Enkripsi Citra Digital Menggunakan Fungsi Chaos Ikeda dan Henon

Suryadi MT[1], Hagi Andi Manurung[2], Yudi Satria[3]
[1,2,]3Departemen Matematika Universitas Indonesia

Abstrak. Seiring pesatnya perkembangan teknologi informasi saat ini, citra digital dengan mudah kita kirimkan kepada orang lain menggunakan internet. Akan tetapi, kemudahan tersebut bisa menjadi sebuah ancaman tindak kejahatan. Maka dari itu keamanan sebuah citra digital menjadi sangat penting agar terhindar dari ancaman tersebut. Untuk meningkatkan keamanan citra digital, dapat digunakan sebuah teknik yaitu teknik kriptografi. Pada paper ini, teknik kriptografi yang digunakan yaitu menggunakan fungsi *chaos* Ikeda dan Henon. Proses enkripsi yang dilakukan menggunakan metode pengacakan baris dan kolom dari citra aslinya menggunakan fungsi *chaos* Ikeda. Setelah itu dilanjuktan dengan proses enkripsi berikutnya dengan metode difusi atau substitusi menggunakan fungsi *chaos* Henon. Hasil analisis dari uji coba yang dilakukan diperoleh bahwa ruang kuncinya mencapai 10^{75}, sehingga algoritma ini bertahan dari serangan *bruteforce attack*. Sensitivitas kunci mencapai 10^{-15} sehingga membuat algoritma ini bertahan dari serangan *differential attack.* Histogram yang dihasilkan oleh proses enkripsi berdistribusi *uniform*. Korelasi tiap tingkat keabuan yang dihasilkan oleh dalam proses enkripsi memiliki *scatter plot* yang sangat menyebar yang berarti citra terenkripsi tidak memberikan informasi yang cukup mengenai citra asli sehingga membuat algoritma ini bertahan dari *statistical attack.*

Kata Kunci. Fungsi Ikeda, Fungsi Henon, pengacakan, difusi, Enkripsi Citra Digital

1. Pendahuluan

Perkembangan teknologi informasi pada zaman modern saat ini sangat pesat. Penyampaian pesan yang kita buat, dengan mudah kita dikirimkan kepada orang lain melalui media elektronik dalam bentuk data digital. Kemudahan tersebut menjadi suatu ancaman bagi diri kita sendiri maupun orang lain, karena data yang kita kirimkan dapat dicuri atau disalahgunakan oleh pihak yang tidak bertanggung jawab. Oleh karena itu keamanan atau kerahasiaan suatu data menjadi hal yang sangat penting untuk menghindari ancaman tersebut.

Terdapat cara untuk meningkatkan kerahasiaan atau keamanan suatu data yaitu menggunakan Teknik kriptografi. Kriptografi adalah salah satu cabang ilmu pengetahuan yang mempelajari teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan suatu data, keabsahan data, integritas data, serta autentikasi data [13]. Teknik kriptografi ini dapat digunakan pada berbagai macam data digital seperti video, audio , citra digital dan lain sebagainya. Pada penelitian ini, difokuskan pada data digital yaitu citra digital.

Dalam menggunakan Teknik kriptografi pada citra digital ataupun data lainnya, terdapat 2 buah proses yang dilakukan yaitu proses enkripsi dan dekripsi. Proses enkripsi adalah proses mengubah citra asli (*plain image*) menjadi citra terenkripsi (*cipher image*). Sebaliknya, proses dekripsi adalah proses mengubah citra terenkripsi (*cipher image*) menjadi citra asli (*plain image*). Didalam proses enkripsi dan dekripsi dibutuhkan sebuah *key* yang hanya diketauhi oleh pengirim dan penerima pesan [21]. Secara sederhana, didalam proses enkripsi dan dekripsi menggunakan skema acak baris dan kolom serta difusi. Acak baris dan kolom adalah menukar posisi dari elemen data ke elemen data yang lain, sedangkan difusi adalah pengubahan nilai dari elemen-elemen data tersebut.
Teknik kriptografi yang banyak digunakan untuk data citra digital yaitu menggunakan fungsi *chaos*. Fungsi *chaos* adalah fungsi yang bersifat acak, sensitif terhadap nilai awal, dan ergodicity [4, 12]. Dimana fungsi *chaos* ini membangkitan barisan bilangan acak yang akan digunakan pada proses acak baris dan kolom serta difusi. Pada penelitian sebelumnya sudah banyak penggunaan fungsi *chaos* untuk membangkitkan bilangan acak dalam proses kriptografi seperti penggunaan beberapa fungsi chaos termasuk fungsi logistic dan modifikasinya [1 – 3, 6, 16 – 19], penggunaan fungsi Henon hanya pada tahap difusi dalam proses enkripsi citra digital [5, 8]. Selain itu terdapat penelitian sebelumnya yang menggunakan fungsi Ikeda dalam proses enkripsi pada tahap acak baris dan kolom serta pada tahap difusi [10]. Juga penelitian dengan menggunakan dua buah fungsi dalam proses kriptografi seperti pengamanan citra digital dengan skema difusi-transposisi bebasis *chaos* dengan fungsi *chaos* yang digunakan adalah *Logistic Map* pada tahap difusi dan *Arnold's Cat Map* pada tahap transposisi [20].

Selanjutnya dalam paper ini akan dibahas terkait pengamanan enkripsi citra digital menggunakan dua buah fungsi chaos yaitu fungsi chaos Ikeda dan fungsi chaos Henon untuk membangkitkan barisan bilangan acak yang akan digunakan pada tahap pengacakan baris kolom serta difusi. Tahap pengacakan baris dan kolom dari citra asli menggunakan barisan key stream yang dihasilkan dari fungsi chaos Ikeda. Selanjutnya dilakukan tahap difusi dengan barisan key stream yang dihasilkan dari fungsi chaos Henon. Kinerja algoritma yang dihasilkan tersebut selanjuntya di ukur berdasarkan analisis sensitivitas kunci (nilai awal), ukuran ruang kunci yang dihasilkan, dan analisis histogram serta analisis korelasi. Hal tersebut dilakukan untuk mengukur tingkat ketahanan terhadap berbagai serangan yaitu *brute force attack, differential attack,* dan *statistical attack*.

2. Metode Penelitian

Teknik kriptografi melibat dua (2) proses utama yakni proses enkripsi dan dekripsi. Proses enkripsi yaitu melakukan proses perubahan dari *plain-image* (citra asli) menjadi *cipher-image* (citra tersandikan). Sedangkan proses dekripsi merupakan proses kebalikan dari proses enkripsi, yakni merubah cipher-image menjadi plain-image. Dalam paper ini, mengacu kepada konsep pemrosesan citra digital [7, 9] dan juga konsep operasi antar bit dari setiap intensitas citra digital [14] serta metode perubahan yang dilakukan menggunakan metode pengacakan baris dan kolom dari citra aslinya serta dilanjutkan dengan metode difusi yang menggunakan beberapa parameter dan nilai awal.

Dalam melakukan tahapan pengacakan baris dan kolom serta tahapan difusi, digunakan fungsi chaos Ikeda dan fungsi chaos Henon. Adapun bentuk fungsi chaos Ikeda yang dimaksud ialah dalam bentuk rekursif didefinisikan sesuai dengan persamaan (1) [11, 15].

$$\begin{aligned} X_{n+1} &= 1 + U.(X_n \cos t_n - Y_n \sin t_n) \\ Y_{n+1} &= U.(X_n \cos t_n - Y_n \sin t_n) \\ t_n &= 0.4 - 6/(1 + X_n^2 + Y_n^2) \end{aligned} \quad (1)$$

dengan nilai $U,\ X_n\ dan\ Y_n \in \mathbb{R}$ dengan $X_0\ dan\ Y_0$ adalah nilai awal serta $U \in [0.5\ ,0.95]$. Sedangkan bentuk fungsi chaos Henon dalam bentuk rekursif didefinisikan sesuai dengan persamaan (2) [11, 15].

$$X_{n+1} = 1 - aX_n^2 + Y_n \quad (2)$$

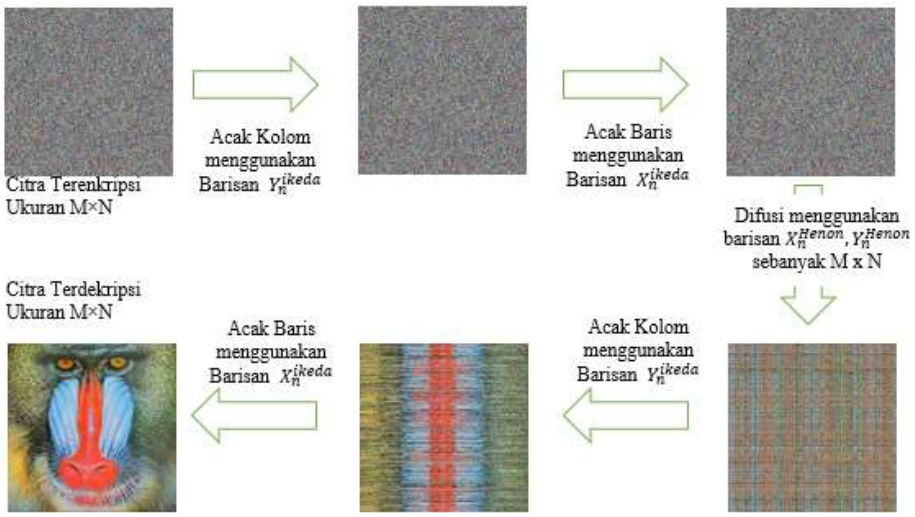
$$Y_{n+1} = bX_n$$

dengan $a = 1.4$, $b = 0.3$ serta $X_n \; dan \; Y_n \in \mathbb{R}$.

Untuk selanjutnya, guna membedakan notasi $X_n \; dan \; Y_n$ dari hasil fungsi chaos Ikeda dan fungsi chaos Henon maka dinotasikan sebagai X_n^{Ikeda}, Y_n^{Ikeda} dan X_n^{Henon}, Y_n^{Henon}.
Nilai parameter dan nilai awal tersebut berperan sebagai kunci enkripsinya. Teknik kriptografi yang digunakan dalam paper ini menggunakan teknik simetris, sehingga kunci untuk proses dekripsi harus sama dengan kunci enkripsi.

Secara umum model operasional untuk proses enkripsi dan dekripsi dapat dilihat pada Gambar 1 dan Gambar 2.

Gambar 1. Model Operasional untuk Proses Enkripsi



Gambar 2. Model Operasional untuk Proses Dekripsi

Berdasarkan model operasional sesuai Gambar 1 dan Gambar 2 dilakukan simulasi terhadap data uji. Data uji citra digital yang digunakan dalam paper ini adalah citra digital Baboon.bmp mode *RGB* berukuran 128×128, 256×256, dan 512×512 sebagai *plain-image*. Nilai awal yang digunakan sebagai kunci pada proses enkripsi pada data uji selalu sama yaitu $X_0^{Ikeda} = 0.857737$, $Y_0^{Ikeda} = 0.857736$, $U = 0.857735$, $X_0^{Henon} = 0.00001$, dan $Y_0^{Henon} = 0.00001$

3. Hasil Penelitian

3.1. Analisis Sensitivitas Kunci

Algoritma enkripsi berbasis fungsi chaos yang baik, harus sensitif terhadap nilai awal yang digunakan. Perubahan yang sangat kecil pada nilai awal proses enkripsi akan mengakibatkan perubahan yang sangat berbeda pada hasil atau outputnya. Hal tersebut Nampak pada hasil uji coba seperti tampak pada Gambar 3 dan Gambar 4.

(a) (b) (c) (d)

Gambar 3. Hasil dekripsi Baboon.bmp dengan perubahan kunci:
(a) kunci $X_0^{Ikeda} + 10^{-14}$, (b) kunci $X_0^{Ikeda} + 10^{-15}$, (c) kunci $X_0^{Ikeda} + 10^{-16}$, (d) kunci $X_0^{Ikeda} + 10^{-17}$

Tampak pada Gambar 3 (a) dan (b), nilai awal kunci pada proses dekripsi yang berbeda sangat kecil dalam hal ini dengan mencapai 10^{-14} dan 10^{-15} dari nilai awal kunci pada proses enkripsi, diartikan sebagai nilai awal kunci yang berbeda. Sehingga hasil dekripsinya tidak mampu menampilkan citra aslinya. Sedangkan pada Gambar 3 (c) dengan selisih mencapai 10^{-16}. Berarti algoritma enkripsi citra dengan fungsi chaos Ikeda memiliki tingkat sensitivitasnya mencapai 10^{-15}.

(a) (b) (c) (d)

Gambar 4. Hasil dekripsi Baboon.bmp dengan perubahan kunci
(a) kunci $U + 10^{-15}$, (b) kunci $U + 10^{-16}$, (c) U+10^{-17}, (d) kunci $U + 10^{-18}$

Sedangkan untuk Gambar 4 (a) dan (b), nilai kunci U pada proses dekripsi yang berbeda sangat kecil dalam hal ini dengan mencapai 10^{-15} dan 10^{-16} dari nilai kunci U pada proses enkripsi, diartikan sebagai nilai awal kunci yang berbeda. Sehingga hasil dekripsinya tidak mampu menampilkan citra aslinya. Sedangkan pada Gambar 4 (c) dengan selisih mencapai 10^{-17}. Berarti algoritma enkripsi citra dengan fungsi chaos Ikeda memiliki tingkat sensitivitasnya pada parameter U mencapai 10^{-16}. Hal tersebut menunjukkan bahwa algoritma ini tahan terhadap *brute-force attack*.

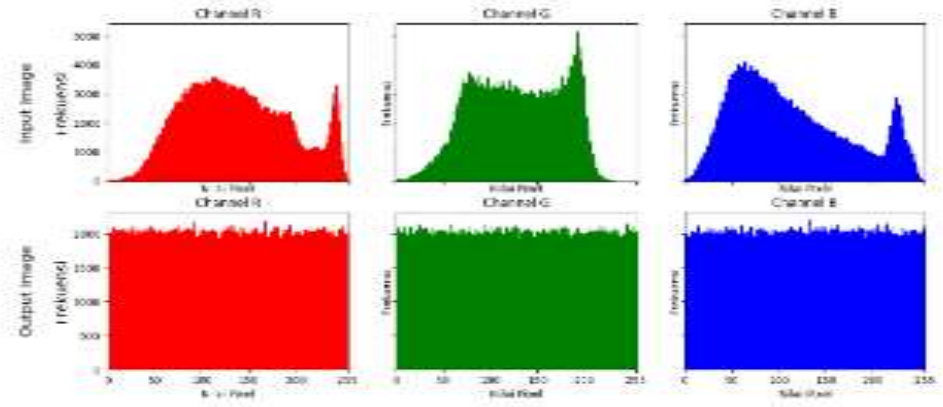
3.2. Ukuran Ruang Kunci

Kunci yang digunakan pada fungsi Ikeda yaitu $X_0^{Ikeda}, Y_0^{Ikeda}, U$ dimana nilai U terletak pada interval $[0.5, 0.95]$ dan kunci yang digunakan pada fungsi Henon yaitu X_0^{Henon}, Y_0^{Henon} dengan $X_0^{Ikeda}, Y_0^{Ikeda}, U, X_0^{Henon}, Y_0^{Henon} \in \mathbb{R}$. Dengan menggunakan level presisi *double precission*, dengan

standar IEEE presisinya maka ruang kunci untuk setiap variabel real sebesar 10^{15}. Sehingga ruang kunci dari algoritma enkripsi ini dengan 5 variabel real tersebut mencapai $10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} = 10^{75}$. Sehingga untuk bisa menemukan kunci agar citra terenkripsi dapat diperoleh citra asli probilitasnya (secara *exhaustive key search*) sangat kecil yakni 10^{-75}. Dengan demikian algoritma ini tahan terhadap *brute-force attack*.

3.3. Analisis Histogram dan Uji Goodness of fit

Hasil uji coba analisis histogram menggunakan data uji babbon.bmp berukuran 512 x 512 menghasil histogram citra terenkripsinya berbentuk relatif datar. Hal tersebut menunjukkan bahwa distribusi dari frekuensu intensitas piksel citra terenkripsi relative sama (*uniform*). Bentuk histogram tersebut tampak pada Gambar 5.



Gambar 5. Histogram citra asli (baris pertama) dan Histogram citra terenkripsi (baris kedua)

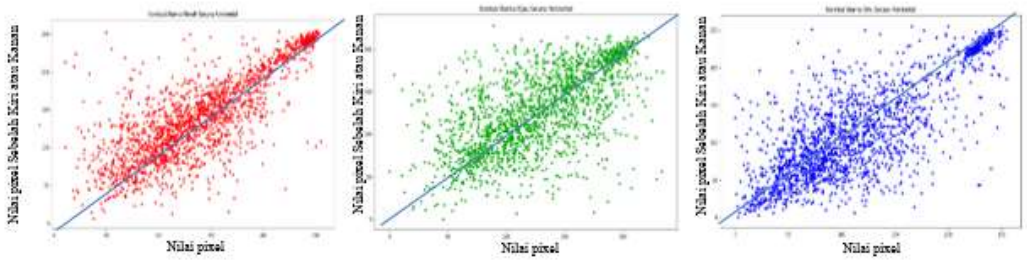
Secara uji statistik dengan menggunakan uji *Goodness of fit* dengan tingkat kepercayaan $\alpha = 1\%$ dan derajat bebasnya 255 (256 – 1) diperoleh nilai kritisnya sebesar 310.4574 (dari tabel *chi-square*) [22]. Berdasarkan hasil uji coba diperoleh bahwa nilai statistik uji dari citra terenkripsi (lihat Tabel 1) semuanya lebih kecil dari nilai kritisnya. Hal tersebut berarti bahwa intensitas piksel semua citra terenkripsi dari seluruh data uji berdistribusi *uniform*. Sehingga algoritma yang dikembangkan ini tahan terhadap *statistical attack*.

Tabel 1. Nilai Statistik Uji

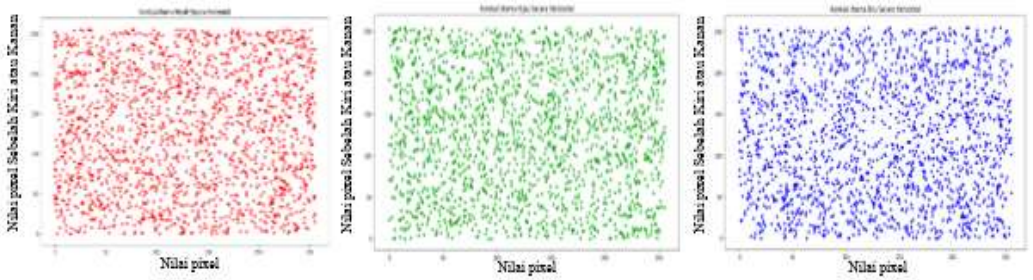
Citra	Ukuran	Ikeda Henon		
		Red	Green	Blue
baboon	128	259.1563	252.8438	265.8125
	256	232.3281	256.8906	270.2031
	512	246.0176	245.3613	307.8477

3.4. Analisis Korelasi

Pengujian ini dilakukan dengan melihat scatter plot antara 2 buah pixel yang bersebelahan pada citra terenkripsi dan menghitung nilai keofisien korelasi antara 2 *pixel* bersebelahan secara acak. Berikut *scatter plot* yang dihasilkan oleh nilai *pixel* citra asli dan citra terenkripsi yang berdekatan secara horizontal pada tiap tingkat keabuan yang disajikan pada Gambar 9 sampai Gambar 4.12



Gambar 6. *Scatter Plot* Nilai *Pixel* Citra Asli Secara Horizontal



Gambar 7. Nilai *Pixel* Citra Terenkripsi Secara Horizontal

Berdasarkan Gambar 6 *scatter plot* yang dihasilkan dari citra asli, terlihat bahwa seluruh titik berkumpul mendekati garis $y = x$ yang berarti nilai *pixel* yang bersebelahan secara horizontal pada tiap tingkat keabuan hampir sama. Namun, pada Gambar 7 *scatter plot* secara umum yang dihasilkan dari citra terenkripsi dengan tiap algoritma yang digunakan, seluruh titik menyebar tidak membentuk suatu pola yang berarti nilai *pixel* yang bersebelahan secara horizontal pada tiap tingkat keabuan sangat berbeda. Hal ini menunjukan bahwa citra terenkripsi tidak memberikan informasi yang cukup mengenai citra asli. Sehingga algoritma yang dikembangkan ini tahan terhadap *statistical attack*.

Analisis Ruang Kunci

Berdasarkan rata - rata waktu yang dibutuhkan untuk *Exhaustive Key Search* pada Tabel 2, dengan menggunakan komputer yang mampu melakukan operasi 10^{12} operasi per detik, pada algoritma ini memiliki waktu yang dibutuhkan untuk mencoba semua kunci yaitu 1.15×10^{58} hari dengan ruang kunci sebesar 10^{75}, Maka ruang kunci dari algoritma yang diuji coba pada penelitian ini cukup besar sehingga dapat bertahan dari serangan *bruteforce attack.*

Tabel 2. Rata-rata waktu yang Dibutuhkan Untuk Exhaustive Key Search

Ruang Kunci	Operasi per Detik	Waktu yang Dibutuhkan	
		Detik	Hari
10^{75}	10^{6}	10^{69}	1.15×10^{64}
	10^{9}	10^{66}	1.15×10^{61}
	10^{12}	10^{63}	1.15×10^{58}

4. Kesimpulan dan Saran

Berdasarkan hasil uji coba dengan data uji yang digunakan diperoleh kesimpulan bahwa ukuran ruang kuncinya mencapai 10^{75} sehingga memilki ketahanan yang sangat baik terhadap *brute-force attack*. Sensitivitas nilai awalnya sebesar 10^{-15} dan sensitivitas parameter mencapai 10^{-16} sehingga memilki ketahanan yang sangat baik terhadap *brute-force attack*. Uji histogram menunjukkan berdistribusi *uniform* pada citra terenkripsi baik secara visual histogram maupun secara uji statistik *Goodness of fit*. Koefisien korelasi yang dihasilkan menunjukkan bahwa citra terenkripsi tidak memberikan informasi yang cukup mengenai citra asli. Sehingga berdasarkan dua uji terakhir menunjukkan bahwa algoritma ini memiliki ketahanan yang baik terhadap *statistical attack*.

5. Daftar Pustaka

[1] Ahmad, J., & Ahmed, F. 2012. Efficiency Analysis and Security Evaluation of Image Encryption Schemes. *International Journal of Video&Image Processing and Network Security*. Vol. 12 . No.4. pp.18-31

[2] A. Jolfaei, A. Mirghadri. 2010. An Image Encryption Approach Using *Chaos* and Stream Cipher. *Journal of Theoretical and Applied Information Technology*. Vol. 19 No. 2. 1446

[3] C. Fu, J. Chen, H.zou, W. Meng, Y. Zhan, Y.yu. 2012. A *Chaos*-based Digital Image Encryption Scheme with an improved Difusion Strategy. *Journal Optic Express* Vol. 20. No. 3. pp. 2363 - 2378

[4] Devaney, R.L. 1989. *An Introduction to Chaotic Dynamical Systems*. Boston: Addison Wesley

[5] Edi S., Suryadi MT, M. Agus M. 2014. The Implementation of Henon Map Algorithm for Digital image Encryption.*TELKOMNIKA*. Vol.12. No.3. pp. 651- 656

[6] Eva Nurpeti and Suryadi MT, (2013), Chaos-based Encryption Algorithm for Digital Image, Proceedings IndoMS International Conference on Mathematics and its Applications, Yogyakarta, pp. 169-177.

[7]. Gonzalez, R.C. dan R.E. Woods. 2008. *Digital Image Processing, 3rd ed.*, Prentice all, Upper Saddle River, NJ

[8] M. Henon. 1976. A two-dimensional mapping with a strange attractor. *Communications in Mathematical Physics*. vol. 50. no. 1. pp. 69–77.

[9] Hirsch, M.W., Smale, S. dan R.L. Devaney. 2004. *Differential Equations, Dynamical Systems, and an Introduction to Chaos Second Edition*. An Imprint of Elsevier. San Diego, California.

[10] Jia, X. 2010. Image Encryption using the Ikeda map. *International Conference on Intelligent Computing and Cognitive Informatics*. pp. 455-458.

[11] K. Ikeda. 1979. Multiple-valued stationary state and its instability of the transmitted light by a ring cavity system. *Optics Communications*. vol. 30. no. 2. pp. 257–261

[12] Kocarev, L. dan Shiguo Lian. 2011. *Chaos-Based Cryptography*. Berlin Heidelberg: Springer-Verlag

[13] Menezes, A.J., van Oorschot, P.C., dan Vanstone, S.A. 1997. *Handbook of Applied Cryptography (Discrete Mathematics and Its Applications) 1st Edition*. CRC Press.

[14] Rosen, K. H. 2012. *Discrete Mathematics and It's Aplication* (7th Ed). New York. McGrawHill.

[15] Sekertekin Y., Atan.O. 2016. An Image Encryption Algorithm Using Ikeda and Henon Chaotic Maps. *Telfor*. pp. 1-4

[16] Suryadi MT, Eva Nupeti, and Dhian Widya, (2014), Performance of Chaos-Based Encryption Algorithm for Digital Image, *TELKOMNIKA Indonesian Journal of Electrical Engineering*. accredited **A** by DIKTI, Decree No: 58/DIKTI/Kep/2013, Scopus Indexed, 12(3), pp. 675-682.

[17] Suryadi MT, dan Dhian Widya, (2014), *Aplikasi Algoritma Steganografi Citra Digital Berbasis Chaos Menggunakan Three Logistic Map*, Prosiding Seminar Nasional Matematika, FMIPA UNS Solo, Vol. 2, No. 1, pp. 344-351

[18] Suryadi MT, Maria YT & Yudi Satria. (2017), New modified map for digital image encryption and its performance, *Journal of Physics : Conference Series / IOP Publishing,* Vol. 893, 012050.
[19] Suryadi MT, dan Tony Gunawan, (2014), *Aplikasi Steganografi Citra Digital Menggunakan Algoritma Gingerbreadman Map*, Prosiding Seminar Nasional KOMMIT 2014, Depok, Vol. 8, pp. 370-375
[20] Suryadi MT, Zuherman R, dan Wiwit W, (2014), *Aplikasi Algoritma Steganografi Citra Digital Menggunakan Skema Transposisi Berbasis Chaos*, Prosiding Seminar Nasional KOMMIT 2014, Depok, Vol. 8, pp. 376-380
[21] Stallings, W. 2011. *Cryptography and Network Security: Principles and Practice*, Edisi 5, Prentice Hall.
[22] Walpole, Ronald E. 2012. *Probability and Statistics for Engineers and Scientists*. Prentice Hall