Seminar Nasional Teknologi Komputer & Sains (SAINTEKS)
SAINTEKS 2020
ISBN: 978-602-52720-7-3
Februari 2020
Hal 405-408

Pengamanan Citra Digital Dengan Algoritma Paillier Criptosystem

Menanti Cristian Sianturi, Firman Telaumbanua, Zul Fikri Sofyan

Program Studi Teknik Informatika, STMIK Budi Darma, Medan Indonesia

Abstrak−Citra digital merupakan keluaran dalam suatu sistem perekaman data yang bisa bersifat optik yaitu berupa foto atau gambar. Informasi yang berupa gambar tersebut, dapat bersifat rahasia yang artinya bukan konsumsi umum. Namun dengan perkembangan teknologi yang begitu pesat saat ini, memungkinkan banyak pihak yang tidak bertanggunggung jawab dengan mudah mengakses informasi tersebut dan menyalah gunakannya. Oleh sebab itu, perlu dibuat sebuah sistem untuk mengamankan informasi tersebut. Pemanfaatan algoritma dari teknik kriptografi dalam mengamankan informasi, merupakan solusi yang dapat digunakan agar keamanan data dapat dipertahankan. Dalam penelitian ini, akan dibahas tentang citra digital. Algoritma ini sangat tahan terhadap perusakkan karena algoritma ini memiliki perhitungan *e-residue* class yang sulit untuk dikomputasi, sehingga mampu mengamankan data.

Kata Kunci: Kriptografi, Citra, Citra Digital, Algoritma Paillier Criptosystem

1. PENDAHULUAN

Masalah kemanan informasi komputer menjadi sangat penting pada era teknologi informasi sekarang. Banyak kejahatan *cyber* sering diberitakan di media massa, seperti pencurian data konsumen, pembobolan ATM, atau menerobos keamanan militer. Kejahatan ini dilakukan dengan memanfaatkan celah kemanan yang ada dalam sistem. Dalam perkembangan selanjutnya, para pengembang juga telah memanfaatkan citra digital sebagai pendukung (pelengkap) data-data yang yang didistribusikan guna memberi informasi yang lebih *valid.* Jadi, citra digital ini juga harus benar-benar aman dari kejahatan *cyber*.

Kriptografi merupakan ilmu yang berperan penting dalam bidang keamanan informasi. Kriptografi digunakan untuk menjaga kemanan data dan informasi, baik yang ditransmisikan melalui saluran komuninkasi atau dalam media penyimpanan. Agar citra yang didistribusikan aman dari kejahatan maka, citra juga harus diamankan. Banyak algoritma yang dikembangkan untuk mengamankan citra digital. Adapun algoritma yang akan digunakan dalam mengamankan citra pada penelitian ini adalah algoritma *paillier cryptosystem.* Begitu pentingnya citra untuk diamankan, sehingga harus diciptakan algoritma yang benar-benar sulit untuk dikomputasi.

Dengan memahami algoritma ini, pembaca diharapkan mampu memahami cara mengamankan citra digital. Dalam penelitian terdahulu yang dilakukan oleh June Taronisokhi Rivalri mengatakatan bahwa algoritma ini sangat membantu dalam mengamankan data karena benar-benar sulit untuk dikomputasi

2. METODOLOGI PENELITIAN

2.1 Kriptografi

Kriptografi merupakan ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek kemanan informasi seperti kerahasiaanm integritas data, serta otentikasi. Saat anda mengirim citra digital, anda tentu berharap bahwa citra tersebut aman.

Aman berarti selama pengiriman tidak dibaca orang yang bukan tujuan, data sampai pada tujuan dengan utuh, penerima yakin bahwa data berasal dari pengirim. Jadi kriptografi akan menghasilkan kerahasiaan (*secret*), integritas data, Kemanan (otentikasi) data, dan anti-penyangkalan.

2.2 Citra Digital

Citra merupakan gabungan antara titik, garis, bidang dan warna sehingga menciptakan suatu kemiripan atau gambar dari suatu objek yang biasanya berupa objek fisik atau manusia. Citra ada dua jenis yaitu citra analog dan citra digital. Penelitian ini focus pada citra digital. Citra digital adalah citra yang dihasil oleh peralatan digital dan dapat langsung diolah komputer.

2.3 Algoritma Pailler Scryptosystem

Pascal Paillier merupakan salah satu peneliti yang berhasil menciptakan algoritma kriptografi yang diberi nama *paillier cryptosystem* yang berbasis asimetris probabilistikgrafi public key dimana, kunci untuk menyandikan persis sama dengan kunci membuka. Algoritma ini menggunakan konsep matematika r-residue class dengan demikian diyakini sangat sulit dibuka pihak lawan. Berikut adalah notasi-notasi yang digunakan dalam algortima Paillier Kryptosystem:

Zn = Himpunan integer n
Z*n= Himpunan integer yang relatif prima terhadap integer n
Z^*n^2 = Himpunan integer yang relative prima terhadap integer n

Langkah-langkah membentuk private key:

1. Pilih dengan acak dan unik dua buah bilangan prima besar p dan q.
2. Cari nilai variable n dimana n= p*q dan cari nilai λ=LCM (p-1, q-1).
3. Pilih bilangan acak integer g di mana g € Z^*n^2
4. Cari nilai μ di mana
   a. $\mu = (L (g^{\lambda} \bmod n^2))^{-1}$.

ISBN: 978-602-52720-7-3
Februari 2020
Hal 405-408

b. L (u) = (u- 1) /n.
5. Public key adalah (n, g).
6. Private key adalah (λ, μ).

Langkah- langkah enkripsi:
1. m adalah pesan yang akan dienkripsi di mana m € Zn
2. Pilih r, di mana r € Z*n
3. Hitung jumlah chiperteks dengan c= $g^m * r^n \bmod n^2$

Langkah-langkah dekripsi:
1. c adalah chiperteks dimana c € $Z*n^2$
2. Hitung jumlah teks dengan m= L ($c^{\lambda} \bmod n^2$) * μ mod n

Adapun prosedur utama dari algoritma *paillier cryptosystem* ini dibagi menjadi 3 bagian besar yaitu:
1. Algoritma Pembentukan Kunci.
   Proses pembangkitan kunci ini dilakukan oleh penerima dan pengirim, dimana proses ini berfungsi untuk menghasilkan nilai kunci privat dan kunci public yang akan digunakan untuk proses enkripsi dan dekripsi. Nilai input dari algoritma tersebut berupa beberapa buah bilangan prima acak x, y dan z.
   a. Tahap pertama masukkan dua buah bilangan prima besar x dan y secara acak
   b. Kemudian hitung nilai n dan h, dimana n = xy and λ = *lcm* (x – 1, *y*– 1)
   c. Setelah itu, pilihlah bilangan integer z dimana z € $Z*n^2$
   d. Hitung nilai u dan L(u)
   e. Tentukan nilai kunci privat (h, μ) dan nilai kunci public (n, z)
2. Algoritma Enkripsi
   Proses enkripsi memiliki fungsi untuk menghasilkan nilai *cipher image* dari pesan yang input, dimana kunci publik yang diperlukan adalah yang diambil dari perhitungan proses pembentukan kunci sebelumnya.
   a. Pada tahap pertama konversikan pesan kebilangan biner
   b. Kemudian kelompokkan pesan menjadi *subblok* bit
   c. Pilihlah bilangan integer r secara acak (sesuai ketentuan)
   d. Kemudian hitunglah nilai Ci
   e. Setelah nilai Ci didapat untuk masing-masing, kemudian gabungkan seluruh nilai tersebut menjadi *chipper value*
3. Algoritma Deskripsi
   Fungsi dari Algoritma Deskripsi ini adalah untuk mendapatkan kembali pesan awal yang telah dienkripsikan sebelumnya dimana untuk mengembalikan pesan yang telah dienkripsikan dengan memerlukan kunci privat dari proses pembentukan kunci.
   a. Mengelompokkan *chipper value* menjadi *subblok*
   b. Menghitung nilai Ui dan L(Ui)
   c. Menghitung nilai Mi dan kemudian diubah menjadi bit biner
   d. Menggambungkan semua nilai Mi dan melakukan tahap konversi kekarakter.

Berikut ini akan dijabarkan cara kerja algoritma paillier dalam mengenkripsi dan dekripsi citra digital. Dalam proses enkripsi dan dekripsi, penelitian akan menggunakan 3pixel untuk dilakukan perhitungan dalam tipe citra grayscale

3. ANALISA DAN PEMBAHASAN

Pendistribusian sebuah data rahasia harus didukung dengan pengamanan yang kuat. Salah satunya adalah dalam mendistribusikan citra digital. Untuk menjamin keamanan data tersebut, diperlukan sebuah algoritma. Selain itu, algoritma yang digunakan bukan sekedar algoritma atau metode tertentu melainkan algoritma yang sesuai dengan masalah yang ada. Untuk itu diperlukan sebuah algoritma yang memang sesuai dengan pengamanan citra digital. Salah satunya adalah algoritma *paillier cryptosystem*. Berikut adalah contoh penerapan algoritma *paillier cryptosystem*:

Tabel 1. Nilai *Decimal Plainmage*

Pixel 1	Pixel 2	Pixel 3
143	163	212

Berdasarkan Tabel 1. di atas maka, nilai decimal dari *plain image* tersebut adalah 143, 163,212.

1. Pembentukan kunci

Dalam mengenkripsi dengan algoritma paillier, hal penting yang akan dikerjakan adalah membentuk kunci, langkah- langkah dalam membentuk kunci dilakukan dengan cara berikut ini.

a. Pilih dua buah bilangan prima besar a dan b.
   a= 37 dan b= 73
b. Hitung nilai n dan λ.
   - n = a * b = 37 * 73= 2701
   - λ = LCM (a-1, b-1), maka λ=LCM (37- 1, 73- 1) = LCM (36, 72),
     LCM (36, 72)
     $36 = 2^2 * 9$ dan $72 = 2^2 * 18$ sehingga LCM $= 2^2 * 9 * 18 = 648$
c. Sekarang memilih bilangan integer acak g dimana g € z * n, g = 57
d. Menghitung nilai μ dan L (μ).

ISBN: 978-602-52720-7-3
Februari 2020
Hal 405-408

- $\mu = g^{\lambda} \bmod n^2 = 57^{648} \bmod 2701^2 = 221.483$
- $648 = 512 + 128 + 8$
- $L(\mu) = (\mu - 1)/n = (221.483-1)/ 2701 = 82$
- $\mu = 82 \bmod 2701 = 82$

e. Maka, $(\lambda, \mu) = 648, 82$
f. Sedangkan kunci public (n, g) = 2701, 57

2. Enkripsi memiliki fungsi sebagai penghasil nilai *chipper image* melalui penginputan. Berikut adalah nilai pixel yang akan diubah ke dalam bilangan biner:
   a. 143 = 10001111
   b. 163 = 10100011
   c. 212 = 11010100
3. Mengelompokan bentuk pesan menjadi *subblock* bit dengan rumus $2^b <= n$. Dimana n = 2701 dan nilai b yang dipilih adalah 7
   M(1) = 001101100010 = 866
   M(2) = 010111111000 = 1528
   M(3) = 001110000000 = 896
   Masukkan nilai r yang didapatkan dari sebuah bentuk bilangan prima yang akan di randomkan.
   Contoh : r = 57
   Selesaikan nilai Ci
   Input nilai Temp = $(r^2) \bmod n^2$ maka Temp = $(57^{2701} \bmod 7295401)$

   Langkah – langkah penyelesaiannya, yaitu :
   Dari bentuk Nilai Temp yang dihasilkan dengan perkalian pada masing-masing nilai n^2 yang dimana n^2 :
   2701 = 2048 + 512 + 128 + 8 + 4 + 1
   untuk ^{1} : 57 mod 6661561 = 57
   untuk ^{2} : 57 mod 6661561 = 4489
   untuk ^{4} : 4.489 mod 6661561 = 166438
   untuk ^{8} : 166438 mod 6661561 = 2837206
   untuk ^{16} : 2837206 mod 6661561 = 835890
   untuk ^{32} : 835890 mod 6661561 = 943493
   untuk ^{64} : 943493 mod 6661561 = 1306180
   untuk ^{128} : 1306180 mod 6661561 = 481568
   untuk ^{256} : 481568 mod 6661561 = 5477092
   untuk ^{512} : 5477092 mod 6661561 = 2095995
   untuk ^{1024} : 2095995 mod 6661561 = 2145501
   untuk ^{2048} : 2145501 mod 6661561 = 2582196

   JADI, nilai U_1 yang dapat diambil yaitu dari hasil perhitungan nilai pangkat yang merupakan hasila dari nilai h.
   U_1 = 2582196 + 2095995 + 481568 + 2837206 + 166438 + 57 mod 7295401
   U_1 = 8163460

   Selesaikan nilai Mi lalu ubahlah ke nilai biner dan setelah itu hitung nilai b untuk mendapatkan hasil 2^b <= n
   n = 2581 ; nilai b yang dipilih = 11
   M(1) = L[U(1)] x m mod n
   M(1) = 2223 x 56 mod 2581
   M(1) = 966 = 001111000110

   M(2) = L[U(2)] x m mod n
   M(2) = 2496 x 56 mod 2581
   M(2) = 1628 = 011001011100

   M(3) = L[U(3)] x m mod n
   M(3) = 934 x 56 mod 2581
   M(3) = 998 = 001111100110

   M(4) = L[U(4)] x m mod n
   M(4) = 1690 x 56 mod 2581
   M(4) = 1640 = 011001101000

   M(5) = L[U(5)] x m mod n
   M(5) = 1309 x 56 mod 2581
   M(5) = = 5521 = 111001110010

   M(6) = L[U(5)] x m mod n
   M(6) = 1702 x 56 mod 2581

ISBN: 978-602-52720-7-3
Februari 2020
Hal 405-408

M(6) =1896 = 011101101000

Bit pesan yang diperoleh dari keseluruhan nilai M(i) adalah :
M=001111000110011001011100001111100110011001100000100111001110111011010000

Dari bentuk nilai M yang telah dikombinasikan dibagi menjadi 8 bit per kelompok agar dapat menghasilkan nilai desimal *pixel* citra yang asli.

4. KESIMPULAN

Berdasarkan pembahasan di atas, maka dapat disimpulkan bahwa algoritma *paillier cryptosystem* sangat cocok digunakan untuk mengamankan gambar. Algoritma ini memberikan hasil enkripsi yang tidak bisa diketahui oleh orang lain dan cukup sulit untuk dibobol oleh pihak yang tidak bertanggung jawab.sehingga file gambar yang ingin kita didistribusikan atau kita simpan, keamanannya terjamin.

REFERENCES

[1] Munir Rinaldi, ”Kriptografi”, Bandung, Informatika Bandung, 2009.
[2] Sadikin Rifki, ”Kriptografi Untuk Keamanan Jaringan”, Yogyakarta, ANDI, 2012.
[3] Taroni Zebua and E. Ndruru, ”Pengamanan Citra Digital Berdasarkan Modifikasi Algoritma Rc4 ”, Jurikom, Teknologi, Informasi dan Ilmu Konput, Vol 4. No.4. pp.275-282, 2017.
[4] Juni Ade Nawer Purba, Taroni, Zebua and Rivalri K Hondro. “Implementasi Algoritma Paillier Cryptosystem Pengamanan Citra Digital Pada Aplikasi Chat”, KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer), Vol. 3, No. 3, pp. 299-306.2019.
[5] M.K. Emy. Setyaningsih, S.Si. “Kriptografi dan Implementasi Menggunakan Matlab”, Jakarta, pp. 71-132, 2015.