Kriptografi Visual Pada Gambar Berwarna (RGB) Menggunakan Algoritma Elliptic Curve Cryptography

Della Annisa Zahra*, Rini Marwati, Ririn Sispiyati

Program Studi Matematika
Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam
Universitas Pendidikan Indonesia
*Surel: della.annisazahra@gmail.com

ABSTRAK. Kriptografi berperan penting pada era digital dalam mengamankan data dari peretas. Seiring berkembangnya teknologi, data yang dapat diamankan menggunakan kriptografi semakin luas, salah satunya adalah mengamankan gambar menggunakan kriptografi visual. Kriptografi visual merupakan kriptosistem yang memecah suatu gambar menjadi beberapa bagian dan hanya dapat dipecahkan jika memiliki semua bagian dari gambar tersebut. Jenis kriptografi lain yang dapat digunakan dalam mengamankan data adalah *elliptic curve cryptography* (ECC). ECC menggunakan suatu lapangan atas bilangan prima yang berisi titik-titik pada kurva eliptik sebagai teknik pengamanan datanya. Dalam penelitian ini dilakukan pengembangan kriptosistem dengan menggabungkan kriptografi visual dan ECC serta implementasinya dalam mengkonstruksi program aplikasi komputer menggunakan MATLAB R2014a. Berdasarkan implementasi, diperoleh hasil bahwan pengembangan kriptografi visual menggunakan *Elliptic Curve Cryptography* dapat mempersulit kriptanalisis karena harus meretas dua algoritma dan tidak akan bisa diretas jika hanya memperoleh salah satu *share image*.

Kata Kunci: Kriptografi, Kriptografi Visual, *Elliptic Curve Cryptography*.

e-ISSN: 2528-4231
p-ISSN: 2776-480X

Visual Cryptography on Colored Image (RGB) Using Elliptic Curve Cryptography Algorithm

ABSTRACT. *Cryptography held an important role in the digital era for securing data from hackers. As technology develops, types of data that can be secured using cryptography is expanding, one of which is securing images using visual cryptography. Visual cryptography is a cryptosystem that splits an image into parts and can only be solved if it has all parts of the image. Another type of cryptography that can be used to secure data is Elliptic Curve Cryptography (ECC). ECC uses a field of prime numbers consists of points on the elliptic curve as a technique to secure data. In this research, a cryptosystem development was carried out by visual cryptography combined with ECC and its implementation in constructing a computer application program using MATLAB R2014a. Results show that the development of visual cryptography using Elliptic Curve Cryptography can complicate cryptanalysis because it has two algorithms and cannot be hacked if only one share image was obtained.*

Keywords: *Cryptography, Visual Cryptography, Elliptic Curve Cryptography.*

1. PENDAHULUAN

Kriptografi berasal dari bahasa Yunani, yaitu *kryptos* (tersembunyi) dan *graphein* (menulis), yang dapat diartikan sebagai keahlian dan ilmu dari cara-cara berkomunikasi dengan aman terhadap pihak ketiga [1]. Kriptografi dapat digunakan untuk mengamankan informasi berupa teks maupun gambar. Untuk data berupa gambar, salah satu metode yang digunakan adalah kriptografi visual.

Kriptografi visual adalah salah satu teknik kriptografi dalam mengamankan data. Media yang digunakan dapat berupa gambar maupun video [2]. Langkah yang dilakukan untuk mengenkripsi data adalah dengan merekonstruksi data awal menjadi beberapa bagian, sedangkan untuk mendekripsinya dapat dilakukan dengan menggabungkan bagian-bagian hasil rekonstruksi sehingga memunculkan isi dari pesan aslinya. Naor dan Shamir [2] mengklaim bahwa data yang dienkripsi dijamin keamanannya, akan tetapi kunci yang digunakan untuk mengenkripsi tidak mudah diamankan. Oleh karena itu diperlukan peningkatan keamanan dari kriptografi visual.

Elliptical Curve Cryptography (ECC) adalah kriptografi asimetris yang dikembangkan oleh Victor Miller [3] dan Neal Koblitz [4]. ECC memanfaatkan permasalahan matematis kurva eliptik sebagai dasar keamanan pada algoritmanya. Keunggulan dari algoritma ECC adalah ukuran kunci enkripsi yang lebih kecil daripada algoritma asimetris lainnya tetapi memiliki tingkat keamanan yang sama.

Penelitian mengenai penggabungan kriptografi visual dengan ECC telah dilakukan oleh Shankar, Devika, dan Ilayaraja [5]. Mereka menyimpulkan bahwa hasil pengembangan kriptografi visual dengan menggunakan ECC untuk lebih dari satu *plain images* dengan teknik pemetaan menggunakan metode Koblitz untuk mengkonversi nilai RGB berhasil mempersingkat waktu komputasi, mempertahankan ukuran citra yang asli dengan yang sudah dienkripsi, menghasilkan *shared images* dengan jumlah yang sama dengan *plain images*, dan peningkatan keamanan pada *shared images*.

Pada makalah ini, penulis menggabungkan kriptografi visual dengan kriptografi ECC untuk mengamankan gambar dengan mengkonversi warna dasar Red, Green, Blue (RGB) menggunakan tabel yang dibentuk dari operasi perkalian pada titik generator. Hasil penggabungan tersebut dibuat program aplikasi komputer menggunakan bahasa pemrograman MATLAB. Metode ini bertujuan mengembangkan teknik kriptografi visual yang ditingkatkan menggunakan ECC dan mengkonstruksinya menjadi sebuah program aplikasi.

e-ISSN: 2528-4231
p-ISSN: 2776-480X

2. METODOLOGI

Secara umum dilakukan pembuatan kriptosistem visual RGB yang ditingkatkan dengan menggunakan ECC. Langkah pertama adalah mengidentifikasi nilai RGB masing-masing pixel pada gambar asli menjadi sebuah matriks untuk tiap warna dasar. Kemudian, tiap anggota matriks masing-masing warna dienkripsi menggunakan kunci publik ECC. Hasil enkripsi tiap matriks digabungkan kembali dan menjadi suatu cipher image. Pada proses dekripsi, semua share disatukan dan nilai RGB masing-masing pixel diidentifikasi. Diperoleh matriks RGB yang terenkripsi, kemudian tiap anggota matriks didekripsi menggunakan kunci privat yang diperoleh dari ECC. Konstruksi program komputer yang dilakukan menggunakan MATLAB terdiri dari bagian yaitu pembangkitan kunci, enkripsi, dan dekripsi data. Data yang diproses adalah gambar dengan format JPEG. Proses pembangkitan kunci dilakukan dengan menggunakan MATLAB dan hasilnya berupa teks. Validasi dilakukan untuk mengetahui apakah *ciphertext* hasil proses enkripsi penggabungan kriptografi visual dan *elliptic curve cryptography* dapat mengembalikan gambar saat melalui proses dekripsi atau tidak, apabila benar maka validasi dianggap berhasil.

3. HASIL DAN PEMBAHASAN

Model dasar dari kriptografi visual berupa suatu gambar yang dipecah menjadi n bagian sehingga gambar asli dapat terlihat untuk sembarang k (atau lebih) bagian disusun, tapi tidak terlihat jika kurang dari k bagian yang disusun. Setiap pixel pada gambar muncul pada n buah *share* yang terdiri dari m buah sub-pixel berwarna hitam dan putih. Seluruh *share* didefinisikan sebagai matriks S berukuran $n \times m$.

$$S = \begin{bmatrix} S_{11} & \cdots & S_{1m} \\ \vdots & \ddots & \vdots \\ S_{n1} & \cdots & S_{nm} \end{bmatrix}$$

$[n, m] = 1$ jika sub-pixel ke-m pada *share* ke-n berwarna hitam.
$[n, m] = 0$ jika sub-pixel ke-m pada *share* ke-n berwarna putih.

Munthe dan Ratnadewi [6] menjelaskan tentang kriptografi visual untuk citra berwarna dengan menggunakan skema (2,2), dimana hasil enkripsi menghasilkan dua buah *share* dan membutuhkan kedua *share* agar proses dekripsi berhasil. Perluasan citra berwarna dimulai dari citra berwarna yang diurai menjadi tiga buah citra yaitu citra *Red*, *Green* dan *Blue*, lalu ketiga citra diubah menjadi citra *halftone* dan kemudian setiap piksel citra *halftone* diuraikan menjadi empat piksel dengan kombinasi warna tertentu untuk kedua *share*.

Berdasarkan Stinson [7] *Elliptic curve cryptography* (ECC) menggunakan menggunakan kurva eliptik pada lapangan $\mathbb{Z}_p$. Bentuk umum kurva eliptik tersebut adalah

$$y^2 = x^3 + ax + b \pmod{p}$$

di mana $p > 3$ bilangan prima, $a, b \in \mathbb{Z}_p$ konstanta yang memenuhi $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$ dengan sebuah titik khusus $\mathcal{O}$ yang dinamakan titik *infinity* (titik di tak hingga). Kurva eliptik pada lapangan $\mathbb{Z}_p$ membentuk grup Abelian, dengan operasi $\oplus$ (penjumlahan titik), yang didefinisikan sebagai berikut:

1. $\mathcal{O}$ merupakan unsur identitas, sehingga $P \oplus \mathcal{O} = \mathcal{O} \oplus P = P$ untuk setiap $P \in E$.
2. Diberikan $P, Q \in E$, di mana $P = (x_1, y_1)$ dan $Q = (x_1, -y_1)$, maka $P \oplus Q = \mathcal{O}$. Titik Q adalah unsur negatif dari P, dapat ditulis $-P$.
3. Diberikan $P, Q \in E$, di mana $P = (x_1, y_1)$, $Q = (x_2, y_2)$, $P \neq \mathcal{O}$, $Q \neq \mathcal{O}$, dan $Q \neq \pm P$, maka $P \oplus Q = R = (x_3, y_3)$ di mana:

   $$x_3 = \lambda^2 - x_1 - x_2 (\mathbf{mod}\ p)$$

   dan

   $$y_3 = (x_1 - x_3) - x_2 (\mathbf{mod}\ p)$$

   dengan

   $$\lambda = \frac{y_2 - y_1}{x_2 - x_1} (\mathbf{mod}\ p)$$
4. Diberikan $P \in E$, di mana $P = (x_1, y_1)$, maka $P \oplus P = 2P = (x_3, y_3)$, disebut juga dengan penggandaan titik, di mana:

   $$x_3 = \lambda^2 - 2x_1 (\mathbf{mod}\ p)$$

   dan

   $$y_3 = \lambda^2 (x_1 - x_3) - y_1 (\mathbf{mod}\ p)$$

   dengan

   $$\lambda = \frac{3{x_1}^2 + a}{2y_1} (\mathbf{mod}\ p)$$

Selain operasi penjumlahan, pada kurva eliptik pada lapangan $\mathbb{Z}_p$ dapat didefinisikan perkalian titik dengan aturan:

$$nP = \underbrace{P \oplus P \oplus P \oplus \ldots \oplus P}_{n}$$

dengan $n \in \mathbb{Z}$ dan $P \in E$.

Kriptosistem *elliptic curve cryptography* merupakan kriptosistem asimetris [7]. Misalkan E adalah suatu kurva eliptik terdefinisi pada $\mathbb{Z}_p$ ($p > 3$ prima) dengan order n.

e-ISSN: 2528-4231
p-ISSN: 2776-480X

$$\mathcal{K} = \{(E, P, m, Q, n): Q = mP\}.$$

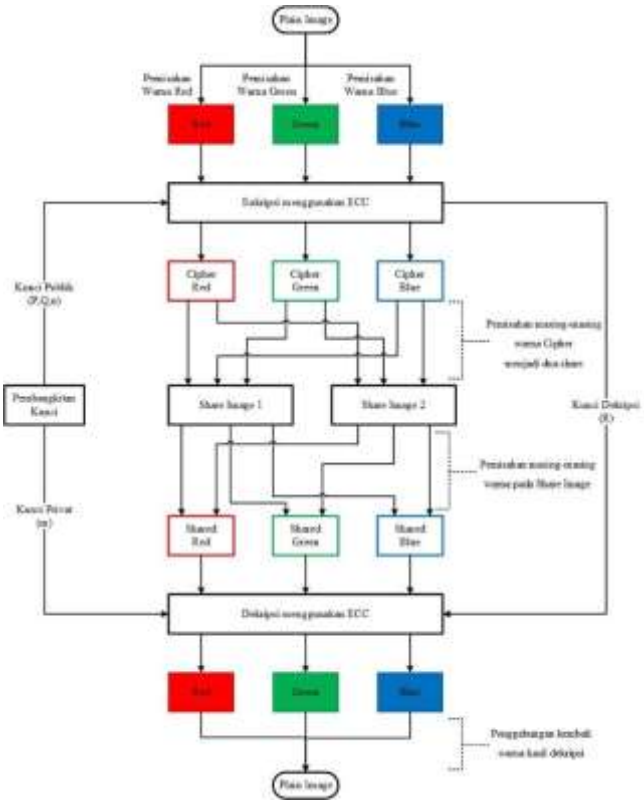
Kunci Publik $_K$: (P, Q, n)

Kunci Privat $d_K: m \in \mathbb{Z}_p^*$

Sebelum melakukan proses enkripsi dan dekripsi, diperlukan proses konversi pesan asli menjadi titik pada kurva eliptik yang ditentukan dengan melakukan perkalian titik generator (pembangkit). Banyaknya titik konversi menyesuaikan dengan jenis pesan asli yang diamankan. Proses enkripsi data dengan menggunakan kunci publik e_K: (P, Q, n) dengan suatu bilangan acak $k \in \mathbb{Z}_n$ untuk plainteks $x = (x_{1,2}) \in E$ adalah $e_K(x, k) = (kP, x + kQ)$.

Proses dekripsi *ciphertext* $y = (y_1, y_2) \in E$, dengan menggunakan kunci privat $d_K: m \in \mathbb{Z}_p^*$ adalah $d(y) = y_2 - my_1$.

Algoritma kriptografi visual menggunakan ECC dapat digambarkan dengan skema sebagai berikut:



Gambar 1. Skema Alur Kriptografi Visual Menggunakan ECC

Skema pada Gambar 1 dapat diwujudkan dalam langkah-langkah sebagai berikut: 1. Pembangkitan kunci; 2. Proses Enkripsi; 3. Proses Dekripsi.

Pihak yang melakukan pembangkitan kunci adalah pihak yang akan menerima foto yang terenkripsi. Berikut langkah pembangkitan kunci privat dan kunci publik:

1. Pilih suatu fungsi kurva eliptik E pada $\mathbb{Z}_p$ ($p > 3$ prima) kemudian pilih sebuah titik $P \in E$ sebagai titik pembangkit. Dari P diperoleh n sebagai orde titik P di mana $nP = P + P + \cdots + P = \mathcal{O}$ (infinity).
2. Penerima memilih suatu bilangan acak $m < n$ sebagai kunci privat dan menghitung $Q = mP$.
3. Penerima mengirimkan $e_k = (P, Q)$ sebagai kunci publik dan m sebagai kunci privat.

Pengirim pesan melakukan proses enkripsi menggunakan kunci publik yang telah diterima. Langkah-langkahnya adalah sebagai berikut:

1. Pengirim menentukan sebuah file foto berwarna sebagai plainteks.
2. Pengirim mengkonversi nilai-nilai RGB per-pixel pada foto tersebut menjadi titik pada E menggunakan tabel konversi yang dibangkitkan menggunakan P. Hasil konversi tiap pixel untuk masing-masing warna dinyatakan sebagai P_m.
3. Pengirim memilih suatu bilangan acak $k < n$ dan menghitung $R = kP$ dan $P_c = P_m + kQ$.
4. Nilai P_c dikonversikan kembali menggunakan tabel konversi menjadi nilai RGB sebagai *shared image*. Nilai R adalah kunci publik dari pengirim pesan.

Setelah menerima *shared image* dan R, penerima melakukan proses dekripsi sebagai berikut.

1. Penerima mengkonversi nilai-nilai RGB per-pixel pada *shared image* tersebut menjadi titik pada E menggunakan tabel konversi yang dibangkitkan menggunakan P. Hasil konversi tiap pixel untuk masingmasing warna dinyatakan sebagai P_c.
2. Dengan menggunakan kunci privat m, penerima menghitung $P_d = P_c - mR$.
3. Nilai P_d dikonversi kembali menjadi nilai RGB menggunakan tabel konversi.

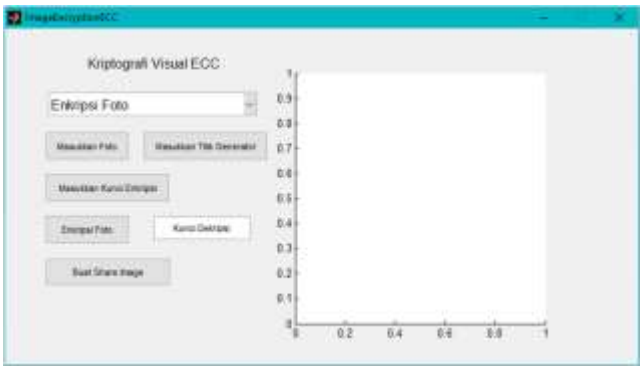
e-ISSN: 2528-4231
p-ISSN: 2776-480X

Program dibuat menggunakan MATLAB R2014a pada komputer dengan sistem operasi Windows 10 Pro, *processor* Intel Core i3-5005U 2.00 GHz dan RAM 8 GB. Pada program menggunakan fungsi kurva eliptik E: $y^2 = x^3 + 9x + 7$ mod 2011. Terdapat tiga pilihan proses dalam program, yaitu pembentukan kunci, enkripsi foto, dan dekripsi foto.

Gambar 2. Tampilan Program Pembangkitan Kunci ECC

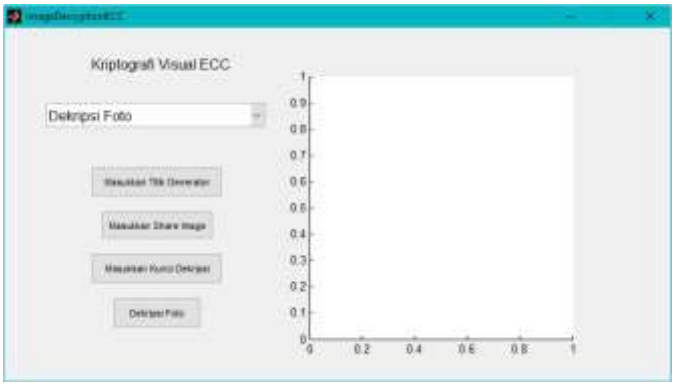
Gambar 2 menampilkan program pembangkitan kunci, dimana pengguna dapat membangkitkan titik generator, kunci publik dan kunci privat. Titik generator dan kunci publik yang diperoleh kemudian dikirimkan kepada pihak yang akan mengenkripsi pesan.

Program enkripsi seperti Gambar 3 dijalankan dengan menginputkan foto yang akan dienkripsi, titik generator dan kunci publik yang diterima. Foto yang diinputkan kemudian dienkripsi menggunakan ECC sehingga menghasilkan *cipher image* dan kunci dekripsi. *Cipher image* dijadikan dua buah *share* dengan menekan tombol "Buat Share Image". *Share* yang dihasilkan disimpan secara otomatis didalam folder program enkripsi dapat dikirimkan pada penerima pesan.



Gambar 3. Tampilan Program Enkripsi Foto

Untuk mendekripsi *share image* yang diterima, digunakan program dekripsi foto seperti yang tertera pada Gambar 4. Data yang diinputkan adalah titik generator, kunci dekripsi, kunci privat, dan kedua *share* yang akan didekripsi. Proses awal yang dilakukan oleh program adalah menumpuk kedua *share* dengan menggunakan *bitxor*. Hasil penumpukkan foto kemudian didekripsi menggunakan ECC dan memberikan output berupa hasil dekripsi foto.



Gambar 4. Tampilan Program Dekripsi Foto

Selanjutnya diberikan contoh dalam penggunaan program dan validasi program. Langkah pertama adalah menggenerasi kunci publik dan kunci privat yang dilakukan oleh penerima pesan. Kunci publik berupa *string* yang dikirimkan kepada pengirim pesan.

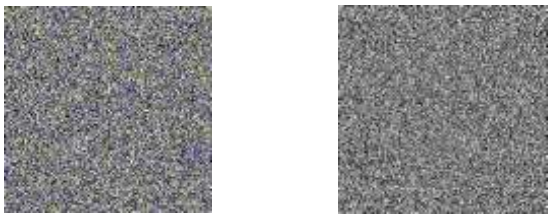
Misalkan Bob ingin membangkitkan titik generator, kunci publik dan kunci privat. Dengan menggunakan program pembangkitan kunci, Bob memperoleh titik generator $P = (1175,385)$, kunci privat $m = 759$, dan kunci publik $Q = (457,1080)$. Bob mengirimkan $e_k = (P, Q)$ kepada Alice.

Gambar 5. Contoh Penggunaan Program Pembangkit Kunci

e-ISSN: 2528-4231
p-ISSN: 2776-480X

Alice membuka program enkripsi foto dan memberi input berupa file foto dalam format .jpg atau .jpeg, titik generator, dan kunci publik yang diterima dari Bob. Hasil enkripsi yang diberikan adalah dua buah *shared image* dengan format .png dan kunci dekripsi $R = (457,1080)$ yang kemudian dikirimkan pada Bob. *Share image* yang dihasilkan dapat dilihat pada Gambar 7.

Gambar 6. Contoh Pengunaan Program Enkripsi Foto



Gambar 7. Hasil *Share Image*

Shared image dan kunci dekripsi yang diterima diinputkan pada program dekripsi foto. Selain itu, kunci privat dan titik generator diinputkan juga pada program dekripsi. Hasil dekripsi kemudian ditampilkan pada program sebagaimana terlihat pada Gambar 8.

Gambar 8. Contoh Penggunaan Program Dekripsi Foto

4. KESIMPULAN

Berdasarkan penelitian ini diperoleh kesimpulan bahwa implementasi kriptografi visual dengan menggunakan *Elliptic Curve Cryptography* dilakukan dengan mengonstruksi suatu program aplikasi komputer menggunakan MATLAB R2014a. Langkah-langkah atau proses pemrograman menggunakan fitur GUIDE kemudian mengkompilasi program dengan bantuan perintah *deploytool* sehingga terbentuk sebuah program yang dapat digunakan untuk mempermudah proses pembangkitan kunci, enkripsi, dan dekripsi. Program tersebut dapat digunakan oleh pengirim maupun penerima pesan. Pengembangan kriptografi visual dengan menggunakan *Elliptic Curve Cryptography* terdiri dari tiga tahap. Tahap pertama adalah pembangkitan kunci oleh pengirim dan penerima pesan, tahap kedua adalah enkripsi gambar oleh pengirim pesan dan tahap ketiga adalah dekripsi *share image* oleh penerima pesan. Pengembangan kriptografi visual dengan menggunakan *Elliptic Curve Cryptography* dapat mempersulit kriptanalisis karena harus meretas dua algoritma dan tidak akan bisa diretas jika hanya memperoleh salah satu *share image*.

5. DAFTAR PUSTAKA

[1] Munir, R. (2010). *Matematika Diskrit* (3rd ed.). Bandung: Informatika Bandung.

[2] Naor, M., & Shamir, A. (1995). *Visual Cryptography*. Advances in Cryptology, Vol. 950.

[3] Miller V.S. (1986). Use of Elliptic Curves in Cryptography. In: Williams

H.C. (eds) Advances in Cryptology — CRYPTO ’85 Proceedings. CRYPTO 1985. Lecture Notes in Computer Science, vol 218. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-39799-X_31

[4] Koblitz, N. (1984) Introduction to Elliptic Curves and Modular Forms, Graduate Texts in Mathematics, vol. 97, Springer-Verlag, New York.

[5] Shankar, K., Devika, G., Ilayaraja, M. (2017). *Scheme based on Boolean Operations ad Elliptic Curve Cryptography*. Nadu: School of Computing, Kalasalingam University.

[6] Munthe, A. R., Ratnadewi. (2014). *Kriptografi Visual Pada Citra Berwarna Menggunakan Metode Kombinasi Perluasan Warna Red, Green dan Blue*. Bandung: Jurusan Teknik Elektro, Universitas Kristen Maranatha.

[7] Stinson, D. (2006). *Cryptography: Theory and Practice* (3rd ed.). Boca Raton, Florida: Chapman & Hall/CR