Vol. 5, No. 3, Desember 2024, hal. 804-813

Jurnal Computer Science and Information Technology (CoSciTech)

p-ISSN: 2723-567X
e-ISSN: 2723-5661

http://ejurnal.umri.ac.id/index.php/coscitech/index

Perbandingan Algoritma SIMON dan SPECK Dalam Pengamanan Citra Digital

Yulia Fatma*[1], Soni, Mikdad Amseno[2]
Email: [1]yuliafatma@umri.ac.id, [2]soni@umri.ac.id, [3]180401046@student.umri.ac.id

[123]Teknik Informatika, Ilmu Komputer, Universitas Muhammadiyah Riau

Diterima: 6 Agustus 2024 | Direvisi: - | Disetujui: 6 Agustus 2024

Abstrak

Kriptografi merupakan teknik pengamanan data dengan melakukan proses penyandian terhadap data yang ingin dirahasiakan sehingga makna asli dari data tidak lagi dapat dimengerti. SIMON dan SPECK merupakan algoritma kriptogragi modern yang dikeluarkan oleh National Security Agency(NSA). SIMON dan SPECK digadang merupakan algoritma yang terkenal karena efisiensinya dan keamanan yang kuat. Penelitian ini akan membandingkan kinerja algoritma SIMON dan SPECK dalam mengamankan citra digital. Perbandingan dilakukan melalui pengujian kinerja waktu, perubahan ukuran file, dan tingkat keacakan file citra menggunakan metric Unified Average Changing Intensity(UACI) dan Number of Pixels Change Rate(NPCR). Hasil penelitian menunjukkan bahwa rata-rata waktu enkripsi dan dekripsi yang dibutuhkan algoritma SIMON lebih besar jika dibandingan dengan algoritma SPECK. Ukuran file citra yang dihasilkan dari enkripsi menggunakan algoritma SIMON dan SPECK sama-sama megalami peningkatan sebesar 24% dari citra aslinya. Tingkat keacakan citra yang dihasilkan berdasarkan nilai UACI yang diperoleh menggunakan algoritma SIMON didapatkan rata-rata sebesar 19,65%, sedangkan nilai UACI yang diperoleh menggunakan algoritma SPECK rata-rata sebesar 20,94%. Hal ini menunjukkan terjadi perubahan intensitas yang signifikan antara citra asli dan citra hasil enkripsi. Namun tidak semua piksel dalam citra terenkripsi berubah jika dibandingkan dengan citra asli, hal ini ditunjukkan dari nilai NPCR yang diperoleh dari citra hasil enkripsi algoritma SIMON dan SPECK didapatkan rata-rata hasil sebesar 49,98% dan 50,17%.

Kata kunci: *kriptografi, simon, speck, UACI, NPCR*

Comparison of SIMON and SPECK Lightweight Algorithm in Digital Image Security

Abstract

Cryptography is a data security technique by encoding data that is to be kept secret so that the original meaning of the data can no longer be understood. SIMON and SPECK are modern cryptographic algorithms issued by the National Security Agency (NSA). SIMON and SPECK are said to be algorithms that are known for their efficiency and strong security. This research will compare the performance of the SIMON and SPECK algorithms in securing digital images. Comparisons were made by testing time performance, changes in file size, and the level of randomness of image files using the Unified Average Changing Intensity (UACI) and Number of Pixels Change Rate (NPCR) metrics. The research results show that the average encryption and decryption time required by the SIMON algorithm is greater when compared to the SPECK algorithm. The image file size resulting from encryption using the SIMON and SPECK algorithms both increased by 24% from the original image. The level of randomness of the resulting image based on the UACI value obtained using the SIMON algorithm was found to be an average of 19.65%, while the UACI value obtained using the SPECK algorithm was an average of 20.94%. This shows that there is a significant change in intensity between the original image and the encrypted image. However, not all pixels in the encrypted image change when compared to the original image, this is shown by the NPCR value obtained from the SIMON and SPECK algorithm encrypted image, with average results of 49.98% and 50.17%.

Keywords: *cryptography, simon, speck, UACI, NPCR*

1. PENDAHULUAN

Pengamanan citra digital menjadi semakin penting karena penggunaan gambar digital yang luas dalam media sosial, bisnis, pendidikan, dan medis. Gambar digital rentan terhadap berbagai ancaman seperti pencurian, manipulasi, dan penyalahgunaan, yang mengancam privasi individu serta hak kekayaan intelektual. Ancaman teknologi seperti *deepfake* menambah urgensi untuk menjaga integritas dan keaslian gambar digital. Selain itu, keamanan jaringan dan penyimpanan gambar digital memerlukan langkah-langkah tambahan untuk mencegah serangan siber. Dalam beberapa kasus, gambar digital digunakan sebagai bukti dalam proses hukum atau sebagai data medis. Keutuhan dan keaslian gambar tersebut sangat penting, dan pengamanan citra digital membantu menjaga integritas data ini. Dengan latar belakang ini, pengamanan citra digital diperlukan untuk melindungi berbagai aspek penting terkait penggunaannya dalam kehidupan sehari-hari.

Simon dan Speck adalah dua algoritma kriptografi yang dikembangkan oleh National Security Agency (NSA) Amerika Serikat pada tahun 2013. Kedua algoritma ini dirancang untuk memberikan keamanan yang kuat dengan efisiensi yang tinggi pada perangkat keras dan perangkat lunak. Simon lebih cocok untuk implementasi di perangkat keras karena penggunaan operasi sederhana yang sangat efisien pada arsitektur hardware(Beaulieu et al. 2015). Sementara itu, Speck dioptimalkan untuk perangkat lunak dengan operasi aritmatika yang efisien pada prosesor umum. Penelitian terdahulu mengenai penggunaan algoritma Simon dan Speck dalam pengamanan citra digital telah menunjukkan berbagai hasil yang signifikan.

Beberapa studi telah meneliti efisiensi dan keamanan algoritma Simon dan Speck dalam konteks pengamanan citra digital. Hasilnya menunjukkan bahwa kedua algoritma ini mampu menawarkan kinerja yang baik dengan tingkat keamanan yang cukup tinggi. Mereka dapat digunakan untuk mengenkripsi gambar dengan cepat, bahkan pada perangkat dengan sumber daya terbatas seperti sensor dan perangkat IoT(Beaulieu et al. 2015). Penelitian oleh berbagai peneliti telah menyoroti keunggulan Simon dan Speck dalam implementasi di perangkat dengan sumber daya terbatas. Misalnya, sebuah studi menunjukkan bahwa kedua algoritma ini dapat diimplementasikan dengan efisien pada perangkat mobile dan embedded system, yang umumnya memiliki keterbatasan dalam hal memori dan kekuatan pemrosesan(Bouzida, Y., & Rachdi 2016). Simon dan Speck lebih unggul dalam hal efisiensi energi dibandingkan dengan algoritma penyandian blok lainnya ketika diterapkan pada perangkat IoT. Hal ini menjadikan kedua algoritma ini sebagai pilihan yang sangat baik untuk aplikasi yang memerlukan efisiensi tinggi dan konsumsi energi rendah(Khatiwada, D., Walia, G. S., & Kavi 2018).

Penelitian lain membandingkan kinerja Simon dan Speck dengan algoritma penyandian blok lainnya seperti AES. Hasil penelitian ini umumnya menunjukkan bahwa Simon dan Speck lebih efisien dalam hal penggunaan energi dan kecepatan enkripsi, menjadikannya pilihan yang lebih baik untuk aplikasi yang memerlukan efisiensi tinggi(Ghosh, S., & Roy 2018). Studi-studi keamanan telah menguji ketahanan Simon dan Speck terhadap berbagai jenis serangan kriptanalisis. Meskipun ada beberapa kekhawatiran tentang potensi kelemahan dalam beberapa konfigurasi, secara umum, kedua algoritma ini dianggap cukup aman untuk penggunaan dalam pengamanan citra digital.

Penelitian ini berusaha menerapkan algoritma Simon dan Speck untuk mengamankan citra digital. Tujuannya adalah untuk mengevaluasi kinerja kedua algoritma ini dari beberapa aspek, yaitu waktu yang dibutuhkan untuk proses enkripsi dan dekripsi, perubahan ukuran citra, serta tingkat keacakan citra yang dihasilkan. Dalam evaluasi algoritma enkripsi citra, nilai NPCR dan UACI digunakan untuk menentukan seberapa baik algoritma tersebut dalam menyembunyikan struktur asli dari citra. Algoritma yang baik akan menghasilkan nilai NPCR dan UACI yang tinggi. Nilai NPCR mendekati 100% dan nilai UACI sekitar 33% hingga 34% dianggap sebagai indikator kuat bahwa algoritma enkripsi citra berfungsi dengan baik dalam menciptakan perbedaan yang signifikan dan acak pada citra yang dienkripsi(Chen, G., Mao, Y., & Chui 2004; Wang, X., & Liu 2013; Zhu, C., Wang, G., & Sun 2011).

Penelitian ini diharapkan dapat memberikan wawasan mengenai efisiensi dan efektivitas algoritma Simon dan Speck dalam konteks pengamanan citra digital.

2. METODE PENELITIAN

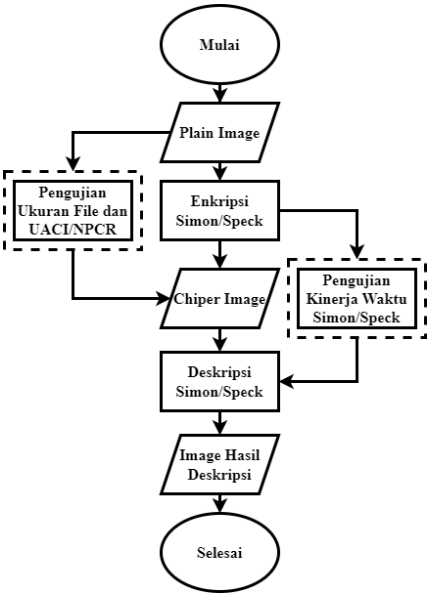
2.1. Data Penelitian

Pada penelitian ini digunakan data sebuah gambar dengan ekstensi jpg dan png dengan dataset berjumlah 10 gambar dengan masing masing dimensi pixel serta ukuran file.

Tabel 1. Data Citra Digital

No	Nama File	Dimesi	Ukuran
1	1024px.png	1024 x 1024	41,1 KB
2	768px.png	768 x 768	39,8 KB
3	600px.png	600 x 600	29,5 KB
4	480px.png	480 x 480	22,6 KB
5	240px.png	240 x 240	10,0 KB
6	jpeg1.jpg	1280 x 853	239 KB
7	jpeg2.jpg	1280 x 870	180 KB
8	jpeg3.jpg	1920 x 1020	89 KB
9	jpeg4.jpg	1280 x 854	309 KB
10	jpeg5.jpg	2480 x 1388	401 KB

2.2. Tahapan Penelitian



Gambar 1. Tahapan Penelitian

2.3. Pengukuran Performa

Makin banyak nilai pixel yang berubah maka makin bagus kualitas keacakan yang dihasilkan pada tiap kali enkripsi dilakukan. Analisis dilakukan dengan membandingkan antara citra asli sebelum dilakukan proses apapun dan hasil enkripsinya. Analisis UACI digunakan untuk menghitung rata-rata perubahan intensitas setiap pixel (Fitriana, Hidayati, and ... 2021).

UACI adalah formula untuk melakukan analisis diferensial dari dua buah citra. UACI digunakan untuk mengetahui seberapa besar interval perbedaan nilai piksel dari kedua citra. Misal *I* dan *I`* adalah dua citra yang berbeda, secara berurutan *I(x,y, z)* dan *I`(x,y, z)* adalah nilai piksel citra *I* dan *I`* pada baris ke-*x*, kolom ke-*y* dan kanal ke-*z*. Kemudian juga misal D adalah array bipolar dengan nilai 0 atau 1 (Riski, Kamsyakawuni, and Arif 2018). Sehingga formula UACI dapat dinyatakan sebagai berikut.

$$\text{UACI} = \frac{\sum_{i,j} |\, C_1(i,j) - C_2(i,j)|}{255 \times T} \times 100\% \qquad (1)$$

$$\text{UACI} = \frac{\sum i,j}{2!} \times 100\% \qquad (2)$$

Analisis NPCR bertujuan untuk mengetahui jumlah pixel yang berubah antara citra yang satu dengan citra yang lain yang dienkripsi menggunakan kunci yang sama. Besarnya nilai NPCR menunjukkan bahwa tiap pixel pada gambar hasil enkripsi mengalami perubahan yang besar pula. Makin banyak nilai pixel yang berubah maka makin bagus kualitas keacakan yang dihasilkan pada tiap kali enkripsi dilakukan. Analisis akan dilakukan dengan membandingkan antara citra asli sebelum dilakukan proses apapun dan hasil enkripsinya(Fitriana, Hidayati, and ... 2021). Perhitungan NPCR dapat dirumuskan sebagai berikut:

$$PCR = \left(\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \sum_{k=0}^{0-1} \frac{d_{i,j,k}}{T}\right) \times 100\% \qquad (3)$$

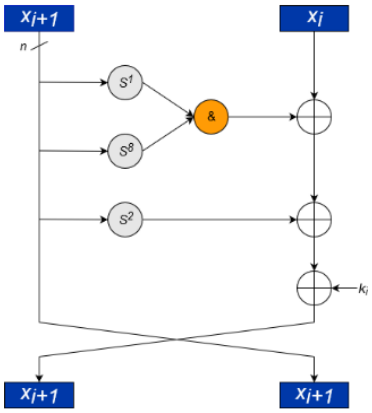
Dimana merupakan jumlah total pixel di cipher image. Untuk menghitung T maka diperlukan m, n, dan o yang melambangkan lebar, tinggi, dan kedalaman citra. Secara teori, nilai minimum yang baik pada indikator NPCR adalah sebesar 99,6094% dan pada indikator UACI sebesar 33,4635%. Sedangkan menurut Boriga, dkk. nilai pada indikator NPCR dapat dikatakan tahan terhadap serangan diferensial pada nilai minimal 98,87% dan pada indikator UACI sebesar minimal 32,17% (Fitriana, Hidayati, and ... 2021).

3. HASIL DAN PEMBAHASAN

3.1. Enkripsi dan Dekripsi menggunakan SIMON

Algoritma Simon merupakan suatu metode yang menjamin keamanan data dan termasuk dalam kategori block cipher yang cocok untuk sebuah aplikasi atau perangkat dengan sumber daya yang terbatas. Algoritma Simon terdiri dari Algoritma yang memiliki berbagai ukuran blok dan kunci yang dapat diterapkan sesuai kebutuhannya. Kerahasiaan data didefinisikan dengan pesan yang telah dienkripsi yang berupa ciphertext. Ketika proses verifikasi gagal maka ciphertext tidak akan dikeluarkan sebagai output. Algoritma Simon merupakan algoritma block cipher yang dapat diterapkan pada perangkat lunak maupun perangkat keras sesuai dengan kebutuhan penggunanya. Algoritma ini memanfaatkan operasi perhitungan seperti XOR, AND, Shift register dan memiliki 10 macam versi berdasarkan ukuran block size maupun key size yang menjadi keunggulan (Asta et al., 2019).

Pada umumnya kriptografi sandi blok seperti AES dan DES dilakukan menggunakan substitution box (Sbox) agar dapat dibentuk menjadi substitutionpermutation networks (SPNs). Keunggulan dari SPNs adalah dia memungkinkan argumen keamanan yang relatif sederhana dan cukup kuat secara kriptografis, tetapi cukup berat pada perangkat yang terbatas. Berdasarkan pertimbangan tersebut, algoritme SIMON dan SPECK dibuat tanpa menggunakan Sbox tetapi menggunakan fungsi ronde berbasis permutasi Feistel yang memberikan keseimbangan antara *linear diffusion* dan *nonlinear confusion operations* (Beaulieu et al. 2015).



Gambar 1. Fungsi Putaran SIMON

Pada Gambar Round Function Simon Algoritma merupakan representasi pembentukan round function pada proses dekripsi dengan melakukan kebalikan dari round function pada proses enkripsi. Pada Algoritma Simon terdapat dua proses utama dalam mengenkripsi dan dekripsi yaitu round function dan key schedule. Pembentukan round function pada proses enkripsi didefinisikan sebagai berikut :

$$R\_k\ (x,y)=(y \oplus f(x) \oplus k,x) \qquad (4)$$

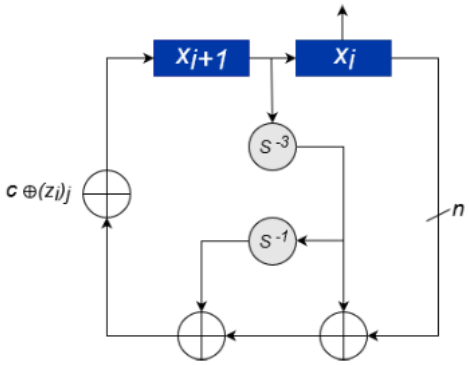
(Ginatka, Kusyanti, and Primananda 2019)

Pada Persamaan rumus ini merupakan fungsi untuk melakukan pergeseran bit. Input dari panjang block adalah 2n yang kemudian block dibagi menjadi dua words. Xi+1 akan menjadi word bagian kanan pada round selanjutnya. Kemudian menggeser sebanyak 1 kali ke kiri (S1), setelah itu geser sebanyak 8 kali ke kiri (S8), setelah itu geser sebanyak 2 kali ke kiri (S2). Kemudian melakukan operasi AND antara S1 dengan S8, setelah itu melakukan operasi XOR dengan S2 dan hasil akhir kemudian di-XOR dengan k.

$$R\_k\text{^}(-1)\ (x,y)=(y,x \oplus f(y) \oplus k) \qquad (5)$$

(Ginata, Kusyanti, and Primananda 2019)

Rumus ini merupakan representasi proses dekripsi Algoritma Simon dengan mengganti words dari ciphertext, membaca round key dengan urutan terbalik kemudian menukar words dari plaintext yang dihasilkan.



Gambar 2. Key Schedule SIMON

Key schedule yang ada dalam Algoritma Simon menggunakan urutan konstanta round 1-bit khusus untuk tujuan menghilangkan slide dan simetri circular shift. Perancang Algoritma Simon menyediakan beberapa pemisahan kriptografi antara versi Simon yang berbeda memiliki panjang block yang sama dengan mendefinisikan lima urutan sebagai berikut (z0,…,z4).

Penjadwalan kunci algoritma simon menggunakan konstanta ronde untuk mengeliminasi slide properties dan circular shift symmetries yang terjadi saat proses enkripsi maupun dekripsi. Cara penjadwalan kunci pada algoritme SIMON tergantung pada pasangan ukuran blok dan kunci, seperti yang terlihat pada persamaan dibawah;

$$c \oplus (zj) \oplus ki \oplus (I \oplus S\,{-}1)\,{-}3ki{+}1 \quad (6)$$
$$c \oplus (zj) \oplus ki \oplus (I \oplus S\,{-}1)\,{-}3ki{+}2\,, \quad (7)$$
$$c \oplus (zj) \oplus ki \oplus (I \oplus S\,{-}1)(S\,{-}3ki{+}2 \oplus ki{+}1) \quad (8)$$

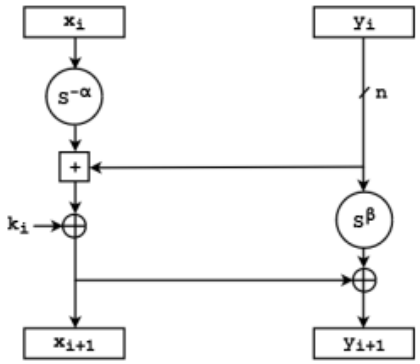
Proses enkripsi menggunakan Algoritma Simon dilakukan setelah mendapatkan hasil dari perhitungan key schedule. Tabel di bawah ini menunjukkan langkah-langkah perhitungan enkripsi, sementara dekripsi dilakukan setelah proses enkripsi selesai. Untuk melakukan dekripsi pada Algoritma Simon, perhitungan dari proses enkripsi harus dibalik.

Pseudocode : Enkripsi Algoritma SIMON

1. For i = 0 . . T - 1
2. Tmp ← x
3. x ← y ⊕ (Sx & S^8 x) ⊕ S^2x ⊕ k [I]
4. y ← tmp
5. end for

3.2. Enkripsi dan Dekripsi menggunakan SPECK

Sejak DES menjadi standar kriptografi pertama, algoritme block cipher telah menjadi popular dalam dunia kriptologi. Pada tahun 2013, NSA memperkenalkan algoritme block cipher SIMON dan SPECK yang merupakan bagian dari lightweight block ciphers. Algoritme ini diciptakan untuk mengoptimalkan kinerja software dan hardware dalam konteks keterbatasan lingkungan computing. Algoritme SPECK menggunakan konstruksi sandi sederhana yang dikenal sebagai ARX (add, rotate, XOR). Dari berbagai variannya, SPECK mempunyai beragam ukuran data blok dan kunci. Secara umum, varian dari cipher disebut sebagai SPECK2n / mn dan dapat di instansiasikan dengan nilai n = 16/24/32/48/64 dan m = 2/3/4. Dimana variabel n adalah ukuran word dan variabel m adalah key word. Proses enkripsi pada algoritme SPECK menggunakan operasi bitwise XOR, modulo addition 2n (+), circular shift ke kanan dan ke kiri (S-a dan S- b).



Gambar 3. Fungsi Putaran SPECK

Alur kerja algoritme SPECK terdiri dari tiga proses utama, yaitu key scheduling, enkripsi dan dekripsi. Proses pada algoritme SPECK menggunakan operasi perhitungan sebagai berikut: 1. bitwise XOR (⊕), 2. addition modulo 2 n (+), 3. substraction modulo 2 n (–), dan 4. Pergeseran rotasi kiri dan kanan (S, S-) Proses key scheduling berfungsi untuk menghasilkan key pada setiap round SPECK (Sulistyowati, Kusyanti, and Data 2019). Proses key scheduling menghasilkan dua variabel yaitu li dan ki . Nilai m adalah jumlah dari key word, n adalah word size, T adalah jumlah round, i adalah ronde saat ini, α dan β adalah jumlah pergeseran rotasi. Rumus proses key scheduling yang ditunjukkan pada Persamaan (9) dan Persamaan (10).

$$l_{i+m-1} = (k_i + S^{-\alpha} l_i) \oplus i \quad (9)$$

$$k_{i+1} = S^{\beta} k_i \oplus l_{i+m-1} \quad (10)$$

Alur kerja proses key scheduling dapat dilihat pada tabel dibawah ini:

Input : $K_{(mn)}$
Output : k_0 , ..., k_{T-1}
Proses :

1. $k_{0\,(n)} \mid l_{0\,(n)} \mid \ldots \mid l_{m-2\,(n)} \leftarrow k_{mn}$
2. untuk i = 1 sampai dengan T-1
   tmp $\leftarrow (k_1 + (s^{-\alpha}\ 1_0)) \oplus$ i
   $k_{i+1} \leftarrow (s^{\beta} k_1) \oplus$ tmp
3. Output
   $K_{0\,(n)} \mid k_{1\,(n)} \mid \ldots \mid k_{T-1\,(n)}$

3.3. Perbandingan Waktu

Pengujian ini bertujuan untuk mengetahui berapa lama waktu yang dibutuhkan pada saat melakukan enkripsi dan dekripsi citra digital menggunakan algoritma simon speck. Pengujian ini dapat dilakukan dengan melihat berapa lama proses enkripsi dan dekripsi berlangsung. Pengujian waktu ini dilakukan dengan mengukur lama proses enkripsi dan dekripsi. Hasil uji lama proses enkripsi dan dekripsi tersaji pada Tabel 2 dan 3. Pengujian yang dilakukan pada sepuluh file yang berbeda-beda baik dari segi ukuran file maupun dimensi.

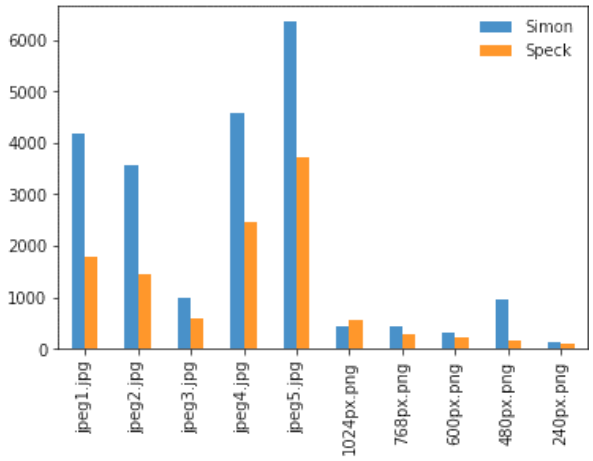
Tabel 2. Waktu Proses Enkripsi dan Dekripsi Simon

No	Nama File	Dimensi	Simon	
			Lama Enkripsi	Lama Dekripsi
1	jpeg1.jpg	1280 x 853	4180 ms	3410 ms
2	jpeg2.jpg	1280 x 870	3570 ms	2580 ms
3	jpeg3.jpg	1920 x 1020	987 ms	1550 ms
4	jpeg4.jpg	1280 x 854	4570 ms	4300 ms
5	jpeg5.jpg	2480 x 1388	6350 ms	7930 ms
6	1024px.png	1024 x 1024	436 ms	594 ms
7	768px.png	768 x 768	428 ms	443 ms
8	600px.png	600 x 600	318 ms	355 ms
9	480px.png	480 x 480	957 ms	243 ms
10	240px.png	240 x 240	113 ms	585 ms

Tabel 3. Waktu Proses Enkripsi dan Dekripsi Speck

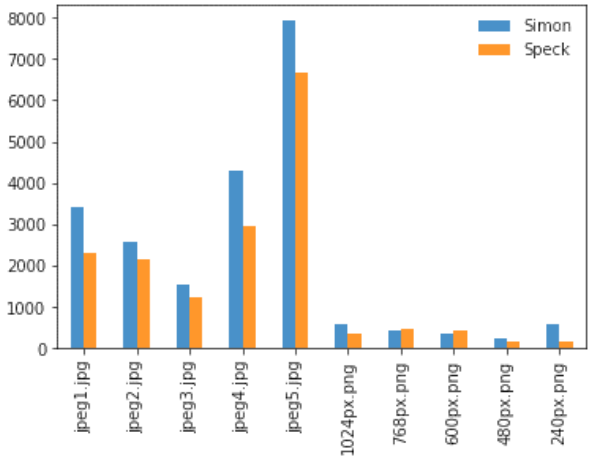
No	Nama File	Dimensi	Speck	
			Lama Enkripsi	Lama Dekripsi
1	jpeg1.jpg	1280 x 853	1780 ms	2310 ms
2	jpeg2.jpg	1280 x 870	1440 ms	2140 ms
3	jpeg3.jpg	1920 x 1020	601 ms	1250 ms
4	jpeg4.jpg	1280 x 854	2450 ms	2970 ms
5	jpeg5.jpg	2480 x 1388	3720 ms	6670 ms

6	1024px.png	1024 x 1024	549 ms	353 ms
7	768px.png	768 x 768	280 ms	464 ms
8	600px.png	600 x 600	211 ms	428 ms
9	480px.png	480 x 480	160 ms	176 ms
10	240px.png	240 x 240	86 ms	170 ms



Gambar 4. Grafik Perbandingan Waktu Enkripsi

Pada hasil penelitian, lama waktu enkripsi yang diperoleh menggunakan Algoritma Simon didapatkan rata rata hasil sebesar 2190.9 ms dan pada algoritma Speck didapatkan rata-rata hasil sebesar 1127,7 ms.



Gambar 5. Grafik Perbandingan Waktu Dekripsi

Pada hasil penelitian, lama waktu dekripsi yang diperoleh menggunakan Algoritma Simon didapatkan rata rata hasil sebesar 2199 ms dan pada algoritma Speck didapatkan rata-rata hasil sebesar 1693,1 ms.

3.4. Perubahan Ukuran File

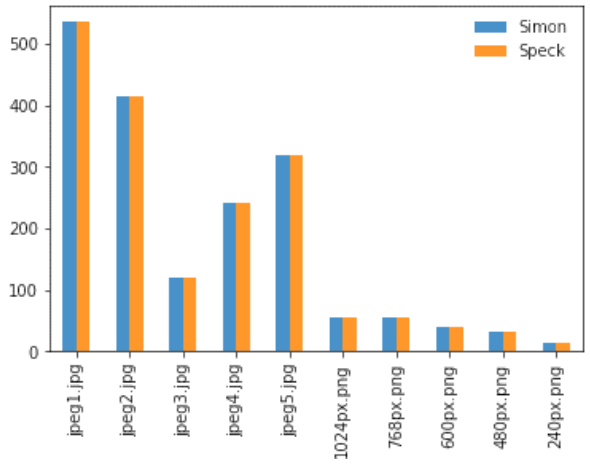
Pengujian ini bertujuan untuk mengetahui presentase perubahan ukuran file setelah dilakukannya proses enkripsi dan juga proses dekripsi citra digital menggunakan algoritma simon dan algoritma Speck. Pengujian ini dilakukan dengan membandingkan ukuran file citra digital pada saat belum melalui proses enkripsi dan sesudah melalui proses enkripsi.

Tabel 4. Perubahan Ukuran Citra hasil Enkripsi Simon

No	**Nama File**	**Dimensi**	**Simon**	
			Ukuran File Asli	**Ukuran File Hasil Cipher**
1	jpeg1.jpg	1280 x 853	240 kb	536 kb
2	jpeg2.jpg	1280 x 870	181 kb	414 kb
3	jpeg3.jpg	1920 x 1020	90 kb	119 kb
4	jpeg4.jpg	1280 x 854	310 kb	242 kb
5	jpeg5.jpg	2480 x 1388	402 kb	319 kb
6	1024px.png	1024 x 1024	42 kb	55 kb
7	768px.png	768 x 768	40 kb	54 kb
8	600px.png	600 x 600	30 kb	40 kb
9	480px.png	480 x 480	23 kb	31 kb
10	240px.png	240 x 240	11 kb	14 kb

Tabel 5. Perubahan Ukuran Citra hasil Enkripsi Speck

No	Nama File	Dimensi	Speck	
			Ukuran File Asli	Ukuran File Hasil Cipher
1	jpeg1.jpg	1280 x 853	240 kb	536 kb
2	jpeg2.jpg	1280 x 870	181 kb	414 kb
3	jpeg3.jpg	1920 x 1020	90 kb	119 kb
4	jpeg4.jpg	1280 x 854	310 kb	242 kb
5	jpeg5.jpg	2480 x 1388	402 kb	319 kb
6	1024px.png	1024 x 1024	42 kb	55 kb
7	768px.png	768 x 768	40 kb	54 kb
8	600px.png	600 x 600	30 kb	40 kb
9	480px.png	480 x 480	23 kb	31 kb
10	240px.png	240 x 240	11 kb	14 kb



Gambar 6. Grafik Perbandingan Perubahan Ukuran File

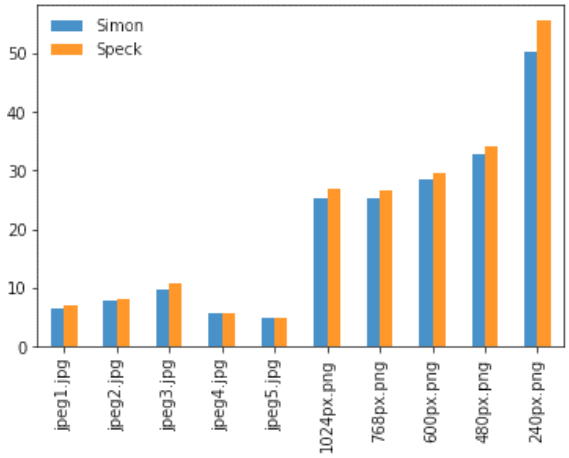
Pengujian yang dilakukan pada sepuluh file citra digital yang berbeda-beda baik dari segi ukuran file maupun dimensi menunjukkan bahwa terjadi penambahan ukuran file rata-rata sebesar 24,9%(Algoritma Simon) dan 24,9%(Algoritma Speck).

3.5. Pengujian *UACI*

Pengujian berikutnya adalah tingkat keacakan file dengan analisis diferensial UACI. UACI adalah formula untuk melakukan analisis diferensial dari dua buah citra. UACI digunakan untuk mengetahui seberapa besar interval perbedaan nilai piksel dari kedua citra. Makin banyak nilai pixel yang berubah maka makin bagus kualitas keacakan yang dihasilkan pada tiap kali enkripsi dilakukan. Analisis dilakukan dengan membandingkan antara citra asli sebelum dilakukan proses apapun dan hasil enkripsinya. Analisis UACI digunakan untuk menghitung rata-rata perubahan intensitas setiap pixel. Nilai UACI dari 10 citra yang di uji dapat dilihat pada table dibawah ini:

Tabel 6. Hasil Pengujian UACI Citra

No	Nama File	Dimensi	UACI	
			Simon	Speck
1	jpeg1.jpg	1280 x 853	6,4 %	7,1 %
2	jpeg2.jpg	1280 x 870	7,7 %	8,0 %
3	jpeg3.jpg	1920 x 1020	9,6 %	10,8 %
4	jpeg4.jpg	1280 x 854	5,6 %	5,8 %
5	jpeg5.jpg	2480 x 1388	4,8 %	5,0 %
6	1024px.png	1024 x 1024	25,4 %	26,8 %
7	768px.png	768 x 768	25,3 %	26,7 %
8	600px.png	600 x 600	28,6 %	29,5 %
9	480px.png	480 x 480	32,9 %	34,1 %
10	240px.png	240 x 240	50,2 %	55,6 %



Gambar 7. Grafik Perbandingan Tingkat Keacakan Citra berdasarkan nilai UACI

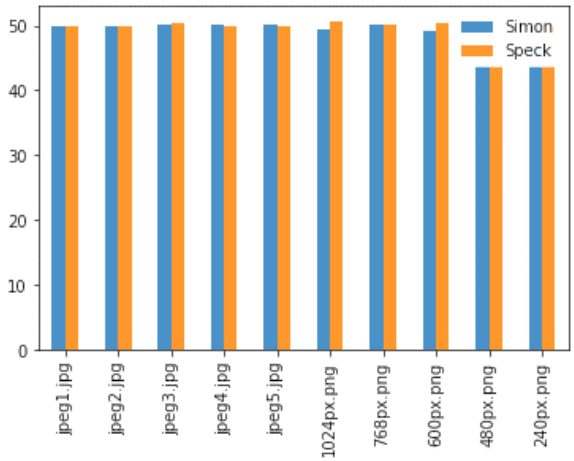
Pada hasil penelitian, nilai UACI yang diperoleh menggunakan Algoritma Simon didapatkan rata rata hasil sebesar 19,65 % dan pada algoritma Speck didapatkan rata-rata hasil sebesar 20,94 %. Secara teori, nilai minimum yang baik pada indikator NPCR adalah sebesar 99,6094% dan pada indikator UACI sebesar 33,4635%. Sedangkan menurut Boriga, dkk. nilai pada indikator NPCR dapat dikatakan tahan terhadap serangan diferensial pada nilai minimal 98,87% dan pada indikator UACI sebesar minimal 32,17% (Fitriana, Hidayati, and ... 2021).

3.6. Pengujian NPCR

Analisis NPCR bertujuan untuk mengetahui jumlah pixel yang berubah antara citra yang satu dengan citra yang lain yang dienkripsi menggunakan kunci yang sama. Besarnya nilai NPCR menunjukkan bahwa tiap pixel pada gambar hasil enkripsi mengalami perubahan yang besar pula. . Nilai NPCR dari 10 citra yang di uji dapat dilihat pada table dibawah ini:

Tabel 7. Hasil Pengujian NPCR Citra

No	Nama File	Dimensi	UACI	
			Simon	Speck
1	jpeg1.jpg	1280 x 853	49,92 %	49,97 %
2	jpeg2.jpg	1280 x 870	49,82 %	49,82 %
3	jpeg3.jpg	1920 x 1020	50,07 %	50,37 %
4	jpeg4.jpg	1280 x 854	50,06 %	49,92 %
5	jpeg5.jpg	2480 x 1388	50,16 %	50,01 %
6	1024px.png	1024 x 1024	49,39 %	50,60 %
7	768px.png	768 x 768	50,20 %	50,02 %
8	600px.png	600 x 600	49,25 %	50,40 %
9	480px.png	480 x 480	49,86 %	50,58 %
10	240px.png	240 x 240	50,56 %	50,09 %



Gambar 8. Grafik Perbandingan Tingkat Keacakan Citra berdasarkan nilai NPCR

Pada hasil penelitian, nilai NPCR yang diperoleh menggunakan Algoritma Simon didapatkan rata rata hasil sebesar 49,98 % dan pada algoritma Speck didapatkan rata-rata hasil sebesar 50,17 %. Secara teori, nilai minimum yang baik pada indikator NPCR adalah sebesar 99,6094% dan pada indikator UACI sebesar 33,4635%. Sedangkan menurut Boriga, dkk. nilai pada indikator NPCR dapat dikatakan tahan terhadap serangan diferensial pada nilai minimal 98,87% dan pada indikator UACI sebesar minimal 32,17% (Fitriana, Hidayati, and ... 2021).

4. KESIMPULAN

Dari hasil penelitian pengamanan citra digital menggunakan algoritma simon dapat diambil kesimpulan sebagai berikut:

1. Performa Algoritma Simon dalam mengamankan citra digital menunjukkan bahwa rata-rata waktu enkripsi adalah 2190,9 ms, sedangkan rata-rata waktu dekripsinya adalah 2199 ms. Sementara itu, Algoritma Speck menghasilkan rata-rata waktu enkripsi 1127,7 ms dan rata-rata waktu dekripsi 1693,1 ms. Ukuran file hasil enkripsi menggunakan Algoritma Simon lebih besar 24,9% dibandingkan file aslinya, dan hasil enkripsi menggunakan Algoritma Speck juga lebih besar 24,9% dari file aslinya.
2. Nilai UACI yang diperoleh menggunakan Algoritma Simon didapatkan rata rata hasil sebesar 19,65% dan nilai UACI yang diperoleh menggunakan Algoritma Speck didapatkan rata rata hasil sebesar 20,94 %. Nilai NPCR yang diperoleh menggunakan Algoritma Simon didapatkan rata rata hasil sebesar 49,98% dan nilai NPCR yang diperoleh menggunakan Algoritma Speck didapatkan rata rata hasil sebesar 50,17 %. Berdasarkan teori analisis diferensial, cipherimage yang dihasilkan dapat dikatakan kurang baik terhadap serangan diferensial. Hal ini didasarkan pada nilai NPCR dan UACI yang belum memenuhi nilai batas minimal pada indikator NPCR adalah sebesar 99,6094% dan pada indikator UACI sebesar 33,4635%. Nilai pada indikator NPCR dapat dikatakan tahan terhadap serangan diferensial pada nilai minimal 98,87% dan pada indikator UACI sebesar minimal 32,17%.

DAFTAR PUSTAKA

[1] Beaulieu, Ray et al. 2015. "The SIMON and SPECK Lightweight Block CIPhers." *Proceedings - Design Automation Conference* 2015-July.
[2] Bouzida, Y., & Rachdi, F. 2016. "Implementing the SIMON and SPECK Lightweight Block Ciphers on Smart Cards." *Journal of Information Security and Applications*: 28–40.
[3] Chen, G., Mao, Y., & Chui, C. K. 2004. "A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps." *Chaos, Solitons & Fractals*: 749–61.
[4] Fitriana, G F, L N Hidayati, and ... 2021. "Perbandingan Keacakan Citra Enkripsi Algoritma AES Dan Camelia Uji NPCR Dan UACI." *JURIKOM (Jurnal Riset ...* 8(6): 274–83.
[5] Ghosh, S., & Roy, A. 2018. "Lightweight Cryptography for IoT Security: Implementation of Simon and Speck on Contiki-NG OS." *IEEE Access*: 49401–12.
[6] Ginata, S, A Kusyanti, and R Primananda. 2019. "Implementasi Algoritme Kriptografi Simon Pada Arsitektur Amazon Web Services." *... Teknologi Informasi dan Ilmu ...* 3(8): 7888–97.
[7] Khatiwada, D., Walia, G. S., & Kavi, K. M. 2018. "On Placement of Hypervisors and Controllers in Virtualized Software Defined Network." *IEEE Transactions on Sustainable Computing*: 233–44.
[8] Riski, Abduh, Ahmad Kamsyakawuni, and M. Ziaul Arif. 2018. "Implementasi Vigenere Cipher Pada Pendahuluan Citra Digital." 02(01): 23–30.
[9] Sulistyowati, Karmila Dewi, Ari Kusyanti, and Mahendra Data. 2019. "Analisis Kinerja Algoritme Speck Pada Keamanan File Teks." 3(4): 3719–27.
[10] Wang, X., & Liu, L. 2013. "A Novel Chaotic Block Image Encryption Algorithm Based on Dynamic Random Growth Technique." *Optics and Lasers in Engineering*: 121–28.
[11] Zhu, C., Wang, G., & Sun, K. 2011. "Cryptanalysis and Improvement of a Chaos-Based Image Encryption Scheme." *Chaos, Solitons & Fractals*: 2191–99.