PENGAMANAN CITRA SIDIK JARI MENGGUNAKAN KRIPTOGRAFI DAN STEGANOGRAFI FRAKTAL

Janoe Hendarto [1], Erwin Eko Wahyudi [2]
[1,2] Departemen Ilmu Komputer dan Elektronika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Gadjah Mada
jhendarto@ugm.ac.id

ABSTRAK

Banyak data multimedia penting yang bertransmisi di internet, seperti data sidik jari, dan perlu dilakukan pengamanan terhadap data tersebut. Pengamanan citra sidik jari dilakukan dengan cara dienkripsi kemudian disembunyikan dengan metode fraktal. Enkripsi dan dekripsi dilakukan dengan menggunakan citra himpunan Mandelbrot. Kemudian citra terenkrip disembunyikan menggunakan citra sampul berupa citra himpunan Julia. Proses enkripsi dilakukan dengan mengubah nilai bit ke-2 setiap piksel dari citra sidik jari kemudian ditambahkan nilai warna dari citra fraktalnya sehingga diperoleh citra terenkrip. Proses dekripsi adalah proses kebalikannya sehingga diperoleh citra sidik jari awal. Sedangkan proses penyembunyian citra terenkrip yang sudah dikonversi dalam bentuk matriks biner ke dalam citra sampul menggunakan manipulasi warna sehingga dihasilkan citra stego yang secara visual sama dengan citra sampulnya dan diharapkan tahan terhadap serangan. Digunakan 10 citra uji sidik jari dari situs Kaggle dan 5 citra fraktal Mandelbrot serta 5 citra himpunan Julia. Hasil analisis citra terenkripsi menghasilkan nilai NPCR adalah 100% dan nilai rerata UACI adalah 40,99%. Hasil analisis citra stego menghasilkan rerata RMSE bernilai 0,22 dan rerata PSNR bernilai 61,297 terhadap citra sampul. Waktu proses enkripsi dan dekripsi reratanya adalah 0,14 detik, sedangkan waktu proses penyembunyian dan pengambilan citra reratanya adalah 4,54 detik.

Keyword : *Enkripsi, Dekripsi, Steganografi fraktal, Himpunan Mandelbrot, Himpunan Julia*

1. PENDAHULUAN

Dalam beberapa tahun terakhir, semakin banyak transmisi data multimedia di internet dan masih ada beberapa informasi penting, seperti data sidik jari, yang bocor atau dicuri oleh penyadap. Sehingga, bagaimana cara mencegah informasi penting agar tidak dicuri oleh penyadap menjadi topik yang sangat penting. Kriptografi merupakan cara pengamanan data yang telah dikenal sejak dahulu, yang pada dasarnya memiliki dua proses yaitu enkripsi dan dekripsi [1]. Sedangkan steganografi fraktal (*fractal steganography*) adalah cara penyembunyikan pesan (citra rahasia), dalam suatu citra sampul (*cover image*) yang berupa citra fraktal (*fractal image*). Dengan menggabungkan kriptografi dan steganografi, diharapkan dapat lebih menjamin keamanan data khususnya citra sidik jari.

Fraktal adalah bidang geometri yang mengupas dan dapat menjelaskan hal-hal yang alamiah dan hal-hal yang kompleks yang mana semakin hari semakin berkembang seiring perkembangan teknologi komputer. Dengan menggunakan fraktal, dapat dibuat gambar-gambar fenomena matematis yang kompleks menggunakan beberapa transformasi sederhana yang disebut sistem fungsi iterasi (*iterated function system*) yang disingkat SFI. Titik tetap/atraktor dari sistem fungsi iterasi inilah yang dapat berupa gambar kompleks yang bisa bermacam-macam bentuknya.

Citra fraktal matematis yaitu citra yang diperoleh dari fenomena matematis [2], seperti citra himpunan Julia dan citra himpunan Mandelbrot yang pada penelitian ini akan digunakan untuk melakukan enkripsi dan dekripsi serta penyembunyian suatu citra sidik jari.

Enkripsi citra adalah sebuah proses penyandian yang mengubah citra yang dapat dimengerti (*plain image*) menjadi citra yang tidak bisa dimengerti (*cipher image*). Sedangkan dekripsi citra adalah sebuah proses pembalikan yang mengubah citra yang tidak bisa dimengerti (*cipher image*) menjadi sebuah citra asli [1].

Proses enkripsi citra dengan menggunakan citra fraktal dilakukan dengan mengubah nilai bit setiap piksel dari citra asli, kemudian ditambahkan nilai warna dari citra fraktalnya. Sehingga, proses ini membuat piksel di dalam citra tidak lagi berhubungan dan diharapkan dapat menyulitkan penyerang dalam melakukan analisis statistik. Enkripsi citra menggunakan metode fraktal dipilih karena dianggap cocok untuk mengenkripsi citra karena sifat fraktal yang *chaotic* serta sensitif terhadap nilai awal [3] dan citra fraktal dapat dikodekan sehingga diharapkan menyulitkan penyadap dalam mengenali citra tersebut.

Agar citra sidik jari semakin aman, hasil enkripsi citra sidik jari akan disembunyikan ke dalam citra fraktal, seperti citra himpunan Julia. Proses ini adalah termasuk steganografi fraktal, dikarenakan citra sampul yang digunakan adalah citra fraktal.

Pada penelitian ini dielaborasi dan dikaji: (a) Bagaimana mengkombinasikan kriptografi dan steganografi fraktal untuk mengamankan citra sidik jari, (b) bagaimana efisiensi dan ketahanan dari metode pengamanan citra sidik jari menggunakan

kombinasi kriptografi dan steganografi fraktal, dan (c) bagaimana program komputer yang interaktif dan mampu melakukan pengamanan citra sidik jari menggunakan kombinasi kriptografi dan steganografi fraktal.

Tujuan dari penelitian ini adalah diharapkan mampu memberikan wawasan bahwa citra himpunan Julia dapat dimanfaatkan sebagai citra sampul yang memuat data sidik jari yang telah terenkripsi. Selain itu, citra himpunan fraktal yang digunakan, Mandelbrot dan Julia, diharapkan tahan terhadap serangan.

2. TINJAUAN PUSTAKA

2.1. Kriptografi

Kriptografi merupakan ilmu yang mempelajari berbagai teknik untuk mengamankan pesan sehingga tidak mudah terbaca oleh pihak lain selain pengirim dan penerima pesan [1]. Terdapat dua proses utama dalam kriptografi, yaitu enkripsi dan dekripsi. Enkripsi merupakan proses mengubah pesan asli (*plaintext*) ke dalam pesan yang tidak mudah dimengerti (*ciphertext*) dengan menggunakan suatu kunci (*key*). Lawan dari enkripsi adalah dekripsi, yaitu mengubah *ciphertext* ke dalam *plaintext*.

Terdapat dua macam kriptografi, yaitu kriptografi simetris dan asimetris. Kriptografi simetris menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Pada kriptografi asimetris, kunci yang digunakan untuk proses enkripsi dan dekripsi umumnya berbeda.

Pesan asli yang digunakan dapat memiliki bentuk yang bermacam-macam, seperti teks atau gambar/citra. Selain itu, jenis kunci yang digunakan juga bisa beragam. Pada pesan berbentuk citra, salah satu jenis kunci yang dapat digunakan adalah kunci berupa citra fraktal, sehingga ini dinamakan kriptografi fraktal.

2.2. Steganografi

Steganografi secara harfiah berarti "tulisan tertutup" yang berasal dari bahasa Yunani. Steganografi, atau sering dikenal dengan stego, adalah ilmu untuk berkomunikasi dengan cara menyembunyikan keberadaan pesan ke dalam media lain [4]. Media yang digunakan untuk menyembunyikan pesan juga bermacam-macam, seperti teks, gambar, dan audio (suara). Tujuan steganografi adalah untuk menyembunyikan pesan di dalam media lain yang tidak berbahaya dengan cara yang tidak memungkinkan musuh untuk mendeteksi bahwa ada pesan kedua.

Steganografi dan kriptografi keduanya dapat diaplikasikan untuk melindungi informasi dari pihak yang tidak diinginkan. Meskipun steganografi dan kriptografi adalah cara yang sangat baik untuk mencapai hal ini, tetapi tidak satu pun teknologi yang sempurna dan keduanya dapat rusak. Karena alasan inilah sebagian besar ahli akan menyarankan menggunakan keduanya untuk menambahkan beberapa lapisan keamanan.

Mirip dengan kriptografi fraktal, steganografi fraktal yaitu menggunakan citra fraktal sebagai citra sampul yang digunakan sebagai media penyembunyian pesan.

2.3. Penelitian Terkait

Pengamanan citra dengan menggunakan kriptografi fraktal telah dilakukan oleh beberapa penelitian, seperti [5] dan [6]. Penelitian [5] mengenalkan ide baru menggabungkan kompresi dan enkripsi dengan menggunakan geometri fraktal. Himpunan Mandelbrot dan gambar terkompresi diubah ke dalam bentuk matriks persegi terlebih dahulu. Gambar dikompresi dengan menggunakan Sistem Fungsi Iterasi, dan selanjutnya operasi matriks diterapkan untuk mengenkripsi citra. Hasil dari penelitian ini adalah penggunaan memori yang lebih kecil dan tahan terhadap serangan. Namun, penelitian ini belum mengkombinasikan dengan steganografi fraktal.

Mirip dengan [5], penelitian [6] memperkenalkan sistem enkripsi citra berdasarkan proses difusi dan konfusi yang mana informasi citra disembunyikan di dalam detail citra fraktal yang kompleks. Dimulai dengan teknik enkripsi citra yang sederhana yaitu menggunakan satu citra fraktal hingga menggunakan 7 citra fraktal agar diperoleh metode enkripsi yang handal, akan tetapi ukuran kunci enkripsi menjadi membesar. Penelitian ini juga belum mengkombinasikan dengan steganografi fraktal.

Penelitian terkait penggunaan steganografi fraktal juga telah dilakukan, seperti [7]–[10]. Pada penelitian [7], dielaborasi metode steganografi fraktal berbasis palet warna dengan citra sampulnya adalah citra himpunan Julia. Ukuran citra rahasia yang diteliti berukuran 90x90 piksel. Proses penanaman bit dari citra rahasia menggunakan pengurutan terhadap palet warna berdasarkan nilai iluminasi dari pikselnya. Hasil dari penelitian ini adalah berhasil menyembunyikan citra rahasia ke citra fraktal hampir tanpa perubahan visual. Penelitian ini belum mengkombinasikan dengan kriptografi fraktal.

Pada penelitian [8] dibahas skema steganografi citra menggunakan *discrete cosine transform* (DCT) 16x16 dan enkripsi *one time pad* (OTP) pada citra rahasia. Nilai PSNR yang dihasilkan adalah 51,1225 dB dan MSE dengan nilai 0,50232. Citra rahasia berupa citra biner dan data yang digunakan hanya memiliki satu ukuran. Penelitian ini tidak mengevaluasi citra hasil enkripsinya serta belum menggunakan citra fraktal.

Penelitian [9] menghadirkan pengkodean citra digital dalam steganografi menggunakan citra fraktal dalam meningkatkan efisiensi algoritmenya. Dengan menggunakan sifat dari citra fraktal dan transformasi region, pesan disembunyikan sehingga

diharapkan tahan terhadap serangan. Percobaan dilakukan terhadap citra sampul warna dan keabuan. Informasi yang disembunyikan adalah teks. Penelitian ini juga belum mengkobinasikan dengan kriptografi fraktal.

Penelitian [10] mengusulkan teknik steganografi yang kuat untuk menyembunyikan *bitcoin* ke dalam citra fraktal yang berupa gambar pohon. Penyisipan kunci *bitcoin* dilakukan dengan menggambar pohon fraktal, dimana sudut dan panjang pohonnya diubah sesuai dengan nilai bit dari kunci. Proses ekstraksi dilakukan dengan menerapakan prosedur pemrosesan citra fraktal. Penelitian ini belum membandingkan terhadap jenis citra sampul lainnya selain pohon fraktal, dan informasi yang disembunyikan berupa *bitcoin*. Selain itu, kriptografi fraktal juga belum digunakan.

Selain penelitian-penelitian yang telah dibahas di atas, terdapat beberapa penelitian lain yang terkait, seperti [11]–[14]. Penelitian [11] mengusulkan skema enkripsi citra berdasarkan invers fungsi interpolasi fraktal yang mempunyai sifat *chaos* yang sempurna sehingga menghasilkan deret *pseudo-random* untuk mengacak posisi piksel citra asli. Kemudian, dilakukan difusi citra yang teracak untuk mendapatkan citra terenkripsi. Penelitian ini belum menggunakan citra fraktal untuk melakukan enkripsi dan steganografi fraktal.

Dalam penelitian [12], dibahas tentang kekurangan dan keterbatasan citra sampul himpunan Julia dalam menyembunyikan pesan. Langkah-langkah untuk mengatasi kekurangan tersebut yaitu dengan menentukan jangkauan nilai parameter dari himpunan Julia, sehingga lebih aman dari serangan untuk mengambil pesan yang disembunyikan. Pada penelitian tersebut belum membahas bagaimana menyembunyikan citra rahasia pada citra sampul himpunan Julia dan belum mengkombinasikan dengan kriptografi fraktal.

Penelitian [13] mengusulkan teknik enkripsi citra baru yaitu berdasarkan sifat pengisian ruang kurva Hilbert dan sifat tak hingga dari fraktal geometris-H, yang menggabungkan *pseudorandomness* dari sistem *hyperchaotic* dan sensitivitas terhadap nilai awal. Penelitian ini juga belum menggunakan citra fraktal dan belum mengkombinasikan dengan steganografi fraktal.

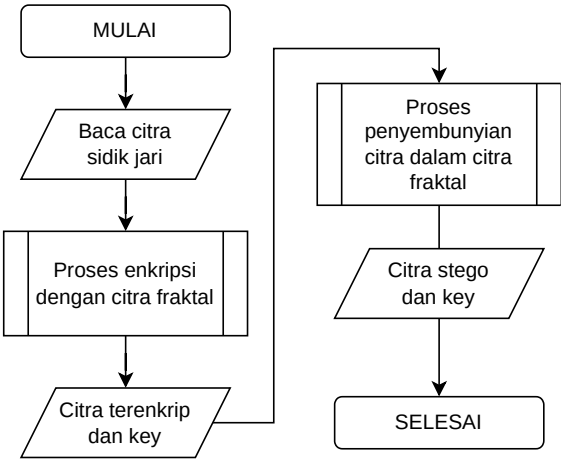
Penelitian [14] menggunakan teknik enkripsi simetris AES dan DES terhadap citra yang dikompresi dengan metode fraktal, sehingga diharapkan ukuran citra menjadi lebih kecil. Penelitian ini belum menggunakan citra fraktal dan belum mengkombinasikan dengan steganografi fraktal.

Dari penelitian-penelitian di atas, sebagian besar membahas enkripsi dan dekripsi citra menggunakan metode fraktal dan steganografi fraktal secara sendiri-sendiri, belum ada yang mengkombinasikan kriptografi fraktal dan steganografi fraktal. Penelitian yang ada hanya menggunakan satu macam citra fraktal dan masih perlu ditingkatkan ukuran *memory* kuncinya agar bisa lebih kecil. Pada penelitian ini akan dibahas metode pengamanan citra sidik jari menggunakan kombinasi kriptografi fraktal dan steganografi fraktal menggunakan beberapa citra fraktal seperti citra himpunan Mandelbrot dan citra himpunan Julia dan akan dicari kunci yang lebih efisien tapi tetap handal dan tahan terhadap serangan.

3. METODE PENELITIAN

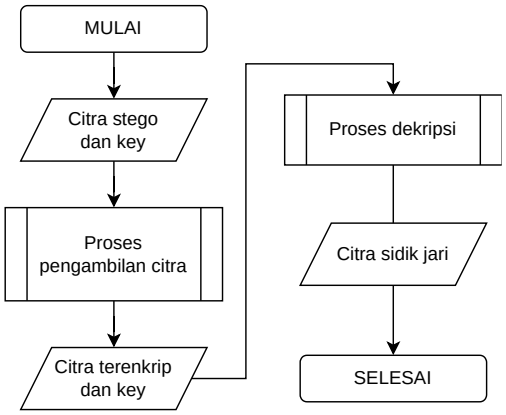
Berikut adalah langkah-langkah yang dilakukan dalam penelitian ini:

1. Studi pustaka, mulai dari referensi buku hingga mempelajari paper-paper mengenai kriptografi dan steganografi citra dengan metode fraktal.
2. Analisis permasalahan dan analisis terhadap metode pengamanan sidik jari menggunakan kombinasi kriptografi dan steganografi fraktal.
3. Perancangan algoritme dan aplikasi yang interaktif dan mampu melakukan pengamanan citra sidik jari menggunakan kombinasi kriptografi dan steganografi fraktal. Untuk menyembunyikan citra sidik jari, program akan membaca citra sidik jari, kemudian melakukan enkripsi berdasarkan citra fraktal dan dilanjutkan dengan menyembunyikan citra terenkripsi ke dalam citra sampul. Proses ini dapat dilihat pada Gambar 1.



Gambar 1. Proses enkripsi dan penyembunyian citra

Untuk mendapatkan citra sidik jari kembali, program akan menerima citra stego beserta key. Kemudian, dilakukan ekstraksi dari citra stego untuk mendapatkan citra terenkrip. Terakhir, program akan melakukan proses dekripsi pada citra terenkripsi untuk mendapatkan citra sidik jari. Proses ini dapat dilihat pada Gambar 2.



Gambar 2. Proses ekstraksi dan dekripsi citra

4. Mengimplementasikan algoritme dalam bentuk program aplikasi, dengan menggunakan bahasa pemrograman Delphi.
5. Menguji kebenaran program dan menganalisis hasil program (efisiensi algoritme dan mengukur kualitas dan ketahanan keamanan) dari aplikasi yang dibangun dengan beberapa parameter evaluasi, yaitu *Peak Signal to Noise Ratio* (PSNR), *Number of Pixel Change Rate* (NPCR) dan *Unified Average Changing Intensity* (UACI) serta waktu prosesnya.

   Metrik PSNR digunakan untuk mengukur kesamaan antara dua citra, dan dihitung dengan Persamaan (1):

$$PSNR = 20 \cdot log \frac{255}{RMSE} \quad (1)$$

   dengan nilai RMSE dihitung dengan Persamaan (2):

$$RMSE = \sqrt{\frac{\sum_{i,j}(X(i,j) - Y(i,j))^2}{m \times n}} \quad (2)$$

   dengan X dan Y merupakan dua citra yang akan dibandingkan, m dan n merupakan ukuran lebar dan tinggi citra, $X(i,j)$ dan $Y(i,j)$ berturut-turut merupakan nilai piksel pada posisi (i,j) untuk citra X dan Y [15].

   Metrik NPCR dan UACI digunakan untuk menguji ketahanan hasil enkripsi citra terhadap serangan diferensial [16]. Dimisalkan C^1 merupakan citra terenkripsi berdasarkan citra asli dan C^2 citra terenkripsi berdasarkan citra asli yang mana satu piksel acak telah diubah nilainya. Nilai NPCR dihitung dengan Persamaan (3):

$$NPCR = \sum_{i,j} \frac{D(i,j)}{N} \quad (3)$$

   dengan N menyatakan berapa banyak piksel yang ada pada citra terenkripsi, dan $D(i,j)$ didefinisikan pada Persamaan (4):

$$D(i,j) = \begin{cases} 0, \text{jika } C^1(i,j) = C^2(i,j) \\ 1, \text{jika } C^1(i,j) \neq C^2(i,j) \end{cases} \quad (4)$$

   dan nilai UACI dapat dihitung dengan Persamaan (5):

$$UACI = \sum_{i,j} \frac{C^1(i,j) - C^2(i,j)}{255 \cdot N} \quad (5)$$

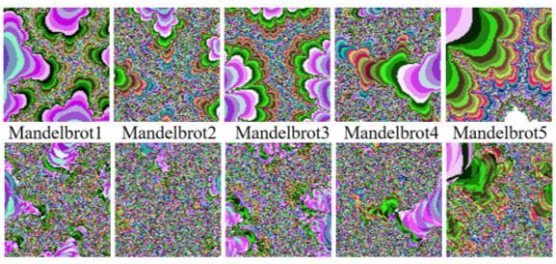
   dengan $C^1(i,j)$ dan $C^2(i,j)$ berturut-turut merupakan nilai piksel pada posisi (i,j) untuk citra C^1 dan C^2.

4. HASIL DAN PEMBAHASAN

Penelitian ini dilakukan pertama menyiapkan citra fraktal yang berupa citra himpunan Mandelbrot yang digunakan sebagai citra kunci dalam proses enkripsi dan dekripsi citra sidik jari (kriptografi). Selanjutnya, disiapkan citra himpunan Julia yang digunakan dalam proses penyembunyian dan pengambilan kembali citra sidik jari terenkrip (steganografi). Beberapa data uji citra sidik jari juga disiapkan. Selanjutnya, dirancang algoritme dan program komputer untuk melakukan pengamanan citra sidik jari dan akhirnya dianalisis hasil program komputernya.

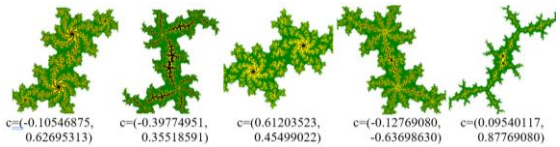
4.1. Penyiapan Citra Fraktal dan Citra Uji

Citra fraktal sebagai citra kunci kriptografi adalah citra Himpunan Mandelbrot dari fungsi kompleks $z^2 - c$ berukuran 96x103 piksel dengan berbagai daerah domain z yang dapat dicari melalui proses zooming. Selanjutnya, citra multi fraktal dibuat dengan operasi geseran dan XOR terhadap citra single fraktal. Pada penelitian ini, digunakan 5 citra single fraktal Mandelbrot dan 5 citra multi fraktal, selengkapnya dapat dilihat pada Gambar 3. Lima gambar di baris pertama Gambar 3 merupakan citra single fraktal dan lima gambar di baris kedua merupakan citra multi fraktal.



Gambar 3. Citra single fraktal (atas) dan citra multi fraktal (bawah)

Citra fraktal sebagai citra sampul dalam penyembunyian citra sidik jari adalah citra himpunan Julia $z^2 - c$ berukuran 512x512 piksel, dengan berbagai nilai c yang dapat dicari melalui citra himpunan Mandelbrot dari fungsi kompleks yang sama. Pada penelitian ini digunakan 5 citra himpunan Julia. Citra himpunan Julia yang terbentuk untuk masing-masing nilai c dapat dilihat pada Gambar 4.



Gambar 4. Beberapa citra himpunan Julia sebagai citra sampul

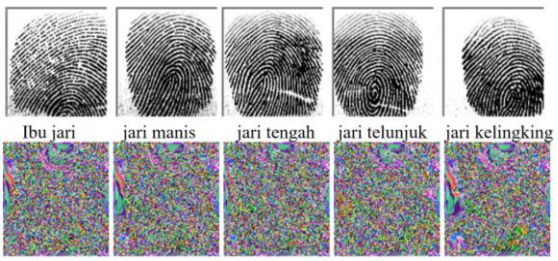
Digunakan 10 citra sidik jari dengan ukuran 96x103 piksel yang diunduh dari situs Kaggle, selengkapnya dapat dilihat pada Gambar 5. Baris pertama di Gambar 5 merupakan citra sidik jari untuk setiap jari di tangan kiri dan baris kedua merupakan citra sidik jari untuk setiap jari di tangan kanan.

Gambar 5. Citra sidik jari kiri (atas) dan citra sidik jari kanan (bawah)

4.2. Algoritme dan Program Pengamanan Citra Sidik Jari menggunakan Citra Fraktal

Pengamanan citra sidik jari dilakukan dengan cara dienkripsi kemudian disembunyikan dengan metode fraktal. Langkah pertama adalah membuat citra fraktal himpunan Mandelbrot yang berukuran sama dengan citra sidik jari. Batas-batas daerah domain dari citra fraktalnya disimpan dan dijadikan sebagai kunci enkripsi. Proses enkripsi dilakukan dengan mengubah setiap piksel dari citra asli, yaitu mengubah nilai bit ke-2 (0 menjadi 1 atau 1 menjadi 0), kemudian ditambahkan nilai warna dari citra fraktalnya sehingga diperoleh citra terenkripsi.

Hasil proses enkripsi dari program dapat dilihat pada Gambar 6. Baris pertama merupakan citra sidik jari asli dan citra kedua merupakan citra terenkripsi.



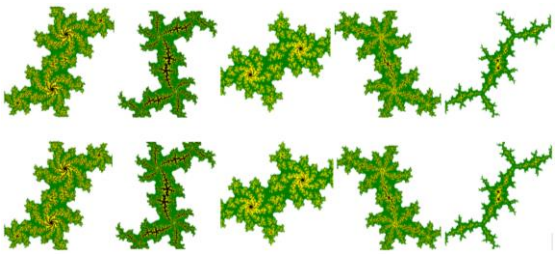
Gambar 6. Hasil enkripsi dari 5 citra sidik jari kiri

Proses dekripsi adalah proses sebaliknya, yaitu nilai warna setiap piksel dari citra terenkripsi dikurangi nilai warna dari citra fraktalnya, kemudian nilai bit ke-2 diubah (0 menjadi 1 atau 1 menjadi 0) sehingga diperoleh citra hasil dekripsi yang diharapkan sama dengan citra asli.

Untuk proses penyembunyian citra rahasia, hal pertama yang dilakukan adalah citra sidik jari terenkripsi diubah ke dalam bentuk data biner, yaitu dalam bentuk matrik yang elemen nya 0 atau 1. Kemudian dilakukan penggambaran citra sampul himpunan Julia dari fungsi kompleks $z^2 - c$, dengan menggunakan algoritme *escape-time* yaitu menggunakan iterasi dan pewarnaan berdasarkan nilai-nilai iterasi tertentu, yaitu nilai n_0, n_1 dan n_2 dan parameter R yang merupakan nilai batas daerah bidang komplek yang keduanya menentukan variasi warnanya. Pada penelitian ini, digunakan nilai R=400 dan 4 macam warna yaitu hitam, putih, kuning dan hijau, yang dijadikan *key* pada penelitian ini adalah nilai c, n_0, n_1, n_2 dan banyak elemen matriks binernya.

Proses penyembunyian citra sidik jari terenkripsi yang telah berupa matriks biner dilakukan dengan mengubah nilai warna RGB, dengan cara menambah atau mengurangi satu poin dari piksel citra himpunan Julia. Berdasarkan matriks binernya, akan didapat citra stego dan *key*.

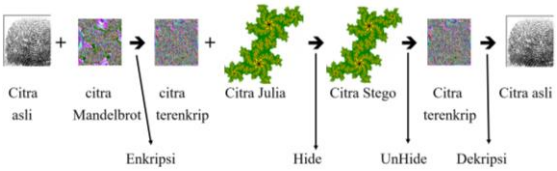
Hasil proses penyembunyian citra sidik jari terenkrip dapat dilihat pada Gambar 7. Baris pertama merupakan citra himpunan Julia sebagai citra sampul, dan baris kedua merupakan citra stego yang telah memuat citra sidik jari terenkripsi.



Gambar 7. Lima citra sampul (atas) dan lima citra stego (bawah)

Proses pengambilan citra rahasia dari citra stego dilakukan dengan cara menggambar ulang citra himpunan Julia berdasarkan *key*, kemudian membandingkannya dengan citra stego sehingga didapat matriks biner. Selanjutnya, matriks biner diubah menjadi citra sidik jari terenkripsi.

Proses pengamanan citra sidik jari menggunakan kombinasi kriptografi fraktal dan steganografi fraktal secara garis besar dapat digambarkan seperti pada Gambar 8. Proses *hide* dimaksudkan untuk proses penyembunyian citra, sedangkan proses *unhide* dimaksudkan untuk proses pengambilan citra.



Gambar 8. Garis besar proses pengamanan citra sidik jari dengan citra fraktal

4.3. Analisis Hasil Program Pengamanan Citra Sidik Jari menggunakan Citra Fraktal

Dilakukan beberapa kali uji hasil program dengan menggunakan 10 citra uji sidik jari berukuran 96x103 piksel dan 5 citra fraktal Mandelbrot, baik yang single maupun multi fraktal serta 5 citra himpunan Julia. Citra hasil enkripsi (*chipper image*) dianalisis dengan menentukan nilai NPCR dan UACI. Diperoleh nilai NPCR semuanya 100% sedangkan nilai UACI mempunyai rerata 40,996%. Selain itu, hasil analisis citra stego yang menyembunyikan citra sidik jari terenkripsi menghasilkan nilai rerata RMSE dengan nilai 0,21964 dan rerata PSNR adalah 61,2968 terhadap citra sampul himpunan Julia. Hasil uji selengkapnya dapat dilihat pada Tabel 1.

Tabel 1. Hasil analisis enkripsi dan penyembunyian citra terenkripsi

Citra sidik jari	UACI (%)	NPCR (%)	RMSE	PSNR
Jari ibu kanan	41,0004	100	0,21739	61,386
Telunjuk kanan	41,6251	100	0,21711	61,3971
Tengah kanan	40,0936	100	0,22062	61,2579
Manis kanan	40,3068	100	0,22121	61,2345
Kelingking kanan	42,2120	100	0,21738	61,3861
Jari ibu kiri	40,3232	100	0,21944	61,3041
Telunjuk kiri	40,5254	100	0,22147	61,2242
Tengah kiri	40,2899	100	0,22252	61,1832
Manis kiri	41,1039	100	0,22068	61,2552
Kelingking kiri	42,4753	100	0,21854	61,3401
Rerata	**40,996**	**100**	**0,21964**	**61,2968**

Nilai NPCR dengan rerata 100% dan nilai UACI dengan rerata 40,996 menunjukkan bahwa sedikit perubahan pada citra awal sangat berpengaruh terhadap citra hasil enkripsi. Nilai ideal untuk kedua metrik ini adalah NPCR lebih besar dari 0,996094 dan UACI lebih besar dari 33,4635 [16].

Selanjutnya, dilakukan uji terhadap hasil enkripsi menggunakan citra single dan citra multi fraktal. Diperoleh hasil bahwa menggunakan kedua jenis citra fraktal tersebut tidak berbeda secara signifikan, yaitu nilai UACI selisih 1,6%. Hasil uji selengkapnya dapat dilihat pada Tabel 2.

Tabel 2. Hasil enkripsi menggunakan citra fraktal single dan multi

Citra Fraktal	UACI jari ibu		UACI jari tengah	
	Multi	single	Multi	single
Mandelbrot1	40,32	41,40	40,28	41,41
Mandelbrot2	41,72	41,56	41,66	41,31
Mandelbrot3	40,21	40,16	40,27	40,25
Mandelbrot4	40,95	40,93	41,04	40,85
Mandelbrot5	39,93	41,34	40,64	41,99
Rerata	**40,63**	**41,08**	**40,78**	**41,16**

Citra hasil dekripsi maupun hasil pengambilan citra mempunyai RMSE bernilai 0 terhadap citra asli. Hal ini menunjukkan bahwa citra sidik jari setelah dilakukan enkripsi dengan citra himpunan Mandelbrot, lalu disembunyikan dalam citra himpunan Julia, kemudian diambil citranya lalu didekripsi dan menghasilkan citra sidik jari yang sama persis dengan citra aslinya. Sedangkan dari hasil nilai UACI dan NPCR dari 10 citra uji dan juga berdasarkan pengamatan secara visual, didapat bahwa citra hasil enkripsi susah dikenali sebagai citra sidik jari. Selain itu, hasil nilai RMSE dan PSNR dari 10 citra uji dan juga berdasarkan pengamatan secara visual, didapat bahwa citra stego tidak tampak berbeda dengan citra sampulnya yaitu citra himpunan Julia.

Waktu yang diperlukan untuk proses enkripsi reratanya adalah 0,15 detik dan waktu yang diperlukan untuk proses dekripsi reratanya 0,13 detik, sehingga rata-ratanya adalah 0,14 detik. Sedangkan waktu untuk proses penyembunyian citra reratanya adalah 4,42 detik dan waktu yang diperlukan untuk proses pengambilan citra reratanya 4,65 detik, sehingga rata-ratanya adalah 4,54 detik.

5. KESIMPULAN

Berdasarkan hasil penelitian, dapat disimpulkan bahwa pada proses enkripsi dan dekripsi menggunakan citra fraktal himpunan Mandelbrot dari fungsi kompleks $z^2 - c$, parameter batas-batas domain dari citra fraktalnya dapat dijadikan kunci. Sedangkan kunci yang digunakan pada proses penyembunyian dan pengambilan citra terenkrip dengan citra sampul himpunan Julia $z^2 - c$ adalah nilai c. Citra hasil enkripsi dianalisis dengan menghitung nilai NPCR dan UACI, yang mana nilai NPCR semuanya 100% sedangkan UACI dengan rerata 40,99%. Semua citra hasil pengambilan kembali dan dekripsi mempunyai RMSE bernilai 0. Penggunaan citra fraktal single atau multi tidak berpengaruh secara signifikan terhadap proses citra hasil enkripsi.

Waktu yang diperlukan untuk proses enkripsi dan dekripsi hampir sama yaitu dengan rerata 0,14 detik untuk citra sidik jari berukuran 96x103 piksel, sedangkan waktu yang diperlukan untuk proses penyembunyian dan pengambilan kembali citra rahasia juga hampir sama yaitu dengan rerata 4,54 detik untuk citra sampul berukuran 512x512 piksel.

DAFTAR PUSTAKA

[1] C. Paar and J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer, 2010.

[2] E. E. Wahyudi, J. Hendarto, N. Rokhman, and A. R. Darusalam, "Konstruksi Pola Fraktal Berdasarkan Bentuk Dasar Persegi Menggunakan Transformasi Affine," *J. Ilm. Ilk.*, vol. 6, no. 1, pp. 87–97, 2023, doi: 10.47324/ilkominfo.v6i1.159.

[3] J. Hendarto, "Penggunaan Citra Himpunan Julia Sebagai Citra Sampul Untuk Menyembunyikan Citra Rahasia," *J. Produktif*, vol. 4, no. 2, pp. 337–346, 2020, doi: 10.35568/produktif.v4i2.1000.

[4] J. Ashok, Y. Raju, S. Munishankaraiah, and K. Srinivas, "Steganography: an Overview," *Int. J. Eng. Sci. Technol.*, vol. 2, no. 10, pp. 5985–5992, 2010, [Online]. Available: http://www.ijest.info/docs/IJEST10-02-10-100.pdf.

[5] A. J. J. Lock, C. H. Loh, S. H. Juhari, and A. Samsudin, "Compression-Encryption Based on Fractal Geometric," in *2010 Second International Conference on Computer Research and Development*, 2010, pp. 213–217, doi: 10.1109/ICCRD.2010.40.

[6] S. K. Abd-El-Hafiz, A. G. Radwan, S. H. Abdel Haleem, and M. L. Barakat, "A fractal-based image encryption system," *IET Image Process.*, vol. 8, no. 12, pp. 742–752, 2014, doi: 10.1049/iet-ipr.2013.0570.

[7] H. N. Patel, D. R. Khant, and D. Prajapati, "Design of a color palette based image steganography algorithm for fractal images," in *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, 2017, pp. 2584–2589, doi: 10.1109/WiSPNET.2017.8300230.

[8] D. R. I. M. Setiadi, E. H. Rachmawanto, and C. A. Sari, "Secure Image Steganography Algorithm Based on DCT with OTP Encryption," *J. Appl. Intell. Syst.*, vol. 2, no. 1, pp. 1–11, 2017, doi: 10.33633/jais.v2i1.1330.

[9] R. Gupta, D. Mehrotra, R. K. Tyagi, and R. Kumar, "Digital image encoding scheme using fractal approach," in *2018 International Workshop on Advanced Image Technology (IWAIT)*, 2018, pp. 1–8, doi: 10.1109/IWAIT.2018.8369799.

[10] O. Hosam, "Hiding Bitcoins in Steganographic Fractals," in *2018 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT)*, 2018, pp. 512–519, doi: 10.1109/ISSPIT.2018.8642736.

[11] R. Ye, H. Lan, and Q. Wu, "A Fractal Interpolation Based Image Encryption Scheme," in *2018 IEEE International Conference on Computer and Communication Engineering Technology (CCET)*, 2018, pp. 291–295, doi: 10.1109/CCET.2018.8542341.

[12] N. Q. Mohammed, Q. M. Hussein, and M. S. Ahmed, "Suitability of Using Julia Set Images as a Cover for Hiding Information," in *2018 Al-Mansour International Conference on New Trends in Computing, Communication, and Information Technology (NTCCIT)*, 2018, pp. 71–74, doi: 10.1109/NTCCIT.2018.8681185.

[13] X. Zhang, L. Wang, Z. Zhou, and Y. Niu, "A Chaos-Based Image Encryption Technique Utilizing Hilbert Curves and H-Fractals," *IEEE Access*, vol. 7, pp. 74734–74746, 2019, doi: 10.1109/ACCESS.2019.2921309.

[14] N. Gupta and R. Vijay, "Effect on Reconstruction of Images by Applying Fractal Based Lossy Compression Followed by Symmetrical Encryption Techniques," in *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 2020, pp. 1–7, doi: 10.1109/ICCCNT49239.2020.9225601.

[15] J. Hendarto, "Enkripsi dan Dekripsi Citra Menggunakan Metode Fraktal," *J. Produktif*, vol. 5, no. 2, pp. 451–460, 2021, doi: 10.35568/produktif.v5i2.1744.

[16] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI Randomness Tests for Image Encryption," *J. Sel. Areas Telecommun.*, vol. 1, no. 2, pp. 31–38, 2011, [Online]. Available: http://www.cyberjournals.com/Papers/Apr2011/05.pdf.