Aplikasi Teori Bilangan Dalam Algoritma Enkripsi-Dekripsi Gambar Digital

Harry Alvin Waidan Kefas 13514036[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13514036@std.stei.itb.ac.id

Abstrak*—Dalam kehidupan sehari-hari pada zaman ini– dimana informasi dengan mudah didapatkan, kadangkala didapatkan gambar-gambar digital yang sebenarnya ada, tetapi tidak terlihat secara kasat mata. Hal itu disebabkan oleh enkripsi yang dilakukan terhadap gambar digital tersebut. Saat gambar digital yang jelas dienkripsikan dengan suatu algoritma, hasilnya gambar tersebut akan tidak jelas terlihat. Dengan mendekripsikan gambar digital yang tidak jelas itu, dapat dilakukan dekripsi terhadap gambar tersebut. Makalah ini akan menjelaskan cara gambar digital tersebut dienkripsikan dan didekripsikan menggunakan teori-teori bilangan dan beberapa algoritma yang digunakan dalam mengenkripsi dan mendekripsi gambar digital.

***Kata Kunci*—Enkripsi, Dekripsi, Chinese Remainder Theorem, Number Theory**

I. PENDAHULUAN

Dalam keseharian insan-insan akademis, biasanya ada saja cara untuk mereka dapat memahami ilmu yang mereka sedang pelajari. Salah satu media untuk memahaminya adalah gambar. Di era internet ini, sangat banyak gambar-gambar digital yang sangat mudah didapatkan. Namun, dalam kenyataannya, agar mendapatkan suatu gambar digital dari internet, proses pengiriman gambar digital bisa terdapat gangguan, misalnya, gambar yang menjadi sama sekali tidak jelas, atau terbongkarnya gambar digital rahasia yang hendak dikirim ke tujuan yang sangat jauh sehingga harus dikirm melalui internet.

Akibatnya, harus adanya penerjemahan dari gambar yang beredar melalui jaringan internet ataupun harus ada pembungkusan gambar tersebut agar tidak terbongkar.

Maka dari itu, orang-orang membuat sebuah algoritma yang akan mengapsulasi gambar digital yang akan melalui jalur jaringan internet sehingga kerahasiaannya tetap terjaga dan penerima dapat membuka isi dari kapsulasi gambar digital tersebut.

Makalah ini akan membahas bagaimana algoritma yang digunakan untuk mengenkripsi dan mendekripsikan gambar digital dengan memanfaatkan teori bilangan.

II. TEORI BILANGAN

A. Teorema Euclidean

Misal m dan n adalah dua buah bilangan bulat dan $n > 0$. Apabila m dibagi dengan n maka akan terdapat bilangan bulat unik q (quotient) dan bilangan bulat r (remainder), dimana

$$m = nq + r$$

B. Greatest Common Divisor (gcd)

Misal a dan b adalah bilangan bulat tidak nol. GCD dari a dan b adalah bilangan bulat terbesar d sehingga d habis dibagi a, dan d habis membagi b. Sehingga kita dapat nyatakan bahwa gcd(a,b) = d.

C. Algoritma Euclidean

Dengan m dan n adalah bilangan bulat tak-negatif, algoritmanya adalah sebagai berikut.

1. Jika n = 0
   m adalah gcd(m,n)
   stop.
   Namun jika n ≠ 0
   Lanjut ke langkah 2.
2. Bagi m dengan n dan misalkan r adalah sisanya
3. Ganti nilai m dengan nilai n dan nilai n dengan nilai r, lalu ulang kembali ke langkah 1

D. Kombinasi Lanjar

gcd(a,b) dapat dinyatakan sebagai kombinasi lanjar a dan b dengan koefisien-koefisiennya.
Teorema : Misalkan a dan b bilangan bulat positif, maka terdapat bilangan bulat m dan n sehingga

gcd(a,b) = ma + nb.

E. Relatif Prima

Dua buah bilangan bulat a dan b dikatakan relatif prima apabila gcd(a, b) = 1.

F. Aritmatika Modulo

Misalkan a dan m bilangan bulat (m > 0). Operasi

a mod m

memberikan sisa jika a dibagi dengan m

Notasi :

a mod m = r sehingga a = mq + r, dengan $0 \le r < m$.

G. Kongruen

Misalkan a dan b bilangan bulat dan m adalah bilangan > 0, maka a ≡ b (mod m) jika dan hanya jika m habis membagi (a-b)

a ≡ b (mod m) dalam bentuk "sama dengan" dapat dituliskan sebagai

a = b + km (k adalah bilangan bulat)

a mod m = r dapat juga ditulis a ≡ r (mod m)

Teorema :

1. Jika a ≡ b (mod m) dan c adalah sembarang bilangan bulat maka
   - (a+c) ≡ (b+c) (mod m)
   - ac ≡ bc (mod m)
   - $a^p \equiv b^p$ (mod m)
2. Jika a ≡ b (mod m) dan c ≡ d (mod m), maka
   - $(a + c) \equiv (b + d) \pmod m$
   - $ac \equiv bd \pmod m$

H. Modulo invers

Syarat : Jika a dan m relatif prima dan m > 1 maka invers dari a (mod m) ada.

Balikan dari $a \pmod m$ adalah bilangan bulat x sedemikian sehingga:

$$xa \equiv 1 \pmod m$$

Dalam notasi lainnya, $a^{-1} \pmod m = x$

I. Chinese Remainder Problem

Pada abad pertama, seorang matematikawan China yang bernama Sun Tse mengajukan pertanyaan sebagai berikut:

Tentukan sebuah bilangan bulat yang bila dibagi dengan 5 menyisakan 3, bila dibagi 7 menyisakan 5, dan bila dibagi 11 menyisakan 7

Maka,

Misakan bilangan bulat tersebut = x. Formulasikan kedalam sistem kongruen lanjar:

x ≡ 3 (mod 5)

x ≡ 5 (mod 7)

x ≡ 7 (mod 11)

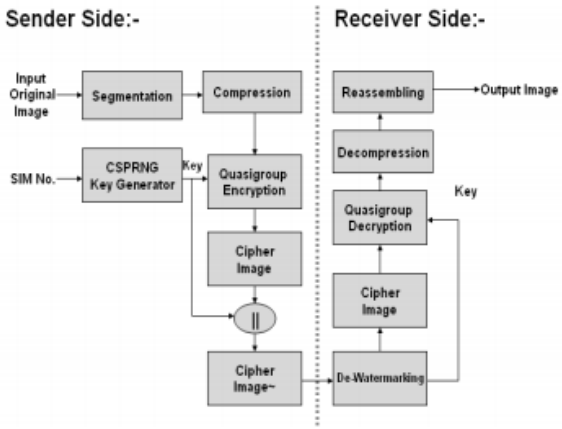
Misalkan m1, m2, …, mn adalah bilangan bulat positif sedemikian sehingga PBB(mi, mj) = 1 untuk i □ j. Maka sistem kongruen lanjar

x ≡ ak (mod mk)

mempunyai sebuah solusi unik dalam modulo m = m1 · m2 · … · mn.

III. ALGORITMA NUMBER THEORY BASED IMAGE COMPRESSION AND QUASIGROUP ENCRYPTION (NTICQE)

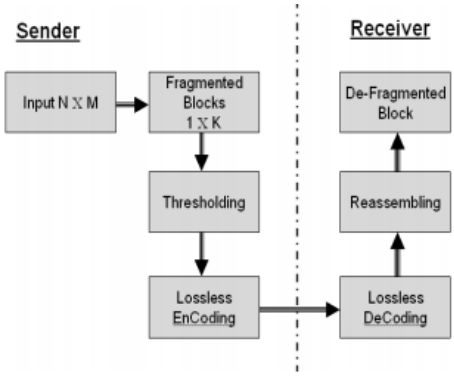
A. Arsitektur skema NTICQE



Gambar 1. Diagram skema NTICQE[2]

Pada gambar diatas terlihat bahwa dari pengirim, gambar awalnya masih jelas, kemudian dikompresi dan dienkripsi dengan menggunakan kunci dari CSPRNG Key Generator dan kemudian menghasilkan Cipher Image, yaitu gambar digital yang terlihat tidak jelas. Setelah gambar sampai ke penerima, barulah gambar didekripsi dan dikompresi sehingga terbentuk kembali gambar asli dari pengirim [2].

B. Segmentation dan Compression



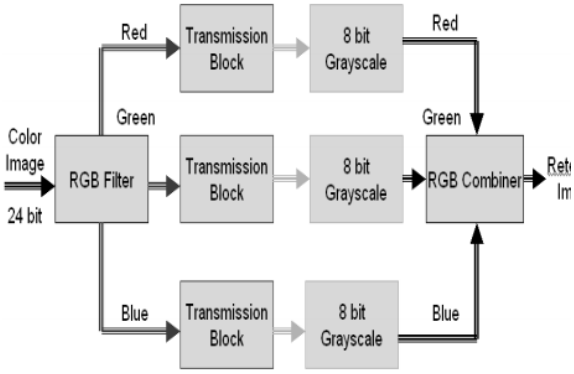
Gambar 2. Segmentasi dan Kompresi[2]

Disaat kompresi,, prinsip dari CRT digunakan. Ide yang

digunakan pada Segmentasi dan Kompresi ini adalah memecah pixel-pixel pada gambar input yang kemudian setiap setengah pixel dari pixel-pixel pada gambar akan di beri beberapa kunci yang unik setiap setengah pixelnya (tresholding) dan kemudian dilakukan transmisi terhadap gambar (lossless EnCoding) dimana hal ini akan membuat gambar terlihat tidak jelas karena sudah terenkripsi.

C. Image Encoding dan Decoding

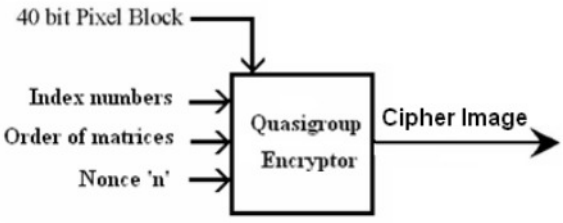
Setelah gambar ditransmisi, algoritma NTICQE selanjutnya dilakukan prosedur untuk membuat perubahan warna pada setiap blok setengah pixel dari gambar.



Gambar 3. Image Encoding dan Decoding[2]

Setelah setiap partisi setengah pixel dari gambar diubah warnanya, dilakukan penyatuan kembali partisi setengah pixel dari gambar sehingga gambar akan terlihat berubah warna.

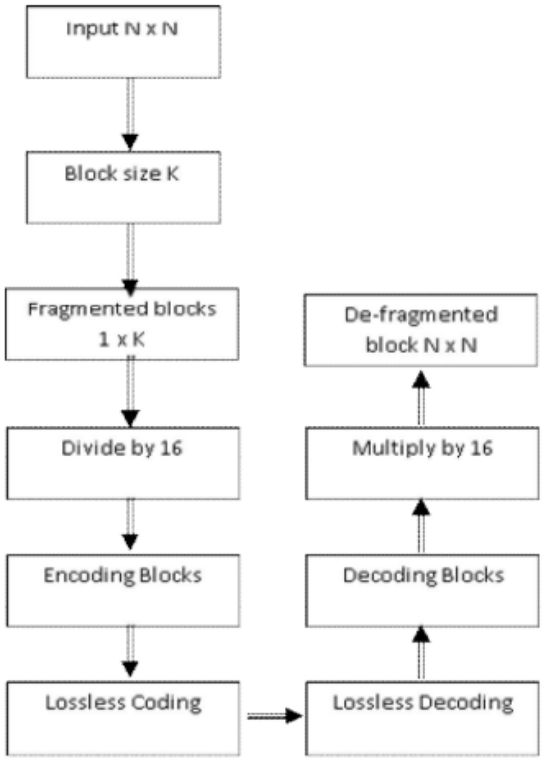
D. Enkripsi Gambar



Gambar 4. Enkriptor

Setelah dilakukan encoding, kemudian blok-blok pada gambar tadi diubah posisinya sesuai dengan key yang diproduksi di awal tadi (CSPRNG Key) di dalam encryptor. Setelah dilakukan pengubahan posisi-posisi blok dalam matriks gambar, terbentuklah Gambar Cipher atau Cipher Image yang terlihat tidak jelas dibandingkan gambar digital sebelum menjadi Cipher Image.

IV. PROSES DEKRIPSI HASIL ENCODING



Gambar 5. Diagram alir dari awal segmentasi hingga de-fragmantasi[3]

Setelah gambar digital berhasil dienkripsi, gambar tersebut dikirimkan melalui jaringan dengan kondisi tidak dapat dibuka hingga mencapai penerima gambar, Setelah gambar mencapai penerima, gambar melakukan Lossless decoding yang akan membuat gambar mulai terlihat jelas dan dapat didefragmantasi. Sebelum dapat didefragmantasi, blok-blok pada gambar didecoding terlebih dahulu dengan *private key* yang terdapat pada penerima. Setelah blok-blok gambar tersebut didecoding, blok-blok tersebut di defragmantasi dan kemudian di dekompresi. Setelah itu gambar digital tersebut di susun ulang seperti susunan dari pengirim dan kemudian gambar didapatkan oleh penerima sama seperti yang dikirm oleh pengirim.

Jika dalam pendekripsian kunci yang digunakan oleh penerima tidak sesuai (improper), maka gambar yang dari pengirim tidak akan terbentuk. Oleh karena itu harus ada data dari rasio kompresi untuk algoritma kompresi varian Lossless, seperti dibawah ini.

Image / Algorithm	Lena (CR)	Pepper (CR)	GoldHill (CR)
JPEG-LS	2.26	2.06	2.04
JPEG2000	1.86	1.41	1.65
CALIC	2.33	1.73	1.74
SPIHT	1.91	-	1.70
FELICS	1.65	1.55	1.95
HUFFMAN	1.56	1.71	-
LWZ	1.18	1.36	-
NTICE	1.85	1.91	2.02

Tabel 1. Rasio kompresi untuk algoritma kompresi varian lossless[2]

Dimana contoh gambar "Lena", "Pepper", dan "GoldHill" seperti dibawah ini.

Gambar 6. Lena[2]

Gambar 7. Pepper[2]

Gambar 8. GoldHill[2]

V. HASIL DARI PEMROSESAN ALGORITMA

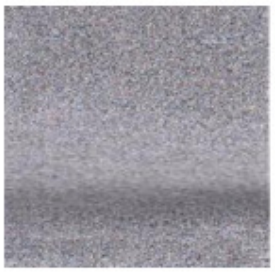
Setelah setiap partisi setengah pixel dari gambar diubah warnanya

.

Gambar 9. Gambar dari pengirim[3]

Sebagai contoh, misalkan gambar ini adalah gambar orisinil yang hendak dikirm melalui jaringan

Kemudian setelah dikompresi, apabila dekompresi menggunakan kunci yang salah, maka akan menjadi seperti gambar dibawah ini.



Gambar 10. Gambar hasil dekompresi yang diterima penerima apabila kunci yang diproses salah

Tetapi, apabila kuncinya benar, gambar yang diterima penerima akan sama seperti yang dikirim oleh pengirim.

.

VI. KESIMPULAN

Membuat sebuah gambar menjadi rahasia adalah hal yang dapat dilakukan untuk mengamankan dari ancaman

apabila terbongkarnya gambar tersebut. Oleh karena itu, menurut algoritma dari sumber yang dimiliki penulis, setiap setengah pixel dari gambar akan dienkripsikan dan posisi serta warna dari gambar digital tersebut pun dienkripsikan dengan kunci yang masing-masingnya unik. Sehingga apabila gambar hendak dibongkar, karena kunci yang tidak sesuai dengan kunci yang dibangun saat encoding, gambar tidak akan terbongkar rahasianya.

VII. Ucapan Terima Kasih

Puji syukur penulis sampaikan kepada Tuhan Yang Maha Esa karena dengan berkat-Nya penulis dapat menyelesaikan makalah ini. Tidak lupa penulis juga berterima kasih kepada Bapak Rinaldi Munir dan Ibu Harlili atas bimbingan yang telah diberikan sehingga penulis dapat menyelesaikan makalah ini. Penulis juga mengucapkan terima kasih juga kepada rekan-rekan yang mendukung penulis untuk dapat menyelesaikan makalah ini.

Referensi

[1] http://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2015-2016/matdis15-16.htm , diakses pada 10 November 2015 pukul 20.19

[2] https://eprint.iacr.org/2012/660.pdf , diakses pada 10 November 2015 pukul 22.31

[3] http://gpublication.com/jcer/;jsessionid=1301C5DEBB944556E8D32F49F56F80B0?wicket:interface=:0:dl_systemfilename::ILinkListener:: , diakses pada 10 November 2015 pukul 23.12

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.

Bandung, 8 Desember 2015

Harry Alvin Waidan Kefas - 13514036