JUIT Vol 1 No. 2 Mei 2022 | P-ISSN: 2828-6936 E-ISSN: 2828-6901, Page 174-182

APLIKASI ENKRIPSI CITRA DIGITAL BERBASIS CHAOS MENGGUNAKAN ALGORITMA ARNOLD'S CAT MAP

Rama Dian Syah [a*], Antonius Angga Kurniawan [b], Rizki Ariyani [c]
[a*] Ilmu Komputer dan Teknologi Informasi, rama_ds@staff.gunadarma.ac.id, Universitas Gunadarma
[b] Teknologi Industri, anggaku@staff.gunadarma.ac.id, Universitas Gunadarma
[c] Ilmu Komputer dan Teknologi Informasi, rizkiariyani@staff.gunadarma.ac.id, Universitas Gunadarma

ABSTRAK

The rapid development of technology can lead to vulnerabilities in data and information. Everyone can access that data and information and disseminate it easily through the internet. The data and information can be in the form of text, video, audio, and images that may be confidential. To prevent misuse and unauthorized access to this confidential data and information, a technique is needed to enhance the security of the data. One of these techniques is by encrypting data. This technique is used to encode data in such a way that the security of the information is maintained and it cannot be read without being decrypted first. The encryption technique that has been developed involves implementing chaos theory, one of which uses the Arnold's Cat Map algorithm. This algorithm is applied in the process of encrypting and decrypting digital images with png and bmp extensions. The results of this trial show that the image files can be encrypted and decrypted properly. The time obtained is directly proportional to the size of the image.

Keywords: Encryption Algorithm, Chaos Function, Arnold's Cat Map, Digital Image.

Abstrak

Perkembangan teknologi yang sangat pesat dapat menyebabkan kerentanan pada suatu data dan informasi. Semua orang dapat memperoleh data dan informasi tersebut dan disebarluaskan dengan mudah melalui jaringan internet. Data dan informasi tersebut dapat berupa teks, video suara dan citra yang bisa bersifat rahasia. Untuk mencegah penyalahgunaan dan pengaksesan data dan informasi yang bersifat rahasia oleh orang lain yang tidak berhak maka dibutuhkan suatu teknik untuk meningkatkan keamanan data tersebut. Salah satu teknik tersebut yaitu dengan cara mengenkripsi data. Teknik tersebut digunakan untuk mengkodekan data sedemikan rupa sehingga keamanan informasinya terjaga dan tidak dapat dibaca tanpa di dekripsi dahulu. Teknik enkripsi yang telah dikembangkan yaitu dengan mengimplementasikan teori chaos, salah satunya dengan menggunakan algoritma Arnold's Cat Map. Algoritma tersebut diterapkan pada proses enkripsi dan dekripsi citra digital yang berekstensi png dan bmp. Hasil uji coba ini menunjukkan bahwa file citra tersebut dapat dienkripsi dan didekripsi kembali dengan baik. Waktu yang diperoleh berbanding lurus dengan ukuran citra.
Kata Kunci: Algoritma Enkripsi, Fungsi Chaos, Arnold's Cat Map, Citra Digital.

1. PENDAHULUAN

Pada era ini kemajuan teknologi komputer yang menyangkut komunikasi dan informasi di internet berkembang pesat. Perkembangan ini membantu manusia untuk proses pencarian dan pengiriman informasi di internet. Informasi ini bisa dengan mudah didapatkan oleh para pencari informasi. Hal ini dapat menimbulkan berbagai ancaman. Salah satu ancaman tersebut yaitu menyangkut dengan privasi manusia, baik secara individu maupun kelompok.

Untuk membatasi pengaksesan informasi oleh orang-orang yang tidak berhak maka diperlukan teknik pengamanan yang ketat supaya data/informasi digital tidak dibaca dan dipergunakan oleh orang yang tidak bertanggung jawab. Metode tersebut dinamakan kriptografi.

Pengertian secara umum dari kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan berita [1,2]. Pengertian lainnya yaitu kriptografi adalah suatu teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, otentikasi entitas dan otentikasi keaslian data [3].

Metode enkripsi sudah diterapkan oleh institusi-instusi penting di berbagai negara maupun organisasi-organisasi besar yang berbasis teknologi informasi. Salah satu teori yang digunakan pada metode enkripsi yaitu teori chaos. Teori chaos merupakan cabang ilmu matematika yang mempelajari bagaimana membangkitkan bilangan acak. Semakin acak bilangan yang dibangkitkan, semakin baik pula keamanan dari proses enkripsi. Fungsi chaos sudah diimplementasikan ke berbagai algoritma, salah satunya yaitu algoritma Arnold's Cat Map. Konsep algoritma ini adalah memutar pixel citra secara terus menerus sehingga menjadi bentuk yang tidak beraturan. Namun, bila iterasi citra sudah mencapai jumlah tertentu, citra tersebut bias kembali seperti semula.

Berdasarkan uraian diatas, maka paper ini akan menjelaskan tentang keamanan data dengan mengimplementasikan algoritma Arnold's Cat Map pada proses enkripsi dan dekripsi.

2. METODOLOGI PENELITIAN

Paper ini memiliki tujuan yakni membuat program aplikasi enkripsi citra digital berbasis chaos dengan menggunakan algoritma *Arnold's Cat Map*, maka penelitian yang dilakukan yaitu dengan mengenkripsi data berupa citra digital agar tidak bisa terbaca informasinya oleh pihak ketiga.

Proses enkripsi yang dilakukan dengan algoritma simetris. Algoritma simetris adalah algoritma kriptografi yang menggunakan kunci enkripsi yang sama dengan kunci dekripsinya. Kunci tersebut digunakan untuk mengacak piksel pada citra. Berikut persamaan enkripsi algoritma Arnold's Cat Map.

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & bc+1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} mod(N) \quad (1)$$

Dimana (x,y) posisi piksel didalam citra N x N (x_{i+1}, y_{i+1}) posisi piksel yang baru setelah transformasi, b dan c adalah bilangan bulat positif sembarang. Determinan matriks harus sama dengan 1 agar hasil transformasinya tetap berada dalam area citra yang sama. Setiap titik dalam matriks dapat ditransfomasikan ke titik lainnya. Hasil citra acak akan berbeda untuk tiap jumlah iterasi m dan berubah secara periodic sesuai dengan perubahan parameter b, c dan besarnya ukuran citra. Nilai b, c dan m adalah kunci rahasia dari algoritma transformasi ACM. Namun sesudah iterasi tertentu citra acak dihasilkan akan kembali ke citra semula, oleh karena itu ACM disebutkan memiliki periode. Sedangkan proses dekripsi ACM kebalikan dari proses enkripsinya sesuai Persamaan 2.

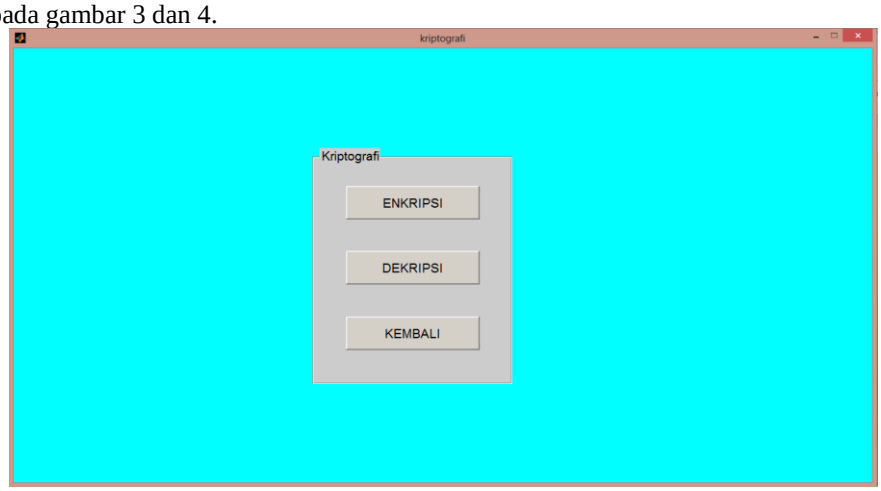
$$\begin{bmatrix} x_i \\ y_i \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & bc+1 \end{bmatrix}^{-1} \begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} mod(N) \quad (2)$$

3. HASIL DAN PEMBAHASAN

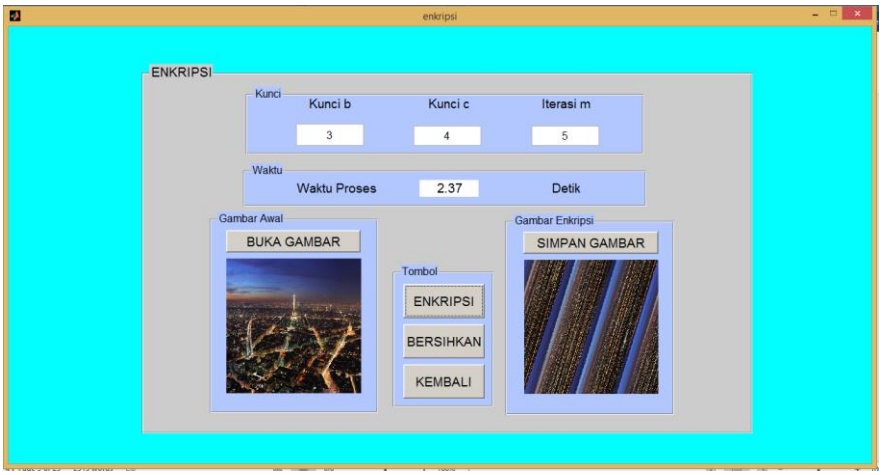
Pembangunan program aplikasinya dengan fasilitas lima menu utama yakni kriptografi, analisis, bantuan, tentang, dan keluar. Tampilan menu utama tampak pada Gambar 1.

Gambar 1. Menu Utama Program Aplikasi Enkripsi Citra

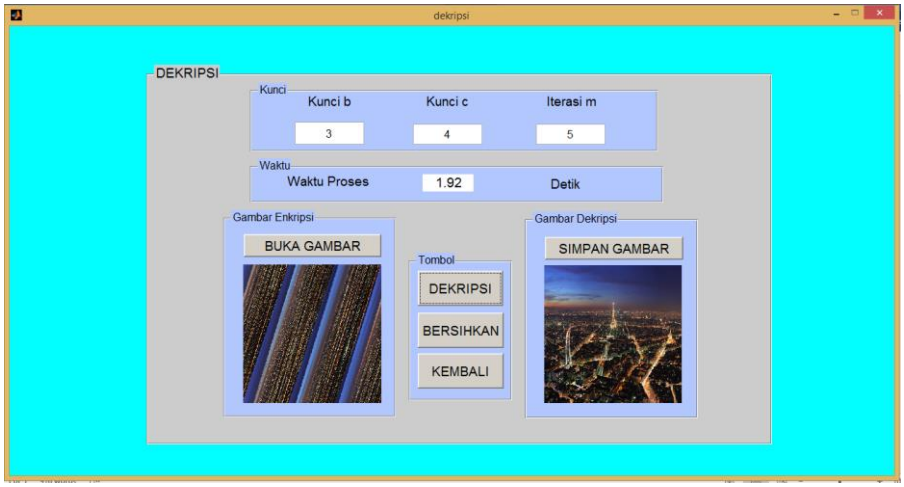
Selanjutnya submenu kriptografi tampak pada Gambar 2, halaman dari menu enkripsi dan dekripsi tampak pada gambar 3 dan 4.



Gambar 2. Submenu Kriptografi



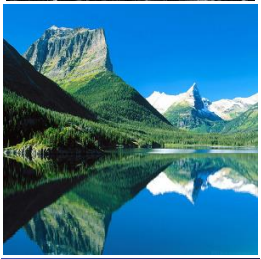
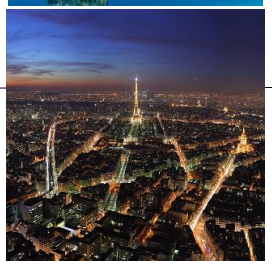
Gambar 3. Halaman menu Enkripsi



Gambar 4. Halaman menu Dekripsi

Gambar 3 dan Gambar 4 memperlihatkan menu untuk proses enkripsi dan dekripsi citra, dengan memasukkan nama file dan juga tiga nilai parameter kunci yang digunakan. Hasil yang diperoleh yaitu berupa file yang sudah terenkripsi atau yang terdekripsi beserta informasi waktu prosesnya. File hasil enkripsi dan dekripsi dapat disimpan di dalam media penyimpanan yang diinginkan. Selanjutnya dilakukan pengujian program terhadap 20 data uji berbeda ukuran, seperti pada Tabel 1.

Tabel 1. Citra Data Uji

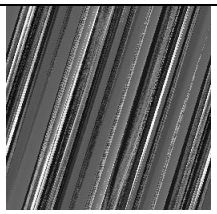
Data Uji Ke-	Tampilan Citra	Nama Citra	Ukuran Citra (*pixel*)	Ukuran File (kb)	Jenis Citra
1		G1Danau.bmp	256 × 256	192	*Grayscale*
2		G3Danau.bmp	400 × 400	468	*Grayscale*
3		G5Danau.bmp	600 × 600	1020	*Grayscale*
4		G7Danau.bmp	800 × 800	1830	*Grayscale*
5		G9Danau.bmp	1000 × 1000	2860	*Grayscale*
6		G2Eiffel.png	280 × 280	89.2	*Grayscale*
7		G4Eiffel.png	420 × 420	194	*Grayscale*
8		G6Eiffel.png	620 × 620	413	*Grayscale*
9		G8Eiffel.png	820 × 820	713	*Grayscale*
10		G10Eiffel.png	1020 × 1020	1050	*Grayscale*
11		C1Danau.bmp	300 × 300	263	*Truecolor*
12		C3Danau.bmp	450 × 450	594	*Truecolor*
13		C5Danau.bmp	650 × 650	1200	*Truecolor*
14		C7Danau.bmp	850 × 850	2060	*Truecolor*
15		C9Danau.bmp	1050 × 1050	3150	*Truecolor*
16		C2Eiffel.png	320 × 320	262	*Truecolor*
17		C4Eiffel.png	480 × 480	569	*Truecolor*

18	C6Eiffel.png	680 × 680	1080	*Truecolor*
19	C8Eiffel.png	880 × 880	1770	*Truecolor*
20	C10Eiffel.png	1080 × 1080	2620	*Truecolor*

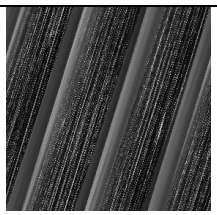
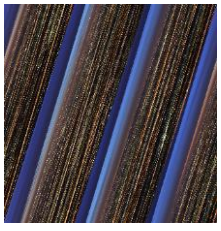
Semua data uji pada Tabel 1, dilakukan pengujian proses enkripsi dan dekripsi dengan kunci b = 3, c=4, dan m = 5, diperoleh hasil enkripsi dan dekripsinya berupa file sebagaimana tampak pada Tabel 2.

Waktu rata- rata enkripsi dan dekripsi untuk setiap data uji citra yang digunakan (Tabel 1) beserta grafiknya dengan nilai kunci yang sama, tampak pada Tabel 3 dan Gambar 5. Tampak dari Tabel 3 dan Gambar 5 proses enkripsi dan dekripsi relatif tidak jauh berbeda. Selain itu, tampak bahwa rata-rata proses enkripsi dan dekripsi berbanding lurus terhadap ukuran citra inputnya.

Tabel 2. Hasil dari Proses Enkripsi dan Dekripsi

Citra asli	**Citra Terenkripsi**	**Citra Terdekripsi**
		

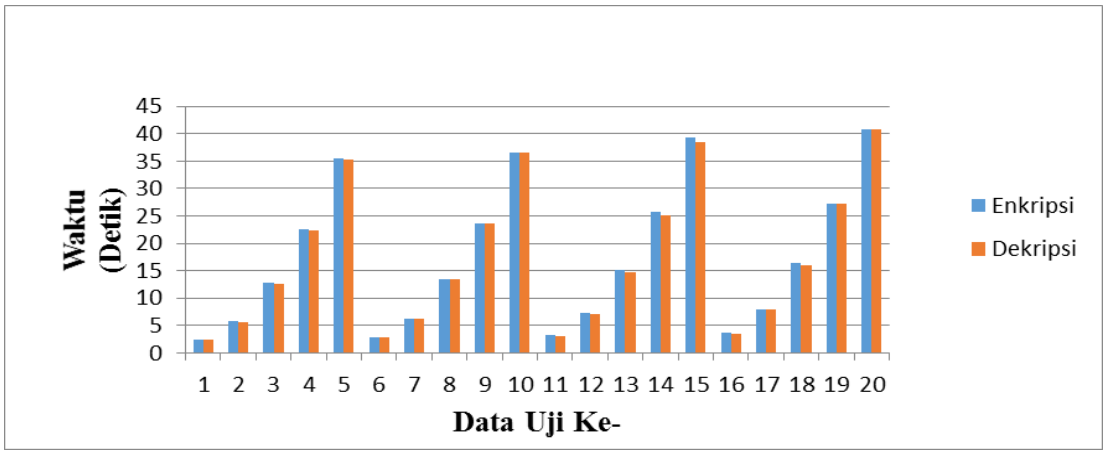
Tabel 2. Hasil dari Proses Enkripsi dan Dekripsi (lanjutan)

Citra asli	**Citra Terenkripsi**	**Citra Terdekripsi**
		
		
		

Tabel 3. Waktu Rata.rata Proses Enkripsi dan Dekripsi

Data Uji	Nama Citra	Ukuran Citra	Rata-rata Waktu Enkripsi	Rata-rata Waktu Dekripsi

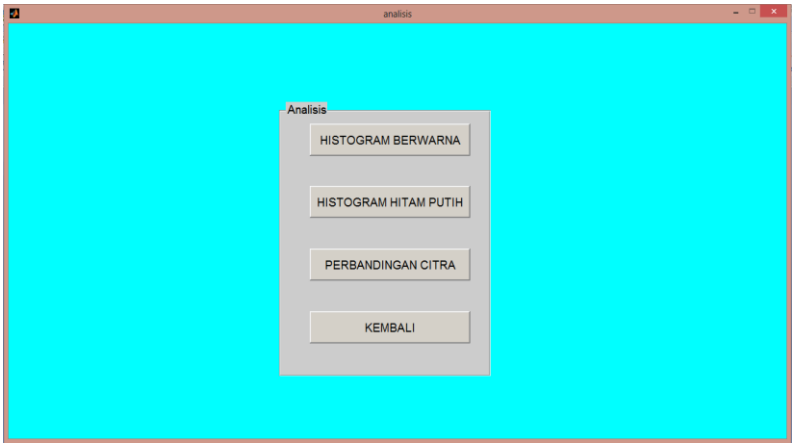
Ke-		(piksel)	(Detik)	(Detik)
1	G1Danau.bmp	256 × 256	2,33	2,33
2	G3Danau.bmp	400 × 400	5,76	5,64
3	G5Danau.bmp	600 × 600	12,74	12,58
4	G7Danau.bmp	800 × 800	22,57	22,39
5	G9Danau.bmp	1000 × 1000	35,48	35,29
6	G2Eiffel.png	280 × 280	2,75	2,73
7	G4Eiffel.png	420 × 420	6,20	6,17
8	G6Eiffel.png	620 × 620	13,45	13,52
9	G8Eiffel.png	820 × 820	23,61	23,71
10	G10Eiffel.png	1020 × 1020	36,54	36,51
11	C1Danau.bmp	300 × 300	3,22	3,14
12	C3Danau.bmp	450 × 450	7,22	7,15
13	C5Danau.bmp	650 × 650	15,07	14,78
14	C7Danau.bmp	850 × 850	25,66	25,11
15	C9Danau.bmp	1050 × 1050	39,32	38,37
16	C2Eiffel.png	320 × 320	3,70	3,54
17	C4Eiffel.png	480 × 480	8,03	7,98
18	C6Eiffel.png	680 × 680	16,33	15,94
19	C8Eiffel.png	880 × 880	27,14	27,12
20	C10Eiffel.png	1080 × 1080	40,71	40,74



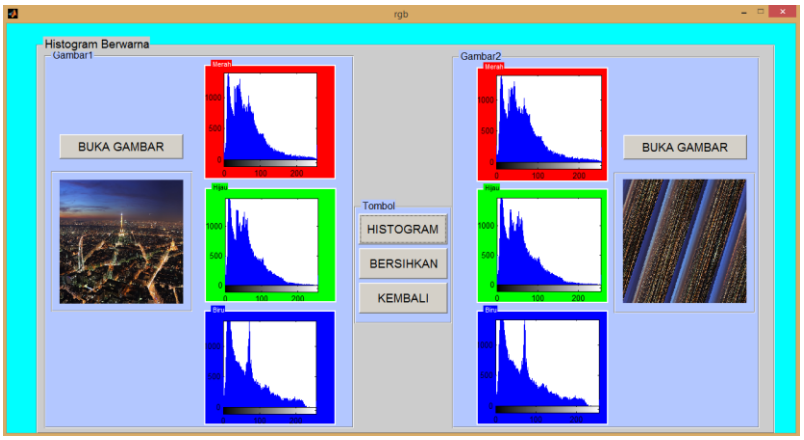
Gambar 5. Rata-rata Waktu Enkripsi dan Dekripsi Data Uji

Selanjutnya submenu analisis tampak pada Gambar 6, halaman menu histogram berwarna pada Gambar 7, halaman menu histogram hitam putih pada Gambar 8, dan halaman menu perbandingan citra pada Gambar 9.

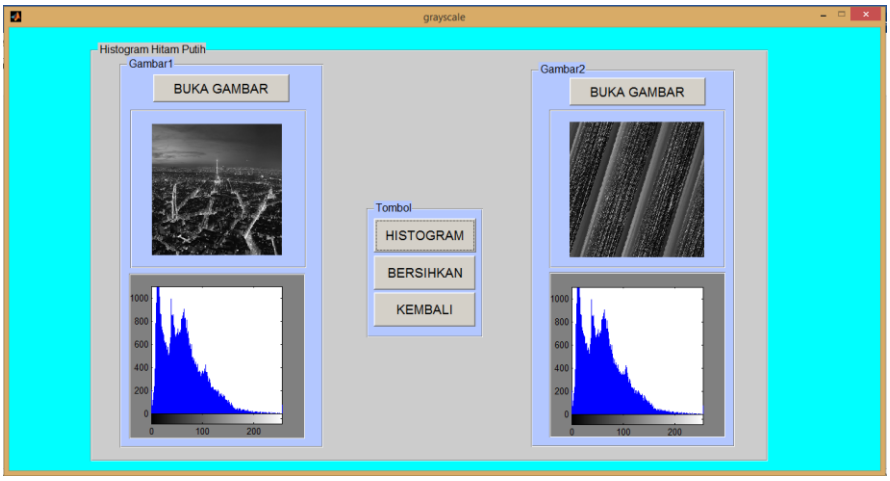
Gambar 7 dan Gambar 8 memperlihatkan perbandingan histogram citra awal dan citra terenkripsi. Histogram yang dihasilkan dari kedua citra adalah histogram yang sama karena pada proses enkripsi nilai piksel tidak berubah tetapi hanya mengacak posisi piksel. Gambar 9 memperlihatkan informasi dasar, mse, psnr, dan tingkat kesamaan dari perbandingan citra awal dan citra terdekripsi. Jika MSE = 0, PSNR = infinite, dan tingkat kesamaan = 100% maka kedua citra yang dibandingkan merupakan citra yang identik.



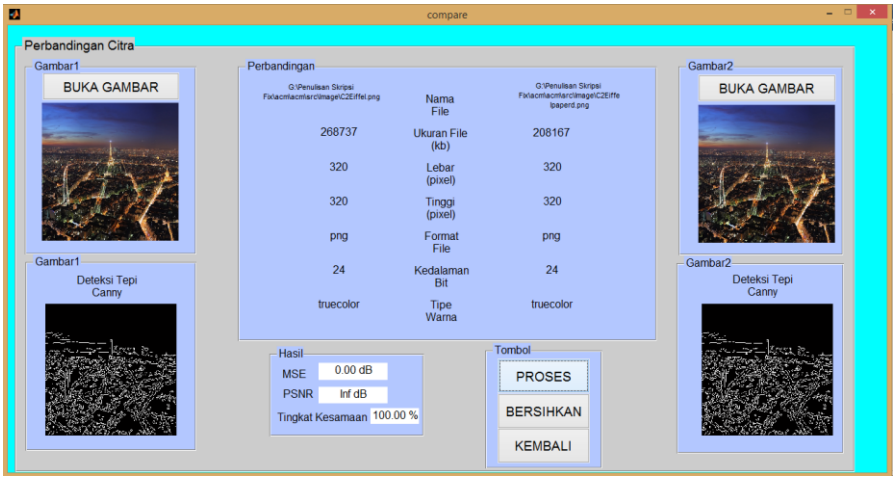
Gambar 6. Submenu Analisis



Gambar 7. Halaman Menu Histogram Berwarna

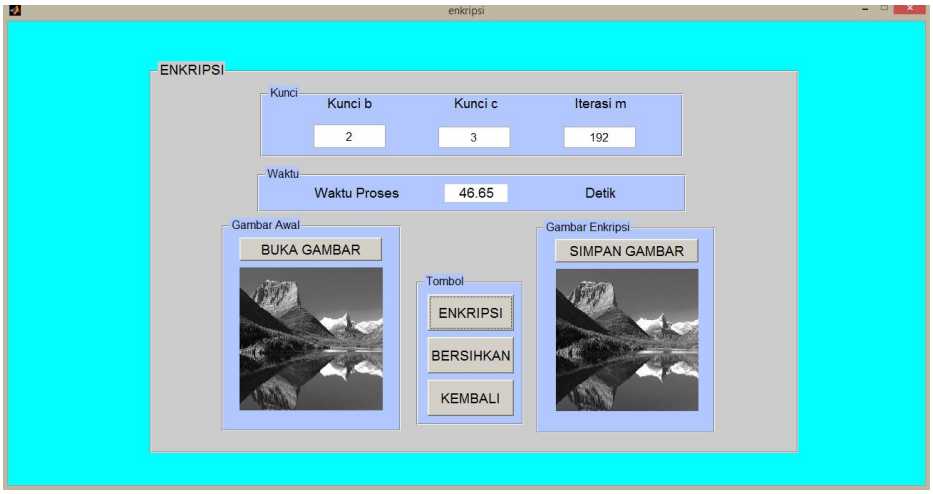


Gambar 8. Halaman Menu Histogram Hitam Putih



Gambar 9. Halaman Menu Perbandingan Citra

Selanjutnya uji coba iterasi. Pada proses enkripsi menggunakan algoritma Arnold's Cat Map citra terenkripsi akan kembali ke citra awal pada iterasi tertentu sesuai dengan ukuran citra. Uji coba iterasi terdapat pada Gambar 10 dan Tabel 4.



Gambar 10. Uji Coba Iterasi

Tabel 4. Hasil Uji Coba Iterasi

Data Uji Ke-	Ukuran Citra	Iterasi
1	256 × 256	192
2	280 × 280	120
3	300 × 300	300
4	320 × 320	240
5	400 × 400	300
6	420 × 420	120
7	450 × 450	300
8	480 × 480	120
9	600 × 600	300
10	620 × 620	30
11	650 × 650	1050
12	680 × 680	90
13	800 × 800	600

14	820 × 820	60
15	850 × 850	450
16	880 × 880	60
17	1000 × 1000	750
18	1020 × 1020	180
19	1050 × 1050	600
20	1080 × 1080	180

4. KESIMPULAN DAN SARAN

Berdasarkan semua hal yang telah diuraikan sebelumnya dapat diambil kesimpulan:

a. Ukuran file dan dimensi dari citra semula dari citra terenkripsi dan citra terdekripsi tetap sama karena proses enkripsi dan dekripsi pada penelitian ini hanya mengacak posisi pixel dan tidak mengubah nilai pixel.
b. Waktu proses enkripsi dan dekripsi berbanding lurus dengan besarnya ukuran citra, semakin besar ukuran suatu citra semakin lama waktu yang dibutuhkan untuk mengenkripsi citra tersebut karena semakin besarnya dimensi citra semakin banyak pula pixel-pixel yang akan diproses dan begitu juga sebaliknya.
c. Pada algoritma Arnold's Cat Map mempunyai periode sehingga citra acak kembali ke citra semula.

DAFTAR PUSTAKA

[1] Schneier, Bruce. *Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed.* John Wiley & Sons. 1996.
[2] Stalling, W.,. *Computer and Network Security: Principle and Practice (5th ed.).* Prentice hall, New York. 2011.
[3] Menezes, Alfred J., Paul C van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press. 1996.
[4] Gonzalez, C, Rafael., and Woods, E, Richard. *Digital Image Processing 3rd ed*. New Jersey, USA: Pearson Prentice Hall. 2008.
[5] Kadir, Abdul., dan Adhi Susanto. *Teori dan Aplikasi Pengolahan Citra*. Yogyakarta: Andi. 2013.
[6] Munir, Rinaldi. "Analisis Keamanan Algoritma Enkripsi Citra Digital Menggunakan Kombinasi Dua Chaos Map dan Penerapan Teknik Selektif." *Juti: Jurnal Ilmiah Teknologi Informasi ITS*, Vol. 10, No.2, 2012.
[7] Nurpeti, E., Suryadi M.T. "Chaos-Based Encryption Algorithm for Digital Image," in Proceedings IndoMS International Conference on Mathematics and Its Application 2013. Indonesia Mathematical Society, 2013, pp. 705-712.
[8] Purba, Ronsen., Arwin Halim, dan Indra Syahpurtra. "Enkripsi Citra Digital Menggunakan Arnold's Cat Map dan Non Linier Chaotic Algorithm." *Mikroskil*. Vol. 15, No.2. 2014.
[9] Sukirman, Edi., Suryadi M.T., Mubarak, M.Agus. "The Implementations of Henon Map Algorithm for Digital Image Encryption." *TELEKOMNIKA Telecommunication, computing, electronics, and control*. Vol.12 No.3. 2013.
[10] Suryadi,M.T., dan Tony Gunawan. "Aplikasi Enkripsi Citra Digital Menggunakan Algoritma Gingerbreadman Map." in Proceedings Kommit 2014. Vol. 8. 2014.
[11] Suryadi,M.T., Nurpeti, E., Widya. (2014). Performance of Chaos-Based Encryption Algorithm for Digital Image. *TELEKOMNIKA Telecommunication, computing, electronics, and control*. Vol.12 No.3.