Implementasi *Secret Sharing Scheme* dan Visual Kriptografi dalam Pembagian Gambar Rahasia

Aira Thalca Avila Putra – 13520101[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
[1]13520101@std.stei.itb.ac.id

***Abstract*—Makalah ini fokus pada implementasi Secret Sharing Scheme dan kriptografi visual dalam konteks pembagian gambar rahasia. Kami menjelaskan konsep dasar dari Secret Sharing Scheme dan kriptografi visual untuk membagi gambar menjadi beberapa bagian yang terenkripsi. Kami membahas langkah-langkah implementasi untuk membagi gambar rahasia menggunakan Secret Sharing Scheme. Dengan menggabungkan Secret Sharing Scheme dan kriptografi visual, makalah ini bertujuan untuk menyediakan metode yang aman dan intuitif untuk membagi dan memulihkan gambar rahasia.**

Keywords—Secret Sharing Scheme, Visual Cryptography, Confidentiality, Skema (t,n),

I. PENDAHULUAN

Keamanan informasi dan kerahasiaan data merupakan hal yang sangat penting dalam dunia digital saat ini. Dalam upaya untuk melindungi data rahasia dari akses yang tidak sah, Secret Sharing Scheme dan kriptografi visual telah menjadi dua bidang yang menarik perhatian.

Secret Sharing Scheme adalah sebuah metode yang digunakan untuk membagi sebuah rahasia menjadi beberapa bagian yang tersebar di antara entitas-entitas yang berpartisipasi. Dalam skenario ini, rahasia hanya dapat direkonstruksi ketika sejumlah tertentu dari bagian-bagian tersebut dikumpulkan. Pendekatan ini memberikan tingkat keamanan yang lebih tinggi karena bahkan jika salah satu bagian rahasia terungkap, informasi yang diperoleh masih belum cukup untuk mengungkapkan keseluruhan rahasia.

Di sisi lain, kriptografi visual merupakan bidang yang menggabungkan konsep kriptografi dengan representasi visual seperti gambar. Dalam kriptografi visual, gambar asli dipecah menjadi beberapa bagian terenkripsi, yang masing-masing tidak memberikan informasi yang berguna tentang gambar asli. Baru ketika bagian-bagian ini dikombinasikan secara tepat, gambar asli dapat direkonstruksi.

Data gambar rahasia merupakan jenis data yang sangat penting dan memerlukan perlindungan yang kuat terhadap akses yang tidak sah. Menggunakan Secret Sharing Scheme dan kriptografi visual dalam konteks ini dapat memberikan beberapa keuntungan. Dengan menggunakan *Secret Sharing Scheme*, gambar rahasia dapat dibagi menjadi beberapa bagian yang tersebar di antara entitas yang berpartisipasi. Hal ini menjamin bahwa untuk mendapatkan akses ke gambar asli, sejumlah *treshold* bagian harus dikumpulkan, sehingga meningkatkan keamanan dan mencegah akses yang tidak sah.

Selain itu, kriptografi visual memberikan tingkat kerahasiaan yang lebih tinggi pada gambar rahasia. Dengan membagi gambar menjadi bagian-bagian terenkripsi, informasi yang diperoleh dari setiap bagian tidak memberikan petunjuk yang berguna tentang gambar asli. Sehingga, walaupun seorang penyerang memperoleh salah satu bagian, ia masih tidak dapat mendapatkan gambar asli kecuali ia memiliki bagian-bagian lainnya.

Melalui kombinasi *Secret Sharing Scheme* dan kriptografi visual, makalah ini bertujuan untuk menjelaskan dan menerapkan metode yang efektif untuk membagi dan memulihkan gambar rahasia dengan tingkat keamanan yang tinggi. Dengan demikian, diharapkan bahwa penggunaan Secret Sharing Scheme dan kriptografi visual dapat menjamin kerahasiaan data gambar rahasia dalam konteks yang lebih aman dan terpercaya.

II. DASAR TEORI

A. *Kriptografi*

Kriptografi merupakan kakas (*tool*) yang sangat penting dalam dunia keamanan informasi. Kriptografi adalah ilmu yang mempelajari teknikteknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi. Kata kriptografi itu sendiri berasal dari Bahasa Yunani, *Cryptos* (*Secret or Hidden)* dan *Graphein* (*Writing*). Kriptografi menjaga sebuah pesan atau data terjamin keamanannya. Prinsip-prinsip pada keamanan kriptografi yaitu:

1) Terjaga kerahasiannya (*Confidentiality)*

Kerahasiaan adalah prinsip kriptografi yang menjamin bahwa informasi atau data hanya dapat diakses oleh pihak yang berwenang atau yang memiliki kunci rahasia, sehingga menjaga kerahasiaan data dari akses yang tidak sah.

2) Terjaga keasliannya (*Integrity)*

Integritas adalah prinsip kriptografi yang menjamin bahwa data atau informasi tidak mengalami perubahan yang tidak sah atau tidak diotorisasi selama penyimpanan,

pengiriman, atau pemrosesan. Hal ini dicapai dengan menggunakan fungsi hash dan tanda tangan digital untuk mendeteksi perubahan atau manipulasi data.

3) Keaslian pengirim pesan (*Authentication)*

Memverifikasi identitas pihak yang berkomunikasi dengan menggunakan metode seperti kunci rahasia, sertifikat digital, atau algoritma challenge-response untuk memastikan keaslian dan integritas data yang dikirimkan.

4) Anti-penyangkalan (*Non-repudiation)*

Non-repudiation adalah prinsip kriptografi yang menjamin bahwa pengirim suatu pesan atau transaksi tidak dapat menyangkal bahwa mereka mengirimkannya. Ini dicapai dengan menggunakan tanda tangan digital yang mengikat pesan dengan kunci pribadi pengirim sehingga tidak dapat diubah atau dibantah oleh pihak yang mengirimkannya.

Dengan memahami dasar-dasar teori kriptografi ini, kita dapat menerapkan teknik-teknik kriptografi yang sesuai untuk melindungi kerahasiaan, integritas, dan otentikasi data dalam berbagai aplikasi, seperti komunikasi jaringan, penyimpanan data, dan transaksi elektronik.

B. Polinomial

Polinomial merupakan konsep dasar dalam matematika yang memiliki peran penting dalam berbagai bidang, termasuk kriptografi. Sebuah polinomial adalah suatu ekspresi matematika yang terdiri dari suku-suku dengan pangkat dan koefisien. Pangkat pada suku-suku polinomial menunjukkan derajat polinomial, yang menentukan jumlah variabel dan kompleksitasnya. Sebuah polinomial biasanya dinotasikan sebagai berikut

$$a_o x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$$

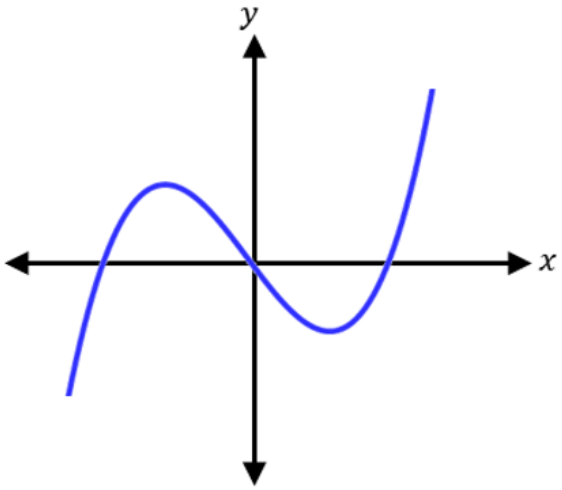
Polinomial memiliki sifat-sifat penting yang berguna dalam kriptografi. Salah satu sifat dasar polinomial adalah kemampuannya untuk melakukan operasi penjumlahan dan perkalian. Operasi penjumlahan polinomial memungkinkan penggabungan polinomial yang memiliki suku-suku dengan pangkat yang sama, sementara operasi perkalian polinomial menghasilkan polinomial baru dengan mengalikan setiap suku satu sama lain.

Pada kriptografi, polinomial sering digunakan dalam skema pembagian data rahasia (*secret sharing scheme*) di mana rahasia dibagi menjadi beberapa bagian dan didistribusikan ke berbagai pihak. Dalam skema ini, polinomial digunakan untuk menghasilkan bagian-bagian rahasia dengan menerapkan nilai-nilai variabel pada polinomial. Untuk mengembalikan rahasia, diperlukan beberapa bagian yang dikombinasikan melalui interpolasi polinomial.

Selain itu, polinomial juga terkait erat dengan algoritma enkripsi kunci-publik seperti RSA dan ElGamal. Dalam algoritma ini, operasi matematika pada polinomial digunakan untuk mengenkripsi dan mendekripsi pesan. Misalnya, algoritma RSA melibatkan perkalian polinomial dalam ruang polinomial modulo. Prinsip-prinsip dasar polinomial, seperti teorema dasar aljabar yang menyatakan bahwa setiap polinomial memiliki akar kompleks, digunakan dalam analisis keamanan dan kompleksitas algoritma kriptografi.

Dalam pemecahan masalah matematika kriptografi, polinomial juga memiliki peran kunci. Misalnya, dalam faktorisasi bilangan bulat, metode seperti Algoritma Lenstra atau Algoritma Berlekamp tergantung pada manipulasi polinomial untuk mencari faktor-faktor bilangan bulat. Demikian pula, dalam logaritma diskret, polinomial digunakan untuk merumuskan persamaan yang membantu dalam mencari nilai-nilai yang memenuhi persamaan eksponensial.

Dengan memahami dasar teori polinomial, termasuk operasi, sifat, dan aplikasinya dalam kriptografi, kita dapat mengembangkan dan menganalisis algoritma kriptografi yang lebih kuat, mengamankan komunikasi dan melindungi data dari akses yang tidak sah.



Gambar 1. Contoh grafik dari sebuah polynomial

C. Interpolasi Lagrange

Interpolasi Lagrange adalah sebuah metode dalam matematika yang digunakan untuk mengkonstruksi polinomial dengan tingkat tertentu yang melalui sejumlah titik data yang diketahui. Dasar teori yang mendasari interpolasi Lagrange adalah konsep polinomial dan metode pencocokan polinomial.

Misalkan kita memiliki $n+1$ titik data $(x_0, y_0), (x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)$ di mana setiap titik data memiliki nilai x dan nilai y yang diketahui. Tujuan dari interpolasi Lagrange adalah untuk menemukan polinomial $p(x)$ dengan derajat n yang memenuhi persamaan $p(x_i) = y_i$ untuk setiap titik data yang diberikan.

Rumus dasar dalam interpolasi Lagrange adalah sebagai berikut:

$$p(x) = \sum_{i=0}^{n} y_i L_i(x_i)$$

Di mana $p(x)$ adalah polinomial yang dicari, y_i adalah nilai y pada titik data ke-i, dan $L_i(x_i)$ adalah fungsi dasar Lagrange yang didefinisikan sebagai berikut:

$$L_i(x) = \prod_{\substack{j=1 \\ j \neq i}}^{t} \frac{x - x_j}{x_i - x_j}$$

Fungsi dasar Lagrange ini memastikan bahwa $p(x)$ memenuhi syarat $p(x_i) = y_i$ untuk setiap titik data, dengan memperhitungkan kontribusi masing-masing titik data dalam pembentukan polinomial.

Rumus ini memberikan polinomial $p(x)$ yang unik yang melalui semua titik data yang diberikan. Dengan menggunakan interpolasi Lagrange, kita dapat mengestimasi nilai $p(x)$ untuk nilai x yang tidak termasuk dalam titik data asli.

Interpolasi Lagrange memiliki kelebihan dalam kesederhanaan dan kemudahan implementasi, tetapi dapat menghasilkan polinomial yang kompleks jika jumlah titik data meningkat. Dalam prakteknya, metode interpolasi Lagrange sering digunakan untuk mendekati fungsi atau menghasilkan perkiraan nilai di antara titik data yang diketahui.

D. Shamir's Secret Sharing Scheme

Shamir's Secret Sharing Scheme adalah salah satu skema pembagian data rahasia yang dikembangkan oleh Adi Shamir. Skema ini bertujuan untuk membagi sebuah rahasia menjadi beberapa bagian yang didistribusikan kepada beberapa pihak, di mana hanya dengan menggabungkan sejumlah bagian yang ditentukan, rahasia tersebut dapat dipulihkan kembali. Dasar teori yang mendasari *Shamir's Secret Sharing Scheme* melibatkan konsep matematika seperti polinomial, interpolasi polinomial, dan aritmetika modulo.

Pada dasarnya, *Shamir's Secret Sharing Scheme* menggunakan interpolasi polinomial untuk membagi rahasia. Misalnya, jika terdapat sebuah rahasia yang ingin dibagi menjadi n bagian dan dapat direkontruksi oleh t bagian, skema ini menggunakan polinomial dengan derajat t untuk menghasilkan bagian-bagian tersebut. Setiap bagian diberikan kepada pihak yang berbeda.

Proses pembagian rahasia melibatkan pembentukan polinomial dengan mengacak koefisien polinomial sehingga suku-suku polinomialnya tidak dapat ditebak. Rahasia tersebut kemudian diwakilkan oleh nilai dari polinomial pada titik 0 (biasanya disebut sebagai koefisien bebas). Bagian-bagian rahasia dihitung dengan menggantikan nilai x pada polinomial dengan angka acak yang berbeda untuk setiap bagian.

Untuk mengembalikan rahasia, setidaknya diperlukan sejumlah bagian yang ditentukan sebelumnya. Dengan menggunakan interpolasi polinomial, rahasia dapat dipulihkan dengan menggabungkan bagian-bagian tersebut. Algoritma interpolasi Lagrange sering digunakan dalam skema ini untuk menghitung nilai rahasia yang asli berdasarkan bagian-bagian yang diterima.

Keamanan *Shamir's Secret Sharing Scheme* didasarkan pada sifat matematika polinomial dan ketidakmungkinan untuk mengidentifikasi polinomial asli dari sejumlah bagian yang diberikan. Selain itu, skema ini juga dapat menangani situasi jika beberapa bagian rahasia hilang atau korupsi.

Shamir's Secret Sharing Scheme telah diterapkan dan digunakan dalam berbagai aplikasi kriptografi dan keamanan, seperti penyimpanan data rahasia, pembagian kunci, dan mekanisme pemulihan dalam sistem yang toleran kesalahan. Skema ini memberikan solusi yang efektif dalam membagi rahasia dan memastikan bahwa rahasia tetap aman meskipun bagian-bagian rahasia tersebut berada di tangan pihak yang berbeda.

E. Kriptografi Visual

Kriptografi visual adalah cabang dari kriptografi yang menggunakan gambar atau visual sebagai media untuk mengamankan informasi. Dasar teori kriptografi visual melibatkan konsep-konsep seperti transformasi gambar, steganografi, dan pengolahan citra.

Pada dasarnya, kriptografi visual bertujuan untuk menyembunyikan informasi rahasia di dalam gambar sehingga hanya penerima yang ditujukan yang dapat mendapatkan akses ke informasi tersebut. Salah satu teknik yang umum digunakan dalam kriptografi visual adalah steganografi, di mana data rahasia disembunyikan dalam gambar dengan cara yang tidak terlihat oleh mata manusia.

Steganografi dalam kriptografi visual melibatkan teknik penggabungan data rahasia ke dalam bit-bit gambar. Misalnya, data rahasia dapat disembunyikan dalam bit-bit piksel yang tampaknya tidak berubah secara visual, seperti mengubah bit yang paling tidak signifikan pada setiap piksel. Dalam proses ini, perubahan yang terjadi pada gambar sangat kecil sehingga tidak terlihat oleh mata manusia.

Selain itu, kriptografi visual juga melibatkan teknik transformasi gambar untuk mengamankan informasi. Misalnya, teknik enkripsi dapat diterapkan pada gambar dengan menggunakan algoritma kriptografi kunci-simetris atau kunci-publik. Dalam proses ini, gambar diubah menggunakan kunci rahasia sehingga hanya penerima yang memiliki kunci yang tepat yang dapat mendekripsi gambar tersebut.

Prinsip dasar kriptografi visual adalah menjaga kerahasiaan informasi dengan cara menyembunyikan atau mengubah informasi rahasia secara visual dalam gambar. Teknik-teknik seperti steganografi dan enkripsi digunakan untuk mencapai tujuan ini. Kriptografi visual memiliki banyak aplikasi, seperti keamanan pesan, keamanan citra medis, dan perlindungan hak cipta pada konten digital.

III. IMPLEMENTASI

Bagian ini bertujuan untuk menjelaskan secara rinci langkah-langkah implementasi dari *Secret Sharing Scheme* dalam pembagian gambar rahasia. Langkah-langkah implementasi ini dibuat dalam Bahasa pemrograman *python* dan akan dijelaskan secara rinci dalam subbab-subbab berikut, termasuk algoritma yang digunakan serta perhitungan matematis yang terlibat.

A. Pembagian gambar menjadi beberapa *shares*

Pada tahap pertama implementasi, gambar rahasia akan dibagi menjadi beberapa bagian, yang disebut sebagai *shares*. Langkah pertama adalah membaca dan memuat gambar asli

yang akan dibagi. Gambar ini dapat berupa format file yang umum digunakan, seperti JPEG, PNG, atau BMP. Gambar dibaca dengan menggunakan modul cv2 yang menghasilkan *array* dua dimensi dimana setiap nilai pada *array* merupakan nilai piksel pada indeks yang berkaitan. File yang sudah berbentuk *array* tersebut kemudian dikonversi menjadi *array grayscale* sehingga setiap elemen pada *array* hanya menyimpan satu nilai saja.

Langkah yang kedua adalah melakukan kalkulasi dan pembagian gambar menjadi beberapa *shares*. Hal ini dlakukan dengan mengiterasi setiap pixel pada *array*. Nilai pada piksel tersebut kemudian menjadi nilai ***Secret*** pada polinomial yang akan dibentuk sehingga polinomial yang terbentuk adalah sebagai berikut:

$$f(x) = Secret + a_0 x^t + a_1 x^{t-1} + \cdots + a_{t-1} x$$

Kemudian dihitung nilai $(1, f(1)), (2, f(2)), \ldots, (n, f(n))$ dengan n adalah banyak *shares* yang akan dibentuk. Untuk setiap *shares*, misalkan *shares* ke-I, nilai pada pixel *share image* adalah hasil konversi dari $f(i)$ menjadi nilai-nilai sensitivitas RGB dengan konversi sebagai berikut:

1) Nilai *Blue* dihitung dengan $B = f(i)/255$
2) Nilai *Red* dihitung dengan $R = Random\ (0, f(i)\ \%\ 255 + 1)$
3) Nilai *Green* dihitung dengan $G = f(i)\ \%\ 255 - R$

Konversi tersebut dilakukan untuk setiap piksel di setiap *shares* yang akan dibentuk. Berikut ini adalah fungsi pembacaan *image* hingga pembagiannya menjadi beberapa *shares*

```
def image_sharing(filename,t,n):
  shares = []
  img = cv2.imread(filename)
  #Mengkonversi gambar menjadi bentuk greyscale
  grey = cv2.cvtColor(img, cv2.COLOR_BGR2GRAY)
  newimg = np.asarray(grey)

  print("Encrypting images. Please wait; this may take a few minutes. ")
  #inisialisasi shares
  rows, cols = newimg.shape
  res_shares = np.zeros((n,rows,cols,3), dtype='uint8')

  # perhitungan nilai seluruh pixel pada setiap shares
  for i in range(rows):
    for j in range(cols):
      #Perhitungan fungsi polinomial sebanyak n titik dengan derajat t
      all_shares = sc.create_shares(t, n, newimg[i][j])
      for shares in all_shares:
        #Perhitungan nilai R, G, dan B dari hasil fungsi polinomial
        remainder = shares[1] % 255
        # Nilai Blue
        res_shares[shares[0]-1][i][j][0] = int(shares[1]/255)
        # Nilai Red
        res_shares[shares[0]-1][i][j][1] = random.randrange(0,remainder+1)
        # Nilai Green
        res_shares[shares[0]-1][i][j][2] = remainder - res_shares[shares[0]-1][i][j][1]

  for i in range(len(res_shares)):
    newfile = filename[:-4] + str(i+1) + ".png"
    print(newfile)
    window = "Share " + str(i+1)
    cv2.imshow(window, res_shares[i])
    cv2.imwrite(newfile, res_shares[i])
  return
```

Fungsi perhitungan $(i, f(i))$ untuk setiap i dari 1 sampai n. Koefisien polinomial dirandomisasi untuk mempersulit kriptanalisis karena *shares* yang terbentuk polanya akan berbeda untuk setiap gambar yang di enkripsi.

```
def create_shares(threshold, shares, pixel, prime = PRIME):
    if threshold > shares:
        raise ValueError("impossible to recover the secret")
    #Koefisien fungsi polinomial yang dirandom
    poly_coeff = [pixel] + [random.SystemRandom().randrange(1000) for i in range(threshold - 1)]
    #Perhitungan nilai f(i)
    points = [(i, f_value(poly_coeff, i, prime)) for i in range(1, shares + 1)]
    return points

def f_value(poly_coeff, x, prime):
    res = 0
    for coeff in reversed(poly_coeff):
        res = (res * x + coeff) % prime
    return res
```

Pada akhir tahap ini, *shares* sebanyak n sudah terbentuk dan dapat dibagikan dengan syarat jika ingin rekontruksi maka dibutuhkan setidaknya t buah *shares.*

B. Pemulihan atau Rekonstruksi Gambar

Untuk melakukan pemulihan dan rekontruksi gambar, digunakan skema (t,n) dimana dari *n shares* yang dibentuk pada pembagian gambar, dibutuhkan setidaknya *t shares* untuk merekontruksi gambar yang terbentuk. Rekontruksi gambar diawali dengan mengubah nilai RGB pada setiap piksel menjadi nilai tunggal dengan formula berikut:

$$f(i) = B(i) * 255 + R(i) + G(i)$$

```
def restore(pictures,keys):

  for i in range(len(pictures)):
    image.append(cv2.imread(pictures[i]))
    image[i] = np.asarray(image[i])

  rows, cols = image[0].shape[:2]
  restored_image = np.zeros((rows,cols), dtype =
'uint8')

  mat = np.zeros((rows,cols,3))
  mat1 = np.full((rows,cols), 1)
  mat255 = np.full((rows,cols), 255)
  mat[:,:,0] = mat255
  mat[:,:,1] = mat1
  mat[:,:,2] = mat1

  ac_share = []
  for i in range(len(pictures)):
    t_mat = np.multiply(image[i][:,:,0], mat255)
    ac_share.append(np.add(image[i][:,:,2] +
image[i][:,:,1], t_mat))

  for i in range(rows):
    for j in range(cols):
      shares = []

      for k in range(len(pictures)):
        shares.append((keys[k],ac_share[k][i][j]))
      restored_image[i][j] =
sc.reconstruct(shares)
  cv2.waitKey(0)
  cv2.destroyAllWindows()
```

```
  return restored_image
```

Nilai pada setiap piksel tersebut kemudian di pasangkan dengan nilai *i* yaitu indeks dari *shares* tersebut (dari 1 sampai n). Setelah perhitungan setiap piksel dari setiap *shares* selesai. Nilai piksel pada indeks yang berkorespodensi kemudian dicari nilai *shares*-nya dengan menggunakan interpolasi lagrange.

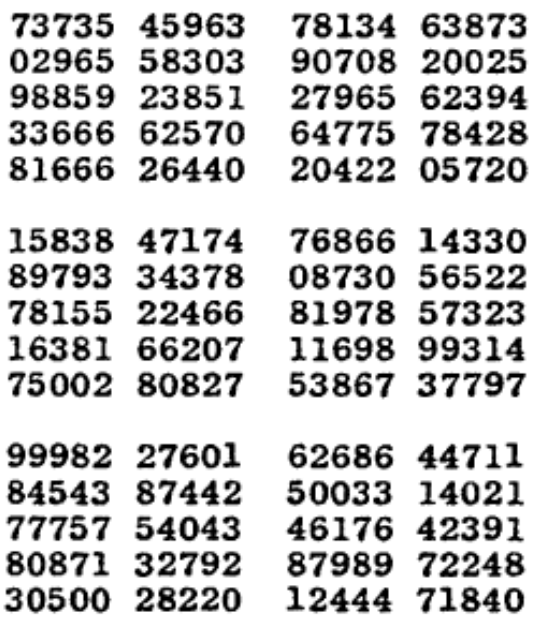
```
def interpolate_lagrange(x, x_s, y_s, p):
    k = len(x_s)
    assert k == len(set(x_s)), "points must be
distinct"
    def PI(vals):
        res = 1
        for v in vals:
            res *= v
        return res
    nums = []
    dens = []
    for i in range(k):
        others = list(x_s)
        cur = others.pop(i)
        nums.append(PI(x - o for o in others))
        dens.append(PI(cur - o for o in others))
    den = PI(dens)
    num = sum([divmod(nums[i] * den * y_s[i] % p,
dens[i], p)
               for i in range(k)])
    return (divmod(num, den, p) + p) % p

def reconstruct(shares, prime= PRIME):
    if len(shares) < 2:
        raise ValueError("need at least two
shares")
    x_s, y_s = zip(*shares)
    return interpolate_lagrange(0, x_s, y_s,
prime)
```

IV. Pengujian Dan Analisis

Pada bagian ini, akan dilakukan pengujian kode program dan juga analisis hasil uji. Pengujian dilakukan terhadap kode program yang digunakan dalam implementasi Secret Sharing Scheme dengan kriptografi visual.

A. Pengujian Kode Program

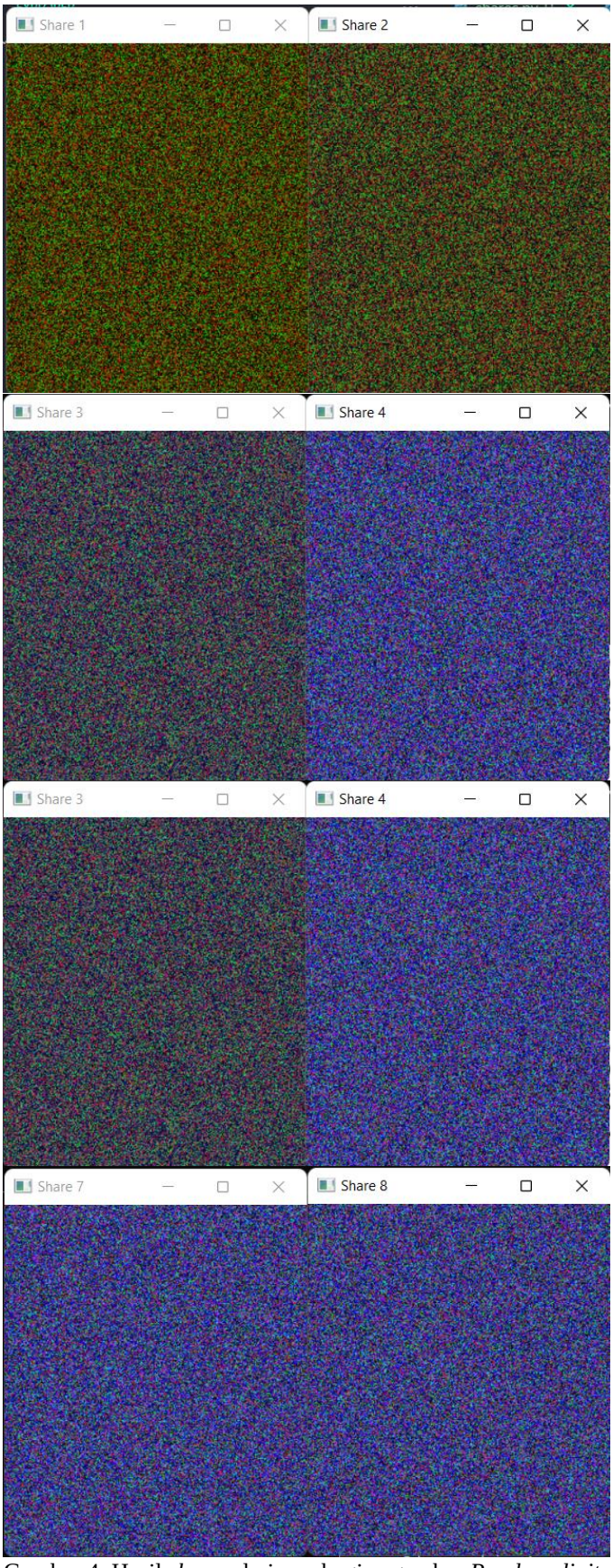
Untuk menguji kode program, akan digunakan gambar *random number* dibawah ini.



Gambar 2. Gambar *Random Number* sebagai Gambar Rahasia

Skema yang akan digunakan adalah Skema(4,8) dimana gambar awal akan dibagi menjadi 8 *shares* dan untuk merekonstruksi akan dibutuhkan setidaknya 4 *shares* yang berbeda.

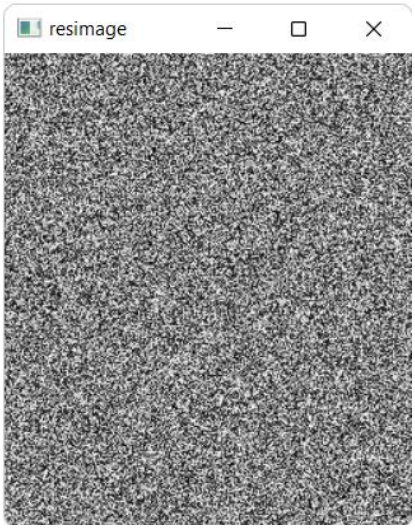
Gambar 3. Pembagian gambar Random_digits dengan skema (4,8)



Gambar 4. Hasil *shares* dari pembagian gambar *Random digits*

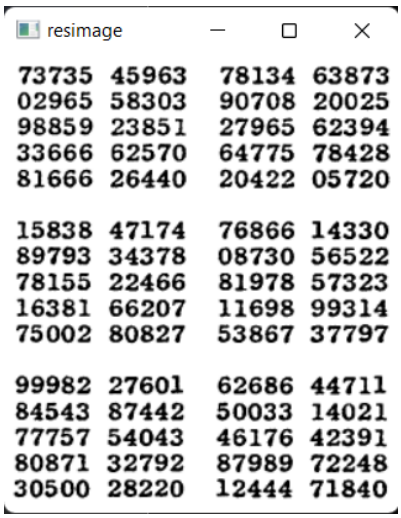
Dari hasil pengujian, dapat dilihat bahwa *shares* sudah tidak dapat dikenali lagi dari gambar aslinya. Setelah itu, akan dilakukan pengujian rekonstruksi dengan banyak *shares* empat dan tiga untuk membuktikan bahwa dibutuhkan minimal empat *shares* untuk merekonstruksi gambar pada skema (4,8).

```
Would you like to restore the image? (y/n): y
Restoring an image...
Enter the filename of a share or 'done' if finished: Random_digits3.png
Enter key value of image: 3
Enter the filename of another share or 'done' if finished: Random_digits6.png
Enter key value of image: 6
Enter the filename of another share or 'done' if finished: Random_digits2.png
Enter key value of image: 2
Enter the filename of another share or 'done' if finished: done
```



Gambar 5. Hasil rekonstruksi dari 3 *shares*

```
Restoring an image...
Enter the filename of a share or 'done' if finished: Random_digits3.png
Enter key value of image: 3
Enter the filename of another share or 'done' if finished: Random_digits6.png
Enter key value of image: 6
Enter the filename of another share or 'done' if finished: Random_digits2.png
Enter key value of image: 2
Enter the filename of another share or 'done' if finished: Random_digits4.png
Enter key value of image: 4
Enter the filename of another share or 'done' if finished: done
```



Gambar 6. Hasil rekonstruksi dari 4 *shares*

B. Analisis

Hasil uji coba menunjukkan bahwa rekonstruksi gambar rahasia menggunakan hanya 3 shares tidak menghasilkan gambar yang dapat dikenali. Gambar yang direkonstruksi masih memiliki tingkat keabuan yang tinggi dan tidak memperlihatkan bentuk atau konten yang jelas. Hal ini menunjukkan bahwa dalam skema (4,8), jumlah minimum shares yang dibutuhkan untuk melakukan rekonstruksi dengan hasil yang memadai adalah lebih dari 3. Hasil ini konsisten dengan prinsip dasar dari Secret Sharing Scheme, di mana keberhasilan rekonstruksi bergantung pada jumlah shares yang digunakan.

Namun, ketika dilakukan rekonstruksi dengan menggunakan 4 shares, gambar rahasia berhasil direkonstruksi dengan baik. Gambar yang dihasilkan identik dengan gambar Random_digits yang sebelumnya dibagi. Hal ini menunjukkan bahwa dengan menggunakan jumlah shares yang lebih banyak dari minimum yang dibutuhkan, rekonstruksi gambar rahasia dapat dilakukan secara akurat dan memuaskan. Hasil ini menunjukkan bahwa metode Secret Sharing Scheme dengan kriptografi visual yang diimplementasikan berhasil menghasilkan pemulihan yang dapat dikenali dan sesuai dengan gambar asli.

Dengan menganalisis hasil uji coba, dapat disimpulkan bahwa implementasi Secret Sharing Scheme dengan kriptografi visual mampu menghasilkan rekonstruksi gambar rahasia yang dapat dikenali dan sesuai dengan gambar asli. Jumlah minimum shares yang dibutuhkan untuk rekonstruksi dengan hasil yang memadai bergantung pada skema yang digunakan, namun hasil yang lebih baik dapat dicapai dengan menggunakan jumlah shares yang lebih banyak. Analisis ini memberikan pemahaman yang lebih baik tentang kekuatan dan keterbatasan metode ini dalam pemulihan gambar rahasia dengan kriptografi visual.

V. KESIMPULAN DAN SARAN

Dapat disimpulkan bahwa implementasi Secret Sharing Scheme dengan kriptografi visual memiliki potensi yang besar dalam menjaga kerahasiaan dan keutuhan data gambar rahasia. Metode ini efektif dalam membagi gambar menjadi beberapa bagian (*shares*) dan merekonstruksinya kembali dengan menggunakan sebagian dari shares tersebut. Uji coba yang dilakukan berhasil membagi gambar menjadi 8 shares dan merekonstruksinya dengan menggunakan 4 shares. Hasil rekonstruksi menunjukkan bahwa metode ini efektif dalam mempertahankan kerahasiaan dan integritas data.

Namun, perlu dilakukan pengembangan lebih lanjut untuk meningkatkan metode ini. Pengujian dengan variasi ukuran gambar dan jumlah shares, serta analisis keamanan yang mendalam, akan memberikan pemahaman yang lebih baik. Integrasi dengan teknik kriptografi lainnya juga dapat meningkatkan tingkat keamanan dan keandalan sistem.

UCAPAN TERIMA KASIH

Pertama-tama, penulis ingin mengucapkan terima kasih kepada Tuhan Yang Maha Esa atas rahmat, berkat, dan petunjuk-Nya yang selalu mengiringi perjalanan penulisan makalah ini. Kehadiran-Nya memberikan inspirasi dan kekuatan dalam menyelesaikan tugas ini. Penulis juga ingin menyampaikan terima kasih kepada Bapak Dr. Ir. Rinaldi Munir, M.T., selaku pembimbing dalam penulisan makalah ini. Tidak lupa, penulis juga ingin berterima kasih kepada keluarga dan teman-teman yang selalu memberikan dukungan, dorongan, dan motivasi selama proses penulisan. Kehadiran mereka membuat perjalanan ini lebih menyenangkan dan menginspirasi.

REFERENSI

[1] Munir,Rinaldi. 2023. *Pengantar Kriptografi: Bahan Kuliah IF4020 Kriptografi*. Merupakan slide bahan ajar perkuliahan yang diunduh dari Edunex pada tanggal 19 Mei 2023.

[2] Munir,Rinaldi. 2023. *Kriptografi Modern: Bahan Kuliah IF4020 Kriptografi*. Merupakan slide bahan ajar perkuliahan yang diunduh dari Edunex pada tanggal 19 Mei 2023.

[3] Munir,Rinaldi. 2023. *Skema Pembagian Data Rahasia* (*Secret Sharing Scheme): Bahan Kuliah IF4020 Kriptografi*. Merupakan slide bahan ajar perkuliahan yang diunduh dari Edunex pada tanggal 19 Mei 2023.

[4] Munir,Rinaldi. 2023. *Kriptografi Visual (Bagian 2): Bahan Kuliah IF4020 Kriptografi*. Merupakan slide bahan ajar perkuliahan yang diunduh dari Edunex pada tanggal 19 Mei 2023.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Yogyakarta, 21 Mei 2023

Aira Thalca Avila Putra
13520101