KOMPARASI HASIL ENKRIPSI ARNOLD CAT MAP DAN LOGISTIC MAP PADA CITRA DIGITAL

Iqbal[1], Kusrini[2], Asro Nasiri[3]
iqbal.iq@students.amikom.ac.id[1], kusrini@amikom.ac.id[2], asro@amikom.ac.id[3]
Universitas AMIKOM Yogyakarta

ABSTRAK

File dalam bentuk citra digital sangat banyak digunakan di berbagai bidang. Banyak gambar bersifat rahasia dan perlu diamankan dari orang yang tidak berwenang. Pencurian atau penyalahgunaan gambar dapat berdampak buruk pada pemilik gambar. Ada banyak teknik untuk mengamankan data dalam bentuk gambar digital, salah satunya adalah teknik kriptografi. *Arnold Cat Map (ACM)* dan *Logistic Map* adalah teknik kriptografi yang banyak digunakan untuk mengamankan gambar dengan mengenkripsi gambar digital yang sulit dikenali, kedua teknik ini diklasifikasikan sebagai Chaotic Maps yang merupakan teknik pengacakan. *ACM* melakukan pengacakan dengan memutar gambar terus menerus sehingga menjadi bentuk acak, sedangkan *Logistic Map* memiliki sensitivitas yang baik dalam mengenkripsi gambar. Dalam penelitian ini akan membandingkan hasil enkripsi gambar dari dua algoritma enkripsi dengan membandingkan histogram, *Number of Pixel Change Rate (NPCR), Unified Average Changing Intensity (UACI),* & koefisien korelasi dari hasil enkripsi dengan gambar asli. Hasil dari pengujian algoritma *ACM* dan *Logistic Map* menunjukkan nilai *NPCR* diatas 90%, nilai *UACI* diatas 30%, dan koefisien korelasi yang jauh dari angka 1 sehingga pixel pixel didalamnya tidak lagi berkorelasi. Hasil analisis histogram dari algoritma *ACM* cenderung mirip dari histogram citra asli, sedangkan histogram *logistic map* terlihat berbeda dengan histogram citra asli serta secara statistik memiliki distribusi yang lebih seragam.

Kata Kunci: Kriptografi, Enkripsi, *ACM, Logistic Map*.

1. Pendahuluan

Citra digital atau gambar merupakan bentuk multimedia yang dapat menyajikan informasi yang lebih kaya daripada informasi secara textual [1]. Perpindahan informasi tersebut dapat melalui perantara jaringan internet yang membuat perpindahan informasi tersebut menjadi semakin cepat [2]. Kelemahan penggunaan media informasi gambar itu mudah dimanipulasi oleh pihak-pihak yang berkepentingan lain didalamnya [1]. Citra dalam bentuk *plainimage* rentan dalam bentuk penyadapan atau pencurian [3]. Informasi yang bersifat rahasia seperti informasi mengenai bisnis atau kepentingan pribadi dapat merugikan pemiliknya jika disalahgunakan oleh pihak yang tidak bertanggung jawab [4]. Cara yang bisa digunakan untuk mengamankan citra digital adalah dengan menggunakan Teknik kriptografi [5].

Kriptografi diartikan sebagai ilmu mengenai cara pengacakan atau enkripsi suatu data, sehingga data tersebut menjadi tidak beraturan dan sulit untuk dibaca atau dipahami [6]. Algoritma kriptografi yang bisa digunakan untuk melakukan enkripsi pada gambar adalah *Arnold Cat Map (ACM)* dan *Logistic Map*. Algoritma ACM berkonsep dimana pixel dari citra tersebut diputar atau diacak secara terus menerus sehingga menjadi bentuk yang tidak beraturan [7]. *Logistic Map* mempunyai sensitivitas yang bagus dalam mengenkripsi citra [1]. *Logistic Map* membangkitkan *keystream* yang kemudian dienkripsikan dengan *pixel-pixel* hasil permutasi [8].

Algoritma *ACM* dan *Losgistic Map* banyak digunakan dalam enkripsi citra digital. Penelitian ini bertujuan untuk membandingkan hasil enkripsi *ACM* dan *Logistic Map* pada citra digital. Komparasi enkripsi *ACM* dan *Logistic Map* akan dievaluasi menggunakan alat ukur *Number of Pixel Change Rate (NPCR), Unified Average Changing Intensity (UACI),* koefisien korelasi dari hasil enkripsi dengan gambar asli, dan analisis histogram citra.

2. Landasan Teori

Berikut ini adalah beberapa teori yang digunakan dalam penelitian ini.

2.1. Citra Digital

Citra dapat diartikan sebagai suatu representasi (gambaran), kemiripan, atau imitasi dari suatu objek [9]. Citra dapat dihasilkan melalui proses perekaman objek

bayangan yang direkam oleh alat-alat optik, dimana bayangan tersebut terjadi ketika suatu sumber cahaya mengenai objek yang kemudian objek tersebut memantulkan cahaya, pantulan cahaya itu kemudian yang ditangkap oleh alat-alat optik sehingga menghasilkan citra.

Dari sifatnya citra bisa dibedakan menjadi 2, yaitu citra yang bersifat analog dan citra yang bersifat digital. Citra yang bersifat analog itu memiliki sifatnya kontinu, citra ini dapat ditangkap oleh alat akuisisi citra analog seperti kamera dan mata manusia, dimana citra jenis ini contohnya dapat dilihat pada televisi. Adapula citra yang bersifat digital itu citra yang diolah oleh komputer yang dimanan alat akuisisi citra digital itu berupa kamera digital, kamera ponsel, mikroskop digital, webcam dan alat alat digital lainnya. Citra digital terbentuk dari pixel-pixel, dimana pixel-pixel ini merupakan elemen penyusun dari sebuah citra. Citra digital dapat dianalogikan sebagai matrix yang memiliki kolom dan baris, perpotongan antara kolom dan baris dalam citra digital itu disebut pixel.

2.2. Kriptografi

Kriptografi adalah ilmu tentang penyandian data. Dengan melakukan penyandian terhadap data, maka hanya orang yang mengetahui penyandian tersebut yang dapat membaca data yang disandikan [10]. Kriptografi adalah teknik pengamanan terhdapat data, baik itu data teks, gambar, dan audio. Teknik pengamanan pada kriptografi dilakukan dengan mengenkripsi data yang ingin diamakan sehingga hanya bisa dimengerti oleh orang yang mempunyai sadi, dimana sandi ini yang digunakan untuk mendekskripsi data yang telah dienkripsi sehingga makna asli dari isi data dapat dimengerti. Salah satu dari berbagai cara yang bisa dimanfaatkan untuk menjaga serta mengamankan informasi pada saat proses pengiriman atau pendistribusian ke suatu tempat adalah dengan memanfaatkan teknik kriptografi [11].

Dalam melakukan teknik kriptografi ada beberapa aspek penting yang harus dicapai, diantaranya kerahasiaan, integritas, nirpenyangkalan, serta sumberdaya pendukun [12]. Kelima aspek tersebut, antara lain: (a) kerahasiaan yaitu informasi hanya dapat diakses oleh pihak yang berhak sehingga kerahasiaan harus dijaga; (b) otentikasi, dalam hal ini terdapat dua jenis otentikasi: otentikasi pesan berarti pesan yang diterima harus sama seperti pesan yang dikirimkam sedangkan otentikasi entitas user berarti pihak yang diajak berkomunikasi merupakan pihak yang benar-benar dikehendaki; (c) integritas merupakan keaslian pesan yang dikirim, (d) anti penolakan merupakan bukti bahwa seseorang telah mengirimkan pesan, (e) ketersediaan yaitu adanya sumber daya dari system komputer untuk mengakses oleh pihak yang berhak pada saat dibutuhkan [13].

2.3. Arnold Cat Map (ACM)

ACM merupakan pengembangan fungsi chaos yang sebelumnya ditemukan pada tahun 1960 oleh Vladimir Arnold, sedangkan kata "cat" berasal dari penggunaan citra seekor kucing di dalam melakukan eksperimennya [14].

Algoritma ACM ini mentransformasikan koordinat pixel (xi,yi) pada sebuah citra N ke koordinat baru (xi+1,yi+1) yang kemudian membentuk sebuah citra baru Ni. Rumus perhitungan ACM ditunjukkan pada persamaan (1) di bawah ini :

$$\begin{bmatrix} Xi & + & 1 \\ Yi & + & 1 \end{bmatrix} = \begin{bmatrix} 1 & & b \\ c & bc & + & 1 \end{bmatrix} \begin{bmatrix} Xi \\ Yi \end{bmatrix} mod\,(n) \ldots (1)$$

(xi+1,yi+1) adalah posisi pixel yang baru, b dan c adalah kunci rahasia, (xi,yi) posisi pixel asli atau posisi semula dan N adalah ukuran pixel citra. Untuk melakukan deskripsi, maka digunakan persamaan (2) berikut ini :

$$\begin{bmatrix} Xi \\ Yi \end{bmatrix} = \begin{bmatrix} 1 & & b \\ c & bc & + & 1 \end{bmatrix}^{-1} \begin{bmatrix} Xi & + & 1 \\ Yi & + & 1 \end{bmatrix} mod\,(n) \ldots (2)$$

2.4. Logisitic Map

Logistic map merupakan system chaos yang sederhana yang berbentuk persamaan iteratif sebagai berikut:

$$x_{i+1} = \mu x_i (1 - x_i) \ldots\ldots\ldots\ldots\ldots (3)$$

Nilai x_i yaitu antara $0 \leq x_i \leq 1$, sedangkan μ adalah parameter fungsi yang menyatakan laju pertumbuhan yang nilainya $0 \leq \mu \leq 4$. *Logistic map* bersifar *chaos* bila nilainya $3.5699456 \leq \mu \leq 4$ [16]. Nilai awal pada persamaan iterasi adalah x_0. Perubahan pada nilai awal berdampak besar pada nilai *chaos* setelah *logisitic map* diiterasi. Pada system ini nilai awal x_0, dan parameter μ berperan sebagai kunci rahasia. Nilai acak yang dihasilkan dari persamaan (1) tidak pernah berulang kembali sehingga *logistic map* dikatakan tidak mempunyai priode.

2.5. Histogram

Histogram pada bidang pengolahan citra digital mampu memperlihatkan distribusi dari pixel-pixel pada sebuah citra. Dimana dalam hal ini histogram bisa dimanfaatkan oleh seseorang yang bermaksud untuk melakukan kriptanalisis terhadap citra yang telah dienkripsi dengan menggunakan frekuensi kemuncula suatu pixel yang ada pada histogram, dengan menggunakan frekuensi tersebut proses kriptanalisis dapat dilakukan dengan mendeduksi kunci atau pixel-pilxel pada gambar yang telah terenkripsi [8].

Agar histogram tidak dapat digunakan dalam analisis frekuensi kemunculan pixel pada histogram, maka histogram dari gambar asli dan gambar yang telah terenkripsi harus berbeda atau secara statistik tidak memiliki kemiripan. Sehingga histogram gambar hasil enkripsi sebaiknya datar atau secara statistik memiliki distribusi yang seragam. Gambar hasil enkripsi yang memiliki distribusi yang seragam dapat diindikasikan bahwa algoritma yang digunakan untuk mengenkripsi citra tersebut memiliki tingkat keamanan yang bagus [15].

2.6. Analisis Diferensial

Analisis diferensial adalah parameter untuk evaluasi kekuatan algoritma dalam mengenkripsi citra dari serangan diferensial. Ada dua indikator pengukuran yang sering digunakan dalam menganalisis diferensial, yaitu Number of Pixels Change Rate (NPCR) dan Unifer Average Changing Intensity (UACI). NPCR digunakan untuk menghitung berapa banyak perbedaan pixel dari dua buah citra, sedangkan UACI berfokus pada interval perbedaan nilai pixel dari kedua citra [17].

Perhitungan NPCR dapat dirumuskan sebagai berikut:

$$NPCR = \left(\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \sum_{k=0}^{0-1} \frac{d_{i,j,k}}{T} \right) \times 100\% \dots (4)$$

Dimana T merupakan jumlah total pixel di cipher image. Untuk menghitung T maka diperlukan m, n, dan o yang melambangkan lebar, tinggi, dan kedalaman citra. Sedangakan $di,,$ melambangkan derajad keabuan dan ditentukan sebagai berikut:

$$d_{i,j,k} = \begin{cases} 0, jika\ c_{i,j,k}^{(1)} = c_{i,j,k}^{(2)} \\ 1, jika\ c_{i,j,k}^{(1)} \neq c_{i,j,k}^{(2)} \end{cases}$$

Dimana $c_{i,j,k}^{(1)}$ dan $c_{i,j,k}^{(2)}$ melambangkan nilai keabuan dari baris *i*, kolom *j*, dan kanal *k* dari citra $c^{(1)}$ *(plain image)* dan $c^{(2)}$ *(cipher image).*

Perhitungan UACI didefinisikan seperti pada persamaan berikut:

$$UACI = \left(\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \sum_{k=0}^{0-1} \frac{\left| c_{i,j,k}^{(1)} - c_{i,j,k}^{(2)} \right|}{F \times T} \right) \times 100\% \dots\dots (5)$$

Dimana F menunjukkan nilai pixel terbesar yang kompatibel dengan format cipher Image [18]. Batas minimal indikator *NPCR* sebesar 99,609375% dan batas minimal *UACI* sebesar 33,463541% untuk citra *grayscale* dan *RGB*, maka cipher image dikatakan baik apabila memenuhi batas minimal dari indikator *NPCR* dan *UACI* [19]. Secara visual, cipher image dikatakan baik apabila sangat "berbeda" dengan citra aslinya dan terlihat acak [17].

2.7. Koefisien Korelasi

Analisis koefisien korelasi digunakan untuk mengukur hubungan antara dua variabel, yaitu plain image dan cipher image. Faktor ini menunjukkan tingkat keamanan algoritma enkripsi terhadap serangan statistik. Koefisien korelasi diukur dengan persamaan sebagai berikut:

$$CorrCoef(x,y) = \frac{\sum_{i=1}^{n} (x_i - \mu(x))(y_i - \mu(y))}{\sigma(x)\sigma(y)} \dots\dots (6)$$

Di mana (x) dan (y) adalah rata-rata dari masing-masing x dan y diperoleh dari persamaan berikut:

$$\mu(x) = \frac{1}{n} \sum_{i=1}^{n} x_i \ dan\ \mu(y) = \frac{1}{n} \sum_{i=1}^{n} y_i \dots\dots (7)$$

x dan y variable dari *plain image* dan *cipher image*. Standar deviasi (σ) digunakan untuk mengetahui seberapa dekat sebaran data dengan nilai rata-ratanya. Persamaan standar deviasi untuk masing-masing x dan y adalah sebgai berikut:

$$\sigma(x) = \sqrt{\sum_{i=1}^{n} \left(x_i - \mu(x)\right)^2} \ dan$$

$$\sigma(y) = \sqrt{\sum_{i=1}^{n} (y_i - \mu(y))^2} \ \dots\dots\dots\dots (8)$$

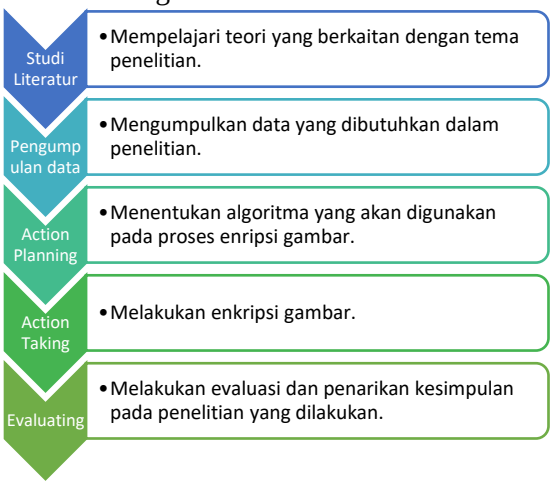
Jika koefisien korelasi sama dengan satu, berarti *plain image* dan *cipher image* identik. Jika korelasi koefisien sama dengan nol, berarti *cipher image* sangat berbeda dari *plain image* yang berarti hasil enkripsinya baik [20].

3. Metode Penelitian

Metode penelitian yang dilakukan pada penelitian ini adalah pendekatan kuantitatif,

yaitu pendekatan yang bersifat sistematis dan menggunakan model model yang bersifat matematis.

Alur penelitian yang dilakukan pada penelitian ini dapat dilihat pada gambar dibawah sebagai berikut :



Gambar 1. Alur penelitian

3.1. Pengumpulan Data

Data yang digunakan dalam penelitian ini dikumpulkan menggunakan metode generate (membuat data) yang berupa desain gambar/citra. Citra yang digunakan adalah citra grayscale dengan resolusi 256px x 256px. Resolusi citra yang digunakan merupakan resolusi yang banyak digunakan untuk penelitian [2].

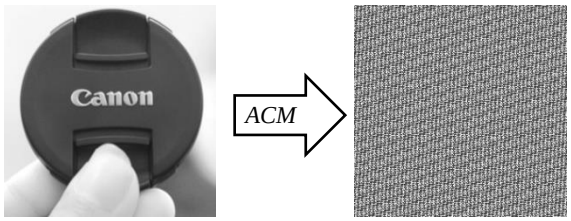
Gambar 2. Sampel citra

3.2. Action Planning

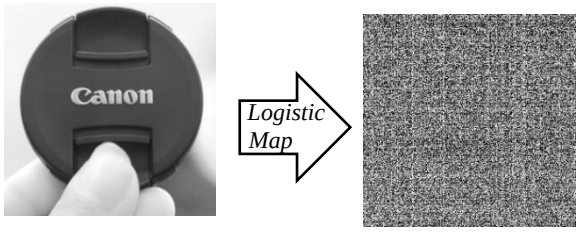
Tahap ini adalah tahap perancangan kegiatan yang akan dilakukan pada penelitian ini dengan menentukan metode yang akan digunaka, serta pembahasan mengenai proses pada metode tersebut.

3.3. Action Taking

Action taking adalah proses implementasi dari metode yang telah dijelaskan pada bagian 2.3 dan 2.4 dengan data yang telah disiapkan pada bagian 3.1.



Gambar 3. Hasil *arnold cat map*



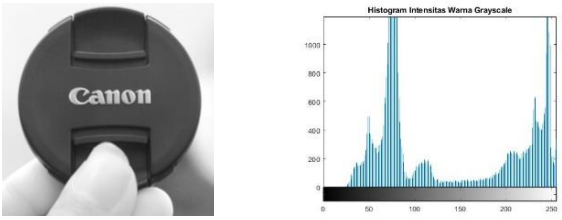
Gambar 4. Hasil *logistic map*

3.4. Evaluating

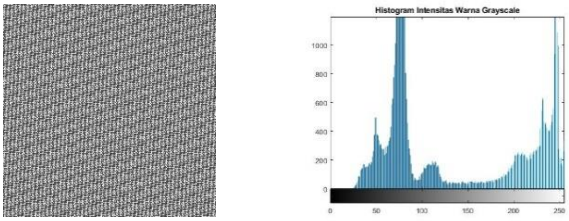
Tahap ini adalah proses pengujian terhadap citra hasil enkripsi dengan membandingkan histogram, melakukan analisis diferensial dan koefisien korelasi.

3.4.1 Analisis Histogram

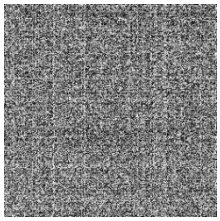
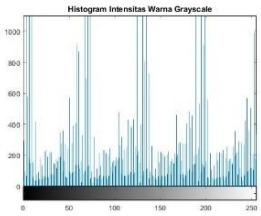
Histogram dianalisis dengan membandingkan histogram citra asli dengan histogram citra hasil enkripsi. Agar histogram tidak dapat dimanfaatkan untuk analisis terhadap frekuensi kemunculan pixel pada histogram, maka histogram dari gambar asli dan gambar yang telah terenkripsi harus berbeda atau secara statistik tidak memiliki kemiripan.



Gambar 5. Histogram citra asli



Gambar 6. Histogram *ACM*

Gambar 7. Histogram *logistic map*

3.4.2 Analisis Diferensial

Nilai *NPCR* dan *UACI* berkisar dari 0 – 100%. Jika hasil *NPCR* dari hasil enkripsi mencapai nilai 0%, maka citra asli sama persis dengan citra yang terenkripsi. Namun, ketika hasil enkripsi menghasilkan nilai *NPCR* 100%, maka keseluruhan pixel dari citra awal berbeda dengan citra terenkripsi. Sedangkan nilai *UACI* menggambarkan seberapa besar perubahan setiap pixel antara citra asli dengan citra terenkripsi, terhadap nilai maksimal yang mungkin dari pixel tersebut. Jika hasil *UACI* di atas 30%, maka rata-rata nilai pixel yang asli berbeda cukup jauh dengan pixel yang terenkripsi [21].

Tabel 1. Hasil analisis differensial

Enkripsi	***NPCR***	***UACI***
ACM	0.9866	0.3349
Logistic Map	0.9960	0.3464

3.4.3 Koefisien Korelasi

Nilai koefisien korelasi maksimal 1 dalam harga mutlak. Koefisien korelasi +1 menyatakan hubungan linier (korelasi) sempurna yang naik, nilai koefisien korelasi -1 menyatakan hubungan korelasi sempurna yang menurun, sedangakan nilai diantara -1 dan +1 menyatakan derajat ketergantungan linier antara dua peubah. Nilai koefisien yang mendekati -1 atau +1 menyatakan hubungan linier yang kuat antara x dan y, sedangkan koefisien yang mendekati 0 menyatakan hubungan linier yang lemah [22].

Pada *natural image*, pixel-pixel bertetangga yang memiliki hubungan linier yang ditandai oleh koefisien korelasinya yang tinggi (mendekati +1 atau -1). Enkripsi citra yang bagus membuat korelasi antara pixel-pixel bertetangga menjadi lemah atau koefisien korelasinya mungkin mendekati nol [23].

Tabel 2. Korelasi antara dua pixel Bertetangga

Koefisien Korelasi	***Horisontal***	***Vertikal***	***Diagonal***
Plain-image	0.9915	0.9935	0.9864
Cippher-image ACM	0.0224	-0.0271	-0.0164
Cippher-image Logistic map	0.0205	0.0229	-0.0060

Tabel 3. Koefisien korelasi terhadap citra asli

Enkripsi	**Koefisien Korelasi**
ACM	0.0013
Logistic Map	0.0075

4. Kesimpulan dan Saran

Dari hasil analisis histogram dan diferensial dapat ditarik kesimpulan sebagai berikut:

1. Dari hasil enkripsi kedua algoritma menunjukkan visual citra yang susah ditebak dan berbeda jauh dari citra aslinya.
2. Histogram hasil enkripsi *ACM* tidak berbeda jauh dari histogram citra asli, sedangkan histogram *logistic map* terlihat berbeda dengan histogram citra asli dan cenderung datar serta secara statistik memiliki distribusi yang lebih seragam.
3. Nilai *NPCR* dari kedua algoritma menunjukkan nilai diatas 90%, sudah menunjukkan nilai yang bagus untuk keamanan, namun nilai *NPCR* dari algoritma *logistic map* lebih besar dari *ACM.*
4. Nilai *UACI* dari kedua algoritma menunjukkan nilai diatas 30%, menunjukkan rata-rata nilai pixel yang cukup jauh dengan pixel citra asli, namun nilai *UACI* dari algoritma *logistic map* lebih besar dari *ACM.*
5. Nilai korelasi antara dua pixel beretetangga menunjukkan hasil yang cukup jauh dari angka 1 dan algoritma *logistic map* lebih unggul dari *ACM.*
6. Koefisien korelasi terhadap citra asli juga menunjukkan hasil yang jauh dari angka 1, namun algoritma *ACM* lebih unggul dari *logistic map.*
7. Pada penelitian ini berkesimpulan bahwa hasil pengujian menunjukkan algorima *logistic map* lebih unggul dari *ACM.*

Untuk penelitian selanjutnya penulis dapat memberikan saran sebagai berikut:

1. Menggunakan ukuran citra yang bervariasi.
2. Melakukan enkripsi pada citra yang berwarna.
3. Menganalisa hasil enkripsi jika kedua algoritma digabungkan.

Daftar Pustaka

[1] Sudirman. 2017. Analisis Enkripsi Citra Digital Menggunakan Algoritma Logistic Map Dengan Algoritma Kompresi Lampel-Ziv-Welch (Lzw). InfoTekJar- Jurnal Nasional Informatika dan Teknologi Jaringan, 1(2), 95-99.

[2] Handoyo, A. E., Rachmawanto, E. H., Sari, C. A., & Susanto, A. 2018. Teknik Penyembunyian dan Enkripsi Pesan pada Citra Digital dengan Kombinasi Metode LSB dan RSA. Jurnal Teknologi dan Sistem Komputer, Vol. 6, No. 1, 37-43.

[3] Chang, C.-C., Hwang, M.-S & Chen, T.-S. 2001. A New Encryption Algorithm For Image Cryptosystems. The Jurnal Of Systems And Software 58 : 83-91.

[4] Sidik, A., Hakim, Z., & Permana, E. A. 2014. Analisis Dan Implementasi Teknik Steganografi Sebagai Fasilitas Pengamanan Proses Pengiriman File Secara Online. Jurnal Sisfotek Global, Vol. 4, No. 1.

[5] Warnilah, A. I., & Nugraha, S. N. 2018. Komparasi Algoritma Kriptografi Elgamal Dan Caesar Cipher Untuk Enkripsi Dan Dekripsi Pesan. IJCIT, Vol. 3, No. 2, 243-252.

[6] Kromodimoeljo, S. 2009. Teori dan aplikasi kriptografi. SPK IT Consulting.

[7] Cahya, I.N., 2015. Penyisipan Pesan Pada Gambar Menggunakan Algoritma Arnold Cat Map (Acm), Least Significant Bit (Lsb) Dan Scale Invariant Feature Transform (Sift). Skripsi, Fakultas Ilmu Komputer.

[8] Munir, R. 2012. Analisis Keamanan Algoritma Enkripsi Citra Digital Menggunakan Kombinasi Dua Chaos Map dan Penerapan Teknik Selektif. JUTI Jurnal Ilmiah Teknologi Informasi, 10(2), 89-95.

[9] Sutoyo, T, dkk. 2009, Teori Pengolahan Citra Digital, Penerbit Andi, Yogyakarta.

[10] Andrian, Y. 2014. Perbandingan Penggunaan Bilangan Prima Aman Dan Tidak Aman Pada Proses Pembentukan Kunci. Creative Information Technology Journal, Vol. 1, No. 3, 194-203.

[11] Ariyus, D. 2008. Pengantar Ilmu Kriptografi, Penerbit Andi, Yogyakarta.

[12] Zebua, T. 2015. Penerapan Metode LSB-2 untuk Menyembunyikan Ciphertext pada Citra Digital. Pelita Inform. Budi Darma, Vol. 10, No. 3, 135–140.

[13] Sari, C. A, dkk. 2016. Penyembunyian Data Untuk Seluruh Ekstensi File Menggunakan Kriptografi Vernam Cipher dan Bit Shiffting. Journal of Applied Intelligent System, Vol. 1, No. 3, 179-190.

[14] Wijaksono, B.A., 2017. Steganografi pada Citra Digital dengan Metode Cat Map dan Outguess. STRING (Satuan Tulisan Riset dan Inovasi Teknologi), Vol. 1, No. 3, 317-324.

[15] A. Jolfaei, A. Mirghadri. 2010. An Image Encryption Approach Using Chaos and Stream Cipher. Journal of Theoretical and Applied Information Technology.

[16] Hongmei, T., Liying, H., Yu, H., Xia, W., (2010), An Improved Compound Image Encryption Scheme, Proceeding of 2010 International Conference on Computer and Communication Technologies in Agriculture Engineering.

[17] PUTRI, E. Y. 2018. Implementasi Vigenere Cipher Pada Penyandian Citra Berbasis Pembangkitan Kunci Algoritma Advanced Encryption Standard (Aes).

[18] Wu, Yue., J. P. Noonan., dan S. Agaian. 2011. NPCR and UACI Randomness Tests for Image Encryption. Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), 31-38.

[19] Boriga, R. E., A. C. Dăscălescu, dan A. V. Diaconu. 2014. A New Fast Image Encryption Scheme Based on 2D Chaotic Maps. IAENG International Journal of Computer Science, 41(4):1-10.

[20] Mousa, A., O. S. F. Allah., dan E. S. M. Nigm. 2013. Security Analysis of Reverse Encryption Algorithm for Databases. International Journal of Computer Applications, 66(14):19-27.

[21] Dharmaadi, I. P. A., Barmawi, A. M., & Gandeva Bayu, S. 2013. Enkripsi Gambar Parsial dengan Kombinasi Metode Stream Cipher RC4 dan Chaotic Function. Universitas Telkom, Bandung.
[22] Rinaldi Munir, 2012. Algoritma Enkripsi Citra dengan Kombinasi Dua Chaos Map dan Penerapan Teknik Selektif Terhadap Bit-bit MSB. Prosiding Seminar Nasional dan Aplikasi Teknologi Informasi (SNATI). Universitas Islam Indonesia Yogyakarta.
[23] Munir, R. 2012. Algoritma enkripsi selektif citra digital dalam ranah frekuensi berbasis permutasi chaos. Jurnal Rekayasa Elektrika. Vol, 10(2), 66-72.