Jurnal Minfo Polgan
Volume 13, Nomor 1, Februari 2024
DOI : https://doi.org/10.33395/jmp.v13i1.13541
e-ISSN : 2797-3298
p-ISSN : 2089-9424

Terbit : 25 Februari 2024

Analisis Metode Secret Sharing Asmuth-Bloom Dan Visual Cryptography

[1]Sugianto, [2]Jimmy, [3]Albert Suwandhi, [4]Wilianto, [5]Benny
[1, 2,3,4,5] Universitas IBBI

[1] sugiantoshi@gmail.com [2] jimmy_khuang@hotmail.co.id [3] albert.suwandhi@gmail.com
[4] wiliantogan@gmail.com [5] bennyshen77@gmail.com

ABSTRAK

Algoritma kriptografi tradisional tidak dapat menguraikan plaintext (pesan) menjadi beberapa ciphertext karena algoritma kriptografi tradisional hanya dapat menghasilkan ciphertext dari plaintext (pesan). Protokol *secret sharing* adalah suatu metode untuk membagikan atau membagi pesan rahasia (secret) kepada 2 (dua) atau lebih penerima sedemikian rupa sehingga penerima rahasia tidak dapat mengetahui hasil dari penggalan pesan (share) kecuali masing-masing penerima saling bertukar bagian untuk merekonstruksi. rahasia. Permasalahan yang muncul adalah pada saat pertukaran *share*, pihak lain mengetahui bagian share, sehingga pihak tersebut dapat merekonstruksi secret juga. Untuk mengatasi masalah ini, penerima harus memiliki kunci lengkap dan membagikannya agar dapat dibaca, misalnya pesan terenkripsi. Penelitian ini menganalisis keamanan pengiriman rahasia yang dikombinasikan dengan *secret sharing*.

Kata Kunci: secret sharing Asmuth-Bloom, visual cryptography, kriptografi, ciphertext, plaintext, shadow.

PENDAHULUAN

Pengamanan information sangat penting untuk menjaga information agar tidak diketahui dan dimanfaatkan oleh pihak yang diinginkan, dan salah satu caranya ialah dengan menerapkan algoritma dalam proses pengamanannya. Algoritma kriptografi yang umum atau tradisional hanya mampu menghasilkan sebuah ciphertext dari sebuah plaintext. Untuk mendapatkan beberapa buah ciphertext dari sebuah plaintext maka harus menggunakan metode yang lain selain algoritma kriptografi tradisional.

Untuk mengatasi masalah ini, protokol kriptografi seperti protokol berbagi secret Asmuth-Bloom dan kriptografi visual dapat diterapkan. Algoritme ini menggunakan bilangan prima dan bilangan acak untuk meningkatkan keamanannya. Selain itu, algoritma ini juga memerlukan n kumpulan angka yang harus memenuhi persyaratan tertentu. Proses pembentukan ciphertext dari algoritma Asmuth-Bloom relatif sederhana, hanya memerlukan penambahan modular. Selain itu menggunakan algoritma yang berbeda pada saat membentuk dan menggabungkan bayangan, pada saat membentuk bayangan menggunakan penambahan modular dan pada saat menggabungkan bayangan menggunakan Teorema Sisa Cina. Proses kerja metode secret sharing Asmuth-Bloom dibagi menjadi tiga bagian yaitu pembentukan kunci, pembentukan bayangan dan penggabungan bayangan. Perangkat lunak dirancang untuk dapat menerapkan metode berbagi secret Asmuth-Bloom untuk melindungi informasi secara efektif dan efisien.

Di sisi lain visual cryptography adalah Sebuah pengembangan dari skema secret sharing yang bertujuan untuk memecahkan citra digital menjadi dua atau lebih share sedemikian sehingga sejumlah share tertentu harus disusun dan ditumpukkan bersama untuk memperoleh citra digital rahasia semula, tanpa memerlukan perhitungan apapun. Namun, pendekatan tradisional pada visual cryptography juga memiliki kelemahan ketidakefisiensian dalam segi jumlah bit dari rahasia yang disimpan per bit share.

Jurnal Minfo Polgan
Volume 13, Nomor 1, Februari 2024 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v13i1.13541 p-ISSN : 2089-9424

TINJAUAN PUSTAKA

Metode Secret Sharing Asmuth-Bloom (ABSS) dan Visual Cryptography (VC) adalah dua pendekatan yang berbeda dalam mengamankan data rahasia. Keduanya digunakan untuk membagi sebuah rahasia menjadi beberapa bagian yang disebarkan di antara beberapa peserta untuk tujuan keamanan. Dalam literatur, keduanya telah dianalisis secara mendalam untuk memahami kelebihan, kelemahan, dan aplikasi praktisnya.Kepuasan Pelanggan

Metode Secret Sharing Asmuth-Bloom adalah teknik untuk membagi sebuah rahasia menjadi beberapa bagian yang disebarkan di antara beberapa peserta. Algoritma ini didasarkan pada aritmetika modular dan teori bilangan. Dalam ABSS, rahasia dibagi menjadi beberapa bagian dengan menggunakan polinomial, dan setiap peserta diberikan bagian unik dari polinomial tersebut. Untuk mengungkapkan rahasia, sejumlah peserta yang ditentukan harus bekerja sama.

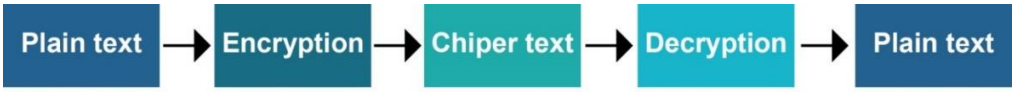
Studi literatur menunjukkan bahwa ABSS memiliki keunggulan dalam hal ketahanan terhadap serangan dan fleksibilitas dalam menentukan jumlah peserta yang diperlukan untuk mengungkapkan rahasia. Namun, kelemahannya adalah kompleksitas matematis yang terlibat dalam pembagian rahasia dan pengungkapan kembali rahasia, yang memerlukan sumber daya komputasi yang signifikan.

Visual Cryptography adalah metode untuk membagi sebuah gambar rahasia menjadi beberapa bagian yang disebarkan di antara beberapa citra. Individu hanya dapat mengungkapkan rahasia dengan menggabungkan citra-citra tersebut secara visual, tanpa memerlukan komputasi tambahan. Teknik ini menghasilkan bagian-bagian yang tampak seperti noise acak ketika dilihat secara individual, namun ketika digabungkan, menghasilkan gambar rahasia yang jelas. Penelitian sebelumnya telah menunjukkan bahwa VC efektif dalam mengamankan gambar rahasia dan memiliki aplikasi praktis dalam penyimpanan dan transmisi data visual. Namun, kelemahannya adalah bahwa kualitas gambar rahasia yang dihasilkan bergantung pada kualitas citra pembagian, dan penggunaan VC terbatas pada data visual.

METODE PENELITIAN

Kriptografi

Di dunia keamanan siber, kriptografi adalah komponen penting untuk menjaga kerahasiaan data. Seiring berkembangnya dunia digital, keamanan data penting dijaga demi mencegah risiko seperti pelanggaran data atau data breach. Kriptografi digunakan sebagai sarana pencegahan data dibaca oleh pihak yang tak berwenang. Teknik kriptografi akan menjaga keamanan informasi dengan penggunaan kode-kode.



GAMBAR CARA KERJA KRIPTOGRAFI

Gambar 1. Cara Kerja Kriptografi

Proses pembentukan kunci

Kunci privat dan publik yang terdapat pada algoritma *Secret Sharing Asmuth-Bloom* ini dapat dirincikan sebagai berikut:

Kunci publik (*public key*) dari semua *user*, yaitu bilangan prima p.

Bilangan prima p ini dapat dibangkitkan dengan menggunakan algoritma pembangkitan bilangan prima dari metode Rabin-Miller ataupun di-*input* secara manual dan dites dengan menggunakan algoritma pengujian bilangan prima dari metode Rabin-Miller. Bilangan prima p ini harus lebih besar dari *ASCII Code* pesan. Karena nilai *ASCII Code* terbesar adalah 255, maka nilai bilangan prima p harus lebih besar daripada 255.

Kunci privat (*private key*) dari masing-masing *user*, yaitu deretan nilai $d_1 \ldots d_n$.

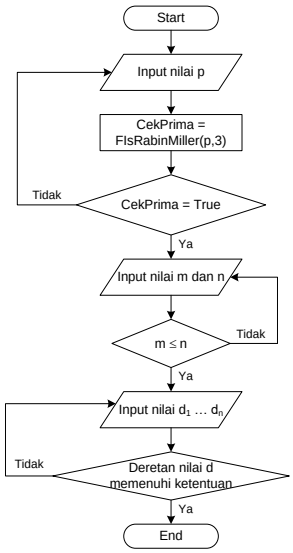
Deretan nilai d ini dapat ditentukan secara manual ataupun dihasilkan secara acak dengan memenuhi beberapa persyaratan berikut:

a. Deretan nilai d dalam urutan menaik, $d_i < d_{i+1}$.

Jurnal Minfo Polgan
Volume 13, Nomor 1, Februari 2024 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v13i1.13541 p-ISSN : 2089-9424

b. Setiap nilai d_i relatif prima terhadap setiap nilai d_i lainnya.
c. $d_1 * d_2 * \dots * d_m < p * d_{n-m+2} * d_{n-m+3} * \dots * d_n$.

Selain itu, proses pembentukan kunci juga akan menghasilkan nilai m dan n dimana nilai m merupakan jumlah *shadow* yang diperlukan untuk membentuk pesan dan nilai n merupakan jumlah *shadow* yang diinginkan. Proses pembentukan kunci ini dapat digambarkan dalam bentuk *flowchart* seperti terlihat pada Gambar 2:



Gambar 2. Flowcart Pembetukan Kunci

Proses pembentukan *shadow* dari algoritma *secret sharing* ini menggunakan *output* dari proses pembentukan kunci yaitu kunci privat dan kunci publik *user*.
Proses pembentukan *shadow* dari algoritma *secret sharing* ini dilakukan oleh pembuat pesan. Hasil dari proses ini adalah n buah *shadow* yang akan dibagikan kepada n orang, dimana setiap *shadow* memiliki nilai yang berbeda-beda.

Proses penggabungan *Shadow*

Proses penggabungan *shadow* dari algoritma *secret sharing* ini menggunakan *output* dari proses pembentukan kunci yaitu kunci privat dan kunci publik *user*, serta m buah *shadow*. Proses penggabungan *shadow* dari algoritma *secret sharing* ini dilakukan oleh m orang yang ingin mendapatkan pesan semula. Hasil dari proses ini adalah pesan semula yang disembunyikan oleh pembuat pesan. Proses penggabungan *shadow* menggunakan bantuan teorema *Chinese Remainder* untuk mencari solusi dari sistem kongruen linier yang dibentuk dari gabungan m buah *shadow* dan m buah nilai d_i.

Algoritma Secret Sharing yang Digunakan

Algoritma yang digunakan untuk merancang aplikasi algoritma Secret Sharing Asmuth-Bloom ini dapat dibagi menjadi 5 bagian besar yaitu:

a. Algoritma Pembentukan Kunci.

Algoritma ini berfungsi untuk menghasilkan nilai-nilai yang akan digunakan pada proses pembuatan shadow dan proses penggabungan shadow. Nilai-nilai output dari algoritma ini, yaitu:

a. Nilai m dan n.
b. Bilangan prima p.
c. Deretan nilai d(1) … d(n).

Prosedur kerja dari algoritma pembentukan kunci ini dapat dijabarkan sebagai berikut:

1. Jika input manual, maka:
   a. Input bilangan p.
   b. Cek prima terhadap bilangan p.
   c. Jika valid, maka lanjut ke langkah (e).
   d. Apabila tidak, maka kembali ke langkah (a).

Jurnal Minfo Polgan
Volume 13, Nomor 1, Februari 2024 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v13i1.13541 p-ISSN : 2089-9424

e. Input bilangan m dan n.
f. Jika m <= n, maka lanjut ke langkah (h).
g. Apabila tidak, maka kembali ke langkah (e).
h. Input deretan bilangan d(1) ... d(n).
i. Jika deretan bilangan d(1) ... d(n) memenuhi ketentuan, maka lanjut ke langkah (k).
j. Apabila tidak, maka kembali ke langkah (h).
k. Simpan nilai p, m, n dan deretan bilangan d(1) ... d(n) ke memori.

2. Apabila tidak, maka:
l. Bangkitkan bilangan prima p.
m. Ambil nilai m dan n yang memenuhi ketentuan secara acak.
n. Ambil deretan bilangan d(1) ... d(n) yang memenuhi ketentuan secara acak.
o. Simpan nilai p, m, n dan deretan bilangan d(1) ... d(n) ke memori.

b. Algoritma Pembuatan Shadow.

Algoritma ini berfungsi untuk menghasilkan pecahan pesan (shadow) dari pesan input. Nilai-nilai yang diperlukan oleh algoritma ini, yaitu:

1. Nilai n, bilangan prima p dan deretan bilangan d(1) ... d(n) yang dihasilkan dari proses pembentukan kunci.
2. Pesan input dan bilangan acak r. Di sisi lain, output dari algoritma ini adalah n buah pecahan pesan (shadow) dari pesan input. Prosedur kerja dari algoritma pembuatan shadow ini dapat dirincikan sebagai berikut:

1. Input pesan.
2. Jika input manual, maka
   a. Input bilangan acak r.
   b. Jika input sama dengan 0 maka kembali ke langkah (a).
3. Apabila tidak, maka ambil sebuah bilangan acak r.
4. Untuk i = 1 sampai [panjang pesan], lakukan proses berikut:
   a. Konversikan karakter ke-i dari pesan ke bentuk ASCII Code dan simpan ke variabel M(i).
   b. Hitung nilai M(i)' = M(i) + rp.
5. Untuk j = 1 sampai n, lakukan proses berikut:
   Untuk i = 1 sampai [panjang pesan], lakukan proses berikut:
   Hitung nilai k(j, i) = M(i) mod d(j)

c. Algoritma Penggabungan Shadow.

Algoritma ini berfungsi untuk menghasilkan pecahan pesan (shadow) dari pesan input. Nilai-nilai yang diperlukan oleh algoritma ini, yaitu:

1. Nilai m, bilangan prima p dan m buah deretan bilangan d(i).
2. Bilangan acak r.
3. Deretan nilai k(j, i). Di sisi lain, output dari algoritma ini adalah pesan semula. Prosedur kerja dari algoritma penggabungan shadow dapat dirincikan sebagai berikut:

1) Tentukan nilai d(i) yang akan digunakan dan simpan ke nilai d1(1) ... d1(m).
2) Tentukan pula deretan nilai k(j, i) yang akan digunakan, detail berikut:
   a. Shadow ke-1 yang digunakan: k1(1, 1) ... k1(1, i).
   b. Shadow ke-2 yang digunakan: k1(2, 1) ... k1(2, i).
   c. Shadow ke-m yang digunakan: k1(m, 1) ... k1(m, i).
   (Keterangan : i = 1 ... [panjang pesan])
3) Untuk i = 1 sampai [panjang pesan]
   a. Bentuk sistem kongruen linier untuk mencari karakter ke-i dari pesan dengan menggunakan k1(1, i) sampai k1(m, i) dan d1(1) ... d1(m).
   b. Cari solusi dari sistem kongruen linier dengan menggunakan algoritma Chinese Remainder dan simpan nilai solusi ke M(i)'.
   c. Hitung nilai M(i) = M(i)' – rp.
   d. Ubah nilai M(i) ke bentuk karakter sehingga diperoleh karakter ke-i dari pesan.

d. Algoritma Chinese Remainder[6]**.**

Algoritma ini memiliki input data yaitu :

Jurnal Minfo Polgan
Volume 13, Nomor 1, Februari 2024 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v13i1.13541 p-ISSN : 2089-9424

1. Variabel array dua dimensi nArrValue, detail dimensi pertama bernilai sebesar jumlah persamaan dan dimensi kedua bernilai sebesar 2 yaitu nilai 1 untuk bilangan sisa modulo dan nilai 2 untuk bilangan modulo.
2. Variabel nJlh merupakan jumlah persamaan.

HASIL DAN PEMBAHASAN

Analisis hasil dari kedua metode tersebut:

Tabel 1 Analisis Hasil

Ukuran citra asli (piksel)	Nilai n	Nilai k	Lama Proses Share (sekon)	Lama Proses Rekonstruksi (sekon)
150 x 150	2	2	0.0970	0.0820
150 x 150	3	3	0.1220	0.1070
150 x 150	4	4	0.1470	0.1150
150 x 150	5	5	0.1730	0.1470
150 x 150	6	6	0.2030	0.1730
150 x 150	7	7	0.2260	0.2030
150 x 150	8	8	0.2500	0.2260
150 x 150	9	9	0.2880	0.2500
150 x 150	10	10	0.2980	0.2880

Rincian Hasil Pengujian II untuk Algoritma Visual Threshold Cryptography dengan Input Citra Berukuran 150

Tabel 2. Rincian Hasil Pengujian II

Ukuran citra asli (piksel)	Nilai n	Lama Proses Share (sekon)	Lama Proses Rekonstruksi (sekon)
150 x 150	2	0,645833333	0,541666667
150 x 150	3	1,083333333	0,868055556
150 x 150	4	1,840277778	1,083333333
150 x 150	5	2,493055556	1,298611111
150 x 150	6	3,576388889	1,520833333
150 x 150	7	4,763888889	1,736111111
150 x 150	8	5,958333333	1,951388889
150 x 150	9	10.760	2,166666667
150 x 150	10	13.260	2,381944444

KESIMPULAN

Algoritma visual threshold cryptography memiliki waktu eksekusi proses pembuatan share yang bagus, namun algoritma ini akan menghasilkan file citra share yang lebih besar ukurannya daripada citra asli. Selain itu, algoritma visual threshold cryptography juga hanya memerlukan dua buah file share saja untuk menghasilkan citra asli semula. Hal ini menyebabkan tingkat sekuritas

dari algoritma ini menjadi kurang bagus. Algoritma secret sharing memiliki waktu eksekusi proses pembuatan share yang cukup lama. Waktu eksekusi ini yang menyebabkan algoritma secret sharing sangat tidak efisien apabila diterapkan untuk mengamankan citra input yang memiliki ukuran piksel yang besar. Algoritma secret sharing memiliki tingkat sekuritas yang lebih bagus karena proses penggabungan menerapkan algoritma Chinese Remainder untuk memperoleh kembali citra rahasia semula. Namun, penerapan algoritma Chinese Remainder ini juga menyebabkan waktu eksekusi dari proses rekonstruksi menjadi sangat lama, sehingga sangat tidak efisien apabila diterapkan secara praktikal jika ditinjau dari segi efisiensi waktu. Pada algoritma secret sharing, dapat dilakukan pengaturan sehingga tidak harus memerlukan semua file share untuk digunakan untuk memperoleh citra semula. Walaupun tingkat sekuritas dari algoritma secret sharing cukup bagus, namun penerapan algoritma secret sharing pada citra digital akan menghasilkan citra share yang kurang bagus, karena kurang teracak secara visual sehingga dapat mengakibatkan adanya kebocoran informasi secara visual.

Pembuatan shadow yang akan memecahkan sebuah file citra menjadi n buah file shadow, sehingga dapat digunakan untuk memecahkan suatu file rahasia menjadi beberapa buah pecahan file shadow. Ukuran file share yang dihasilkan oleh algoritma secret sharing adalah jauh lebih besar daripada file citra input, dimana ukuran file share tergantung pada ukuran citra input dan juga besar nilai kunci yang digunakan.

REFERENSI

F. Zhang *et al.*, “Meta-optics empowered vector visual cryptography for high security and rapid decryption,” *Nat Commun*, vol. 14, no. 1, Dec. 2023, doi: 10.1038/s41467-023-37510-z.

Amelia Shinta and dewaweb.com, “Mengenal Kriptografi, Pengertian, Jenis dan Algoritmanya,” www.dewaweb.com.

M. Pratama and J. Damanik, “PENERAPAN METODE SECRET SHARING ASMUTH-BLOOM UNTUK PENGAMANAN DATA TEKS,” 2017.

J. Tripathi, A. Saini, Kishan, Nikhil, and Shazad, “Enhanced Visual Cryptography: An Augmented Model for Image Security,” in *Procedia Computer Science*, Elsevier B.V., 2020, pp. 323–333. doi: 10.1016/j.procs.2020.03.232.

K. Shankar, D. Taniar, E. Yang, and O. Yi, “Secure and optimal secret sharing scheme for color images,” *Mathematics*, vol. 9, no. 19, Oct. 2021, doi: 10.3390/math9192360.

R. Lestari, R. Buaton, and I. Gultom, “Penerapan Algoritma OTP dan Algoritma RSA CRT dalam Pengamanan Citra,” *Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD*, vol. 4, no. 2, pp. 180–190, 2021, [Online]. Available: https://ojs.trigunadharma.ac.id/index.php/jsk/index

N. C. H. Wibowo, K. Umam, A. M. I. Khaq, and F. A. Rizki, “Komparasi Waktu Algoritma RSA dengan RSA-CRT Base On Computer,” *Walisongo Journal of Information Technology*, vol. 2, no. 1, p. 13, Jun. 2020, doi: 10.21580/wjit.2020.2.1.5402.