PENERAPAN *SECRET SHARING SCHEME* PADA *JOINT OWNERSHIP WATERMARKING* UNTUK CITRA DIGITAL

Made Windu Antara Kesiman*, Rinaldi Munir**

Departemen Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesa No. 10 Bandung 40132, Indonesia
***Email : if10036@students.if.itb.ac.id**
****Email : rinaldi@informatika.org**

ABSTRAKSI

Digital watermarking merupakan metode untuk menyisipkan suatu informasi, yang biasanya disebut sebagai watermark, pada suatu data digital penampung. Masalah yang dihadapi pada metode digital watermarking saat ini adalah semua metode yang telah ada hanya mampu menangani perlindungan hak cipta dari satu pemilik saja. Solusi yang kemudian ditawarkan untuk menangani masalah kepemilikan bersama suatu citra digital adalah dengan menerapkan secret sharing scheme pada digital image watermarking. Makalah ini membahas tentang penerapan secret sharing scheme pada joint ownership watermarking yang meliputi protokol-protokol dan metode-metode untuk proses penyisipan (embedding) watermark serta protokol-protokol untuk proses pendeteksian kepemilikan (detection) watermark. Robustness watermark diuji dengan melakukan beberapa proses manipulasi terhadap citra digital yang telah mengandung watermark, kemudian dilakukan proses pendeteksian kepemilikan watermark terhadap citra digital tersebut. Hasil uji menunjukkan, watermark cukup robust terhadap beberapa proses manipulasi citra digital, seperti perubahan brightness, kontras, scaling, flipping, rotasi, printscreen, serta kompresi JPEG 2000. Namun watermark masih rentan terhadap proses cropping dan penyisipan watermark ganda pada citra digital.

Kata Kunci :
Hak Cipta, Secret Sharing Scheme, Joint Ownership Watermarking, Citra Digital, Robustness

1. PENDAHULUAN

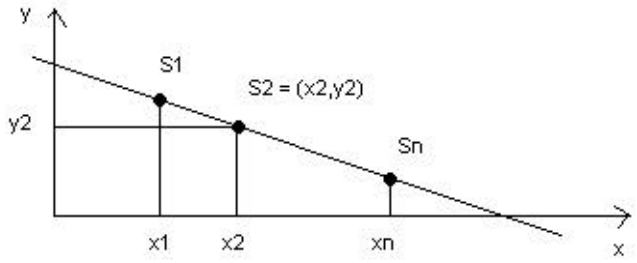
Secara garis besar, *secret sharing scheme* merupakan metode untuk melakukan pembagian suatu *secret*, biasanya berupa kunci, menjadi beberapa bagian yang disebut *share*, kepada sejumlah pihak yang disebut *participant*, dengan kondisi-kondisi tertentu. Kondisi yang dimaksud menyangkut sekelompok *participant* mana saja yang memungkinkan untuk menyatukan kembali *secret* yang telah dibagi-bagi tersebut [HUN99]. Menurut [DAN99], secara umum *secret sharing scheme* adalah komponen yang diperlukan untuk melakukan distribusi komputasi diantara sejumlah pihak yang tidak saling mempercayai. Dewasa ini, *secret sharing scheme* telah digunakan pada bidang-bidang aplikasi yang beragam, misalnya kontrol akses, peluncuran senjata atau proyektil, membuka kotak deposito, dan lain-lain.

Digital watermarking merupakan salah satu bentuk pengembangan metode penyembunyian data yang sebenarnya lebih ditekankan pada fungsionalitas dari data digital yang disisipkan, maupun data digital yang digunakan sebagai penampung. *Digital watermarking* telah banyak diterapkan dalam berbagai bentuk aplikasi dengan fungsionalitas yang beragam.

Penerapan *secret sharing scheme* pada *joint ownership watermarking* tentu saja membutuhkan protokol-protokol dan metode-metode untuk proses penyisipan (*embedding*) *watermark* serta protokol-protokol untuk proses pendeteksian kepemilikan (*detection*) *watermark*.

2. SECRET SHARING SCHEME

Pada skema awal yang diajukan, *secret* dipilih oleh seseorang yang bertanggung jawab terhadap proses perhitungan dan pendistribusian *share*, yang disebut *dealer*. Koleksi himpunan bagian dari himpunan *participants* yang bisa membentuk kembali *secret*, disebut struktur akses (*access structure*). *Secret sharing scheme* dikatakan *perfect* jika sebuah *secret* bisa di-*share* dalam sebuah himpunan *participants* sedemikian sehingga hanya himpunan bagian tertentu saja dari himpunan *participants* tersebut yang bisa membentuk kembali *secret* tersebut, sementara himpunan bagian lainnya tidak akan mampu untuk membentuk kembali *secret* tersebut [HUN99]. Salah satu jenis *secret sharing scheme* adalah *threshold secret sharing scheme*. Pada *threshold secret sharing scheme*, kondisi yang harus dipenuhi dari suatu himpunan bagian untuk bisa membentuk kembali sebuah *secret* adalah jumlah *participants* minimal yang harus terdapat dalam himpunan bagian tersebut. *Shamir's secret sharing scheme* ditemukan oleh Adi Shamir. *Shamir's scheme* didasarkan atas sebuah fakta yang sangat dikenal dalam ilmu matematika yaitu, suatu himpunan *n* buah titik akan mendefinisikan sebuah kurva unik dengan derajat *n-1*. *Shamir's scheme* bekerja sebagai berikut. Untuk membagi sebuah *secret S* antara *n* pihak, sehingga minimal *m* pihak dari *n* pihak tersebut bisa membentuk kembali *secret S*, maka bentuklah sebuah kurva yang melalui titik *(0,S)* dengan derajat *m-1*. Secara rahasia, setiap pihak akan menerima *share* dari *secret S* berupa sebuah koordinat titik yang dilalui kurva tersebut, masing-masing pihak harus menerima koordinat titik yang berbeda. Untuk nilai $m = 2$, kurva yang dibentuk seperti Gambar 1 berikut ini :



Gambar 1. Skema Kurva Polinom *Shamir's Scheme* dengan *Threshold* = 2

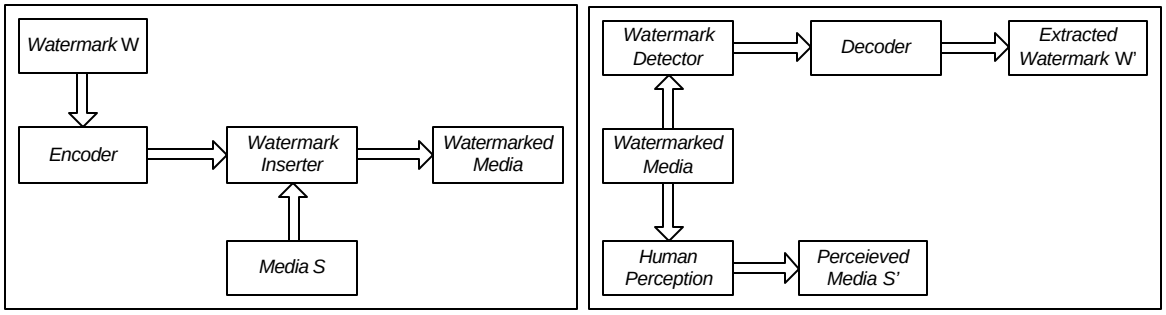
Kurva yang dibentuk adalah sebuah garis lurus dan *secret S* yang dibagi merupakan perpotongan antara kurva dengan sumbu *y*, yaitu untuk nilai $x = 0$. Masing masing *share* yang dibagi-bagikan adalah titik-titik yang dilalui kurva tersebut, misalnya S1 dan S2 [RSA04]. Jika hanya terdapat kurang dari *m* pihak yang bergabung untuk membentuk kembali *secret S*, bahkan walaupun hanya terdapat *m-1* pihak, maka akan terdapat sejumlah tak terhingga persamaan kurva yang bisa dibentuk, dan tidak terdapat cara untuk memilih persamaan kurva mana yang benar. Oleh karena itu, *Shamir's scheme* dianggap *information-theoretically secure* dan *perfect sharing scheme*. *Generalized secret sharing scheme* diperkenalkan oleh Ito, Saito, dan Nishizeki. *Generalized secret sharing scheme* merupakan pengembangan dari *threshold secret sharing scheme*, dimana struktur akses yang digunakan dapat bersifat lebih flexibel. Kondisi yang harus dipenuhi dari sebuah himpunan bagian dari himpunan *participants* yang ada untuk dapat membentuk kembali *secret* yang telah di-*share*, tidak hanya berupa jumlah minimal *participants* yang harus ada dalam himpunan bagian tersebut, tetapi harus memenuhi kondisi kombinasi *participants* yang

terotorisasi untuk dapat membentuk kembali *secret* tersebut [AMO04]. Untuk bisa memenuhi kondisi tersebut, *generalized secret sharing scheme* tetap menggunakan *threshold secret sharing scheme*, namun nilai *threshold*-nya ditentukan dari jumlah himpunan bagian yang tidak terotorisasi. *Share-share* yang dihasilkan akan didistribusikan kepada participants yang tidak termasuk dalam suatu himpunan bagian yang tidak terotorisasi.

Shamir's scheme bersifat *homomorphism* bahwa jumlah *share* yang dipegang oleh masing-masing *participants* yang berasal dari beberapa *secret*, merupakan *share* yang dipegang oleh *participants* tersebut untuk penjumlahan seluruh *secret*. Konsep inilah yang digunakan untuk membentuk *super-secret* dari beberapa *secret*, dengan menggunakan *super-share* dari beberapa *share* [JOS04]. *Jackson's scheme* merupakan salah *satu secret sharing scheme* yang menerapkan sifat *homomorphism* pada *secret sharing scheme*, sehingga dimungkinkan untuk melakukan *secret sharing scheme* tanpa *dealer*.

3. DIGITAL WATERMARKING

Menurut [DAV02], pada dasarnya pemberian *watermark* dapat dipandang sebagai proses menggabungkan dua buah data digital sedemikian rupa sehingga masing-masing dari data digital tersebut hanya dapat dideteksi oleh detektor yang besesuaian.



Gambar 2. Skema Umum Proses *Digital Watermarking*

Indera manusia hanya dapat mendeteksi data digital penampung saja. Sedangkan w*atermark* hanya dapat dideteksi oleh detektor *watermark*. Skema umumnya dapat dilihat pada Gambar 2.

Perlu diperhatikan bahwa data digital penampung ber-*watermark* maupun *watermark* yang terdeteksi, keduanya tidak sama dengan data digital penampung dan *watermark* sebelum proses penyisipan. Perbedaan ini terjadi karena berbagai hal seperti adanya distorsi selama proses penyisipan *watermark*, adanya *noise* selama transmisi data digital penampung, maupun akibat adanya proses modifikasi terhadap data digital penampung yang telah di-*watermark*. Sebenarnya pada saat melakukan persepsi terhadap data digital penampung seperti suara, citra maupun video, indera manusia tidak mampu memproses keseluruhan sinyal data digital penampung tersebut. Dengan kata lain, kepekaan indera manusia terhadap bagian-bagian data digital penampung tidaklah sama. Karakteristik inilah yang dimanfaatkan untuk menyisipkan *watermark*. *Watermark* diusahakan agar hanya memodifikasi sedikit bagian dari data digital penampung yang dapat dipersepsi oleh indera manusia dengan baik, sebaliknya banyak memodifikasi bagian yang kurang dapat dipersepsi oleh indera manusia.

Terdapat beberapa karakteristik penting yang dimiliki oleh *watermark* [DAV02]. Menurut [SHA03], *digital watermarking* mementingkan karakteristik *robustness* dimana aspek kemungkinan bahwa data digital penampung dapat dimodifikasi lebih diperhatikan. Karena itulah

dengan mengimplementasikan *digital watermarking* diusahakan *watermark* yang telah disisipkan pada suatu data digital tidak rusak ketika data digital penampung mengalami perubahan.

4. PROTOKOL PENERAPAN SECRET SHARING SCHEME PADA JOINT OWNERSHIP WATERMARKING

Pada *joint ownership watermarking*, akan terdapat lebih dari satu pihak yang berhak atas kepemilikan hak cipta dari citra digital. Tentu saja semua pihak yang memegang hak cipta akan citra digital tersebut berhak juga untuk berkontribusi dalam proses pemberian *watermark*, serta memiliki hak-hak tertentu dalam pengakuan hak cipta citra digital tersebut. Dalam proses *watermarking*, bagian yang biasanya menjadi rahasia yang dipegang hanya oleh pemegang hak cipta adalah kunci untuk proses-proses dalam watermarking, baik itu kunci untuk proses penyisipan *watermark* (*embedding*) dan pendeteksian *watermark* (*detection*), maupun kunci untuk melakukan pemilihan bilanganbilangan random. Kunci-kunci inilah yang dapat dianggap sebagai suatu *secret* dalam *secret sharing scheme.* Sedangkan pihak-pihak pemegang hak cipta merupakan *participants* didalamnya.

Misalkan terdapat tiga orang *participants* yaitu Alice, Bob, dan Carol, maka protokol untuk proses penyisipan *watermark* dengan *dealer* adalah sebagai berikut :

1. Alice, Bob, dan Carol memberikan citra digital yang akan diberi *watermark* kepada *dealer*.
2. Alice, Bob, dan Carol memberikan nilai jumlah *participants* kepada *dealer*.
3. Alice, Bob, dan Carol harus menentukan nilai ambang jumlah *participants* yang bisa membentuk kembali *secret* dan memberikannya kepada *dealer*.
4. *Dealer* menentukan kunci rahasia *watermark*.
5. *Dealer* memasukkan data nama *participants.*
6. Alice, Bob, dan Carol harus menentukan apakah akan menggunakan seluruh struktur akses atau menggunakan struktur akses tertentu saja.
7. Jika Alice, Bob, dan Carol ingin menggunakan struktur akses tertentu, maka mereka harus menyepakati struktur akses yang terotorisasi dan memberikannya kepada *dealer*.
8. *Dealer* membangkitkan *shares* dengan *secret sharing scheme*, jika dengan menggunakan seluruh struktur akses maka dilakukan *Shamir's scheme*, dan jika menggunakan struktur akses tertentu maka dilakukan *Ito's scheme.*
9. Dealer membagikan *shares* kepada Alice, Bob, dan Cely, masing-masing akan menerima *share* yang bersifat rahasia.
10. Alice, Bob, dan Carol menentukan nilai kekuatan *watermark*.
11. *Dealer* melakukan proses penyisipan *watermark* berdasarkan pembagian *shares* tersebut.

Protokol untuk proses penyisipan *watermark* tanpa *dealer* adalah sebagai berikut :

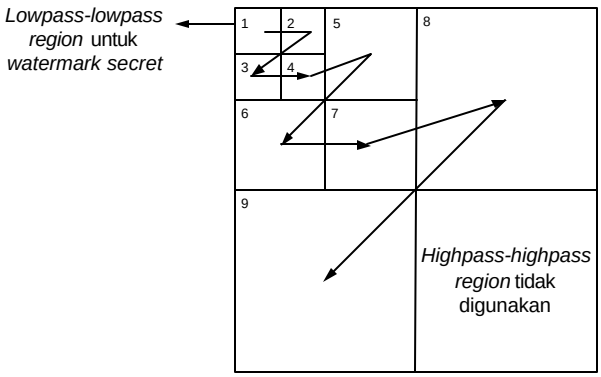
1. Alice, Bob, dan Carol menentukan citra digital yang akan diberi *watermark*.
2. Alice, Bob, dan Carol memasukkan nilai jumlah *participants.*
3. Alice, Bob, dan Carol memasukkan data nama *participants.*
4. Alice menentukan *sub secret watermark* untuk dirinya.
5. Alice membangkitkan *sub shares* untuk *sub secret watermark* tersebut.
6. Alice membagikan *sub shares* kepada Bob dan Carol, masing-masing akan menerima *sub shares* secara rahasia.
7. Alice menyimpan sub shares tersebut.
8. Bob dan Carol kemudian melakukan hal yang sama seperti yang telah dilakukan Alice dari langkah 4.
9. Alice, Bob, dan Carol bersama-sama membangkitkan *super shares* dengan menggunakan *Jackson's scheme.*

10. Alice, Bob, dan Carol bisa melihat *super shares* secara rahasia dengan menggunakan *sub secret*-nya masing-masing.
11. Alice, Bob, dan Carol menentukan nilai kekuatan *watermark*.
12. Alice, Bob, dan Carol melakukan proses penyisipan *watermark* berdasarkan pembagian *super shares* tersebut.

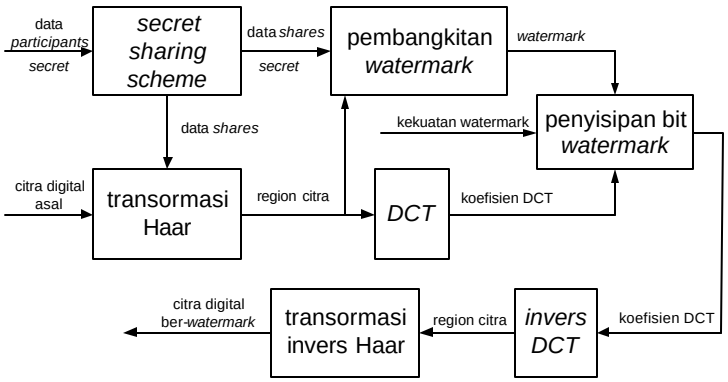
Protokol untuk proses pendeteksian kepemilikan *watermark* adalah sebagai berikut :

1. Alice, Bob, dan Cely memasukkan citra digital asal.
2. Alice, Bob, dan Cely memasukkan citra digital uji.
3. Alice, Bob, dan Cely memasukkan nilai jumlah *shares* dalam citra digital uji.
4. Alice, Bob, dan Cely akan memberikan dan menyimpan data index *shares* dan nilai *shares* mereka masing-masing.
5. Alice, Bob, dan Cely menggabungkan seluruh data *shares* mereka.
6. Alice, Bob, dan Cely melakukan proses pendeteksian kepemilikan watermark berdasarkan data *shares* tersebut.

Setelah proses *secret sharing scheme* dilaksanakan, maka masing-masing *participants* yang terotorisasi akan memegang *share* dari sebuah *secret*. *Watermark* yang akan disisipkan ke dalam citra digital akan dibangkitkan berdasarkan *share* dan *secret* tersebut. *Watermark* yang dibangkitkan berupa string biner yang diusahakan berdistribusi normal, dengan menggunakan pembangkit bilangan *pseudorandom* yaitu *Linear Congruential Generators* (LCG). Jika terdapat *n* buah *shares*, maka akan dibangkitkan *n+1* buah *watermark*. Nilai *n* buah *shares* dan satu buah *secret* akan menjadi nilai awal (*seed*) untuk proses pembangkitan *watermark*. Untuk menampung *n+1* buah *watermark* tersebut, diperlukan *n+1* buah *region* pada citra digital. Transformasi Haar digunakan untuk membentuk *region–region* pada citra digital. Jika dilakukan transformasi Haar *k* level, citra digital akan terbagi menjadi *3n+1* buah *region*. Namun *highpass-highpass region* terlalu *fragile* untuk disisipi *watermark*, sehingga hanya terdapat *3n* buah *region* yang bisa digunakan. Untuk itu perlu diperhitungkan jumlah level transformasi Haar yang harus dilakukan sehingga tersedia jumlah *region* yang cukup untuk menampung seluruh *watermark*. Masing-masing *watermark* akan disisipkan pada sebuah *region*, dimana *watermark* yang dibangkitkan dari nilai *secret* disisipkan pada *region* yang paling penting yaitu *lowpass-lowpass region*, sedangkan *n* buah *watermark* lainnya yang dibangkitkan dari nilai *shares* disisipkan sesuai dengan urutan index *shares* yang bersangkutan, dengan pemilihan *region* terpenting berikutnya. Pemilihan *region* terpenting dilakukan seperti pada Gambar 3 berikut :



Gambar 3. Pemilihan *Region* Matriks Transformasi Haar

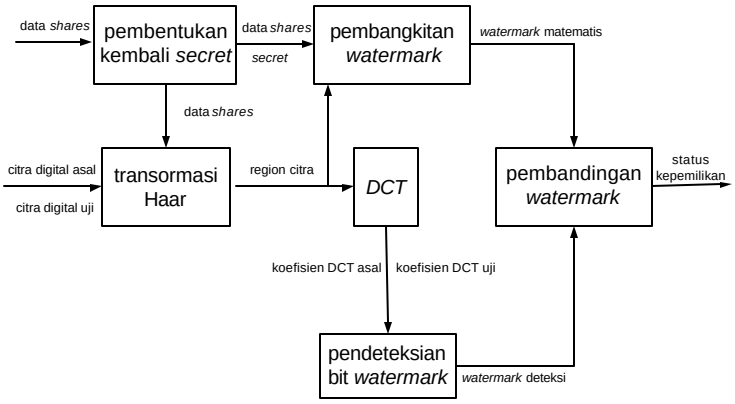


Gambar 4. Skema Proses Penyisipan *Watermark*

Setelah pembentukan *region* dengan transformasi Haar dan pembangkitan *watermark* dilakukan, maka proses penyisipan *watermark* siap dilakukan. Setiap *region* akan disisipi *watermark* dengan metode *Discret Cosine Transform* (DCT). Jika seluruh *watermark* telah disisipkan pada *region* yang bersesuaian, maka akan dikenakan transformasi invers DCT dan Haar pada citra digital tersebut, sehingga akan diperoleh citra digital yang telah mengandung *watermark*. Skema proses penyisipan *watermark* dapat dilihat pada Gambar 4.

Untuk mendeteksi *watermark*, diperlukan baik citra digital asal maupun citra digital uji. Berdasarkan data *shares* yang diberikan oleh *participants*, maka akan dilakukan pembentukan kembali *secret*. Kemudian dilakukan proses yang sama seperti proses penyisipan *watermark*, yaitu proses pembentukan *region* citra digital dengan transformasi Haar sesuai dengan jumlah *watermark* yang diperhitungkan terdapat pada citra digital uji. Jika data jumlah *shares* yang diberikan *participants* tidak benar, maka tidak akan terbentuk *region-region* yang benar pada citra digital, sehingga proses pendeteksian *watermark* selanjutnya tidak akan menghasilkan *watermark* yang diharapkan.

Proses transformasi Haar dan DCT dilakukan pada citra digital asal dan citra digital uji. Proses pendeteksian *watermark* yang terdapat pada suatu *region* dilakukan dengan membandingkan jumlah nilai koefisien DCT pada citra digital asal dengan jumlah nilai koefisien DCT pada citra digital uji. *Watermark* yang dideteksi pada citra digital uji tersebut akan dibandingkan dengan *watermark* yang dibangkitkan secara matematis sesuai dengan data *shares* yang diberikan *participants* dan secret yang dibentuk kembali dari data *shares* tersebut. Skema proses pendeteteksian kepemilikan *watermark* dapat dilihat pada Gambar 5.



Gambar 5. Skema Proses Pendeteksian Kepemilikan *Watermark*

5. PENGUJIAN ROBUSTNESS WATERMARK

Untuk melakukan pengujian tingkat ketahanan (*robustness*) *watermark*, teknik yang digunakan adalah dengan melakukan proses pendeteksian kepemilikan *watermark* terhadap citra digital ber-*watermark* yang sudah mengalami proses-proses manipulasi citra digital. Proses-proses manipulasi citra yang digunakan dalam pengujian *robustness watermark* ini adalah perubahan kontras dan *brightness*, rotasi, *flipping*, *scaling*, *cropping*, serta kompresi JPEG. Selain keenam proses manipulasi citra digital tersebut, dilakukan pula pengujian *robustness* watermark terhadap proses *printscreen* dan penyisipan *watermark* kembali pada citra digital ber-*watermark*.

Hasil proses penyisipan *watermark* dapat dilihat pada Tabel 1.

Tabel 1. Hasil Penyisipan *Watermark*

No	Citra Digital Asal	Proses Penyisipan *Watermark*	PSNR (dB)
1.	Camera	*Dealer*, Seluruh Struktur Akses	54,1091977007776
2.	Camera	*Dealer*, Struktur Akses Tertentu	49,3255774803264
3.	Camera	Tanpa *Dealer*	54,0445786591727
4.	Bird	*Dealer*, Seluruh Struktur Akses	54,0872027565743
5.	Bird	*Dealer*, Struktur Akses Tertentu	49,3224374975923
6.	Bird	Tanpa *Dealer*	54,0167358687794
7.	Boat	*Dealer*, Seluruh Struktur Akses	54,0822431195778
8.	Boat	*Dealer*, Struktur Akses Tertentu	49,3159902093777
9.	Boat	Tanpa *Dealer*	54,0710395481236
10.	Lena	*Dealer*, Seluruh Struktur Akses	54,0538993980243
11.	Lena	*Dealer*, Struktur Akses Tertentu	40,5683299425054
12.	Lena	Tanpa *Dealer*	54,0684382034403

Tabel 2. Hasil Uji *Robustness Watermark*

No.	Citra Digital Uji	Manipulasi Citra Digital	Akurasi *Watermark* Hasil Ekstraksi (%)
1.	Camera	Kontras +50	95,8333333333333
2.	Camera	Brightness +75	98,9583333333333
3.	Lena	Kontras +15	98,046875
4.	Lena	Brightness +15	99,7395833333333
5.	Camera	Rotasi $+15^0$	65,1041666666667
6.	Lena	Rotasi $+15^0$	72,1354166666667
7.	Camera	Flipping	100
8.	Lena	Flipping	100
9.	Camera	Scaling 4x	99,4791666666667
10.	Lena	Scaling 2x	100
11.	Camera	Cropping	63,0208333333333
12.	Lena	Cropping	62,3697916677777
13.	Camera	Kompresi JPEG 30 %	94,7916666666667
14.	Lena	Kompresi JPEG 20 %	90,234375
15.	Camera	Printscrenn	100
16.	Lena	Printscreen	100
17.	Camera	Watermark Ganda	73,9583333333333
18.	Lena	Watermark Ganda	74,3489583333333

6. PENUTUP

Penerapan *secret sharing scheme* pada *joint ownership watermarking* untuk citra digital merupakan salah satu solusi yang baik untuk mengatasi permasalahan kepemilikan hak cipta citra digital yang dipegang oleh lebih dari satu pihak. *Secret sharing scheme* juga dapat diterapkan diberbagai aplikasi yang memerlukan skema pembagian suatu rahasia kepada beberapa pihak. Skema pembagian rahasia menjadi lebih fleksibel dengan adanya pengembangan skema-skema baru *secret sharing scheme* yang didasarkan pada *Shamir's scheme*, seperti *Ito's scheme* dan *Jackson's scheme*. Untuk pengembangan lebih lanjut, dapat difokuskan pada masalah penyisipan *watermark* ganda, dimana sebaiknya digunakan *watermark* berupa citra digital. Sehingga jika *watermark* yang pertama tertutupi oleh *watermark* yang kedua, masih bisa dilakukan pengenalan terhadap *watermark* citra digital tersebut. Jika *watermark* hanya berupa string biner, sulit untuk melakukan pengenalan kembali *watermark* tersebut. Untuk melakukan *joint ownership watermarking*, masih banyak jenis transformasi citra digital yang dapat diterapkan. Sehingga diharapkan bisa digunakan sebagai transformasi citra digital yang lebih tahan terhadap proses manipulasi *cropping*, dibandingkan dengan transformasi Haar.

DAFTAR PUSTAKA

[JOS04] Josh Cohen Benalloh, "*Secret Sharing Homomorphisms : Keeping Shares of a Secret Secret (Extended Abstract)*", http://www.cs.cornell.edu/courses/cs754/2001fa/homo.pdf, Tanggal akses : 9 Maret 2004

[HUN99] Hung-Min Sun, Shiuh-Pyng Shieh, "*Constructing Perfect Secret Sharing Schemes for General And Uniform Access Structures*", Journal of Information Science and Engineering 15, 679-689, 1999, http:// www.iis.sinica.edu.tw/JISE/1999/199909_04.pdf, Tanggal akses : 9 Maret 2004

[DAN99] Daniel Gottesman, "*Quantum Secret Sharing*", http://perimeterinstitute.ca/people/researchers/dgottesman/QSS.html, 1999, Tanggal akses : 9 Maret 2004

[BET04] Betrsuted, "*Shamir's secret sharing scheme : description*", http://www.betrusted.com/downloads/products/keytools/v50/crypto/c-docs/html/cryptocdevguide-15.1.html, Tanggal akses : 11 Februari 2004

[RSA04] RSA Security, "*What are some secret sharing schemes ?*", http://www.rsasecurity.com/rsalabs/faq/3-6-12.html, Tanggal akses : 11 Februari 2004

[AMO04] Amos Beimel, Yuval Ishai, "*On the Power of Nonlinear Secret-Sharing*", http://www.cs.bgu.ac.il/~beimel/Papers/Nonlinear.pdf, Tanggal akses : 9 Maret 2004

[DAV02] David Andriyano, "*Watermark Beramplitudo Tinggi pada Sinyal Suara*", Tesis Magister Bidang Khusus Teknologi Informasi, Program Studi Telekomunikasi, Program Pasca Sarjana, Institut Teknologi bandung, 2002

[SHA03] Shanty Meliani Hendrawan, "*Robust and Non Blind Watermarking pada Citra Dijital dengan Teknik Spread Spectrum*", Tugas Akhir Departemen Teknik Informatika, Institut Teknologi Bandung, 2003

[ART96] Arthur R. Weeks Jr., "*Fundamentals of Electronic Image Processing*", IEEE PRESS, USA, 1996

[RIN02] Rinaldi Munir, *"Diktat Kuliah IF472 Pengolahan Citra"*, Departemen Teknik Informatika, Institut Teknologi Bandung, 2002

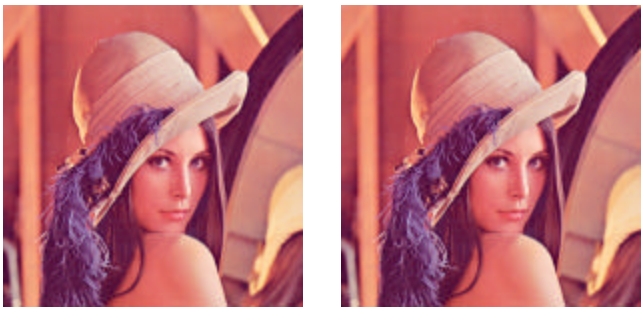
[RAT99] Ratnadewi, "*Pengolahan Citra dengan memakai Transformasi Wavelet*", Tesis Magister Bidang Khusus Elektroteknik, Program Studi Sistem Informasi Telekomunikasi, Program Pasca Sarjana, Institut Teknologi Bandung, 1999

[AVE00] Averill M.Law, W. David Kelton, *"Simulation Modeling and Analysis"*, Third Edition, Mc Graw Hill, 2000

[HUI03] Huiping Guo, Nicolas D. Georganas, *"A Novel Approach to Digital Image Watermarking based on A Generalized Secret Sharing Scheme"*, Multimedia Systems 9, 2003

[PEI99] Pei-chun Chen, Yung-seng Chen, Wen-hsing Hsu, *"Adaptive-Rate Image Watermarking based on Spread Spectrum Communication Technique"*, http://amp.ece.cmu.edu/publication/Trista/cscc1999_trista.pdf, 1999, Tanggal akses : 11 Februari 2004

[MOH03] Alex Mohr, *"CSE391 Introduction to Data Compression Lecture 15 Wavelet Transform Coding"*, http://www.cs.sunysb.edu/~amohr/cse391/2003-spring/lectures/cse391-lecture13.pdf, 2003, Tanggal akses : 13 Februari 2004



Gambar 6. Citra Lena Asal dan Citra Lena yang mengandung *watermark*

Gambar 7. Citra Camera Asal dan Citra Camera yang mengandung *watermark*

Tabel 3. Citra Uji

No.	Citra Digital	Ukuran	Kedalaman Warna	Keterangan
1.		256x256 *pixels*	8 bit	camera256gray.bmp Citra digital asal
2.		256x256 *pixels*	8 bit	bird256gray.bmp Citra digital dsal
3.		512x512 *pixels*	8 bit	boat512gray.bmp Citra digital asal
4.		512x512 *pixels*	24 bit	lena512colour.bmp Citra digital asal