ENKRIPSI DAN DEKRIPSI CITRA RGB MENGGUNAKAN ALGORITMA ARNOLD'S CAT MAP

***Eko Hari Rachmawanto*[1], *Candra Irawan*[2]**
[1,2]Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro Semarang
e-mail: [1]eko.hari@dsn.dinus.ac.id, [2]candra.irawan@dsn.dinus.ac.id

ABSTRAK

Kriptografi merupakan proses untuk mengamankan data dari penyadapan atau dari para hacking. Nama lain dari mengamankan data dalam ilmu computer yaitu enkripsi. Citra merupakan gambaran atau imitasi suatu objek. Proses Enkripsi Citra memiliki berbagai macam algoritma salah satunya algoritma Arnold's Cat Map (ACM). Algoritma ACM merupakan salah satu algoritma yang dapat digunakan untuk mengenkripsi citra RGB. Proses enkripsi citra dengan menggunakan algoritma Arnold's Cat Map pada prinsip mengubah pola pixel yang ada pada citra, menjadi pola lain sesuai dengan kunci dan iterasi yang sudah dimasukkan. Pada proses enkripsi diperlukan tingkat keakurasian untuk menunjukkan kerataan citra setelah di proses, hasil entropy berkisar 6.9262 - 7.9272 Dan memiliki range untuk mengukur kemiripan gambar sebelum dienkripsi dan citra setelah didekripsi (PSNR) dan hasil PSNR memiliki range 32.587 - 108.079.

***Kata Kunci**: Arnold Cat Map (ACM), Kriptografi, Citra Digital, Peak Signal to Noise Ratio (PSNR)*

1. PENDAHULUAN

Informasi telah menjadi bagian terpenting dalam kehidupan manusia. Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat penting bagi seluruh kalangan baik organisasi, perguruan tinggi, lembaga pemerintahan, perusahaan, sampai dengan individual. Perkembangan teknologi informasi telah membuat penyimpanan dan transmisi citra menjadi lebih mudah dan efisien. Persoalan yang timbul dari kemudahan ini adalah terdapatnya celah keamanan bagi pihak – pihak tidak bertanggung jawab untuk melakukan pencurian terhadap data, baik dari proses transmisi atau yang tersimpan pada harddrive. Meningkatkan jumlah pencurian data oleh hacker di seluruh penjuru dunia menjadikan kebutuhan sistem keamanan sangat penting diterapkan, sehingga keamanan data yang disimpan atau dikirimkan akan terjamin.Citra adalah suatu representasi (gambaran), kemiripan, atau imitasi dari suatu objek. Citra sebagai keluaran suatu sistem perekaman data dapat bersifat optik berupa foto, bersifat analog berupa sinyal – sinyal video seperti gambar pada monitor televisi, atau bersifat digital yang dapat langsung disimpan pada suatu media penyimpanan.

Kriptografi merupakan ilmu dan seni untuk menjaga kerahasian pesan dengan cara menyandikan ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Proses menyandikan plainteks menjadi chipertext disebut enkripsi atau enciphering [1]. Sedangkan proses mengembalikan chipertext menjadi plaintext semula dinamakan dekripsi atau deciphering. Kriptografi pada citra digital menjadi salah satu solusi dalam pengamanan file-file gambar tersebut sehingga lebih terlindungi dan memiliki akses terbatas [2]. Kriptografi dapat dikembangkan dengan memanfaatkan algoritma – algoritma yang ada guna mengamankan data – data pada citra digital.

Citra salah satu media yang menyediakan informasi secara visual, terkadang informasi yang ada pada citra bersifat privasi dan rahasia sehingga aspek keamanannya perlu diperhatikan. Algoritma kriptografi konvensional seperti RC4, AES, DES [3], IDEA [4] dan yang lainnya sebagian dianggap kurang cocok dalam pengamanan informasi citra. Karena data citra berbeda dengan data tekstual, data citra memiliki unsur spesial seperti volume data besar, redudansi tinggi dan pixel saling berhubungan. Proses enkripsi seharusnya membuat pixel di dalam citra tidak lagi berhubungan sehingga menyulitkan penyerang dalam melakukan analisis statistik.

Solusi terhadap keamanan citra digital dari penyadapan atau serangan adalah dengan mengenkripsinya. Enkripsi citra merupakan teknik untuk melindungi citra dengan cara menyandikan citra (plain-image) [5]. Arnold Cat Map dipilih karena dianggap cocok untuk mengenkripsi citra [6]. Pada umumnya Arnold Cat Map hanya bisa mengenkripsi citra grayscale. Namun pada penelitian ini kami mencoba untuk mengenkripsi citra RGB atau berwarna. Untuk menyulitkan penyadap dalam mengenali citra tersebut

2. TINJAUAN PUSTAKA

2.1 Arnold Cat Map (ACM)

Kriptografi yaitu ilmu yang berdasarkan pada teknik matematika yang erat kaitannya dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas. Jadi, pengertian kriptografi modern adalah bukan hanya penyembunyian pesan namun lebih pada sekumpulan teknik yang menyediakan keamanan informasi [7]. Metode Arnold's Cat Map diperkenalkan pertama kali oleh seorang ahli matematik yang bernama Vladimir I. Arnold, pada tahun 1960 yang mendesmontrasikan algoritmanya tersebut dengan menggunakan citra kucing. Fungsi operasi dari algoritma Arnold's Cat Map seperti ditujukkan pada persamaan (1) dan persamaan (2).

1

+1

(1)

Penggunaan modulo dengan nilai N pada operasi ACM dimaksudkan agar nilai posisi pixel yang dilakukan pengacakan tetap pada area gambar yang ada. Karena itu, maka algoritma ACM pada dasarnya hanya dapat digunakan pada gambar dengan panjang dan lebarnya sama [8]. Citra yang sudah teracak oleh ACM dapat terekontruksi menjadi citra semula [9] dengan menggunakan kunci yang sama (a,b dan m) [10]. Persamaan iterasinya [11] :

1

(2)

2.2 Pengukuran Eksperimen

Dalam makalah ini, digunakan alat ukur yaitu Peak Signal to Noise Ratio (PSNR) dimana akan dihitung nilai Mean Square Error (MSE) terlebih dahulu. MSE merupakan ukuran yang digunakan untuk menilai seberapa baik sebuah metode dalam melakukan rekontruksi atau restorasi citra relatif terhadap citra aslinya. Semakin kecil nilai MSE, ini menunjukkan bahwa hasil pemrosesan citra semakin bagus, atau dengan kata lain citra setelah proses semakin mendekati citra aslinya seperti pada persamaan (3).

$$MSE = \frac{1}{MxN}\sum_{x}^{M}\sum_{y}^{N}[f1(x,y) - f2(x,y)]^2 \quad (3)$$

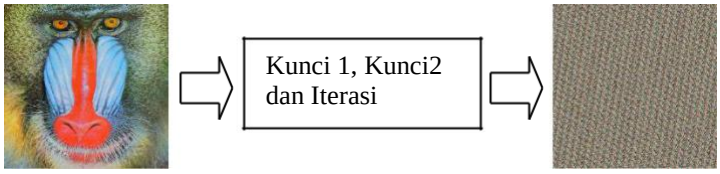
PSNR adalah perbandingan antara nilai maksimum dari kedalaman bit citra yang diukur (citra 8 bit, mempunyai nilai maksimum 255) dengan besarnya noise yang berpengaruh pada sinyal tersebut. Di dalam hal ini, besarnya noise diwakili oleh nilai MSE. PSNR biasanya dikukur dalam satuan desibel (dB) seperti pada persamaan (4). PSNR digunakan untuk mengetahui perbandingan kualitas citra sebelum dan citra sesudah di proses [12]. Semakin besar nilai PSNR, maka hasil pemrosesan citra semakin bagus atau semakin mendekati aslinya.

$$PSNR = 20Log_{10}\left(\frac{255}{\sqrt{MSE}}\right)$$

3. METODE PENELITIAN

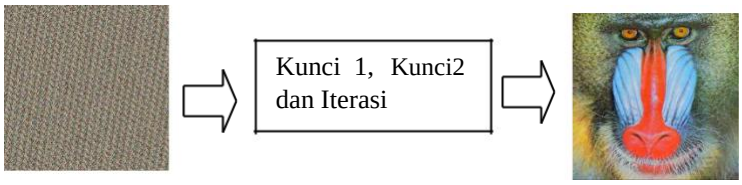
Sistem yang akan dibangun pada penelitian ini yaitu sistem kriptografi citra digital, dimana hanya pembuat kunci dan penerima kunci yang akan mengetahui citra tersebut. Dengan menggunakan algoritma Arnold's Cat Map, proses enkripsi dan dekripsi memerlukan 2 kunci dan 1 iterasi. Kedua kunci tersebut berguna untuk merahasiakan citra tersebut dari penyadapan atau serangan. Sedangkan untuk iterasi berfungsi untuk mengacak citra tersebut, dengan melakukan iterasi berkali kali maka akan diperoleh hasil citra enkripsi yang berbeda beda.

1. Proses Enkripsi
   Proses Enkripsi pada citra RGB dapat dilihat pada Gambar 1.
   - Input Plain Citra.
   - Masukkan kunci 1 dan kunci 2 serta jumlah iterasi.
   - Akan dipisahkan warna pixel tersebut menjadi 3 channel RGB.
   - Selanjutnya akan diacak citra tersebut sesuai dengan channelnya.
   - Setelah proses pengacakan selesai maka akan tampil Cipher Citra yang tidak berbentuk seperti Plain Citra sebelumnya.



Gambar 1. Skema enkripsi citra

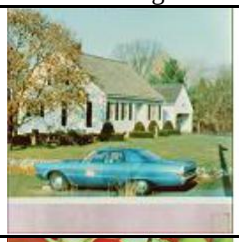
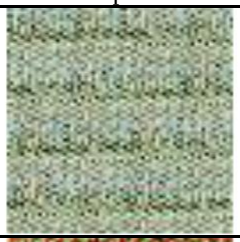
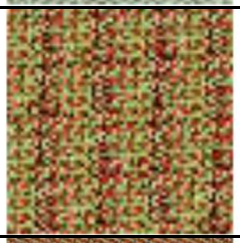
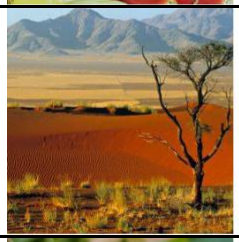
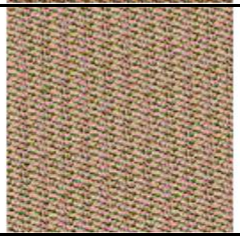
2. Proses Dekripsi
   Proses Dekripsi pada citra RGB dapat dilihat pada Gambar 2 dengan urutan proses sebagai berikut:
   - Input Cipher Citra.
   - Masukkan kunci 1 dan kunci 2 juga jumlah iterasi sesuai dengan pada proses Enkripsi.
   - Citra akan disatukan kembali sesuai warna pixel tersebut
   - Lalu citra yang telah diacak akan dikembalikan seperti Plain Citra.
   - Jika kunci 1, kunci 2 dan jumlah iterasi sesuai maka yang tampil adalah Plain Citra tetapi jika salah maka akan menjadi citra acak yang tidak berbentuk.

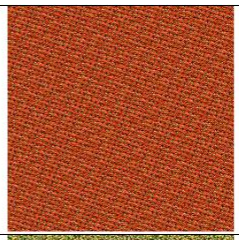
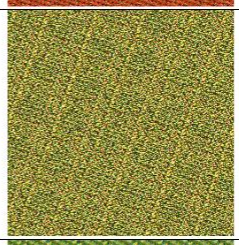
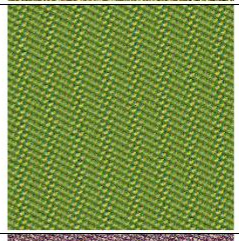
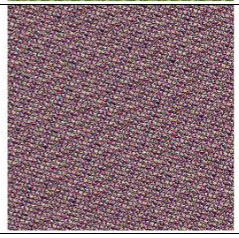


Gambar 2. Skema dekripsi citra

Dalam penelitian ini digunakan 3 macam citra berbeda yaitu citra dengan ukuran 1024x1024, citra 512x512, citra 256x256 dan citra 128x128. Dan citra - citra tersebut yang telah dilakukan proses enkripsi juga dekripsi akan dilakukan pengujian untuk dijadikan sebagai alat ukur kualitas citra dengan mengguakan MSE juga PSNR. PSNR berfungsi sebagai pembanding anatara citra yang telah dilakukan enkripsi. Untuk MSE sendiri digunakan untuk nilai kesalahan pada plain citra dan cipher citra. Tabel 1 merupakan hasil dari enkripsi dan dekripsi pada citra original atau plain image

Tabel 1. Hasil enkripsi dan dekripsi pada citra uji

Nama Citra	Ukuran Citra	Citra Original	Enkrip Citra	Dekripsi Citra
House Color.bmp 20	128			
Peppers Color.bmp 20	128			
Gurun Color.bmp 20	256			
Teratai Color.bmp 30	256			

hibiscus.bmp 60	512			
Bunga2 Color.bmp 60	512			
Birds Color.bmp 20	1024			
Bunga Color.bmp 40	1024			

Dengan dilakukan pengujian maka akan diketahui kualitas citra tersebut.pada Tabel 2 berikut merupakan pengujian terhdap MSE, PSNR, Entropy dan Time Elapsed. Entropy merupkan nilai hasil perbandingan antara citra asli dengan citra hasil dekripsi. Nilai entropy dikatakan sempurna apabila mencapai nilai 8. Dari hasil percobaan diketahui bahwa ukuran piksel tidak mempengaruhi nilai entropy. Nilai entropy yang dihasilkan oleh semua citra mendekati 8. Nilai PSNR dikatakan baik dan tidak dapat dibedakan oleh mata manusia berkisar di atas 40dB. Pada Tabel 2 diketahui masih terdapat nilai PSNR di bawah 40 dB, yaitu pada citra dengan ukuran 128x128 piksel. Untuk citra ukuran 256, 512 dan 1024 menghasilkan nilai PSNR sangat memuaskan. Di sisi lain, waktu operasi untuk melakukan proses dekripsi berbanding lurus dengan ukuran citra. Semakin besar citra maka semakin lama pula proses dekripsinya.

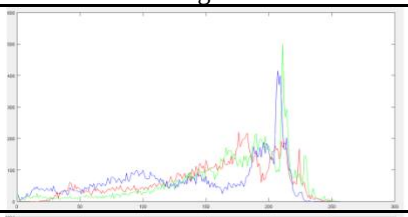
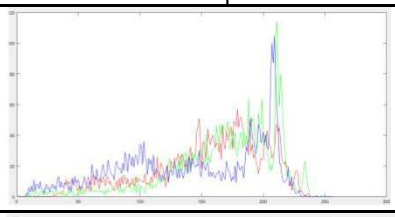
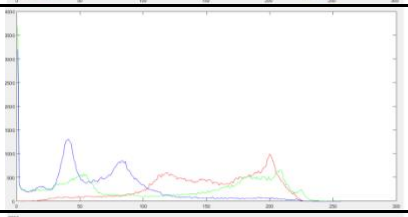
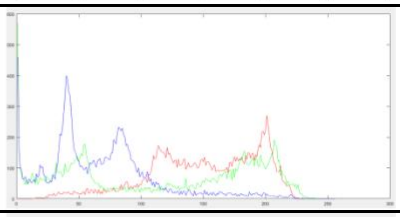
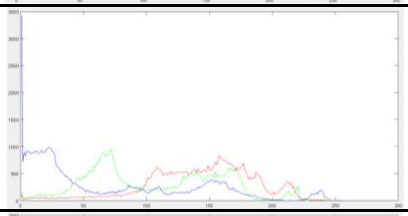
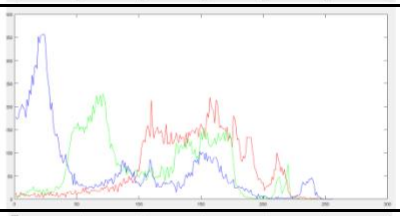
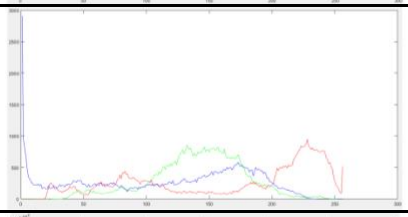
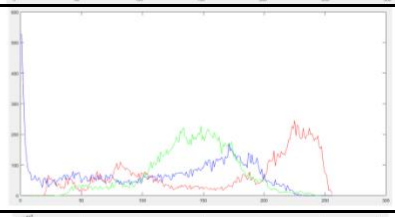
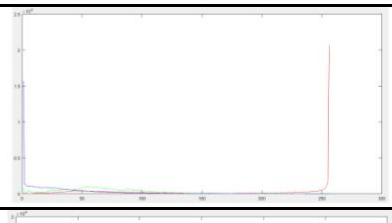
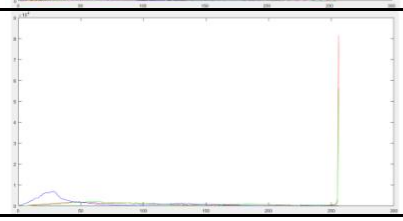
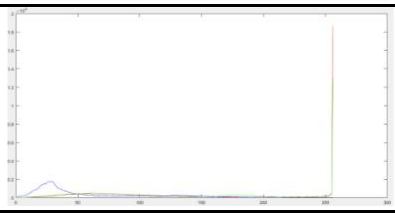
Tabel 2. Nilai MSE, PSNR, Entropy dan Time Elapsed

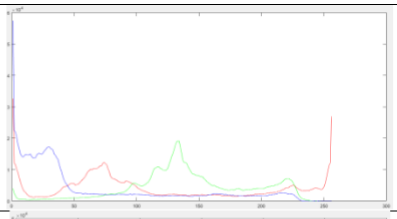
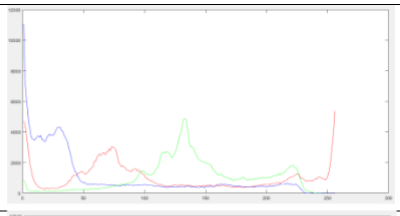
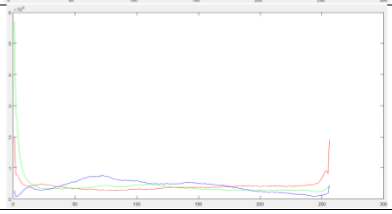
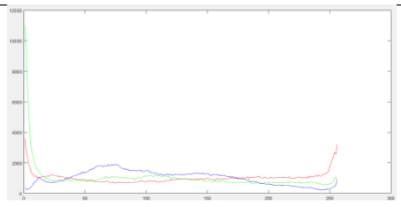
Nama Citra	Layer	Ukuran Pixel	MSE	PSNR	Entropy	Time Elapsed
House Color.bmp 20	R	128	357.6254	33.2198	7.4471	2.271316 sec
	G		384.6526	32.587		
	B		382.9165	32.6262		
Peppers Color.bmp 20	R	128	184.1087	38.9869	7.7303	2.295266 sec
	G		373.6537	32.839		
	B		197.3252	38.3847		
Gurun Color.bmp 20	R	256	105.2683	55.8836	7.6955	6.719635 sec
	G		101.9054	56.1657		
	B		90.46485	57.2		
Teratai Color.bmp 30	R	256	23.6717	68.845	7.8470	7.655974 sec
	G		24.0474	68.7082		
	B		25.9854	68.035		
hibiscus.bmp 60	R	512	17.4368	83.5415	6.9262	52.672083 sec
	G		31.9075	78.2929		
	B		20.7272	82.04		

Bunga2 Color.bmp 60	R	512	29.4636	78.9851	7.7366	45.300703 sec
	G		31.7161	78.2452		
	B		31.7058	78.348		
Birds Color.bmp 20	R	1024	4.1365	108.0793	7.8350	58.021175 sec
	G		4.2082	107.9302		
	B		4.3519	107.6384		
Bunga Color.bmp 40	R	1024	7.1825	103.2865	7.9272	117.027959 sec
	G		7.0547	103.4424		
	B		7.296	103.1503		

Untuk membuktikan bahwa citra hasil enkripsi berhasil dan mengalami sedikit perubahan apabila dilihat dari sisi histogram, maka pada Tabel 3 telah dipaparkan perbedaan nilai piksel melalui histogram.

Tabel 3. Perbedaan histogram citra asli dan citra enkripsi

Nama	Original	Enkrip
House Color.bmp		
Peppers Color.bmp		
Gurun Color.bmp		
Teratai Color.bmp		
Hibiscus.bmp		
Bunga2 Color.bmp		

Birds Color.bmp		
Bunga Color.bmp		

Gambar – gambar histogram diatas merupakan penggambaran proporsi frekuensi pada plain image dan cipher image. Berdasarkan Tabel 3, dapat disimpulkan bahwa semakin besar ukuran citra maka histogram citra enkripsi tidak berbeda jauh dengan citra asli. Perbedaan piksel ini terlihat sangat mencolok pada citra ukuran 128 piksel.

5. KESIMPULAN

Dengan menggunakan aloritma Arnold's Cat Map dapat mengenkripsi citra RGB dengan piksel yang bervariasi. Pada citra ACM yang telah dienkripsi dapat membentuk berbagai macam pola, karena pada prinsipnya Algoritma ACM hanya mengacak pola sesuai dengan kunci dan iterasi yang sudah diinputkan. Kunci pada proses enkripsi akan membuat keamanan menjadi lebih kuat karena jika kunci salah maka citra tidak akan kembali seperti semula. Untuk tingkat kemiripan plain image dengan cipher image PSNR menjadi alat ukurnya dan mempunyai nilai dari 32.587 - 108.0793, sementara untuk tingkat kesalahan digunakan alat ukur yaitu MSE yang memiliki nilai dari 4.1365 - 384.6526. Dan hasil pengukuran menggunkan Entropy adalah dari 6.9262 - 7.9272. Dapat disimpulkan bahwa semakin kecil ukuran piksel akan mempengaruhi nilai MSE dan PSNR, serta jika nilai iterasi semakin besar maka akan menghabiskan waktu cukup lama dalam melakukan Enkripsi dan Dekripsi citra.

DAFTAR PUSTAKA

[1] W. Staling, Cryptography and Network Security, New Jersey: Principles and Practice, 2014.

[2] N. A. Setiyanto dan E. H. Rachmawanto, "Pengacakan Citra Digital Berwarna Dengan Kriptografi Arnold Cat Map (Acm)," dalam *Prosiding SNST Fakultas Teknik 1* , Semarang, 2018.

[3] A. Widarma, "Kombinasi Algoritma AES, RC4 dan El Gamal Dalam Skema Hybrid Untuk Keamanan Data," *Journal of Computer Engineering, System and Science,* vol. 1, no. 1, 2016.

[4] Rosmasari, R. A. Dwi, N. Dengen dan M. Taruk, "Implementasi Metode Kriptografi International Data Encryption Algorithm (IDEA) Untuk Pengamanan Data Berita Publik Khatulistiwa Televisi Bontang," *Jurnal Rekayasa Teknologi Informasi (JURTI),* vol. 2, no. 2, 2018.

[5] A. Chandra, W. S. Raharjo dan J. K. Tampubolon, "Implementasi steganografi dengan metode end of file pada teks yang terenkripsi menggunakan block cipher rivest code-6 ke dalam citra," *Jurnal Informatika,* vol. 11, no. 1, 2015.

[6] S. Keshar dan S. G. Modani, "Image Encryption Algorithm based on Chaotic Map Lattice and Arnold cat map for Secure Transmission," *IJCST,* vol. 2, no. 1, pp. 132-135, 2011.

[7] Abdussalam, E. H. Rachmawanto, N. A. Setiyanto dan C. A. Sari, "Optimasi Keamanan Watermarking pada Daubechies Transform Berbasis Arnold Cat Map," *Jurnal Informatika: Jurnal Pengembangan IT,* vol. 4, no. 1, Februari 2019.

[8] N. A. Abbas, "Image encryption based on Independent Component Analysis and Arnold's Cat Map," *Egyptian Informatics Journal,* vol. 17, no. 1, pp. 139-146, Maret 2016.

[9] E. Hariyanto dan R. Rahim, "Arnold's Cat Map Algorithm in Digital Image Encryption," *International Journal of Science and Research (IJSR),* vol. 5, no. 10, Oktober 2016.

[10] N. A. Abbas, "Image encryption based on Independent Component Analysis and Arnold's Cat Map," *Egyptian Informatics Journal,* vol. 17, no. 1, 2016.

[11] A. K. Prusty, A. Pattanaik dan S. Mishra, "An image encryption & decryption approach based on pixel shuffling using Arnold Cat Map & Henon Map," dalam *International Conference on Advanced Computin and Communication Systems,* Coimbatore, India, 2013.

[12] A. Soleymani, M. J. Nordin dan E. Sundararajan, "A Chaotic Cryptosystem for Images Based on Henon and Arnold Cat Map," *The Scientific World Journal,* pp. 1-21, 2014.