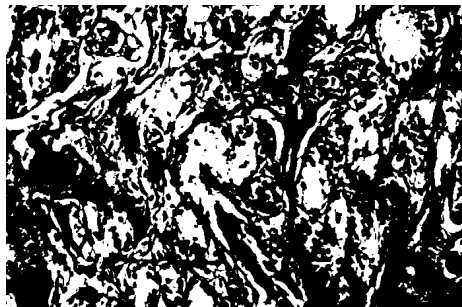


Gambar 7: Citra Cipher Vigenere Baru

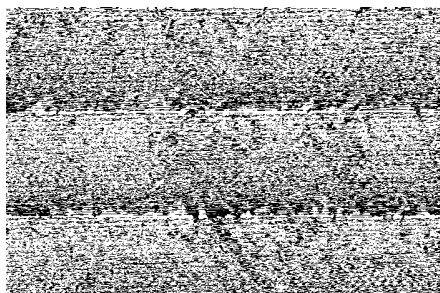


Gambar 8: Citra Cipher Vigenere Lama

dibandingkan pada citra cipher vigenere baru, ketiga citra RGB tersebut ditransformasi menjadi citra biner (hitam-putih). Gambar 9 adalah citra biner dari citra asli, Gambar 10 adalah citra biner dari citra cipher vigenere baru, dan Gambar 11 adalah citra biner dari citra cipher vigenere lama. Kemudian dihitung UACI kesepuluh citra cipher biner dari kedua metode, dimana untuk metode vigenere baru hanya digunakan citra kunci pertama. Nilai UACI yang diperoleh ditampilkan pada Tabel 3.



Gambar 9: Citra Asli Biner



Gambar 10: Citra Cipher Biner Vigenere Baru



Gambar 11: Citra Cipher Biner Vigenere Lama

Tabel 3 menunjukkan bahwa UACI metode vigenere cipher yang diusulkan jauh lebih besar daripada UACI dari metode vigenere pada [4]. Hal ini terjadi karena pola citra asli terlihat jelas pada citra cipher vigenere lama, Gambar 9 mirip dengan Gambar 11. Sedangkan pada Gambar 10 sudah tidak lagi terlihat pola citra asli.

Tabel 3: Nilai UACI Citra Biner

Vigenere Cipher	Citra Asli									
	1	2	3	4	5	6	7	8	9	10
Baru	49.08	46.70	44.34	39.76	38.13	46.80	38.18	37.30	44.19	42.68
Lama	11.73	33.89	29.07	19.76	13.06	35.43	31.93	21.48	20.22	16.87

Kunci yang digunakan dalam metode yang diusulkan masih bersifat simetris. Yaitu kunci untuk mengenkripsi dan mendekripsi menggunakan citra sidik jari yang sama. Karena ekstraksi ciri citra sidik jari hanya dengan menggunakan nilai piksel warnanya. Sehingga perubahan sedikit saja pada gambar tentu menghasilkan nilai piksel yang berbeda. Sehingga untuk menjadi proses dekripsi juga diperoleh citra asli yang sama persis, maka digunakan citra sidik jari yang sama sebagai kunci pada proses enkripsi dan dekripsi.

7 Kesimpulan

Hasil penelitian ini, metode vigenere cipher yang diusulkan dapat digunakan untuk pengamanan data medis berupa citra. Berdasarkan pada Tabel 3, metode vigenere yang diusulkan lebih baik dari metode vigenere lainnya dalam pengamanan citra. Selanjutnya metode vigenere yang diusulkan dapat digunakan oleh siapa saja untuk pengamanan data medis berupa citra.

Pada penelitian selanjutnya akan dilakukan peningkatan keamanan data yang dienkripsi dengan menggunakan metode lain dalam mengekstraksi ciri citra kunci sedemikian hingga menghasilkan nilai UACI yang lebih baik dan kunci menjadi non-simetris.

Referensi

- [1] A. Ampera, "Tanggung jawab rumah sakit terhadap pasien dalam pelaksanaan pelayanan kesehatan," *Jurnal Al-Ishlah*, vol. 19, no. 2, pp. 197–212, 2017.
- [2] A. A. Bruen and M. A. Forcinito, *Cryptography, Information Theory, and Error-Correction*. John Wiley & Sons, Inc., 2004.
- [3] E. Gunadhi and A. Sudrajat, "Pengamanan data rekam medis pasien menggunakan kriptografi vigenere cipher," *Jurnal Algoritma*, vol. 13, no. 1, 2016.
- [4] Y. A. Gerhana, E. Insanudin, U. Syarifudin, and M. R. Zulmi, "Design of digital image application using vigenere cipher algorithm," in *2016 4th International Conference on Cyber and IT Service Management*, IEEE, Apr. 2016.
- [5] F. A. Spanhol, L. S. Oliveira, C. Petitjean, and L. Heutte, "A dataset for breast cancer histopathological image classification," *IEEE Transactions on Biomedical Engineering*, vol. 63, no. 7, pp. 1455–1462, 2016.
- [6] C. A. of Sciences Institute of Automation (CASIA), "Casia-fingerprintv5." <http://biometrics.idealtest.org/>.

- [7] Y. Wu, J. P. Noonan, and S. Aghaian, "Npcr and uaci randomness tests for image encryption," in *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT)*, pp. 31–38, 2011.