UNIVERSITAS INDONESIA

SKEMA *SECRET IMAGE SHARING* MENGGUNAKAN FUNGSI *HASH* SATU ARAH DUA VARIABEL

SKRIPSI

M. ADHIARMAN HASAN

0806325604

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
PROGRAM STUDI MATEMATIKA
DEPOK
JUNI 2012

UNIVERSITAS INDONESIA

SKEMA *SECRET IMAGE SHARING* MENGGUNAKAN FUNGSI *HASH* SATU ARAH DUA VARIABEL

SKRIPSI

Skripsi ini diajukan sebagai syarat untuk memperoleh gelar Sarjana Sains

M. ADHIARMAN HASAN

0806325604

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
PROGRAM STUDI MATEMATIKA
DEPOK
JUNI 2012

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya saya sendiri,

dan semua sumber baik yang dikutip maupun dirujuk

telah saya nyatakan dengan benar.

Nama	: M. Adhiarman Hasan
NPM	: 0806325604
Tanda Tangan	: 
Tanggal	: 13 Juni 2012

HALAMAN PENGESAHAN

Skripsi ini diajukan oleh :
Nama : M. Adhiarman Hasan
NPM : 0806325604
Program Studi : Matematika
Judul Skripsi : Skema *Secret Image Sharing* menggunakan Fungsi *Hash* Satu Arah Dua Variabel

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Sains pada Program Studi Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Indonesia.

DEWAN PENGUJI

Pembimbing	: Dr. Kiki Ariyanti Sugeng	(.....)
Penguji I	: Drs. Suryadi MT, M.T.	(.....)
Penguji II	: Dr. rer. nat. Hendri Murfi	(.....)
Penguji III	: Dhian Widya, M.Kom.	(.....)

Ditetapkan di : Depok
Tanggal : 13 Juni 2012

KATA PENGANTAR

Alhamdulillah, puji syukur penulis panjatkan kepada Allah SWT atas semua rahmat dan karunia yang telah diberikan, sehingga penulis dapat menyelesaikan skripsi ini. Penulisan skripsi ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana Sains Program Studi Matematika pada Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Indonesia.

Penulis menyadari bahwa penyelesaian skripsi ini tidak terlepas dari bantuan dan bimbingan dari berbagai pihak. Oleh karena itu, penulis mengucapkan terima kasih kepada pihak-pihak yang telah berjasa dalam penulisan skripsi ini maupun selama penulis kuliah. Penulis mengucapkan terima kasih kepada:

(1) Dr. Kiki Ariyanti Sugeng selaku pembimbing skripsi penulis yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan penulis dalam penyusunan skripsi ini.
(2) Bapak Dr. Yudi Satria, M.T. selaku Ketua Departemen, Ibu Rahmi Rusin, S.Si, M.ScTech. selaku Sekretaris Departemen, dan Ibu Dr. Dian Lestari selaku Koordinator Pendidikan yang telah membantu penyelesaian tugas akhir ini.
(3) Dra. Netty Sunandi, M. Si. selaku Pembimbing Akademis penulis selama menjalani perkuliahan di Departemen Matematika UI.
(4) Seluruh staf pengajar di Departemen Matematika UI. Penulis mengucapkan terima kasih atas segala ilmu yang telah diberikan, semoga penulis dapat menggunakan ilmu tersebut dengan sebaik-baiknya.
(5) Seluruh karyawan di Departemen Matematika UI. Penulis mengucapkan terima kasih atas segala bantuan yang telah diberikan untuk penulis.
(6) H. Darham Heyder dan Hj. Melly Azhari sebagai orang tua penulis. Penulis mengucapkan terima kasih atas segala doa dan dukungan yang telah diberikan baik secara moral maupun material.

(7) Aida Rachmidar dan Muthiah Maulida sebagai kakak penulis. Penulis mengucapkan terima kasih atas doa dan dukungan yang telah diberikan.

(8) Rizki Ali Akbar dan Ekwan Riyadi sebagai kakak ipar penulis. Penulis mengucapkan terima kasih atas doa dan dukungan yang telah diberikan.

(9) Unaisyah Azkia Husna dan Rafiq As-Syaukani Akbar sebagai keponakan penulis yang selalu membuat hari-hari penulis di rumah menjadi lebih ceria.

(10) Seluruh keluarga penulis yang telah memberikan doa dan dukungan kepada penulis.

(11) Riza Nur Adinda. Penulis mengucapkan terima kasih atas segala dukungan, saran, semangat, perhatian, dan doanya.

(12) Sahabat-sahabat penulis di Pondokan Asri, yaitu Aji, Nizar, Aziz, Dodo, Rio, Ronggo, Candra, Nikki, Arif, Rian, David, Surya, dan lain-lain. Penulis mengucapkan terima kasih telah membuat waktu-waktu luang penulis menjadi tidak membosankan.

(13) Teman-teman Teknik Elektro PNJ angkatan 2009, yaitu Aji, Nizar, Arif, Dwiki, Avif, Handi, Oji, Agung, Ali, Rizka, dan lain-lain. Penulis mengucapkan terima kasih atas segala dukungan dan doa yang diberikan, semoga diberikan kelulusan semester ini dengan hasil yang memuaskan.

(14) Semua teman-teman yang tergabung dalam grup *facebook* Kosan Tarno.

(15) Teman-teman SMA Martia Bhakti, Ifan, Labora, Ayu, Sasa, Rahmi, Fiqi, Reza, Saiful, dan lain-lain.

(16) Andy Marhadi Sutanto dan Septyadi Prabowo sebagai teman seperjuangan dalam penulisan skripsi dengan topik *Secret Sharing*.

(17) Teman-teman seperjuangan dalam tugas akhir. (Andy, Bowo, Tuti, Qiqi, Cindy, Risya, Ines, Numa, Citra, Hendry, Mei, Nita, Ade, Awe, Dhila, Anisah, Maul, Asri, Uci L, Vika, Resti, Emy, Janu, Dhea, Oline, Ega, Eka, Icha, Sita, Luthfa, Arief, Fani, Wulan, Umbu, Anis 2007, Ashari 2007, Fauzan 2007, Putri 2007).

(18) Teman-teman angkatan 2008, (Ade, Agnes, Maimun, Awe, Hindun, Dhewe, Nora, Qiqi, Luthfa, Umbu, Anisah, Puput, Arief, Arkies, Arman, Andy, Ifah, Maulia, May, Mei, Yulial, Asri, Olin, Cindy, Citra, Danis, Nadia, Nita, Vika, Numa, Resti, Lian, Dede, Dhea, Dheni, Dian, Agy, Sita, Risya, Bowo,

Ines, Tuti, Janu, Eka, Emy, Dhila, Siwi, Ega, Wulan, Fani, Icha, Uchi, Uci L, Hendry, Purwo, Masykur, Juni, Ramos, Dini, Aya). Semoga persaudaraan yang kita bangun selama kurang lebih 4 tahun ini terus kontinu dalam interval waktu yang tak terhingga.

(19) Teman-teman angkatan 2004, 2005, 2006, 2007, 2009, 2010.

(20) Semua pihak yang telah membantu penulis yang namanya tidak dapat disebutkan satu-persatu.

Akhir kata, saya berharap semua pihak yang telah membantu mendapatkan kebaikan yang tak ternilai. Semoga skripsi ini membawa manfaat bagi pengembangan ilmu.

Penulis

2012

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Indonesia, saya yang bertanda tangan di bawah ini:

Nama	: M. Adhiarman Hasan
NPM	: 0806325604
Program Studi	: S1
Departemen	: Matematika
Fakultas	: Matematika dan Ilmu Pengetahuan Alam
Jenis karya	: Skripsi

demi pengembangan ilmu pengetahuan, menyetujui untuk memberika kepada Universitas Indonesia Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalti Free Right*) atas karya ilmiah saya yang berjudul:
Skema *Secret Image Sharing* Menggunakan Fungsi *Hash* Satu Arah Dua Variabel beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Indonesia berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan memublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok

Pada tanggal : Juni 2012

Yang menyatakan

(M. Adhiarman Hasan)

ABSTRAK

Nama : M. Adhiarman Hasan
Program Studi : Matematika
Judul : Skema *Secret Image Sharing* Menggunakan Fungsi *Hash* Satu Arah Dua Variabel

Kriptografi adalah ilmu untuk menjaga suatu pesan agar tetap aman. Pesan dalam bentuk gambar atau citra digital menjadi suatu masalah tersendiri untuk dijaga keamanannya karena memiliki kesulitan yang berbeda untuk mengelolanya. Skema *secret sharing* memungkinkan untuk membagi pesan rahasia baik berbentuk teks maupun citra digital kepada sekelompok orang (partisipan) sedemikian sehingga hanya kombinasi orang tertentu yang dapat mengembalikan isi dari pesan tersebut. Dalam skripsi ini akan dibahas skema *secret sharing* dengan rahasia berupa citra digital yang di dalamnya menggunakan suatu fungsi *hash* satu arah dua variabel yang berguna untuk merahasiakan informasi yang dimiliki oleh setiap partisipan.

Kata Kunci : Kriptografi, skema *secret sharing*, fungsi *hash* satu arah dua variabel, citra digital.
xiii+42 halaman : 17 gambar; 6 tabel
Bibliografi : 9 (1979-2011)

ABSTRACT

Name : M. Adhiarman Hasan
Program Study : Mathematics

Topic : Secret Image Sharing Scheme Using Two Variable One Way Hash Function

Cryptography is the science of keeping message secure. Message in the form of pictures or digital images becomes a separate issue to be taken care of security because it has a different difficulty to manage it. Secret sharing scheme allows to share a secret message either in the form of text or digital images to a group of people (participants) so that only certain combinations of people who can restore the contents of the message. In this *skripsi* will be discussed a secret sharing scheme with secrets of digital image in which the use of a two-variables one-way hash function that are useful to keep confidential information held by each participant.

Keyword : Cryptography, secret sharing scheme, two-variable one-way hash function, digital images.
xiii+42 pages : 17 pictures; 6 tables
Bibliography : 9 (1979-2011)

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Dewasa ini, kebutuhan data dan informasi sangatlah besar bagi berbagai kalangan di seluruh dunia. Data dapat berbentuk elektronik maupun nonelektronik. Namun, data atau informasi yang berbentuk elektronik lebih diminati karena lebih mudah diakses baik menggunakan internet maupun melalui media penyimpanan digital. Kemudahan inilah yang menjadi bumerang jika data atau informasi tersebut tidak dijaga dan disimpan dengan baik. Apalagi teknologi yang semakin maju yang memungkinkan untuk dapat berkomunikasi dan saling bertukar data atau informasi secara jarak jauh serta akses komputer dan internet bisa dibilang tidak dapat dipisahkan dari keseharian setiap orang sehingga data atau informasi tersebut sangatlah riskan jika diakses dan disalahgunakan oleh pihak lain. Untuk menghindari penyalahgunaan tersebut, tentunya keamanan data atau informasi tersebut harus selalu dijaga dengan baik.

Keamanan itu sendiri menjadi masalah ketika mempertimbangkan untuk menyimpan dan mengirimkan informasi berupa gambar yang dinilai penting misalnya foto satelit atau gambar medis. Untuk itu perlu adanya suatu cara atau mekanisme untuk mengamankan informasi yang berupa gambar tersebut agar tidak diketahui oleh pihak yang tidak berkepentingan. Masalah keamanan ini secara umum dapat diatasi dengan ilmu kriptografi.

Kriptografi (*cryptography*) berasal dari bahasa Yunani yang terdiri dari dua suku kata yaitu kripto dan graphia. Kripto artinya menyembunyikan, sedangkan graphia artinya tulisan. Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Menurut Scheiner (1996), kriptografi adalah seni dan ilmu dalam menjaga pesan agar tetap aman.

Seiring dengan berjalannya waktu, kriptografi banyak mengalami perkembangan. Untuk mengamankan suatu informasi dalam kriptografi dikenal suatu

istilah yang disebut enkripsi, yaitu suatu cara untuk menyandikan suatu pesan asli (*plaintext*) menjadi pesan rahasia (*ciphertext*). Sedangkan cara untuk mengembalikan pesan rahasia (*ciphertext*) kembali menjadi pesan asli (*plaintext*) disebut dekripsi. Enkripsi dan dekripsi ini berlaku juga untuk informasi berupa citra atau gambar. Namun, informasi yang telah terenkripsi tidak dapat dikembalikan jika kunci untuk melakukan dekripsi hilang akibat kesalahan dari pengguna. Hal inilah yang menjadikan perkembangan metode dalam kriptografi berkembang pesat. Salah satu metode yang dinilai baik untuk menjaga suatu informasi tetap aman adalah *secret sharing scheme.*

Secret sharing scheme atau dapat disebut skema *secret sharing* pertama kali diusulkan oleh Shamir dan Blakley pada tahun 1979. Skema *secret sharing* merupakan salah satu metode untuk mengamankan suatu rahasia dengan membagi atau mendistribusikan rahasia tersebut menjadi beberapa bagian yang disebut *share*, setiap bagian dari rahasia tersebut tidak memberikan informasi apapun mengenai rahasia yang dimaksud bila tidak digabungkan dengan bagian yang lainnya. Skema *secret sharing* berdasarkan Tilborg dan Jajodia (2011) memungkinkan untuk berbagi rahasia di antara sekelompok orang sedemikian sehingga hanya kombinasi orang tertentu yang dapat mengembalikan isi dari rahasia tersebut. Skema *secret sharing* untuk informasi berupa citra atau gambar dapat disebut sebagai skema *secret image sharing*.

Skema *secret image sharing* banyak mengalami perkembangan dan penyempurnaan dari tahun ke tahun. Sampai pada tahun 2010, Alexandrova, dkk. merumuskan skema *secret image sharing* menggunakan fungsi *hash* satu arah dua variabel.

1.2 Perumusan Masalah dan Ruang Lingkup

Permasalahan dalam tugas akhir ini adalah bagaimana mengkonstruksi skema *secret image sharing* menggunakan fungsi *hash* satu arah dua variabel.

Ruang lingkup permasalahan dibatasi dengan informasi yang dirahasiakan berupa citra digital hitam putih dengan tingkat gambar abu-abu (*grayscale*) berdimensi $m \times m$.

1.3 Jenis Penelitian

Penelitian yang digunakan dalam penulisan tugas akhir ini adalah berdasarkan studi literatur serta melakukan pembuatan program komputer untuk implementasi skema *secret image sharing* menggunakan fungsi *hash* satu arah dua variabel.

1.4 Tujuan Penelitian

1. Menjelaskan konsep skema *secret image sharing*
2. Mengkaji konstruksi skema *secret image sharing* menggunakan fungsi *hash* satu arah dua variabel
3. Mengimplementasikan skema *secret image sharing* menggunakan fungsi *hash* satu arah dua variabel pada informasi berupa citra digital dengan tingkat gambar abu-abu (*grayscale*) dengan menggunakan program yang diproses secara komputasi

BAB 2
LANDASAN TEORI

Pada bab ini akan diberikan beberapa definisi dan konsep dasar dari skema *secret image sharing* yang akan digunakan pada bab selanjutnya.

2.1 Operasi XOR

Dalam tugas akhir ini digunakan operasi XOR atau eksklusif-*or* untuk membentuk fungsi *hash* satu arah dua variabel serta untuk memproses citra yang akan dirahasiakan. Berikut diberikan definisi dari operasi XOR.

Definisi 2.1 (Rosen, 2007) Misalkan p dan q adalah proposisi. Eksklusif-*or* antara p dan q, dinotasikan sebagai $p \oplus q$, adalah proposisi yang bernilai benar ketika salah satu dari p dan q bernilai benar atau salah satu dari p dan q bernilai salah.

Tabel 2.1 menyatakan nilai kebenaran dari eksklusif-*or* antara proposisi p dan q.

Tabel 2.1 Nilai kebenaran eksklusif-*or* dari dua proposisi

p	q	$p \oplus q$
Benar	Benar	Salah
Benar	Salah	Benar
Salah	Benar	Benar
Salah	Salah	Salah

Operasi XOR biasanya digunakan untuk mengoperasikan dua variabel *Boolean* (bernilai 1 atau 0), yaitu misalkan A dan B sehingga operasi XOR dapat disebut juga sebagai operasi *Boolean* XOR. Tabel 2.2 menyatakan hasil dari operasi *Boolean* XOR.

Tabel 2.2 Hasil operasi *Boolean* XOR

A	B	A⊕B
0	0	0
1	0	1
0	1	1
1	1	0

2.2 Lapangan Galois

Proses perhitungan dalam tugas akhir ini menggunakan operasi aritmatika yang berlaku dalam suatu lapangan berhingga, yaitu lapangan yang memiliki jumlah elemen yang berhingga. Salah satu bentuk lapangan berhingga yaitu lapangan Galois. GF(q) adalah suatu lapangan berhingga dengan orde q, yaitu himpunan Z_q bilangan bulat $\{0, 1, \ldots, q-1\}$ dengan operasi aritmatika modulo q.

Contoh 2.1

GF(2) = {0, 1}

GF(3) = {0, 1, 2}

GF(7) = {0, 1, 2, 3, 4, 5, 6}

GF(19) = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18}

Lapangan berhingga yang paling sederhana yaitu GF(2). Perhitungan aritmatika penjumlahan dan perkalian dalam GF(2) dapat dilihat dalam Tabel 2.3 dan Tabel 2.4.

Tabel 2.3 Penjumlahan dalam GF(2)

+	0	1
0	0	1
1	1	0

Tabel 2.4 Perkalian dalam GF(2)

×	0	1
0	0	0
1	0	1

Dalam kasus di atas, terlihat bahwa penjumlahan dalam GF(2) sama dengan operasi *Boolean* XOR dan perkalian dalam GF(2) sama dengan operasi AND. Sifat tersebut tidak berlaku secara umum, contohnya untuk nilai q yang lebih besar, misalkan $q = 7$, diperoleh penjumlahan dan perkalian dalam GF(7) dalam Tabel 2.5 dan Tabel 2.6.

Tabel 2.5 Penjumlahan dalam GF(7)

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Tabel 2.6 Perkalian dalam GF(7)

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

2.3 Skema (*t, n*) Shamir's *Secret Sharing*

Skema Shamir's *Secret Sharing* (*t, n*), dimana *n* adalah banyaknya partisipan (orang yang memperoleh *secret*) dan *t* adalah banyaknya partisipan minimal yang dapat merekonstruksi *secret* ($t \leq n$), direpresentasikan berdasarkan pendekatan polinomial. Misalkan untuk membentuk persamaan linier $y = a_0 + a_1 x$, diperlukan minimal 2 titik yaitu (x_1, y_1) dan (x_2, y_2). Selain itu, untuk membentuk persamaan kuadrat $y = a_0 + a_1 x + a_2 x^2$ diperlukan minimal 3 titik yaitu (x_1, y_1), (x_2, y_2), dan (x_3, y_3). Secara umum, untuk membentuk polinomial $y = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ diperlukan minimal sebanyak $(n + 1)$ titik yaitu (x_1, y_1), (x_2, y_2), …, (x_{n+1}, y_{n+1}).

Skema (t, n) Shamir's *Secret Sharing* dideskripsikan dalam langkah-langkah sebagai berikut:

1. Misal $K \in GF(q)$ merupakan rahasia yang akan dibagikan kepada n partisipan (U_1, U_2, …, U_n), dimana q adalah bilangan prima dan $q \geq n + 1$.
2. Pilih sembarang a_1, …, $a_{t-1} \in GF(q)$, dan konstruksi polinomial $h(x)$:
$$h(x) = K + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}.$$
3. Pilih n bilangan bulat berbeda yaitu $x_i \in GF(q)$, $1 \leq i \leq n$, dimana x_i adalah nilai publik dari masing-masing partisipan dan tidak dirahasiakan.
4. Distribusikan $v_i = h(x_i)$ kepada partisipan U_i, $1 \leq i \leq n$, dimana v_i dirahasiakan.

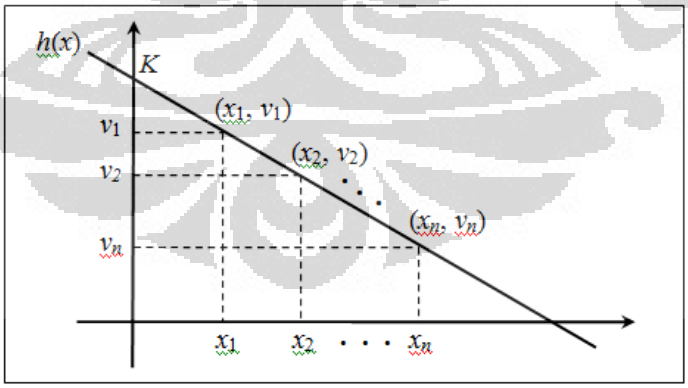
Untuk merekonstruksi K, digunakan interpolasi Lagrange dengan mengetahui t titik, yaitu $(x_1, h(x_1))$, $(x_2, h(x_2))$, …, $(x_t, h(x_t))$. Maka polinomial $h(x)$ dapat dikonstruksi dengan rumus:

$$h(x) = \sum_{i=1}^{t} h(x_i) \prod_{1 \leq j \leq t, j \neq i} \frac{x - x_j}{x_i - x_j}$$

Dari polinomial $h(x)$, dapat diperoleh nilai dari K, yaitu $K = h(0)$, yaitu:

$$K = \sum_{i=1}^{t} h(x_i) \prod_{1 \leq j \leq t, j \neq i} \frac{x_j}{x_j - x_i}$$

Pendekatan secara geometri dapat dilihat melalui Gambar 2.1:

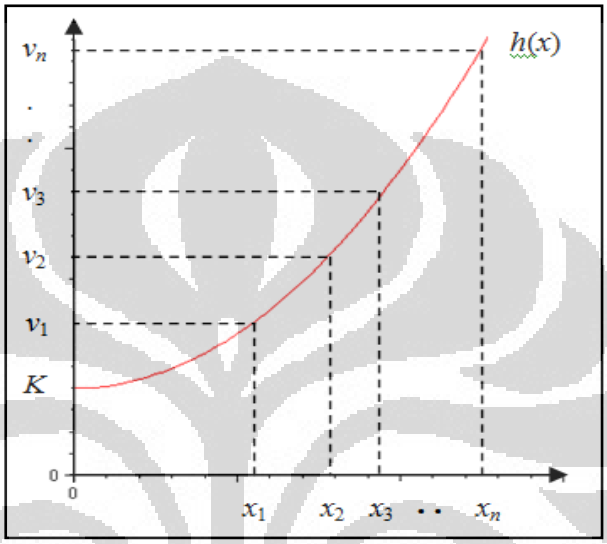


Gambar 2.1 Kurva skema shamir's *secret sharing* derajat satu

Berdasarkan Gambar 2.1, apabila diambil minimal dua titik dari titik-titik (x_i, v_i), dimana $1 \leq i \leq n$, maka dapat dibentuk persamaan garis $h(x) = K + a_1 x$

dengan menggunakan interpolasi Lagrange. Setelah diperoleh persamaan garis $h(x)$, maka nilai dari rahasia K dapat diketahui, yaitu $K = h(0)$.

Berdasarkan Gambar 2.1, polinomial $h(x)$ berupa fungsi linier. Namun, polinomial $h(x)$ dapat dikonstruksi berupa fungsi dengan derajat lebih dari satu seperti pada Gambar 2.2, yaitu misalkan $h(x) = x^2 + 40$. Dalam hal ini, nilai rahasia K adalah 40.



Gambar 2.2 Kurva skema shamir's *Secret Sharing* derajat dua

Contoh 2.2

Misalkan akan digunakan skema Shamir's *Secret Sharing* (4, 6) dengan $q = 7$ untuk membagikan rahasia $K = 3 \in GF(7)$

Dalam hal ini, banyaknya partisipan yaitu $n = 6$ dan banyaknya partisipan yang dapat merekonstruksi K yaitu $t = 4$.

Pilih $a_0 = K = 3$, $a_1 = 2$, $a_2 = 5$, $a_3 = 4$. Konstruksi polinomial $h(x) = K + a_1x + a_2x^2 + a_3x^3$ sebagai berikut.

$$h(x) = 3 + 2x + 5x^2 + 4x^3.$$

Pilih $x_1 = 1$, $x_2 = 2$, $x_3 = 3$, $x_4 = 4$, $x_5 = 5$, $x_6 = 6$ sebagai identitas masing-masing partisipan $U_1, U_2, \ldots, U_6$.

Hitung $v_i = h(x_i)$, $i = 1, 2, \ldots, 6$ dan distribusikan kepada masing-masing partisipan U_i, $i = 1, 2, \ldots, 6$.

$v_1 = h(1) = 14 \equiv 0 \in GF(7)$;

$v_2 = h(2) = 59 \equiv 3 \in GF(7)$;

$v_3 = h(3) = 162 \equiv 1 \in GF(7)$;

$v_4 = h(4) = 347 \equiv 4 \in GF(7)$;

$v_5 = h(5) = 638 \equiv 1 \in GF(7)$;

$v_6 = h(6) = 1059 \equiv 2 \in GF(7)$.

Misalkan partisipan yang akan merekonstruksi K adalah U_1, U_3, U_4, dan U_6.
Maka akan diketahui 4 titik yaitu $(x_1, h(x_1))$; $(x_3, h(x_3))$; $(x_4, h(x_4))$; dan $(x_6, h(x_6))$.

$(x_1, h(x_1)) = (1, 0)$;

$(x_3, h(x_3)) = (3, 1)$;

$(x_4, h(x_4)) = (4, 4)$;

$(x_6, h(x_6)) = (6, 2)$.

Berdasarkan 4 titik di atas, akan dikonstruksi polinomial $h(x)$ dengan menggunakan interpolasi Lagrange dimana seluruh perhitungan dilakukan dalam $GF(7)$.

$$h(x) = h(x_1)\left(\frac{x-x_3}{x_1-x_3}\right)\left(\frac{x-x_4}{x_1-x_4}\right)\left(\frac{x-x_6}{x_1-x_6}\right)$$
$$+ h(x_3)\left(\frac{x-x_1}{x_3-x_1}\right)\left(\frac{x-x_4}{x_3-x_4}\right)\left(\frac{x-x_6}{x_3-x_6}\right)$$
$$+ h(x_4)\left(\frac{x-x_1}{x_4-x_1}\right)\left(\frac{x-x_3}{x_4-x_3}\right)\left(\frac{x-x_6}{x_4-x_6}\right)$$
$$+ h(x_6)\left(\frac{x-x_1}{x_6-x_1}\right)\left(\frac{x-x_3}{x_6-x_3}\right)\left(\frac{x-x_4}{x_6-x_4}\right)$$
$$= 0\left(\frac{x-3}{1-3}\right)\left(\frac{x-4}{1-4}\right)\left(\frac{x-6}{1-6}\right) + 1\left(\frac{x-1}{3-1}\right)\left(\frac{x-4}{3-4}\right)\left(\frac{x-6}{3-6}\right)$$
$$+ 4\left(\frac{x-1}{4-1}\right)\left(\frac{x-3}{4-3}\right)\left(\frac{x-6}{4-6}\right) + 2\left(\frac{x-1}{6-1}\right)\left(\frac{x-3}{6-3}\right)\left(\frac{x-4}{6-4}\right)$$
$$= 3 + 2x + 5x^2 + 4x^3$$

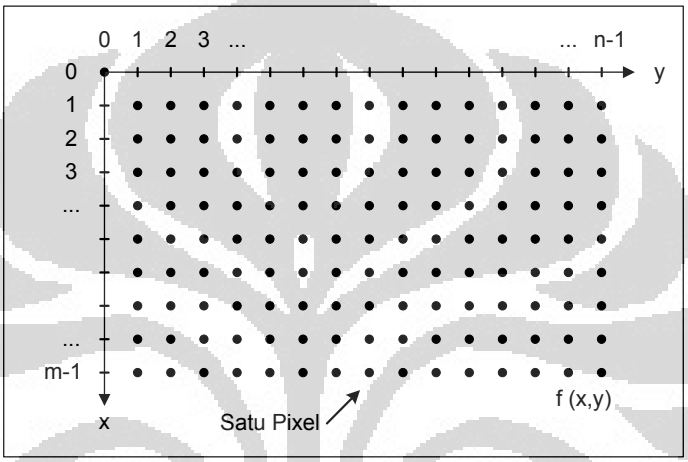
Maka, diperoleh $K = h(0) = 3 + 2\times0 + 5\times0^2 + 4\times0^3 = 3$.

2.4 Citra Digital

Suatu citra atau gambar (Gonzales & Woods, 2002) didefinisikan sebagai fungsi dimensi dua, $f(x, y)$, dimana x dan y merupakan bidang koordinat, dan nilai dari f pada setiap pasangan koordinat (x, y) disebut intensitas atau tingkat keabuan dari citra atau gambar pada titik tersebut. Ketika x, y, dan nilai dari f

seluruhnya terbatas, maka citra tersebut disebut citra digital (Gonzales & Woods, 2002).

Elemen yang dikenal secara luas untuk merepresentasikan citra digital yaitu piksel. Dalam citra digital, piksel direpresentasikan dalam koordinat (*x*, *y*) yang telah dijelaskan dalam pembahasan di atas, dan nilai dari setiap pikel memiliki nilai yang menunjukkan tingkat keabuan dari citra pada koordinat piksel tersebut. Pada Gambar 2.3 dapat dilihat representasi piksel dalam suatu citra digital.



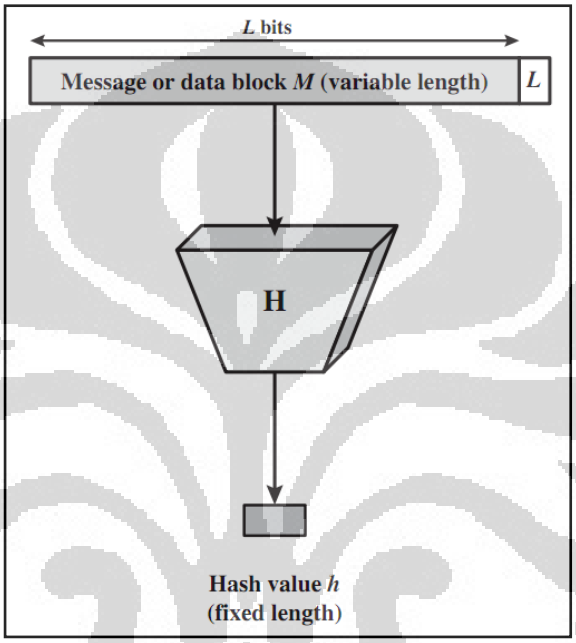
Gambar 2.3 Representasi citra digital

Citra digital itu sendiri terdiri dari berbagai tipe, diantaranya citra biner, citra hitam putih, dan citra berwarna. Dalam tugas akhir ini akan digunakan citra hitam putih. Citra hitam putih dibentuk dari piksel-piksel yang masing-masing memiliki nilai suatu bilangan sesuai dengan tingkat keabuan citra pada lokasi tertentu yang berkisar antara 0 – 255 (Sachs, 1996). Tingkat keabuan itu sendiri diilustrasikan dalam Gambar 2.4.

Gambar 2.4 Tingkat keabuan pada citra hitam putih

2.5 Fungsi *Hash*

Fungsi *hash* (Tilborg & Jajodia, 2011) adalah fungsi yang menerima input berupa pesan yang ukurannya sembarang dan menghasilkan nilai *hash* yang berukuran tetap. Menurut Stallings (2011), suatu fungsi *hash* H menerima blok data *M* dengan panjang bervariasi dan memproduksi nilai *hash* berukuran tetap yaitu $h = H(M)$. Gambar 2.5 menggambarkan diagram dari suatu fungsi *hash*.



Gambar 2.5 Diagram fungsi *Hash*; $h = H(M)$

Dalam tugas akhir ini digunakan fungsi hash satu arah. Fungsi *hash* satu arah pertama kali dijelaskan oleh Diffie dan Hellman.

Definisi 2.2 (Tilborg dan Jajodia, 2011) Fungsi *hash* satu arah adalah suatu fungsi H yang memenuhi kondisi berikut:

1. Pesan X dapat memiliki ukuran panjang sembarang dan nilai *hash* $h = H(X)$ memiliki panjang tetap.
2. Fungsi *hash* harus bersifat satu arah yaitu jika diberikan Y sebagai peta dari H, maka sangat sulit secara komputasi untuk mencari pesan X sedemikian sehingga $H(X) = Y$. Selain itu, jika diberikan pesan X dan $H(X)$ maka sangat sulit secara komputasi untuk mencari pesan $X' \neq X$ sedemikian sehingga $H(X') = H(X)$.

BAB 3
KONSTRUKSI SKEMA *SECRET IMAGE SHARING* MENGGUNAKAN FUNGSI *HASH* SATU ARAH DUA VARIABEL

Metode *secret sharing* yang telah dibahas pada bab sebelumnya sangatlah sederhana serta kurang aman dan efisien sehingga metode ini banyak mengalami perkembangan. Kemudian, Alexandrova, dkk. mengembangkan metode tersebut yang kemudian diimplementasikan untuk rahasia berupa citra digital. Pada bab ini akan dibahas skema *multi secret sharing* yang merupakan dasar dari metode yang dikembangkan oleh Alexandrova, dkk dan skema *secret image sharing* yang dikembangkan Alexandrova, dkk.

3.1 Fungsi *Hash* Satu Arah Dua Variabel

Fungsi *hash* yang biasa digunakan adalah fungsi *hash* dengan satu variabel. Namun, fungsi *hash* tersebut dapat diperluas untuk dua variabel. Berikut ini diberikan definisi dan sifat-sifat dari fungsi *hash* satu arah dua variabel yang digunakan untuk skema *secret image sharing* yang dibahas dalam tugas akhir ini.

Definisi 3.1 (Pang & Wang, 2005) Fungsi *hash* satu arah dua variabel $f(r, s)$ adalah suatu fungsi yang memetakan bilangan bulat r dan s dengan panjang sembarang pada *bit string*
$f(r, s)$ dengan panjang tetap yang memiliki sifat-sifat berikut:

a. Jika diberikan r dan s, maka mudah untuk menghitung $f(r, s)$.
b. Jika diberikan s dan $f(r, s)$, maka sulit untuk menghitung r.
c. Jika s tidak diketahui, maka sulit untuk menghitung $f(r, s)$ untuk sembarang r.
d. Jika diberikan s, maka sulit untuk menghitung dua nilai berbeda r_1 dan r_2 sedemikian sehingga $f(r_1, s) = f(r_2, s)$.
e. Jika diberikan r dan $f(r, s)$, maka sulit untuk menghitung s.
f. Jika diberikan pasangan r dan $f(r, s)$, maka sulit untuk menghitung $f(r', s)$ untuk $r' = r$.

Pada skripsi ini dipilih fungsi *hash* satu arah dua variabel yang memetakan pasangan bilangan bulat (*r, s*) ke himpunan *bit string* pada persamaan (3.1).

$$f(r, s) = (r \times s) \oplus (r \bmod s) \quad (3.1)$$

Fungsi *hash* satu arah dua variabel dalam persamaan (3.1) memenuhi sifat-sifat yang ada dalam Definisi 3.1 yang selanjutnya akan digunakan dalam skema *secret image sharing* yang dibahas dalam bab ini.

Akan dibuktikan fungsi tersebut memenuhi sifat-sifat dari fungsi *hash* satu arah dua variabel yang ada pada Definisi 3.1.

$$\begin{aligned} f(r,s) &= (r \times s) \oplus (r \bmod s) \\ &= (a_{dec}) \oplus (b_{dec}) \\ &= (a_{bin}) \oplus (b_{bin}) \\ &= c_{bin} \\ &= c_{dec} \end{aligned}$$

Keterangan:

- r dan s merupakan bilangan bulat sembarang.
- a_{dec} dan b_{dec} masing-masing merupakan hasil perhitungan $r \times s$ dan $r \bmod s$ dalam bilangan desimal.
- a_{bin} dan b_{bin} masing-masing merupakan representasi bilangan biner dari a_{dec} dan b_{dec}.
- c_{bin} merupakan hasil perhitungan menggunakan operasi XOR dari a_{bin} dan b_{bin}.
- c_{dec} merupakan representasi bilangan decimal dari c_{bin}.

a. Jika diberikan *r* dan *s*, maka mudah untuk menghitung *f*(*r*, *s*).
   Jelas, karena perhitungan dari *f*(*r*, *s*) di atas mudah.

b. Jika diberikan *s* dan *f*(*r*, *s*), maka sulit untuk menghitung *r*.
   Jika hanya diketahui nilai *s* dan *f*(*r*, *s*) maka hanya akan diketahui nilai dari c_{dec} dan mudah untuk mengetahui nilai dari c_{bin}. Tapi sulit mencari nilai dari a_{bin} dan b_{bin} karena nilai yang diperoleh lebih dari satu. Jadi, sulit untuk mengetahui nilai dari *r*, karena dibutuhkan informasi dari nilai a_{dec} dan b_{dec}.

c. Jika *s* tidak diketahui, maka sulit untuk menghitung *f*(*r*, *s*) untuk sembarang *r*.
   Jelas, karena dibutuhkan nilai *s* untuk menghitung *f*(*r*, *s*).

d. Jika diberikan *s*, maka sulit untuk menghitung dua nilai berbeda r_1 dan r_2 sedemikian sehingga $f(r_1, s) = f(r_2, s)$.
   Jika hanya diketahui nilai *s* maka untuk nilai r_1 dan r_2 yang berbeda, akan menghasilkan nilai $f(r_1, s)$ dan $f(r_2, s)$ yang berbeda.
e. Jika diberikan *r* dan $f(r, s)$, maka sulit untuk menghitung *s*.
   Jelas. Kasus ini sama dengan poin b.
f. Jika diberikan pasangan *r* dan $f(r, s)$, maka sulit untuk menghitung $f(r', s)$ untuk $r' = r$.
   Jelas, karena karena dibutuhkan nilai *s* untuk menghitung $f(r, s)$.

Contoh 3.2

Misalkan diambil nilai $r = 7$ dan $s = 4$.

Maka diperoleh nilai $f(r, s)$ sebagai berikut:

$$\begin{aligned} f(r,s) &= (r \times s) \oplus (r \bmod s) \\ &= (7 \times 4) \oplus (7 \bmod 4) \\ &= (28) \oplus (3) \\ &= 11100 \oplus 00011 \\ &= 11111 \\ &= 31 \end{aligned}$$

3.2 Skema (*t*, *n*) *Multi-Secret Sharing*

Dalam skema *multi-secret sharing* (Pang & Wang, 2005), suatu himpunan *p* rahasia yaitu $K_1, K_2, \ldots, K_p$ dapat dibagikan sekaligus kepada sejumlah *n* partisipan $\{U_1, U_2, \ldots, U_n\}$ sedemikian sehingga setiap partisipan hanya perlu menjaga satu *share*, yang disebut *secret share*. Dalam (*t*, *n*) skema *multi-secret sharing*, dengan mengkombinasikan sembarang *t* ($t \leq n$) *secret share*, maka *p* rahasia dapat direkonstruksi sekaligus, tapi mengkombinasikan sembarang $(t - 1)$ atau kurang dari $(t - 1)$ *secret shares*, *p* rahasia tersebut tidak dapat direkonstruksi. Untuk merekonstruksi rahasia-rahasia tersebut, partisipan-partisipan harus memberikan *pseudo-share* yang dihitung dari *secret share*

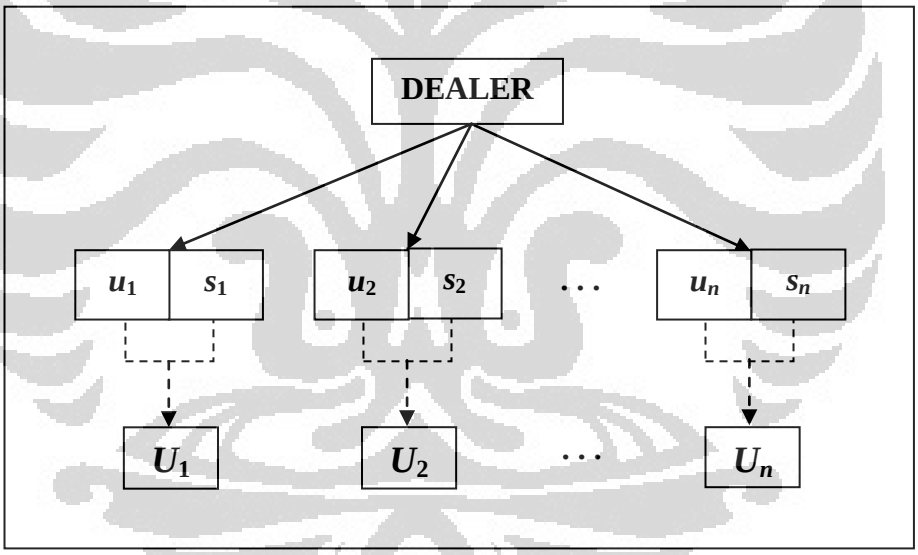
masing-masing partisipan. *Secret share* akan aman dikarenakan sifat-sifat yang dimiliki oleh fungsi satu arah dua variabel.

Skema (*t*, *n*) *multi-secret sharing* dideskripsikan menjadi 3 langkah, yaitu langkah awal, pembagian rahasia, dan rekonstruksi rahasia.

3.2.1 Langkah Awal Skema (*t*, *n*) *Multi-Secret Sharing*

Dealer (yaitu pihak yang melakukan pembagian rahasia) memilih secara acak *n* buah bilangan bulat berbeda $s_1, s_2, \ldots, s_n \in GF(q)$ dimana *q* bilangan prima. $s_1, s_2, \ldots, s_n$ merupakan *secret share* masing-masing partisipan dan diberikan kepada masing-masing partisipan.

Dealer memilih *n* bilangan bulat berbeda $u_1, u_2, \ldots, u_n \in [p, q-1]$ sebagai identitas publik dari masing-masing partisipan.



Gambar 3.1 Ilustrasi langkah awal skema (*t*, *n*) *multi-secret sharing*

3.2.2 Pembagian Rahasia dalam Skema (*t*, *n*) *Multi-Secret Sharing*

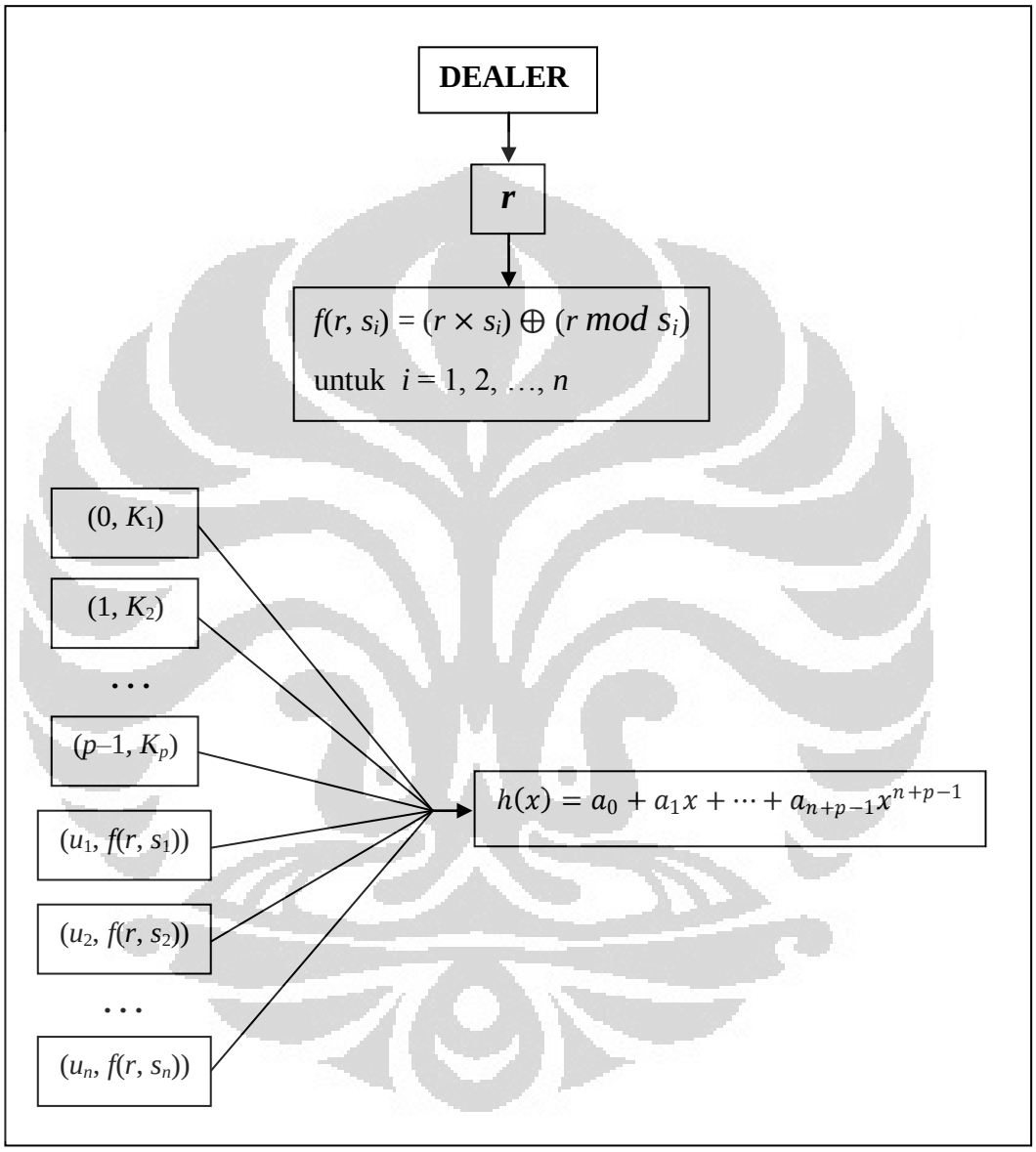
Dealer melakukan langkah-langkah berikut untuk membagikan sejumlah *p* rahasia kepada *n* partisipan:

a. Pilih secara acak bilangan bulat *r* dan hitung *pseudo-shares* $f(r, s_i) = (r \times s_i) \oplus (r \bmod s_i)$, i = 1, 2, …, *n*.

b. Gunakan $(n + p)$ pasangan dari $(u_i, f(r, s_i))$, $i = 1, 2, \ldots, n$; dan $(0, K_1)$, $(1, K_2)$, …, $(p - 1, K_p)$ untuk mengkonstruksi sebuah polinomial berderajat $n + p - 1$.

$$h(x) = a_0 + a_1 x + \cdots + a_{n+p-1} x^{n+p-1}$$

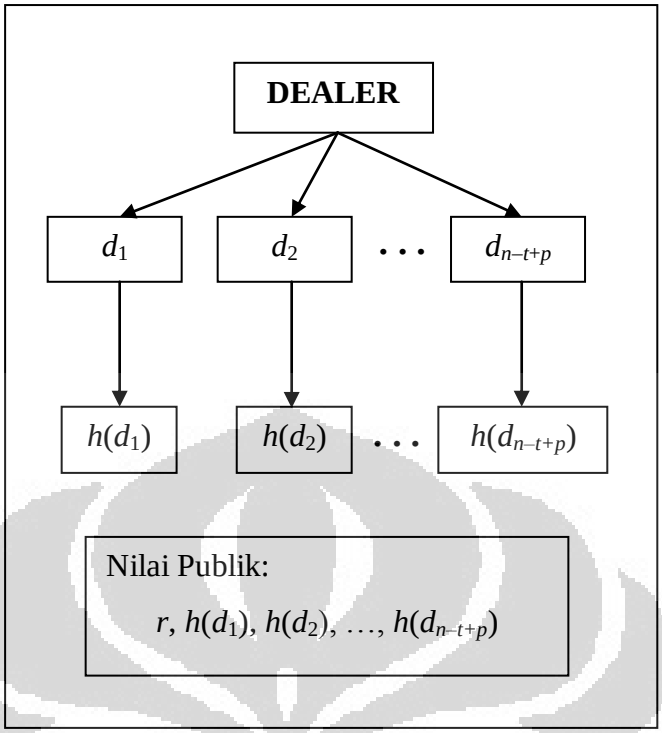
Gambar 3.2 menunjukkan ilustrasi pembentukan polinomial $h(x)$.



Gambar 3.2 Ilustrasi pembentukan polinomial $h(x)$ dalam skema (t, n) *multi-secret sharing*

c. Pilih sebanyak $(n + p - t)$ bilangan bulat $d_1, d_2, \ldots, d_{n+p-t} \in [p, q - 1] \setminus \{u_i \mid i = 1, 2, \ldots, n\}$ dan hitung $h(d_i)$, $i = 1, 2, \ldots, n + p - t$.

d. Publikasikan nilai-nilai dari $(r, h(d_1), h(d_2), \ldots, h(d_{n+p-t}))$.



Gambar 3.3 Nilai publik dalam skema (*t, n*) *multi-secret sharing*

Setelah diperoleh nilai publik $r, h(d_1), h(d_2), \ldots, h(d_{n+p-t})$, maka sebanyak p rahasia $K_1, K_2, \ldots, K_p$ telah disembunyikan dalam polinomial $h(x)$ dan dibagikan kepada setiap partisipan dalam bentuk nilai-nilai publik yaitu $r, h(d_1), h(d_2), \ldots, h(d_{n+p-t})$.

3.2.3 Rekonstruksi Rahasia dalam Skema (*t, n*) *Multi-Secret Sharing*

Untuk merekonstruksi rahasia, dibutuhkan sebanyak t partisipan dari n partisipan. Setiap partisipan dapat menghitung *pseudo-shares* $f(r, s_i)$, $i = 1, 2, \ldots, n$ dengan menggunakan nilai publik r dan *secret share* s_i dari masing-masing partisipan. Langkah-langkah untuk merekonstruksi rahasia adalah sebagai berikut:

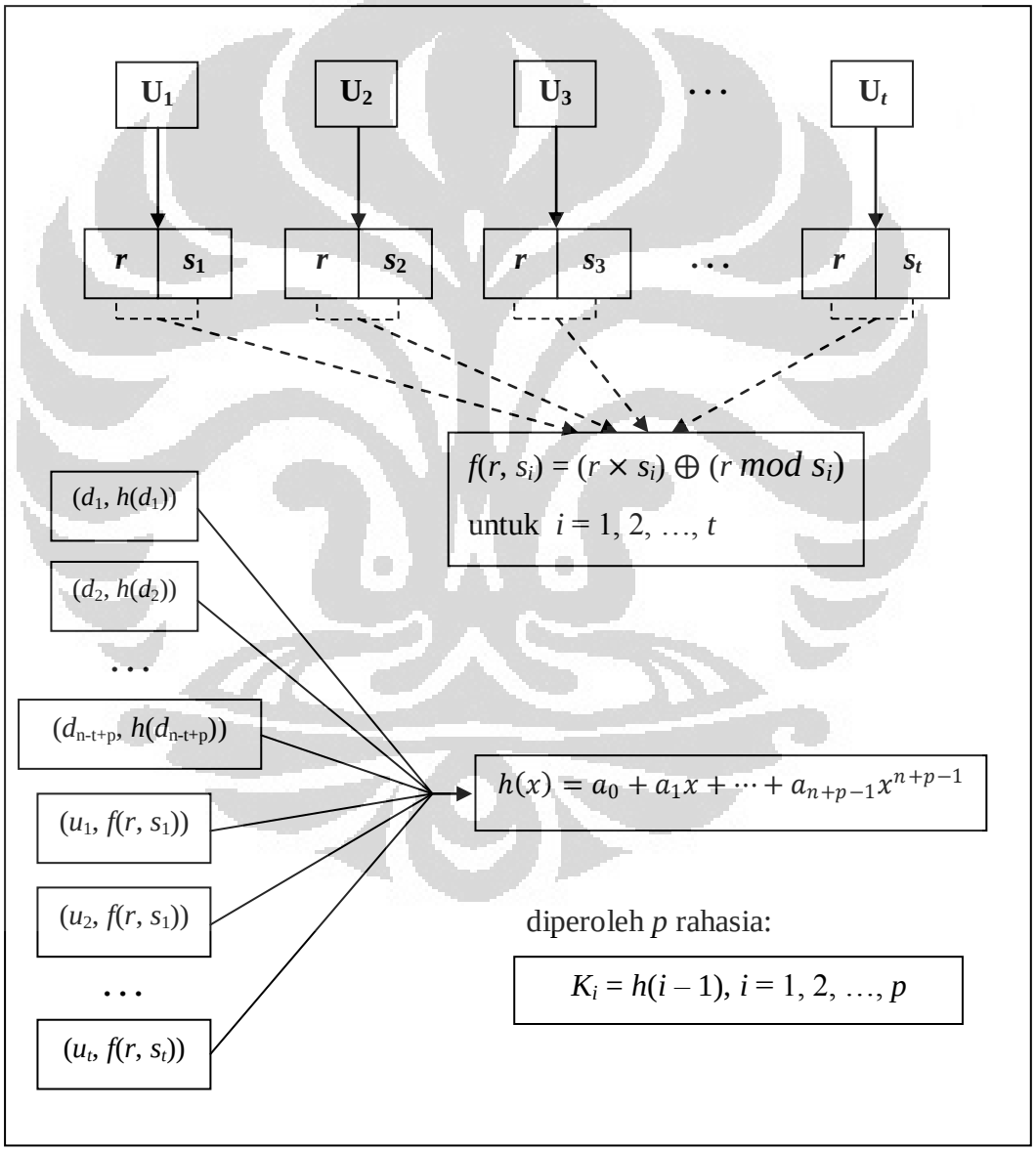
a. Sebanyak t partisipan memberikan *pseudo-shares* mereka yaitu $f(r, s_{i_j})$ untuk $j = 1, 2, \ldots, t$, maka akan diperoleh t pasangan $(u_i, f(r, s_{i_j}))$ untuk $j = 1, 2, \ldots, t$.

b. Dengan diketahuinya nilai publik dari $h(d_i)$, $i = 1, 2, \ldots, n + p - t$, maka akan diperoleh $n + p - t$ pasangan $(d_i, h(d_i))$, $i = 1, 2, \ldots, n + p - t$.

c. Gabungkan pasangan titik-titik $(u_i, f(r, s_{ij}))$, $j = 1, 2, \ldots, t$ dan $(d_i, h(d_i))$, $i = 1, 2, \ldots, n + p - t$ sehingga diperoleh $(n + p)$ titik untuk mengkonstruksi polinomial berderajat $n + p - 1$. Dalam hal ini, polinomial yang diperoleh adalah $h(x)$ yang ditentukan menggunakan interpolasi Lagrange.

d. Hitung p rahasia $K_1, K_2, \ldots, K_p$ dengan menggunakan formula berikut:

$$K_i = h(i - 1),\ i = 1, 2, \ldots, p.$$



Gambar 3.4 Ilustrasi rekonstruksi rahasia dalam skema (t, n) *multi-secret sharing*

Contoh 3.3

Misalkan akan digunakan skema (2, 3) *multi-secret sharing* dengan rahasia sejumlah 3 yaitu $K_1 = 12$, $K_2 = 17$, dan $K_3 = 32$. Dalam hal ini, banyaknya partisipan adalah $n = 3$ dan banyaknya partisipan yang dapat merekonstruksi rahasia adalah $t = 2$.

Berikut ini diberikan proses skema (t, n) *multi-secret sharing* dengan t, n, K_1, K_2, dan K_3 di atas.

- Pilih bilangan prima $q = 53$ dan $r = 3$.
- Untuk $i = 1, 2, 3$, identitas publik dan *secret-shares* dari partisipan yaitu:

  $u_1 = 3$, $u_2 = 4$, $u_3 = 5$;

  $s_1 = 8$, $s_2 = 11$, $s_3 = 5$; $s_1, s_2, s_3 \in GF(q)$
- Hitung *pseudo-share* $f(r, s_i)$, $i = 1, 2, 3$.

  Dengan menggunakan fungsi *hash* satu arah dua variabel $f(r, s) = (r \times s) \oplus (r \bmod s)$, diperoleh *pseudo-share* untuk partisipan ke-i, $i = 1, 2, 3$.

  $f(r, s_1) = (3 \times 8) \oplus (3 \bmod 8) = 27$

  $f(r, s_2) = (3 \times 11) \oplus (3 \bmod 11) = 34$

  $f(r, s_3) = (3 \times 5) \oplus (3 \bmod 5) = 12$
- Bentuk polinomial dari titik-titik $(u_1, f(r, s_1))$, $(u_2, f(r, s_2))$, $(u_3, f(r, s_3))$, $(0, K_1)$, $(1, K_2)$, dan $(2, K_3)$. Dari 6 titik akan diperoleh polinomial derajat 5.

  $$h(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5$$

  Himpunan titik-titik $(x_i, h(x_i))$ diketahui yaitu:

  $(x_1, h(x_1)) = (3, 27)$;

  $(x_2, h(x_2)) = (4, 34)$;

  $(x_3, h(x_3)) = (5, 12)$;

  $(x_4, h(x_4)) = (0, 12)$;

  $(x_5, h(x_5)) = (1, 17)$;

  $(x_6, h(x_6)) = (2, 32)$.

  Berdasarkan 6 titik di atas, akan dikonstruksi polinomial $h(x)$ dengan menggunakan interpolasi Lagrange dimana seluruh perhitungan dilakukan dalam $GF(53)$.

$$h(x) = h(x_1)\left(\frac{x-x_2}{x_1-x_2}\right)\left(\frac{x-x_3}{x_1-x_3}\right)\left(\frac{x-x_4}{x_1-x_4}\right)\left(\frac{x-x_5}{x_1-x_5}\right)\left(\frac{x-x_6}{x_1-x_6}\right)$$
$$+ h(x_2)\left(\frac{x-x_1}{x_2-x_1}\right)\left(\frac{x-x_3}{x_2-x_3}\right)\left(\frac{x-x_4}{x_2-x_4}\right)\left(\frac{x-x_5}{x_2-x_5}\right)\left(\frac{x-x_6}{x_2-x_6}\right)$$
$$+ h(x_3)\left(\frac{x-x_1}{x_3-x_1}\right)\left(\frac{x-x_2}{x_3-x_2}\right)\left(\frac{x-x_4}{x_3-x_4}\right)\left(\frac{x-x_5}{x_3-x_5}\right)\left(\frac{x-x_6}{x_3-x_6}\right)$$
$$+ h(x_4)\left(\frac{x-x_1}{x_4-x_1}\right)\left(\frac{x-x_2}{x_4-x_2}\right)\left(\frac{x-x_3}{x_4-x_3}\right)\left(\frac{x-x_5}{x_4-x_5}\right)\left(\frac{x-x_6}{x_4-x_6}\right)$$
$$+ h(x_5)\left(\frac{x-x_1}{x_5-x_1}\right)\left(\frac{x-x_2}{x_5-x_2}\right)\left(\frac{x-x_3}{x_5-x_3}\right)\left(\frac{x-x_4}{x_5-x_4}\right)\left(\frac{x-x_6}{x_5-x_6}\right)$$
$$+ h(x_6)\left(\frac{x-x_1}{x_6-x_1}\right)\left(\frac{x-x_2}{x_6-x_2}\right)\left(\frac{x-x_3}{x_6-x_3}\right)\left(\frac{x-x_4}{x_6-x_4}\right)\left(\frac{x-x_5}{x_6-x_5}\right)$$
$$= 27\left(\frac{x-4}{3-4}\right)\left(\frac{x-12}{3-12}\right)\left(\frac{x-0}{3-0}\right)\left(\frac{x-1}{3-1}\right)\left(\frac{x-2}{3-2}\right)$$
$$+ 34\left(\frac{x-3}{4-3}\right)\left(\frac{x-5}{4-5}\right)\left(\frac{x-0}{4-0}\right)\left(\frac{x-1}{4-1}\right)\left(\frac{x-2}{4-2}\right)$$
$$+ 12\left(\frac{x-3}{5-3}\right)\left(\frac{x-4}{5-4}\right)\left(\frac{x-0}{5-0}\right)\left(\frac{x-1}{5-1}\right)\left(\frac{x-2}{5-2}\right)$$
$$+ 12\left(\frac{x-3}{0-3}\right)\left(\frac{x-4}{0-4}\right)\left(\frac{x-5}{0-5}\right)\left(\frac{x-1}{0-1}\right)\left(\frac{x-2}{0-2}\right)$$
$$+ 17\left(\frac{x-3}{1-3}\right)\left(\frac{x-4}{1-4}\right)\left(\frac{x-5}{1-5}\right)\left(\frac{x-0}{1-0}\right)\left(\frac{x-2}{1-2}\right)$$
$$+ 32\left(\frac{x-3}{2-3}\right)\left(\frac{x-4}{2-4}\right)\left(\frac{x-5}{2-5}\right)\left(\frac{x-0}{2-0}\right)\left(\frac{x-1}{2-1}\right)$$
$$= 12 + 27x + 34x^2 + 13x^3 + 5x^4 + 32x^5$$

- Pilih ($n + p - t$) bilangan bulat (dalam contoh ini, $n = 3$, $p = 3$, $t = 2$) yaitu d_1, $d_2, \ldots, d_{n+p-t} \in [p, q-1] \setminus \{u_i \mid i = 1, 2, 3\}$, yaitu:
  $d_1 = 6$, $d_2 = 7$, $d_3 = 8$, dan $d_4 = 9$.
- Hitung $h(d_i)$, $i = 1, 2, \ldots, 4$ dalam $GF(q)$, yaitu:

$$h(6) = 12 + 27 \times 6 + 34 \times 6^2 + 13 \times 6^3 + 5 \times 6^4 + 32 \times 6^5 = 30$$
$$h(7) = 12 + 27 \times 7 + 34 \times 7^2 + 13 \times 7^3 + 5 \times 7^4 + 32 \times 7^5 = 26$$
$$h(8) = 12 + 27 \times 8 + 34 \times 8^2 + 13 \times 8^3 + 5 \times 8^4 + 32 \times 8^5 = 43$$
$$h(9) = 12 + 27 \times 9 + 34 \times 9^2 + 13 \times 9^3 + 5 \times 9^4 + 32 \times 9^5 = 41$$

- Publikasikan nilai-nilai berikut:

  $r = 3$;

  $(d_1, h(d_1)) = (6, 30)$;

  $(d_2, h(d_2)) = (7, 26)$;

  $(d_3, h(d_3)) = (8, 43)$;

  $(d_4, h(d_4)) = (9, 41)$.

Untuk merekonstruksi rahasia K_1, K_2, dan K_3, dibutuhkan minimal 2 partisipan. Misalkan partisipan 1 dan partisipan 3 akan merekonstruksi K_1, K_2, dan K_3. Langkah-langkah yang dilakukan yaitu:

- Partisipan 1 dan partisipan 2 menghitung *pseudo-share* menggunakan nilai public *r* dan *secret share* masing-masing, yaitu:

  $f(r, s_1) = (3 \times 8) \oplus (3 \; mod \; 8) = 27$

  $f(r, s_3) = (3 \times 5) \oplus (3 \; mod \; 5) = 12$

  Maka diperoleh pasangan titik $(u_1, f(r, s_1))$ dan $(u_3, f(r, s_3))$ yaitu (3, 27) dan (5, 12).

- Gabungkan titik-titik $(d_i, h(d_i))$, $i = 1, 2, \ldots, 4$ yang merupakan nilai publik serta titik $(u_1, f(r, s_1))$ dan $(u_3, f(r, s_3))$ sehingga diperoleh sebanyak 6 titik untuk membentuk polinomial $h(x)$ berderajat 5.

  $$h(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5$$

  Himpunan titik-titik $(x_i, h(x_i))$ diketahui yaitu:

  $(x_1, h(x_1)) = (6, 30)$;

  $(x_2, h(x_2)) = (7, 26)$;

  $(x_3, h(x_3)) = (8, 43)$;

  $(x_4, h(x_4)) = (9, 41)$;

  $(x_5, h(x_5)) = (3, 27)$;

  $(x_6, h(x_6)) = (5, 12)$.

  Berdasarkan 6 titik di atas, akan dikonstruksi polinomial $h(x)$ dengan menggunakan interpolasi Lagrange dimana seluruh perhitungan dilakukan dalam $GF(53)$.

$$h(x) = h(x_1)\left(\frac{x-x_2}{x_1-x_2}\right)\left(\frac{x-x_3}{x_1-x_3}\right)\left(\frac{x-x_4}{x_1-x_4}\right)\left(\frac{x-x_5}{x_1-x_5}\right)\left(\frac{x-x_6}{x_1-x_6}\right)$$
$$+ h(x_2)\left(\frac{x-x_1}{x_2-x_1}\right)\left(\frac{x-x_3}{x_2-x_3}\right)\left(\frac{x-x_4}{x_2-x_4}\right)\left(\frac{x-x_5}{x_2-x_5}\right)\left(\frac{x-x_6}{x_2-x_6}\right)$$
$$+ h(x_3)\left(\frac{x-x_1}{x_3-x_1}\right)\left(\frac{x-x_2}{x_3-x_2}\right)\left(\frac{x-x_4}{x_3-x_4}\right)\left(\frac{x-x_5}{x_3-x_5}\right)\left(\frac{x-x_6}{x_3-x_6}\right)$$
$$+ h(x_4)\left(\frac{x-x_1}{x_4-x_1}\right)\left(\frac{x-x_2}{x_4-x_2}\right)\left(\frac{x-x_3}{x_4-x_3}\right)\left(\frac{x-x_5}{x_4-x_5}\right)\left(\frac{x-x_6}{x_4-x_6}\right)$$
$$+ h(x_5)\left(\frac{x-x_1}{x_5-x_1}\right)\left(\frac{x-x_2}{x_5-x_2}\right)\left(\frac{x-x_3}{x_5-x_3}\right)\left(\frac{x-x_4}{x_5-x_4}\right)\left(\frac{x-x_6}{x_5-x_6}\right)$$
$$+ h(x_6)\left(\frac{x-x_1}{x_6-x_1}\right)\left(\frac{x-x_2}{x_6-x_2}\right)\left(\frac{x-x_3}{x_6-x_3}\right)\left(\frac{x-x_4}{x_6-x_4}\right)\left(\frac{x-x_5}{x_6-x_5}\right)$$
$$= 30\left(\frac{x-7}{6-7}\right)\left(\frac{x-8}{6-8}\right)\left(\frac{x-9}{6-9}\right)\left(\frac{x-3}{6-3}\right)\left(\frac{x-5}{6-5}\right)$$
$$+ 26\left(\frac{x-6}{7-6}\right)\left(\frac{x-8}{7-8}\right)\left(\frac{x-9}{7-9}\right)\left(\frac{x-3}{7-3}\right)\left(\frac{x-5}{7-5}\right)$$
$$+ 43\left(\frac{x-6}{8-6}\right)\left(\frac{x-7}{8-7}\right)\left(\frac{x-9}{8-9}\right)\left(\frac{x-3}{8-3}\right)\left(\frac{x-5}{8-5}\right)$$
$$+ 41\left(\frac{x-6}{9-6}\right)\left(\frac{x-7}{9-7}\right)\left(\frac{x-8}{9-8}\right)\left(\frac{x-3}{9-3}\right)\left(\frac{x-5}{9-5}\right)$$
$$+ 27\left(\frac{x-6}{3-6}\right)\left(\frac{x-7}{3-7}\right)\left(\frac{x-8}{3-8}\right)\left(\frac{x-9}{3-9}\right)\left(\frac{x-5}{3-5}\right)$$
$$+ 12\left(\frac{x-6}{5-6}\right)\left(\frac{x-7}{5-7}\right)\left(\frac{x-8}{5-8}\right)\left(\frac{x-9}{5-9}\right)\left(\frac{x-3}{5-3}\right)$$
$$= 12 + 27x + 34x^2 + 13x^3 + 5x^4 + 32x^5$$

- Maka K_1, K_2, K_3 dapat diperoleh yaitu:

$K_1 = h(0)$

$= 12 + 27 \times 0 + 34 \times 0^2 + 13 \times 0^3 + 5 \times 0^4 + 32 \times 0^5$

$= 12 \in GF(53)$

$K_2 = h(1)$

$= 12 + 27 \times 1 + 34 \times 1^2 + 13 \times 1^3 + 5 \times 1^4 + 32 \times 1^5$

$= 123$

$\equiv 17 \in GF(53)$

$$K_3 = h(2)$$
$$= 12 + 27 \times 2 + 34 \times 2^2 + 13 \times 2^3 + 5 \times 2^4 + 32 \times 2^5$$
$$= 1410$$
$$\equiv 32 \in GF(53)$$

3.3 Skema *Secret Image Sharing*

Skema *secret image sharing* yang dibahas dalam bab ini merupakan suatu skema *secret sharing* dimana rahasia yang disembunyikan adalah berupa citra digital (dalam hal ini citra digital berupa citra *grayscale*) yang akan dibagikan kepada n partisipan dan sejumlah t partisipan ($t \leq n$) dapat mengkonstruksi citra digital yang disembunyikan. Skema ini dikembangkan oleh Alexandrova, dkk. pada tahun 2010 dengan berdasarkan kepada skema (t, n) *multi-secret sharing* (Pang, L. J. & Wang, Y. M., 2005).

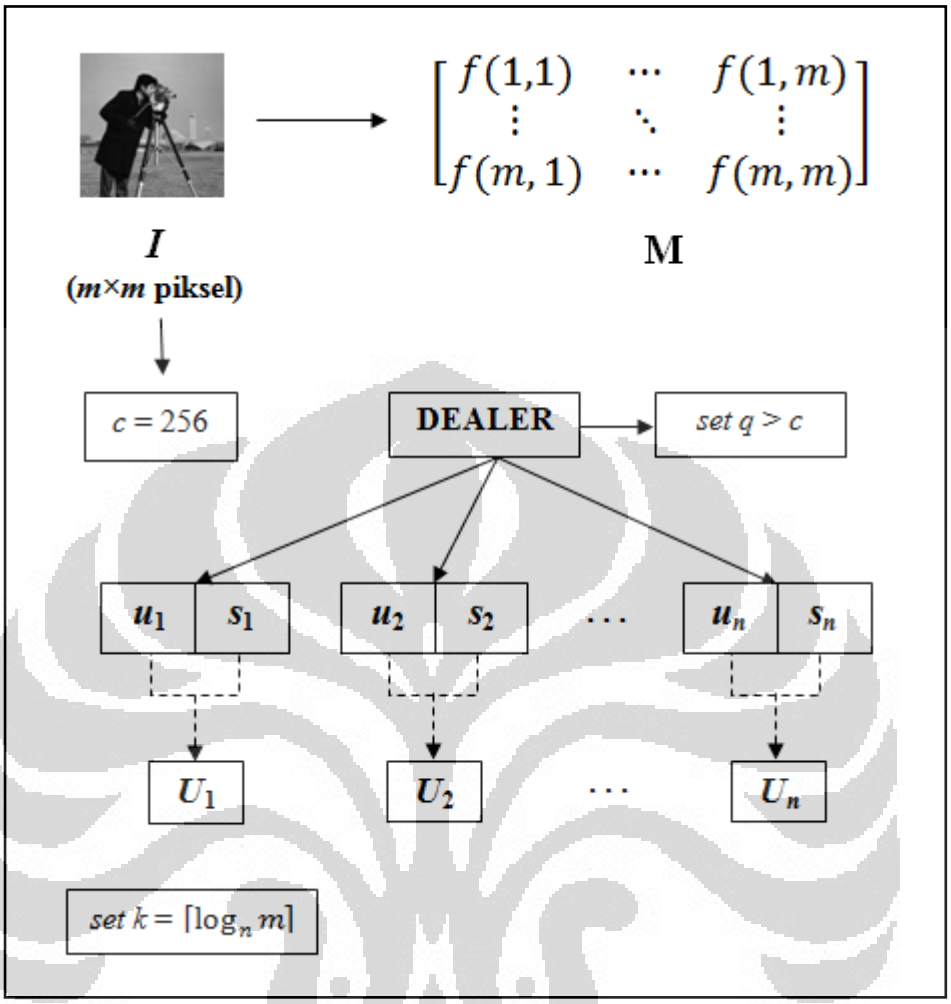
Skema *secret image sharing* dideskripsikan menjadi 3 langkah, yaitu langkah awal, pembagian citra rahasia, dan rekonstruksi citra rahasia.

3.3.1 Langkah Awal

Misalkan I merupakan citra yang akan disembunyikan dengan ukuran $m \times m$ piksel dan M adalah matriks berukuran $m \times m$ yang merepresentasikan citra I. Definisikan $k = \lceil \log_n m \rceil$. *Dealer* memilih bilangan prima $q > c$ dimana c merupakan jumlah intensitas kecerahan pada citra I, dimana pada citra *grayscale*, nilai c adalah 256, yaitu jumlah intensitas kecerahan pada citra *grayscale* (0-255). *Dealer* memilih n buah bilangan bulat berbeda $s_1, s_2, \ldots, s_n \in GF(q)$.

Bilangan $s_1, s_2, \ldots, s_n$ merupakan *secret share* masing-masing partisipan dan diberikan kepada masing-masing partisipan.

Dealer memilih n bilangan bulat berbeda $u_1, u_2, \ldots, u_n \in [n - t + 1, q - 1]$ sebagai identitas publik dari masing-masing partisipan.



Gambar 3.5 Ilustrasi langkah awal skema *secret image sharing*

3.3.2 Pembagian Citra Rahasia

Dealer melakukan langkah-langkah berikut yang dilakukan dalam $GF(q)$ untuk membagikan citra rahasia I kepada n partisipan:

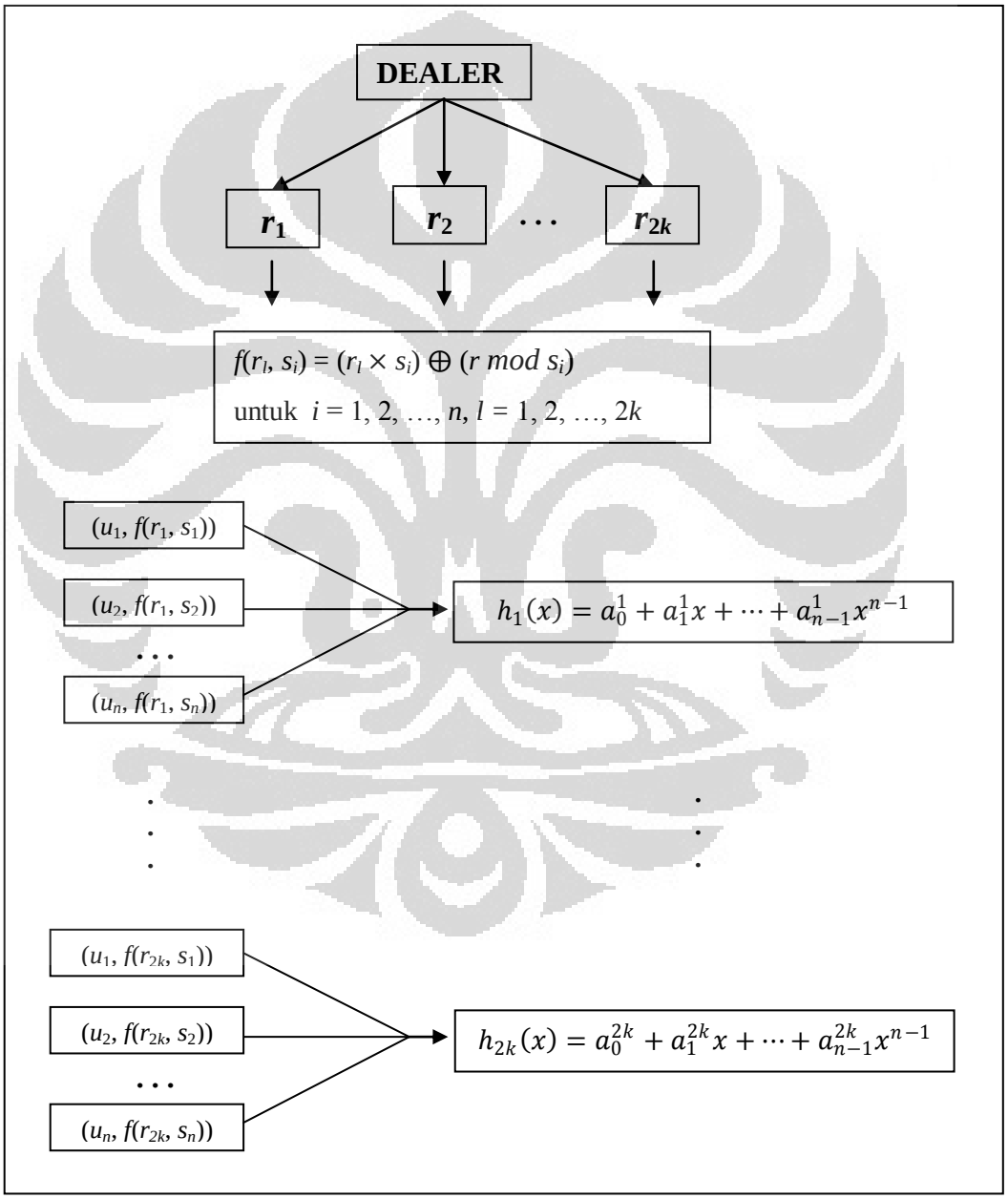
a. Pilih sembarang bilangan bulat $r_1, r_2, \ldots, r_{2k} \in GF(q)$ dan hitung *pseudo-share* dengan menggunakan fungsi *hash* satu arah dua variabel:

$$f(r_1, s_i) = (r_1 \times s_i) \oplus (r_1 \; mod \; s_i), i = 1, \ldots, n,$$
$$f(r_2, s_i) = (r_2 \times s_i) \oplus (r_2 \; mod \; s_i), i = 1, \ldots, n,$$
$$\ldots$$
$$f(r_{2k}, s_i) = (r_{2k} \times s_i) \oplus (r_{2k} \; mod \; s_i), i = 1, \ldots, n,$$

b. Gunakan pasangan dari $(u_i, f(r_1, s_i))$, $(u_i, f(r_2, s_i))$, …, $(u_i, f(r_{2k}, s_i))$, $i = 1$, …, n untuk membentuk $2k$ polinomial berderajat $n - 1$.

$$h_1(x) = a_0^1 + a_1^1 x + \cdots + a_{n-1}^1 x^{n-1},$$
$$h_2(x) = a_0^2 + a_1^2 x + \cdots + a_{n-1}^2 x^{n-1},$$
$$\ldots$$
$$h_{2k}(x) = a_0^{2k} + a_1^{2k} x + \cdots + a_{n-1}^{2k} x^{n-1},$$

dimana $h_l(u_i) = f(r_l, s_i)$, untuk $i = 1, \ldots, n$ dan $l = 1, \ldots, 2k$.



Gambar 3.6 Ilustrasi pembentukan polynomial $h_1(x)$, $h_2(x)$, …, $h_{2k}(x)$ dalam skema *secret image sharing*

c. Hitung z_i^1, z_i^2, …, z_i^{2k} dengan menggunakan polynomial $h_1(x)$, $h_2(x)$, …, $h_{2k}(x)$.

$$z_i^1 = h_1(i), i = 1, 2, \dots, n-t,$$
$$z_i^2 = h_2(i), i = 1, 2, \dots, n-t,$$
$$\dots$$
$$z_i^{2k} = h_{2k}(i), i = 1, 2, \dots, n-t,$$

d. Hitung matriks M' berukuran $n^k \times n^k$ dengan aturan berikut.

Untuk $k = 1$ dan $1 \le i, j \le n$,

$$m'_{i,j} = \left(a_{i-1}^1 + a_{j-1}^2\right) mod\ c,$$

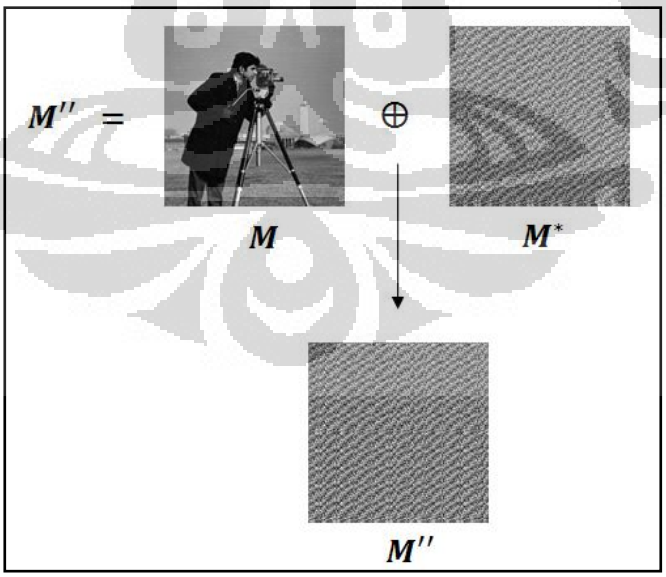
dan untuk $k > 1$, dan $1 \le i, j \le n^k$,

$$m'_{i,j} = \left(\sum_{r=1}^{k-1} a^r_{\left(\left\lfloor \frac{i}{n^{k-r}} \right\rfloor\right) mod\ n} + \sum_{r=k+1}^{2k-1} a^r_{\left(\left\lfloor \frac{j}{n^{2k-r}} \right\rfloor\right) mod\ n} + a^k_{((i-1)\ mod\ n)} + a^{2k}_{((j-1)\ mod\ n)}\right) mod\ c$$

e. Hitung matriks M'' berukuran $m \times m$ sebagai berikut:

$$M'' = M \oplus M^*,$$

dimana M^* adalah matriks berukuran $m \times m$ dengan $m^*_{i,j} = m'_{i,j}$, untuk $1 \le i, j \le m$.



Gambar 3.7 Ilustrasi perolehan citra publik M''

f. Publikasikan nilai-nilai dari $(r_1, z_1^1, z_2^1, \dots, z_{n-t}^1)$, $(r_2, z_1^2, z_2^2, \dots, z_{n-t}^2)$, …, $(r_{2k}, z_1^{2k}, z_2^{2k}, \dots, z_{n-t}^{2k})$ dan citra publik M''.

3.3.3 Rekonstruksi Citra Rahasia

Untuk merekonstruksi citra *I*, dibutuhkan sebanyak *t* partisipan dari *n* partisipan. Langkah-langkah bagi *t* partisipan untuk merekonstruksi citra I adalah sebagai berikut:

a. Setiap partisipan menghitung *pseudo-shares* $f(r_1, s_{i_j})$, $f(r_2, s_{i_j})$, …, $f(r_{2k}, s_{i_j})$ untuk $j = 1, 2, \ldots, t$ dengan menggunakan nilai publik $r_1, r_2, \ldots, r_{2k}$ dan *secret share* s_{i_j} dari masing-masing partisipan.

b. .Setelah *t* partisipan memberikan *pseudo-share* mereka yaitu $f(r_1, s_{i_j})$, $f(r_2, s_{i_j})$, …, $f(r_{2k}, s_{i_j})$ untuk $j = 1, 2, \ldots, t$, maka akan diperoleh himpunan *t* pasangan $(u_{i_j}, f(r_1, s_{i_j}))$; $(u_{i_j}, f(r_2, s_{i_j}))$; …; $(u_{i_j}, f(r_{2k}, s_{i_j}))$.

c. Dengan diketahui nilai publik dari $z_i^1, z_i^2, \ldots, z_i^{2k}$, untuk $i = 1, 2, \ldots, n - t$, maka akan diperoleh $(n - t)$ pasangan $(i, z_i^1); (i, z_i^2); \ldots; (i, z_i^{2k})$.

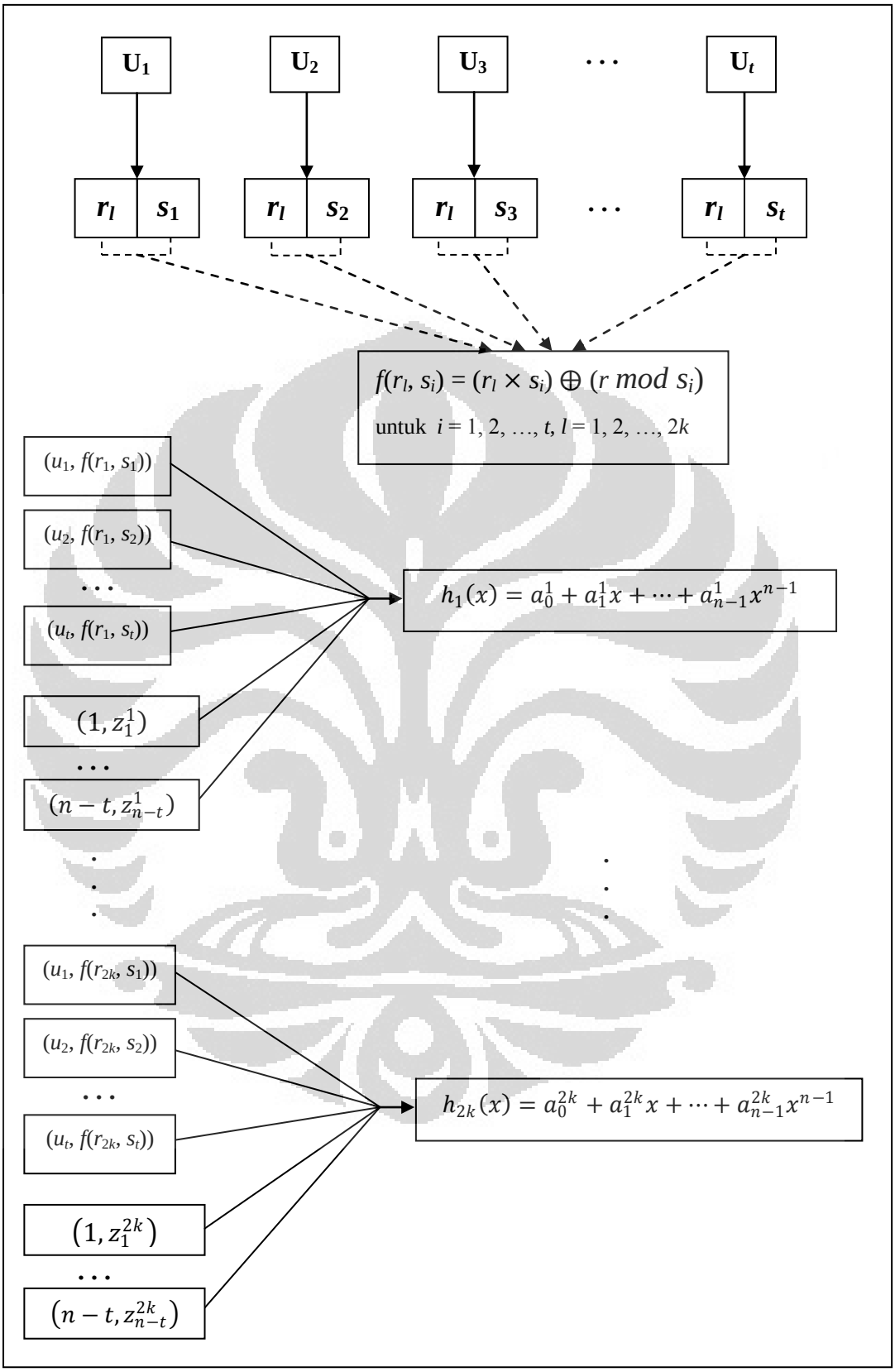
d. Gabungkan pasangan titik-titik yang telah diperoleh untuk membentuk $2k$ polynomial berderajat $n - 1$.

   Pasangan titik-titik $(u_{i_1}, f(r_1, s_{i_1}))$, $(u_{i_2}, f(r_1, s_{i_2}))$, …, $(u_{i_t}, f(r_1, s_{i_t}))$, $(1, z_1^1)$, $(2, z_2^1)$, …, $(n - t, z_{n-t}^1)$ membentuk $h_1(x)$.

   Pasangan titik-titik $(u_{i_1}, f(r_2, s_{i_1}))$, $(u_{i_2}, f(r_2, s_{i_2}))$, …, $(u_{i_t}, f(r_2, s_{i_t}))$, $(1, z_1^2)$, $(2, z_2^2)$, …, $(n - t, z_{n-t}^2)$ membentuk $h_2(x)$.

   …

   Pasangan titik-titik $(u_{i_1}, f(r_{2k}, s_{i_1}))$, $(u_{i_2}, f(r_{2k}, s_{i_2}))$, …, $(u_{i_t}, f(r_{2k}, s_{i_t}))$, $(1, z_1^{2k})$, $(2, z_2^{2k})$, …, $(n - t, z_{n-t}^{2k})$ membentuk $h_{2k}(x)$.



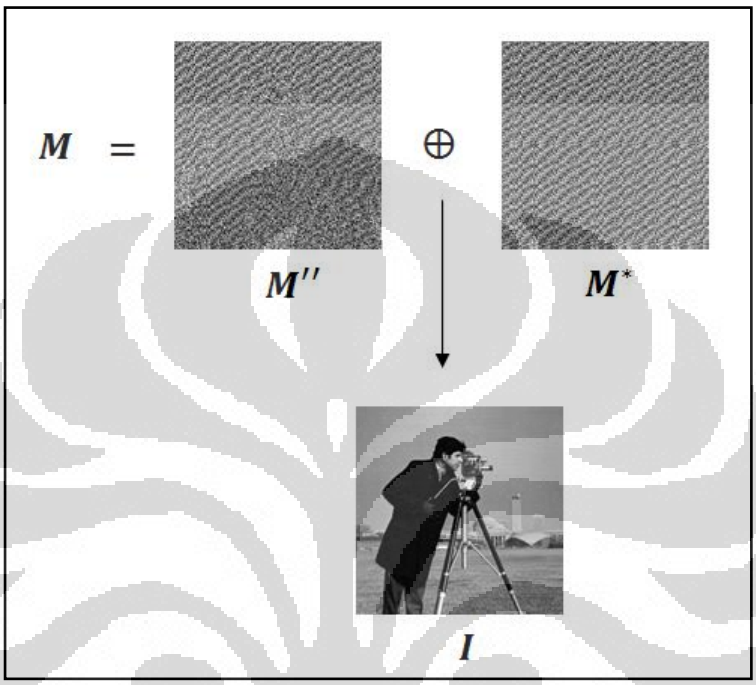
Gambar 3.8 Ilustrasi pembentukan polinomial oleh *t* partisipan

e. Bentuk matriks M' berdasarkan poin 2d.

f. Hitung matriks M berukuran $m \times m$ sebagai berikut:

$$M = M'' \oplus M^*$$

g. Citra rahasia *I* akan diperoleh berdasarkan matriks *M* dengan ukuran $m \times m$.



Gambar 3.9 Ilustrasi perolehan citra awal *I*

Pada Bab berikutnya akan diberikan hasil implementasi dari skema *secret image sharing* menggunakan fungsi *hash* satu arah dua variabel yang telah diberikan pada Bab ini.

BAB 4
IMPLEMENTASI DAN HASIL

Pada Bab sebelumnya telah dibahas skema *secret sharing* dengan rahasia berupa citra digital. Pada Bab ini, skema tersebut akan diimplementasikan ke dalam program dengan perangkat lunak MATLAB versi 7.11.0.584 (R2010b), pada komputer dengan spesifikasi sebagai berikut:

Processor : Intel® Core™ i5 CPU M460 @2.53 GHz
Memory : 4.00 GB (2.99 GB *usable*)
OS : Windows 7 Professional SP1 x86 (32bit)
HD Free Space : ± 100 GB

Skema yang akan diimplementasikan adalah skema *secret image sharing* menggunakan fungsi *hash* satu arah dua variabel.

4.1 Implementasi untuk Citra *Grayscale* Berukuran 256×256 Piksel

Dengan menggunakan program yang telah dibuat, akan diimplementasikan skema *secret image sharing* menggunakan fungsi *hash* satu arah dua variabel dengan rahasia citra *grayscale* pada Gambar 4.1 dengan ukuran 256×256 piksel.

Gambar 4.1 Citra *grayscale* 256×256 piksel

4.1.1 Pembagian Citra *Grayscale* kepada *n* Partisipan

Untuk citra yang dirahasiakan (yaitu pada Gambar 4.1), misalkan akan dibagikan kepada 10 orang partisipan, dengan jumlah partisipan yang dapat merekonstruksi citra awal (yaitu pada Gambar 4.1) yaitu sebanyak 5 partisipan.

Dengan menjalankan program yang telah dibuat, dengan memasukkan *input* berupa citra *grayscale* pada Gambar 4.1, *n* (banyaknya partisipan) = 10, dan *t* (banyaknya partisipan yang dapat merekonstruksi citra awal) = 5, akan diperoleh *output* yaitu sebagai berikut:

- Identitas publik dari masing-masing partisipan yaitu:

  $u_1 = 6$;
  $u_2 = 7$;
  $u_3 = 8$;
  $u_4 = 9$;
  $u_5 = 10$;
  $u_6 = 11$;
  $u_7 = 12$;
  $u_8 = 13$;
  $u_9 = 14$;
  $u_{10} = 15$.

- *Secret share* yang dimiliki oleh masing-masing partisipan yaitu:

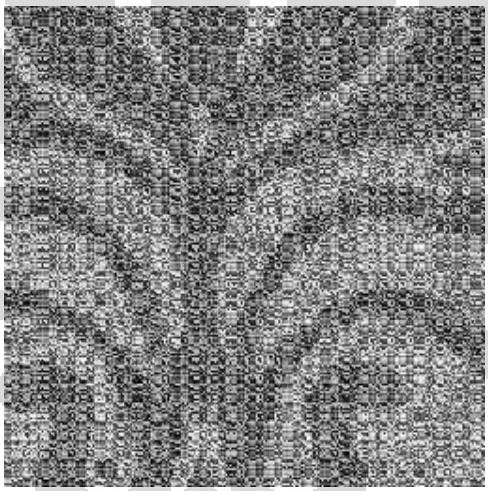
  $s_1 = 122$;
  $s_2 = 98$;
  $s_3 = 173$;
  $s_4 = 243$;
  $s_5 = 31$;
  $s_6 = 39$;
  $s_7 = 21$;
  $s_8 = 174$;
  $s_9 = 33$;
  $s_{10} = 151$;

- Nilai-nilai yang akan dipublikasikan yaitu:

Tabel 4.1 Nilai-nilai publik

$r_1 = 194$	$r_2 = 190$	$r_3 = 75$	$r_4 = 138$	$r_5 = 36$	$r_6 = 23$
$z_1^1 = 92$	$z_1^2 = 96$	$z_1^3 = 244$	$z_1^4 = 3$	$z_1^5 = 209$	$z_1^6 = 250$
$z_2^1 = 84$	$z_2^2 = 88$	$z_2^3 = 125$	$z_2^4 = 73$	$z_2^5 = 199$	$z_2^6 = 245$
$z_3^1 = 61$	$z_3^2 = 65$	$z_3^3 = 246$	$z_3^4 = 177$	$z_3^5 = 137$	$z_3^6 = 64$
$z_4^1 = 19$	$z_4^2 = 23$	$z_4^3 = 17$	$z_4^4 = 255$	$z_4^5 = 149$	$z_4^6 = 72$
$z_5^1 = 33$	$z_5^2 = 37$	$z_5^3 = 157$	$z_5^4 = 256$	$z_5^5 = 87$	$z_5^6 = 182$

Selain nilai-nilai publik yang ada pada Tabel 4.1, terdapat pula *output* berupa citra *grayscale* berukuran 256×256 piksel yang dipublikasikan.



Gambar 4.2 Citra publik *grayscale* 256×256

Jadi, hasil pembagian citra *grayscale* berukuran 256×256 pada Gambar 4.1 yaitu citra publik pada Gambar 4.2 serta nilai-nilai publik yang ada pada Tabel 4.1.

4.1.2 Rekonstruksi Citra *Grayscale* oleh *t* Partisipan

Sebelumnya telah ditentukan, untuk merekonstruksi citra *grayscale* pada Gambar 4.1, dibutuhkan sebanyak 5 partisipan. Misalkan partisipan yang akan merekonstruksi adalah partisipan 1, partisipan 2, partisipan 5, partisipan 7, dan partisipan 10.

Dengan menjalankan program yang telah dibuat, dengan memasukkan *input* yaitu citra publik *grayscale* pada Gambar 4.2 dan nilai-nilai publik yang ada pada Tabel 4.1 serta dengan memasukkan *secret share* dari partisipan yang akan merekonstruksi citra *grayscale* pada Gambar 4.1, maka akan diperoleh *output* yaitu citra *grayscale* berukuran 256×256 yang terlihat pada Gambar 4.3.

Gambar 4.3 Citra *grayscale* hasil rekonstruksi

BAB 5
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Kesimpulan yang diperoleh dari tugas akhir ini antara lain:

- Suatu rahasia berupa citra digital dapat dijaga keamanannya dengan menggunakan skema *secret image sharing* menggunakan fungsi *hash* satu arah dua variabel.
- Skema *secret image sharing* menggunakan fungsi *hash* satu arah dua variabel akan menghasilkan satu citra publik serta nilai-nilai publik berupa bilangan bulat. Untuk merekonstruksi citra awal, dibutuhkan sebanyak minimal *t* partisipan untuk memberikan *secret share* masing-masing yang kemudian digunakan untuk merekonstruksi citra awal.
- Fungsi *hash* satu arah dua variabel yang digunakan dalam skema *secret image sharing* dalam tugas akhir ini bertujuan untuk mengamankan *secret share* dari masing-masing partisipan agar tidak diketahui oleh orang lain.
- Dengan menggunakan perangkat lunak Matlab, berhasil dilakukan implementasi skema *secret image sharing* menggunakan fungsi *hash* satu arah dua variabel kepada *n* partisipan dengan hasil pembagian berupa nilai-nilai publik berupa bilangan bulat serta satu buah citra publik yang isinya tidak diketahui. Untuk merekonstruksi citra digital awal, sebanyak *t* partisipan memasukkan *secret share* masing-masing yang nilainya akan diproses dengan nilai publik $r_1, \ldots, r_{2k}$ menggunakan fungsi *hash* satu arah dua variabel. Kemudian hasilnya akan digunakan untuk digabungkan dengan nilai-nilai publik lainnya untuk merekonstruksi citra digital awal.

5.2 Saran

Saran untuk pengembangan tugas akhir ini:

- Dalam tugas akhir ini hanya dibahas mengenai skema *secret image sharing* menggunakan fungsi *hash* satu arah dua variabel dengan citra yang dirahasiakan berupa citra digital *grayscale*. Oleh karena itu skema tersebut dapat dikembangkan untuk citra berwarna.
- Fungsi *hash* satu arah dua variabel yang penulis gunakan dalam tugas akhir ini adalah $f(r, s) = (r \times s) \oplus (r \bmod s)$. Fungsi *hash* satu arah dua variabel yang digunakan dapat memiliki bentuk-bentuk lain. Oleh karena itu skema *secret image sharing* menggunakan fungsi *hash* satu arah dua variabel yang dibahas dalam tugas akhir ini dapat dikembangkan dengan menggunakan bentuk fungsi *hash* satu arah dua variabel yang berbeda.

DAFTAR PUSTAKA

Alexandrova, T., Suzuki, Y., Okubo, K., & Tagawa, N. (2010). Secret Images Sharing Scheme Using Two-Variable One-Way Functions. *IEEE International Conference on Wireless Communications Networking and Information Security (WCNIS)*, (pp. 553-557). Beijing.

C. A. van Tilborg, H. & Jajodia, S. (2011). *Encyclopedia of Cryptography and Security*. New York: Springer.

Gonzales, R. C. & Woods, R. E. (2002). *Digital Images Processing, Second Edition*. New Jersey: Prenyice Hall.

Pang, L. J. & Wang, Y. M. (2005). A New Multi-Secret Sharing Scheme Based on Shamir's Secret Sharing. *Applied Mathematics and Computation*, 167, 840-848.

Rosen, K. H. (2007). *Discrete Mathematics and Its Application, Sixth Edition*. New York: McGraw-Hill.

Sachs, J. (1996). *Digital Image Basics*. 18 April 2012. <http://*www.dl-c.com/basics.pdf*>.

Scheiner, B. (1996). *Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C*. California: John Wiley & Sons, Inc.

Shamir, A. (1979). How to Share a Secret. *Communication of the ACM 22*, 612-613.

Stallings, William. (2011). *Cryptography and Network Security, Fifth Edition*: *Principle and Practice*. New York: Prentice Hall.

LAMPIRAN

File matlab1.m (Proses pembagian citra awal)

```
clear; clc;
file = input('Nama Gambar: ','s');
img = imread(file);
c=256;
%Periksa input gambar apakah hitam-putih (grayscale) dan berukuran
m x m
[m l]=size(img);
if m==l
    fprintf('Gambar yang anda masukkan berukuran %d x %d
piksel\n',m,l);
    n = input('Masukkan jumlah partisipan: ');
    t = input('Masukkan jumlah partisipan yang dapat
merekonstruksi secret (t<n): ');
    k = ceil(log(m)/log(n));
    q = 257;
    fprintf('\n');

    %Dealer memilih sembarang secret share untuk n partisipan
    rand1=randperm(q);
    for i=1:n
        s(i)=rand1(i)-1;
        fprintf('secret share partisipan ke-%d : %d\n',i,s(i));
    end

    %Dealer memilih identitas publik dari n partisipan
    u(1)=n-t+1;
    temp = 1;
    fprintf('\nu1 = %d\n',u(1));
    for i=2:n
        u(i)=u(1)+temp;
        temp=temp+1;
        fprintf('u%d = %d\n',i,u(i));
    end
    fprintf('\n');

    %Dealer memilih sembarang r1,...,r2k
    rand2=randperm(q);
    for i=1:2*k
        r(i)=rand2(i)-1;
        fprintf('r%d = %d\n',i,r(i));
    end
    fprintf('\n');

    %Dealer menghitung pseudo-share menggunakan fungsi hash satu
arah dua variabel
    %dan konstruksi sebanyak 2k polinomial
    f1=inline('r*s','r','s');
    f2=inline('mod(r,s)','r','s');
    for i=1:2*k
        r(i);
        for j=1:n
```

```
            s(j);

f(i,j)=bitxor(uint8(f1(r(i),s(j))),uint8(f2(r(i),s(j))));
            fprintf('f(%d,%d)=%d\n',i,j,f(i,j));
        end
        f = double(f);
        h(i,:)=lagrp(u,f(i,:),q);

        fprintf('h(%d) = \n',i); disp(h(i,:));

        for j=1:n-t
            z(i,j)=mod(polyval(h(i,:),j),q);
            fprintf('z(%d,%d)=%d\n',i,j,z(i,j));
        end
        fprintf('\n');
    end

    %Hitung matriks M' berukuran n^k x n^k
    if k == 1
        for i=1:n
            for j=1:n
                M(i,j)=mod(h(1,n-i+1)+h(2,n-j+1),c);
            end
        end

    elseif k > 1
        for i=1:n^k
            for j=1:n^k
                tmp1=0;
                for r1=1:k-1
                    z1=h(r1,mod(floor(((n^k)-i)/(n^(k-
r1))),n)+1)+tmp1;
                    tmp1=z1;
                end
                tmp2=0;
                for r2=k+1:2*k-1
                    z2=h(r2,mod(floor(((n^k)-j)/(n^(2*k-
r2))),n)+1)+tmp2;
                    tmp2=z2;
                end
                M(i,j)=mod(tmp1 + tmp2 + h(k,mod(((n^k)-i+1),n)+1)
+ h(2*k,mod(((n^k)-j+1),n)+1),c);
            end
        end
    end

    M1=M(1:m,1:m);

    for i=1:m
        for j=1:m
            M2(i,j)=bitxor(uint8(img(i,j)),uint8(M1(i,j)));
        end
    end

    %Nilai-nilai yang dipublish:
    fprintf('Publikasikan nilai-nilai berikut:\n');
    for i=1:2*k
```

```
        fprintf('\nr%d : %d\n',i,r(i));
        for j=1:n-t
            fprintf('z(%d,%d)=%d\n',i,j,z(i,j));
        end
    end

    imshow(M2);
    imwrite(M2,'lena.bmp','bmp');

else
    fprintf('Gambar yang Anda masukkan tidak berukuran m x m
piksel\n');
end
```

File matlab2.m (Proses perekonstruksian citra awal)

```
clear; clc;
%Sebanyak t partisipan akan merekonstruksi citra I
file = input('Nama Gambar: ','s');
img = imread(file);
[m m]=size(img);
q=257;
c=256;
n=input('Jumlah partisipan awal: ');
t=input('Jumlah partisipan yang akan merekonstruksi secret: ');
fprintf('\n');
k = ceil(log(m)/log(n));

%input nilai-nilai publik
for i=1:2*k
    fprintf('Masukkan nilai r%d = ',i);
    r(i)=input('');
    for j=1:n-t
        fprintf('Masukkan nilai z(%d,%d) = ',i,j);
        z(i,j)=input('');
    end
end
fprintf('\n');

%input identitas publik dan secret share dari t partisipan yang
akan merekonstruksi secret
for i=1:t
    fprintf('Masukkan nilai u%d = ',i);
    u(i)=input(' ');
    fprintf('s(%d) = ',i);
    s(i)=input('');
end
fprintf('\n');

f1=inline('r*s','r','s');
f2=inline('mod(r,s)','r','s');
for i=1:2*k
    r(i);
    for j=1:t
        s(j);
        f(i,j)=bitxor(uint8(f1(r(i),s(j))),uint8(f2(r(i),s(j))));
        fprintf('f(%d,%d)=%d\n',i,j,f(i,j));
```

```
    end
    f = double(f);

    L=[1:n-t];
    for l=1:n-t
        z(i,l);
    end

    N=[u L];
    g(i,:)=[f(i,:) z(i,:)];
    h(i,:)=lagrp(N,g(i,:),q);
    fprintf('h(%d) = \n',i); disp(h(i,:));

    fprintf('\n');
end

%Hitung matriks M' berukuran n^k x n^k
if k == 1
    for i=1:n
        for j=1:n
            M(i,j)=mod(h(1,n-i+1)+h(2,n-j+1),c);
        end
    end

elseif k > 1
    for i=1:n^k
        for j=1:n^k
            tmp1=0;
            for r1=1:k-1
                z1=h(r1,mod(floor(((n^k)-i)/(n^(k-
r1))),n)+1)+tmp1;
                tmp1=z1;
            end
            tmp2=0;
            for r2=k+1:2*k-1
                z2=h(r2,mod(floor(((n^k)-j)/(n^(2*k-
r2))),n)+1)+tmp2;
                tmp2=z2;
            end
            M(i,j)=mod(tmp1 + tmp2 + h(k,mod(((n^k)-i+1),n)+1) +
h(2*k,mod(((n^k)-j+1),n)+1),c);
        end
    end
end

M1=M(1:m,1:m);

for i=1:m
    for j=1:m
        M2(i,j)=bitxor(uint8(img(i,j)),uint8(M1(i,j)));
    end
end

imshow(M2);
imwrite(M2,'lena1.bmp','bmp');
```

File lagrp.m (Fungsi untuk interpolasi Lagrange di GF(p))

```
function pol = lagrp(x,y,p)
m = length(x);
n = length(y);
if m == n
    pol = zeros(1,m);
    for i = 1:m
        Pi = 1;
        for j = 1:m
            if i ~= j
                bagi = mod(x(i)-x(j),p);
                Pi = mod((conv(Pi,[1 -x(j)])*mulinv(bagi,p)),p);
            end
        end
        pol = pol + y(i)*Pi;
    end
end

pol = mod(pol,p);
```

File mulinv.m (Fungsi untuk mencari invers terhadap perkalian di GF(p))

```
%MULINV(X,P) is a function that finds the multiplicative inverse
of
%vector X over finite (Galois) field of order P, i.e. if Y =
MULINV(X,P)
%then (X*Y) mod P = 1 or Y = X^(-1) over field of order P.
%
%The input parameters are vector of integers X and a scalar P
which
%represents the field order. The output is a size(X) vector which
%is the multiplicative inverses of X over P.
%
%The field order P must be a prime number and all elements of X
%should belong to the field i.e. X < P. Note: Over any field of
numbers
%the multiplicative inverse of one is one and the multiplicative
inverse of
%zero doesn't exist.
%
%Example:   X = [1 2 5], P = 7.
%           Y = MULINV(X,P) => Y = [1 4 3];
%
%The function doesn't check the format of input parameters.
%
%Reference:
%S. Bruce, Applied Cryptography: Protocols, Algorithms, and Source
Code in
%C, 2nd edition, John Wiley and Sons, Inc., US-Canada, 1996.
%
%G. Levin, Oct. 2004

function y=mulinv(x,p)

if ~isprime(p)
```

```
    disp('The field order is not a prime number');
    return
elseif sum(x>=p)
    disp('All or some of the numbers do not belong to the field');
    return
elseif sum(~x)
    disp('0 does not have a multiplicative inverse');
    return
end

k=zeros(size(x));    %set the counter array
m=mod(k*p+1,x);      %find reminders
while sum(m)         %are all reminders zero?
    k=k+sign(m);     %update the counter array
    m=mod(k*p+1,x); %caculate new reminders
end
y=(k*p+1)./x;        %find the multiplicative inverses of X
```