Implementasi Skema Pembagian Data Rahasia untuk Data Video menggunakan Nilai Rata-Rata Angka Acak

Stefanus Jeremy Aslan - 13519175 (*Author*)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail (gmail): 13519175@std.stei.itb.ac.id

***Abstract*—Perlindungan kerahasiaan pesan melalui enkripsi dan dekripsi pesan mungkin saja tidak cukup untuk memenuhi kebutuhan akan pengaksesan isi pesan yang menuntut partisipasi antarpenerima. Untuk itu, dikembangkanlah skema pembagian data rahasia yang mengharuskan partisipasi dari sejumlah atau semua penerima pesan agar dapat mengakses isi pesan rahasia. Makalah ini membahas tentang implementasi skema pembagian data rahasia, tidak untuk data teks, tetapi untuk data video yang berupa runtutan gambar. Algoritma yang diimplementasikan memanfaatkan pembangkitan angka acak yang apabila dijumlahkan, menghasilkan nilai rata-rata berupa piksel data rahasia semula. Berdasarkan hasil implementasi, didapatkan bahwa algoritma ini jauh dari sempurna, terutama apabila digunakan untuk video berwarna sangat terang atau sangat gelap.**

Keywords—kerahasiaan; skema pembagian data rahasia; partisipasi; penerima; pembangkitan angka acak

I. PENDAHULUAN

Data dan informasi merupakan hal yang abstrak, dan dapat diperoleh dari apapun dan dapat juga berupa apapun. Dalam kehidupan sehari-hari di masyarakat, data dan informasi tidak selalu hanya ditujukan atau disimpan untuk diri sendiri. Ada kala ketika individu menginginkan data dan informasi yang dimilikinya untuk diketahui oleh orang lain. Pemilik data mungkin saja tidak keberatan apabila data dan informasi miliknya diketahui oleh publik secara luas, tetapi ada juga data yang bersifat rahasia dan hanya boleh diketahui oleh orang berwenang. Oleh sebab itu, ketika data dan informasi rahasia dikirimkan dalam pesan kepada pihak lain, perlu adanya jaminan sehingga hanya pihak yang berwenang saja yang dapat mengakses isi dari pesan tersebut. Adapun ilmu yang mempelajari praktik keamanan pesan kerap dikenal secara luas sebagai kriptografi.

Salah satu cara yang umum digunakan dalam menjamin kerahasiaan data yaitu melalui proses penguncian pesan yang dikenal sebagai enkripsi. Proses ini merupakan proses pengubahan isi pesan sedemikian sehingga pesan tidak dapat dipahami hingga dilakukan proses pengembalian pesan ke bentuk semula yang dikenal sebagai dekripsi. Proses dekripsi dilakukan menggunakan kunci yang hanya dimiliki oleh penerima pesan. Oleh sebab itu, apabila pesan jatuh ke pihak tidak berwenang, kerahasiaan isi pesan tetap terjamin karena pihak tersebut tidak memiliki kunci untuk mendekripsi pesan.

Pesan yang sehari-hari digunakan sering kali berupa data teks. Akan tetapi, pesan teks umumnya dibatasi oleh kemampuan deskripsi dan ekspresi pembuat pesan dalam bahasa sehari-hari, baik dari sisi kemahiran pengguna bahasa maupun dari kelengkapan bahasa. Masalah ini kerap disebut dengan informal sebagai ‘tidak bisa dideskripsikan dengan kata-kata’, dan tentunya akan berpengaruh terhadap kualitas isi pesan. Oleh sebab itu, ada baiknya apabila menggunakan bentuk lain untuk menyusun isi pesan. Adapun salah satu alternatif teks untuk informasi visual yaitu gambar atau citra. Dengan menggunakan gambar, penerima dapat secara langsung memahami pesan tanpa harus memvisualisasi gambar dari deskripsi teks. Mengingat invensi video yang dibentuk dari penangkapan gambar yang diambil secara runtut dengan interval sangat kecil, gambar atau video dapat mensimulasikan kejadian nyata secara visual dengan detail yang jauh melampaui apa yang bisa dideskripsikan dari teks. Ini berarti gambar, dalam bentuk video, memiliki potensi sangat besar sebagai wujud data dan informasi untuk dikirimkan.

Dengan semakin berkembangnya wujud data dan informasi yang disalurkan, perkembangan penyaluran data dan informasi tersebut harus semakin diperhatikan. Tidak hanya tingkat keamanan, kriptografi juga selayaknya dapat memperluas variasi kasus keamanan yang dapat ditangani di bidangnya. Salah satu skenario unik dalam penerapan kriptografi yaitu skema pembagian data rahasia. Berbeda dengan skenario pengiriman pesan pada umumnya, skema pembagian data rahasia memerlukan interaksi antara sejumlah penerima pesan.

II. DASAR TEORI

A. *Kriptografi*

Kriptografi adalam adalah ilmu yang mempelajari Teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi[1]. Adapun penerapan kriptografi dalam platform digital disebut sebagai kriptografi modern. Untuk lebih detail, berikut adalah empat layanan yang diberikan oleh kriptografi.

1. Kerahasiaan
   Kriptografi menjamin kerahasiaan isi pesan, sedemikian sehingga hanya penerima pesan saja yang memiliki kapabilitas untuk mengakses isi pesan. Adapun kerahasiaan umumnya dijamin dengan menerapkan proses enkripsi dan dekripsi.
2. Integritas data
   Kriptografi menjamin keabsahan isi pesan. Ini berarti pesan tidak dapat dicegat dalam pengiriman untuk dimodifikasi tanpa diketahui oleh pihak penerima. Integritas data dapat dijamin dengan membandingkan hasil fungsi hash yang dikirim bersama pesan dengan hasil fungsi hash dari pesan yang diterima.
3. Otentikasi
   Kriptografi menjamin kebenaran identitas pengirim pesan atau kepemilikan data. Ini berarti pihak ketiga tidak dapat melakukan impersonifikasi tanpa dibantah oleh pemilik yang sah atau pengirim pesan. Otentikasi dapat dilakukan dengan menerapkan tanda tangan digital
4. Non-repudiation
   Kriptografi menjamin bahwa pengirim pesan tidak dapat membantah bahwa dirinyalah yang mengirimkan pesan. Non-repudiation dijamin dnegan tidak mungkinnya pemalsuan identitas yang tercantum dalam pengiriman pesan. Sama dengan otentikasi, non-repudiation dapat dilakukan dengan menerapkan tanda tangan digital.

B. *Skema Pembagian Data Rahasia*

Seperti yang diimplikasikan oleh namanya, skema pembagian data rahasia adalah alur atau proses pembagian data rahasia ke sejumlah partisipan sedemikian sehingga data rahasia hanya dapat diakses ketika semua atau sebagian dari anggota menggunakan bagian data rahasianya untuk membentuk data rahasia semula. Skema pembagian data rahasia ditujukan untuk memastikan bahwa semua atau sejumlah partisipan menerima data secara bersama-sama dan adil, tanpa ada yang lebih cepat atau lebih lambat dari yang lain.

Berikut adalah beberapa terminologi yang digunakan dalam skema pembagian data rahasia[2].

1) Secret

Secret adalah data rahasia yang hendak dibagikan menjadi sejumlah *share*.

2) Share

Share adalah potongan atau bagian dari data rahasia yang dibangkitkan menggunakan *secret*

3) Participantl

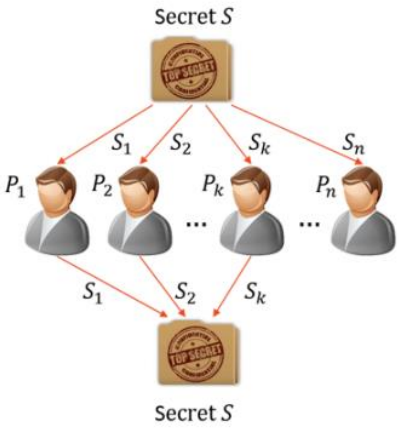
Participant adalah pemegang *share*. Setiap *participant* memegang sebuah *share*.

4) Dealer

Dealer adalah pihak yang dipercayai oleh pemilik *secret* untuk membentuk *share* yang kemudian dibagikan kepada *participant*.

Salah satu kasus di mana skema pembagian data rahasia dapat digunakan yaitu pembagian warisan tanpa meliputi badan/organisasi formal. Sebagai contoh, kode sandi (*secret)* untuk membuka brankas warisan yang disimpan di dalam rumah. Berdasarkan kode sandi, dilakukan pembangkitan sejumlah kunci parsial *(share)* yang masing-masing dibagikan kepada seorang *participant*. Untuk mendapatkan kembali kata sandi *(secret)* yang digunakan untuk membangkitkan kunci parsial *(share)*, dibutuhkan masukan dari sebagian atau semua kunci parsial *(share)*.

Untuk lebih jelas, skema pembagian data rahasia dapat divisualisasikan menjadi Gambar 2.1 sebagai berikut.



Gambar 2.1. Skema pembagian data rahasia[2]

C. *Kriptografi Visual*

Kriptografi Visual adalah kriptografi yang diterapkan pada gambar atau citra dengan tujuan untuk melindungi citra tersebut. Tidak hanya sebagai karya yang menjadi subjek proteksi dari klaim kepemilikan yang tidak benar, gambar atau citra dapat menjadi wadah penyaluran informasi seperti halnya teks pesan. Oleh sebab itu, citra, baik berdasarkan hak kepemilikan, nilai moneter maupun kerahasiaan, dapat memanfaatkan layanan perlindungan dari kriptografi.

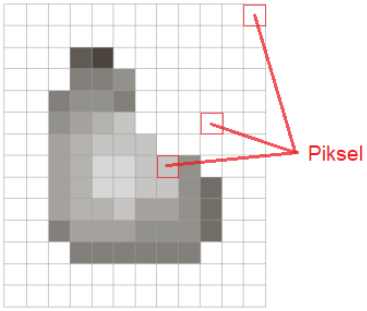
D. *Pemrosesan Citra Digital*

Pemrosesan citra digital adalah ilmu yang mempelajari pemrosesan gambar atau citra digital untuk memenuhi tujuan tertentu. Dengan melakukan pemrosesan citra digital, kriptografi visual dapat diimplementasikan dengan lebih luas terhadap citra digital. Adapun beberapa penerapan kriptografi yang dapat dilakukan terhadap citra digital yaitu steganografi, tanda tangan digital, dan *secret sharing*.

Berikut adalah berberapa dari terminologi dasar yang digunakan dalam pemrosesan citra digital.

1) Piksel

Piksel adalah elemen penyusun citra dengan rupa berupa titik-titik persegi berukuran kecil. Untuk lebih jelas, diberikan visualisasi piksel pada Gambar 2.2 sebagai berikut.



Gambar 2.2. Piksel[3]

2) Intensitas Cahaya

Setiap piksel memiliki nilai intensitas cahaya yang menentukan terang-redupnya warna piksel. Jangkauan dan variasi intensitas cahaya ditentukan oleh nilai yang dikenal sebagai skala keabuan, dengan nilai maksimum sebagai nilai intesitas cahaya paling terang dan nilai minimum sebagai nilai intensitas cahaya yang paling rendah. Jangkauan intensitas cahaya biasanya bernilai 2^{bit}. Sebagai contoh, 8-bit berarti 2^8 = 256 nilai intensitas cahaya, dengan nilai dari 0 hingga 255.

3) Jenis Citra Digital

Secara umum, terdapat tiga jenis citra digital, yaitu citra berwarna, citra grayscale, dan citra biner[3]. Citra berwarna pada umumnya, yaitu citra RGB, memiliki tiga kanal warna, yaitu *red* (merah), *green* (hijau), dan *blue* (biru), berbeda dengan citra *grayscale* dan citra biner yang hanya memiliki kanal warna hitam-putih. Citra *grayscale* memiliki intensitas cahaya nilai skala keabuan lebih besar dari 2 yang memungkinkan adanya piksel berwarna abu-abu, sedangkan citra biner hanya memiliki dua nilai intensitas cahaya, sehingga setiap piksel berwarna hitam atau putih.

Contoh gambar setiap jenis citra digital ditampilkan pada Gambar 2.3 sebagai berikut, dengan citra warna 24-bit RGB (8-bit *red*, 8-bit *green*, 8-bit *blue*), citra *grayscale* 8-bit, dan citra biner 2-bit.

Gambar 2.3. Jenis citra digital[3]

III. Implementasi Program

Pada kesempatan ini, penulis melakukan implementasi skema pembagian data rahasia sederhana dengan data rahasia berupa runtutan citra atau video. Detail rancangan dapat dilihat sebagai berikut.

A. Bahasa Pemrograman

MATLAB adalah bahasa pemrograman tingkat tinggi yang digunakan untuk mengimplementasi skema pembagian data rahasia. MATLAB dipilih karena MATLAB memiliki koleksi fungsi yang mendukung pemrosesan citra dan proses matematik dasar, dua aspek yang membantu implementasi kriptografi pada data citra. Berikut adalah objek dan fungsi yang digunakan untuk membantu pemrosesan terhadap citra.

1) VideoReader

Objek VideoReader digunakan untuk membaca data video menjadi kumpulan *frame* atau *image* terurut. Setiap data *frame* inilah yang diproses dengan algoritma *secret sharing* sehingga menghasilkan sejumlah citra *share*.

2) rgb2gray (RGB Image to Grayscale Image)

Fungsi *rgb2gray* digunakan untuk mengonversi citra berwarna kanal RGB menjadi citra *grayscale*.

3) mat2gray(Matrix to Grayscale Image)

Fungsi *mat2gray* digunakan untuk mengonversi matriks dua dimensi menjadi citra *grayscale*

B. Algoritma

Adapun algoritma yang diimplementasi memiliki tiga proses utama sebagai berikut.

1) Pembacaan video

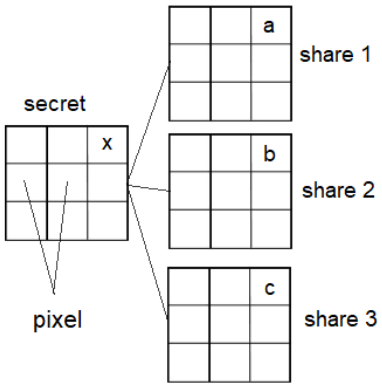
Proses ini berisi pembacaan video oleh program dan pembukuan setiap citra atau *frame* di dalam video untuk menghasilkan daftar gambar yang urut. Setiap gambar dalam daftar akan diubah menjadi citra *grayscale* sebelum diberlakukan algoritma *secret sharing* pada tahapaan pemrosesan daftar *frame*. Pengubahan citra berwarna menjadi citra *grayscale* dilakukan untuk mengurangi jumlah total komputasi yang perlu dilakukan tanpa menghilangkan informasi penting yang tersirat dalam citra.

2) Pemrosesan daftar frame

Proses ini berisi penerapan algoritma *secret sharing*. Adapun algoritma *secret sharing* yang diimplementasikan menggunakan pembangkitan angka acak sejumlah banyaknya partisipan. Pada implementasi program, jumlah partisipan yang digunakan adalah 3 orang.

Pembangkitan angka acak sejumlah banyaknya partisipan dilakukan terhadap piksel untuk semua *frame* dan sifatnya terpisah antarpiksel. Setiap pembangkitan angka acak sejumlah banyaknya partisipan terhadap piksel harus memenuhi dua kondisi: berada dalam jangkauan nilai intensitas cahaya 8-bit (bilangan integer antara 0-255), dan menghasilkan nilai piksel apabila semua angka dirata-ratakan. Setiap angka dari kumpulan angka acak yang memenuhi kondisi tersebut kemudian akan digunakan sebagai nilai piksel piksel *share* dengan koordinat piksel referensi yang sama, dengan setiap angka acak untuk sebuah share. Setelah proses ini selesai, didapatkan sejumlah daftar *share* sebanyak jumlah partisipan.

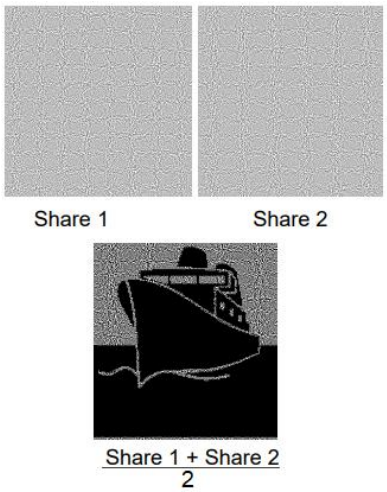
Agar lebih jelas, ditampilkan Gambar 3.1 yang memvisualisasikan pemrosesan piksel dalam frame tertentu.



Gambar 3.1. Pembangkitan piksel *share* dalam frame tertentu

3) Penulisan video

Setelah daftar *frame* diproses dan dihasilkan sejumlah daftar *share*, setiap daftar share dijadikan ditulis *(write)* menjadi *video*. Untuk membangkitkan video semula, setiap piksel dari semua share dengan koordinat dan frame yang sama hanya perlu dirata-ratakan. Berikut ditampilkan Gambar 3.1 untuk memvisualisasikan rekonstruksi sebuah frame dari *secret*, tetapi dengan dua share ketimbang tiga share.



Gambar 3.2. Ilustrasi pembangkitan kembali *frame secret*

IV. Pengujian Program

A. Hasil Pengujian

Karena keterbatasan dokumen dalam melampirkan video, hasil pengujian yang akan dilampirkan dalam dokumen berupa citra, yaitu citra *share* 1, citra *share* 2, dan citra *share* 3, dan citra *secret* untuk tiga *frame* berbeda, yaitu *frame* 1, *frame* 16, dan *frame* 35. Adapun citra adalah sebagai berikut.

1) Frame 1

a) Share 1

Gambar 4.1. Citra *share 1 pada Frame 1*

b) Share 2

Gambar 4.2. Citra *share 2 pada Frame 1*

c) Share 3

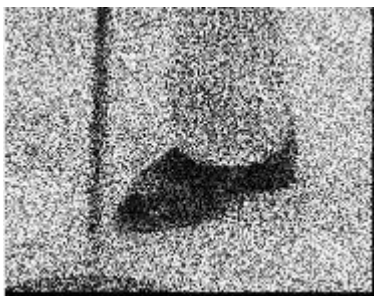
Gambar 4.3. Citra *share 3 pada Frame 1*

d) Generated Secret

Gambar 4.4. Citra *secret pada Frame 1*

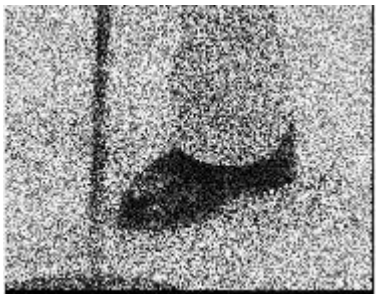
2) Frame 16

a) Share 1



Gambar 4.5. Citra *share 1 pada Frame 16*

b) Share 2



Gambar 4.6. Citra *share 2 pada Frame 16*

c) Share 3

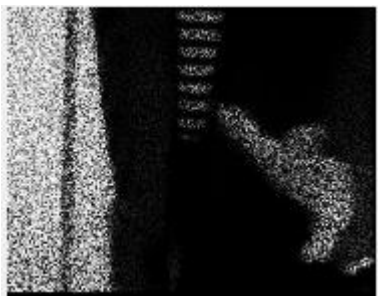
Gambar 4.7. Citra *share 3 pada Frame 16*

d) Secret

Gambar 4.8. Citra *secret pada Frame 16*

3) Frame 35

a) Share 1

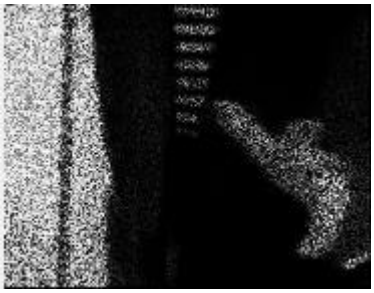


Gambar 4.9. Citra *share 1 pada Frame 35*

b) Share 2

Gambar 4.10. Citra *share 2 pada Frame 35*

c) Share 3



Gambar 4.11. Citra *share 3 pada Frame 35*

d) Generated Secret

Gambar 4.12. Citra *secret pada Frame 35*

B. Analisis Pengujian

Dari hasil pengujian yang dilakukan, didapatkan bahwa pembangkitan share masih jauh dari sempurna, terutama untuk piksel dengan intensitas cahaya sangat rendah dan sangat tinggi. Pada Gambar 4.1, Gambar 4.2, dan Gambar 4.3, dapat dilihat bahwa latar belakang yang berwarna abu-abu pada Gambar 4.4 berhasil dibagi menjadi piksel-piksel *share* yang acak, tetapi untuk piksel yang merepresentasikan wujud laki-laki dengan pakaian gelap, didapati bahwa piksel *share* yang didapat tidaklah acak dan masih dengan kuat merepresentasikan piksel *secret*.

Lemahnya nilai keacakan piksel share untuk piksel *secret* dengan intensitas yang sangat rendah disebabkan piksel-piksel secret tersebut berada pada batas atas dan batas bawah jangkauan nilai intensitas cahaya. Semakin dekatnya nilai intensitas cahaya dengan batas atas dan batas bawah, semakin sedikit kombinasi nilai acak a, b, dan c sedemikian sehingga nilai rata-rata ketiga nilai acak sama dengan nilai piksel *secret*. Sebagai contoh, untuk piksel *grayscale* dengan intensitas cahaya bernilai 1, hanya ada tujuh permutasi tiga nilai acak dengan rata-rata nilai acak sama dengan 1, yaitu: [2,0,1], [2,1,0], [0,2,1], [1,2,0], [0,1,2], [1,0,2], dan [1,1,1]. Sementara

itu, untuk piksel *grayscale* dengan intensitas cahaya bernilai 255,

V. KESIMPULAN

Berdasarkan hasil dan analisis pengujian program *secret sharing scheme* untuk citra dan radio, didapatkan bahwa algoritma *secret sharing* menggunakan nilai rata-rata angka acak jauh dari ideal, terlebih apabila banyak dari citra piksel memiliki intensitas cahaya yang sangat tinggi atau sangat rendah. Oleh sebab itu, apabila pembaca ingin menggunakan algoritma *secret* sharing, penulis menganjurkan pembaca untuk menggunakan algoritma *secret sharing* yang lebih teruji.

ACKNOWLEDGMENT

Puji dan Syukur penulis panjatkan kepada Tuhan Yang Maha Esa sebab tanpa berkat dan karunia-Nya, tidak mungkin bagi penulis untuk menghasilkan makalah ini. Penulis juga mengucapkan terima kasih kepada:

1. Dr. Ir. Rinaldi Munir, M.T. selaku dosen pengampu mata kuliah IF4020 Kriptografi yang membimbing dan mengajar penulis selama perkuliahan.
2. Rahmat Rafid Akbar, selaku rekan tugas kelompok yamg membantu penulis dalam menghadapi tantangan perkuliahan IF4020 Kriptografi.
3. M. Akyas David Al Aleey, selaku rekan tugas kelompok yamg membantu penulis dalam menghadapi tantangan perkuliahan IF4020 Kriptografi.

REFERENCES

[1] "Pengantar Kriptografi". Rinaldi Munir. Diakses pada 22/05/2023

[2] "Skema Pembagian Data Rahasia (Secret Sharing Scheme)". Rinaldi Munir. Diakses pada 22/05/2023

[3] "Pembentukan Citra dan Digitalisasi Citra - 2022". Rinaldi Munir. Diakses pada 22/05/2023

[4] "Kriptografi Visual Bag. 1 - 2023". Rinaldi Munir. Diakses pada 22/05/2023