JOINT OWNERSHIP PADA TEKNIK WATERMARKING MENGGUNAKAN SKEMA SECRET SHARING UNTUK AUDIO DIGITAL

Shelvie Nidya Neyman[1], Dewi Rosaria Indah[2], Fernissa Fahamalathi[3]

[1,2,3]Departemen Ilmu Komputer FMIPA IPB
JL. Meranti Wing 20 Lv V, Kampus Dramaga, Bogor, 16680
[1]shelvie@ipb.ac.id, [2]dew_pinkers@yahoo.com, [3]fernissa@gmail.com

Abstrak

Watermarking adalah sebuah proses untuk menyisipkan suatu informasi, yang biasanya disebut sebagai watermark, pada suatu data (digital) penampung, seperti gambar, audio, dokumen text, video dan bentuk produk digital lainnya. 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 ditawarkan untuk menangani masalah kepemilikan bersama suatu audio digital adalah dengan menerapkan skema *secret sharing* pada *digital audio watermarking*. Tulisan ini membahas tentang penerapan skema *shamir's secret sharing* pada *joint ownership watermarking*. Hasil pengujian memperlihatkan bahwa *watermarked audio* yang dihasilkan memiliki kualitas yang baik dilihat dari kriteria *Imperceptibility* dan *Robustness*. *Imperceptibility* dari audio digital yang telah mengandung watermark (*watermarked audio*) diuji melalui pengukuran kuantitatif menggunakan PSNR. *Robustness* watermark diuji dengan melakukan beberapa proses manipulasi audio terhadap *watermarked audio* kemudian dilakukan proses pendeteksian watermark terhadap audio digital tersebut. Hasil uji menunjukkan, watermark cukup *robust* terhadap beberapa proses manipulasi audio digital, seperti *resampling* dan penambahan *noise*/derau. Namun watermark masih rentan terhadap proses *cropping* dan *time stretching*. Pengujian pada skema *shamir's secret sharing* memenuhi kriteria *secret, bahwa proses pembangkitan dan pembuktian hak cipta/watermark harus dan hanya melibatkan seluruh participants* yang merupakan pemilik dari audio digital tersebut.

Kata kunci : *audio watermarking, joint ownership,* skema *secret sharing, imperceptibility, robustness,*

1. Pendahuluan

Teknologi jaringan komputer pada saat ini memungkinkan seperti gambar, video, dan audio dapat ditransmisikan dengan mudah dari satu tempat ke tempat lain tanpa kehilangan banyak kualitasnya. Kemudahan tersebut juga menimbulkan permasalahan baru, yaitu pertukaran atau penggunaan produk digital secara ilegal misalnya pemalsuan kepemilikan produk digital dan pelanggaran hak cipta. *Watermarking* merupakan salah satu teknik yang dapat digunakan untuk menyelesaikan permasalahan tersebut. *Digital watermarking* merupakan metode untuk menyisipkan suatu informasi pada suatu data *digital* penampung dengan tujuan perlindungan isi atau kepemilikan data.

Digital audio watermarking melibatkan penyembunyian data pada sebuah file audio. Hak atas kekayaan intelektual adalah pendorong utama untuk penelitian di bidang ini. Untuk melawan pembajakan musik online, sebuah digital watermark ditambahkan pada semua rekaman sebelum diterbitkan yang dapat digunakan tidak hanya untuk menentukan pencipta aslinya tapi juga menentukan user yang telah membelinya secara legal. Sistem operasi saat ini sudah memiliki perangkat lunak Digital Right Management (DRM) yang akan mengambil watermark dari sebuah file audio sebelum memainkannya. Perangkat lunak DRM ini akan memastikan bahwa user sudah membayar untuk lagu tersebut dengan membandingkan watermark yang ada pada file audio tersebut.

Metode *digital watermarking* saat ini pada umumnya hanya mampu menangani perlindungan hak cipta dari satu pemilik saja sehingga sulit diterapkan untuk kepemilikan lebih dari satu pihak. *Joint ownership* pada teknik watermarking memungkinkan terdapat lebih dari satu pihak yang berhak atas kepemilikan hak cipta dari audio digital. Semua pihak yang memegang hak cipta akan audio digital tersebut akan berhak untuk berkontribusi dalam proses pemberian watermark dan pengakuan hak cipta audio digital tersebut.

Skema *secret sharing* adalah komponen yang diperlukan untuk melakukan distribusi komputasi diantara sejumlah pihak yang tidak saling mempercayai[1]. Skema ini dapat dilakukan untuk pembagian suatu *secret*, menjadi beberapa bagian yang disebut *share*, kepada sejumlah pihak yang

disebut *participant*. *Secret* yang menjadi titik utama, diketahui oleh mereka hanya sebagai potongan informasi atau *share* yang secara langsung tidak terlihat berkaitan dengan *secret*. Salah satu jenis skema *secret sharing* adalah *threshold secret sharing scheme* [2]. Skema Shamir's secret sharing termasuk jenis *threshold secret sharing scheme* ditemukan oleh Adi Shamir.

Pada saat ini penelitian terkait joint ownership untuk teknik watermarking masih terfokus pada kepemilikan citra digital [3], [4], dan [5]. Untuk itu penelitian ini mencoba menawarkan solusi untuk penanganan masalah penerapan pemberian tanda kepemilikan bersama (*joint ownership*) pada audio digital. Solusi ini menggunakan teknik *Shamir's secret sharing scheme* dan teknik watermarking *Direct Sequence Spread Spectrum* (DSSS). Pengujian dilakukan untuk teknik watermarking DSS pada kriteria *imperceptibility,* dan *robustness* serta kriteria *security* untuk skema *Shamir's Secret Sharing*.

Dari hasil penelitian ini dapat diketahui *Shamir's secret sharing scheme* pada *joint ownership watermarking* dapat diterapkan untuk audio digital. Teknik watermarking yang digunakan memenuhi kriteria *imperceptibility*, yakni berkas audio hasil penyisipan watermark telah berhasil dibuat semirip mungkin dengan berkas aslinya. Tingkat *robustness* dari teknik watermarking tersebut berhasil melewati serangan manipulasi audio seperti *resampling* dan penambahan derau, tetapi gagal mengatasi serangan *cropping* dan *time stretching*. Proses penyisipan dan pendeteksian *ownership watermark* telah berhasil memenuhi kriteria *security,* dikarenakan proses tersebut harus melibatkan seluruh *participants* yang benar-benar merupakan pemilik dari audio digital tersebut.

Pada bagian selanjutnya dari tulisan ini akan menjelaskan penelitian-penelitian terkait yang sudah ada, penjelasan metode skema secret sharing dan teknik watermarking, teknik usulan untuk joint-ownership pada watermaking audio digital, dilanjutkan pengujian kualitas dan ketahanan dari hasil percobaan, dan diakhiri dengan penutup yang berisi kesimpulan dan saran pengembangan penelitian lebih lanjut.

2. Penelitian Terkait

Penelitian *joint ownership* pada teknik watermarking selama ini masih ditujukan untuk bukti kepemilikan citra digital. Penelitian [3], mengusulkan tentang penerapan skema *secret sharing* pada *joint ownership* watermarking untuk citra digital. Teknik watermarking yang digunakan pada penelitian tersebut menggunakan transformasi Haar dan DCT, tanpa menjelaskan jenis skema *secret sharing* yang digunakan. Penelitian lain mengusulkan dua algoritma baru untuk penggunaan skema *secret sharing* kriptografi untuk menyelesaikan permasalahan joint ownership pada watermarking citra digital [4]. Algoritma pertama menggunakan Shamir's, yakni skema dengan threshold untuk algoritma watermarking. Watermark berupa vektor distribusi acak gaussian ditentukan dengan dua kunci, disisipkan pada koefisien untuk semua *middle band* pada citra dalam domain wavelet, sehingga bukti kepemilikkan hanya bisa diverifikasi bila memiliki kedua kunci tersebut. Algoritma kedua yang diusulkan merupakan modifikasi dari algoritma pertama, dimana verifikasi kepemilikan bisa dilakukan secara parsial. Algoritma watermarking baru diusulkan untuk skema *secret sharing* dalam permasalahan verifikasi joint ownership tanpa adanya dealer terpercaya [5]. Para participants secara bersama-sama melakukan pembangkitan share dari secret yang ada tanpa ada pihak lain yang terlibat. Dan untuk deteksi hanya beberapa pihak tertentu saja yang bisa melakukan verifikasi kepemilikan.

3. Skema Secret Sharing

Skema *secret sharing* merupakan metode untuk melakukan pembagian suatu *secret*, biasanya berupa kunci, menjadi beberapa bagian yang disebut *shares*, kepada sejumlah pihak yang disebut *participants*, dengan kondisi-kondisi tertentu. Kondisi yang dimaksud menyangkut sekelompok *participants* mana saja yang memungkinkan untuk menyatukan kembali *secret* yang telah dibagi-bagi tersebut [6]. Dewasa ini, skema *secret sharing* telah digunakan pada bidang-bidang aplikasi yang beragam, misalnya kontrol akses, peluncuran senjata atau proyektil, membuka kotak deposito, dan lain-lain.

Salah satu jenis *secret sharing scheme* adalah skema *Shamir's secret sharing* atau biasa disebut sebagai skema *threshold secret sharing*. Pada skema *threshold secret sharing,* 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. Berikut merupakan algoritma *Shamir's secret sharing scheme* pada [4]:

1. *Setup. Dealer T* menentukan *secret* berupa *integer* $S \geq 0$ yang akan dibagikan kepada *n participats*.
   a. *T* memilih bilangan prima $p > max\ (S, n)$, dan mendefinisikan $a_0 = S$.
   b. *T* memilih bilangan acak sebanyak *t-1* sebagaikoefisien
      $a_1, \ldots, a_{t-1}$ dimana $0 \leq a_j \leq p-1$,
      kemudian mendefinisikan fungsi polinomial acak dalam $\mathbb{Z}_p$ yaitu :

$$f(x) = \sum_{j=0}^{t-1} a_j x^j \qquad (1)$$

c. *T* menghitung $S_i = f(i) \bmod p, 1 \leq i \leq n$ (atau untuk sembarang *n* titik *i* yang berbeda, $1 \leq i \leq p-1$), dan secara rahasia memberikan *share* S_i kepada *participant* P_i beserta dengan index *i*.

2. Rekonstruksi *secret*. Sembarang himpunan dari sebanyak *t* atau lebih *shares* milik *participants* (sebanyak *t* atau lebih titik $(x,y) = (i,S_i)$ yang berbeda) dapat merekonstruksi kembali *secret* dengan menggunakan interpolasi *Lagrange*. *Secret* yang dimaksud adalah $f(0)=a_0=S$. Berikut adalah persamaan interpolasi *Lagrange*:

$$f(x) = \sum_{i=1}^{t} y_i \prod_{1 \leq j \leq t, j \neq i} \frac{x - x_j}{x_i - x_j} \qquad (2)$$

4. Teknik Watermarking

Watermarking merupakan teknik untuk menyisipkan informasi ke dalam data, terutama data yang berbentuk *digital*. Informasi yang disisipkan disebut *watermark* (tanda air). *Watermark* dapat berupa teks seperti informasi *copyright*, gambar, data audio atau rangkaian bit yang tidak bermakna. Proses penyisipan yang dilakukan tidak boleh merusak data yang dilindungi.

Jenis-jenis *watermark*ing berdasarkan penyebarannya adalah *public* atau *blind watermarking* dan *non-blind watermarking* atau *private watermarking*. *Public watermarking* tidak memerlukan berkas asli untuk proses deteksi *watermark,* sedangkan skema proses *private watermark* yang membutuhkan berkas asli sebelum disisipi *watermark* untuk mendeteksi *watermark* [7].

Terdapat beberapa kriteria yang harus dipenuhi oleh aplikasi watermarking. Kriteria yang paling utama adalah *imperceptibility* atau *fidelity* yaitu berkas hasil penyisipan watermark harus dibuat semirip mungkin dengan berkas aslinya, *robustness* yaitu berkas hasil penyisipan watermark harus tahan terhadap berbagai teknik manipulasi digital dan watermark harus dapat dideteksi kembali, dan *security* dimana watermark yang disisipkan tidak boleh meninggalkan jejak dalam arti tidak terlalu menonjol agar pihak lain tidak bisa dengan mudah menghilangkan watermark yang sudah disisipkan [6].

Direct sequence spread spectrum atau DSSS adalah teknik yang memultiplikasi sinyal audio asli dengan rangkaian biner dan koefisien *watermark*. Rangkaian biner tersebut umumnya disebut sebagai sinyal *chip*. Sinyal *chip* tersebut harus lebih besar dari data *rate* atau *information rate*. Sinyal *chip* pada dasarnya merupakan *key* yang dibutuhkan baik pada proses penyisipan maupun deteksi untuk memodulasi rangkaian data [8]. Proses penyisipan *watermark* ke dalam sinyal audio pada metode ini dilakukan dengan perumusan sebagai berikut :

$$x'[f] = x_i[f] + \alpha * w[i] \qquad (3)$$

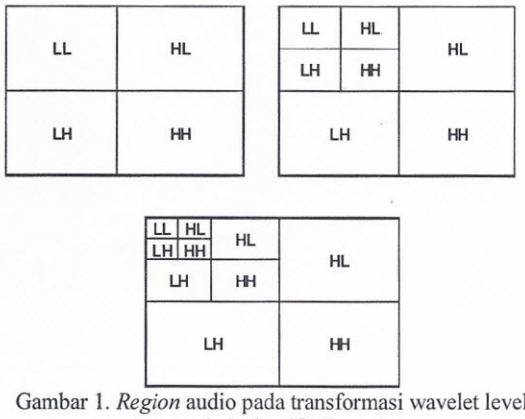
dengan α merupakan tingkat kejelasan *watermark* atau *watermarkamplitude* atau koefisien *watermark* yang akan disisipkan ke dalam sinyal audio yang rentang nilainya adalah: $0 < \alpha \leq 1$, *x(f)* adalah sinyal audio yang telah ditransfomasikan ke domain frekuensi dan $x_i[f]$adalah nilai blok-blok hasil transformasi ke-*i*. Proses deteksi *watermark* dilakukan sebaliknya yaitu dengan mengurangkan sinyal hasil transformasi frekuensi *watermarked* audio dengan sinyal hasil transformasi frekuensi audio asli lalu dibagi dengan *scaling factor*. Proses tersebut akan menghasilkan *carier signal watermark*yang kemudian dikalkulasikan untuk mendapatkan rangkaian biner *watermark* dan dikonversikan menjadi informasi sesungguhnya [9].

5. Joint Ownership pada Teknik Watermarking untuk Audio Digital

Joint ownership pada teknik watermarking memungkinkan terdapat lebih dari satu pihak yang berhak atas kepemilikan hak cipta dari audio digital. Semua pihak yang memegang hak cipta akan audio digital tersebut akan berhak untuk berkontribusi dalam proses pemberian watermark, serta memiliki hak-hak tertentu dalam pengakuan hak cipta audio digital tersebut. Dalam proses watermarking, bagian yang biasanya menjadi rahasia adalah kunci untuk proses-proses dalam watermarking, baik itu kunci untuk proses penyisipan watermark (*embedding*) dan pendeteksian watermark (*detection*), maupun kunci untuk melakukan pembangkitan bilangan-bilangan random. Kunci-kunci ini yang dianggap sebagai suatu *secret* dalam skema *secret sharing*, sedangkan pihak-pihak pemegang hak cipta merupakan *participants* didalamnya. Setelah proses skema *secret sharing* dilaksanakan, maka masing-masing *participants* yang terotorisasi akan memegang *share* dari sebuah *secret*. Watermark yang akan disisipkan ke dalam audio *digital* akan dibangkitkan berdasarkan *secret* yang dibentuk dari *shares* tersebut.

Watermark yang dibangkitkan berupa *integer* dengan menggunakan pembangkit bilangan *pseudorandom* yaitu *Linear Congruential Generators* (LCG). Nilai *secret* akan menjadi nilai awal (*seed*) untuk proses pembangkitan *watermark*. Proses penyisipan akan dilakukan pada domain frekuensi. *Lifting wavelet transform* (LWT) digunakan untuk mengubah berkas audio dari domain waktu ke dalam domain frekuensi serta untuk membentuk *region* dari audio yang akan disisipi. LWT level 1 akan membagi data audio ke dalam 4 *region* yaitu *region* LL, *region* HL, *region*

LH dan *region* HH atau secara umum LWT level ke-*k* akan membagi data audio ke dalam *3k+1 region*. Transformasi *Wavelet* level 1, 2 dan 3 dapat dilihat pada Gambar 1.

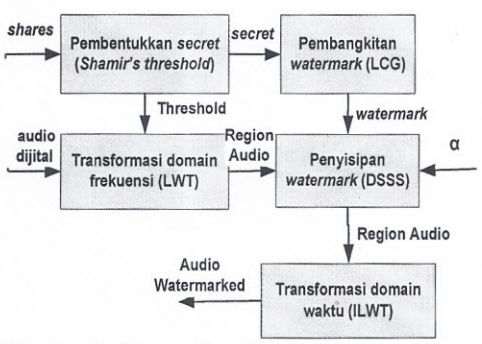


Gambar 1. *Region* audio pada transformasi wavelet level 1, 2, dan 3[14].

Watermark akan disisipkan pada *region* LL yang merupakan *region* paling tidak *fragile* dibandingkan dengan *region* lain. Letak *region* LL bergantung pada level yang akan digunakan pada LWT, dengan perhitungan sebagai berikut:

$$Level = (secret \ / \ threshold\ )\ mod\ L \qquad (4)$$

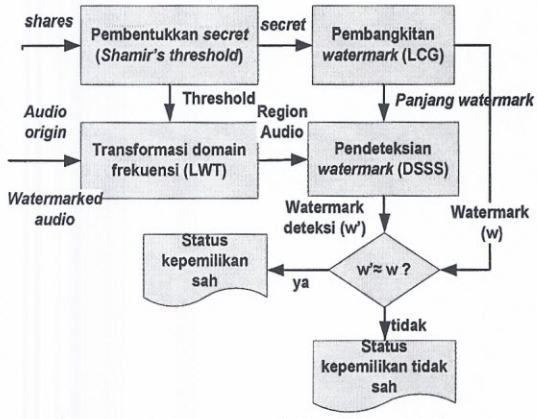
dimana *L* merupakan level LWT maksimal yang dapat digunakan. Setelah berkas audio diubah ke dalam domain frekuensi dan *region* telah dibuat dengan LWT serta pembangkitan *watermark telah* dilakukan, maka dilakukan proses penyisipan *watermark*. Berkas audio disisipi *watermark* dengan metode *Direct Sequence Spread Spectrum* (DSSS). Jika seluruh watermark telah disisipkan pada *region* yang bersesuaian, maka akan dikenakan transformasi *Lifting Wavelet* pada audio digital tersebut, sehingga akan diperoleh audio digital yang telah mengandung watermark. Skema proses penyisipan watermark dapat dilihat pada Gambar 2.



Gambar 2. Proses Penyisipan *Watermark.*

Untuk pendeteksian watermark, diperlukan baik audio digital asal maupun audio digital uji serta data shares (teknik *non-blind watermarking*). Berdasarkan data *shares*(x_i,y_i)yang diberikan oleh *participants*, maka akan dilakukan pembentukan kembali *secret* dengan menggunakan interpolasi *Lagrange*. *Secret* yang terbentuk akan digunakan sebagai *seed* pembangkit bilangan acak menggunakan LCG yang nantinya akan digunakan untuk mengetahui panjang *watermark*yang telah disisipkan serta pembanding asli tidaknya *watermark* deteksi. Kemudian dilakukan proses yang sama seperti penyisipan *watermark*, yaitu proses transformasi audio *digital* dari domain waktu ke dalam domain frekuensi serta membagi data audio ke dalam *region-region* sesuai level LWT yang didapat dari informasi *secret*. Proses transformasi LWTdilakukan pada audio *digital* asal dan audio *digital* uji.

Proses pendeteksian watermark dilakukan dengan cara membandingkan watermark pada audio *digital* uji dengan *watermark* yang dibangkitkan secara matematis dari *secret* yang dibentuk berdasarkan data *shares* tersebut. Skema proses pendeteteksian kepemilikan *watermark* dapat dilihat pada Gambar 3 .



Gambar 3. Proses Pendeteksian Watermark.

6. Pengujian Fidelity Watermark

Pengujian *imperceptibility* atau *fidelity* pada *watermarked audio* dilakukan dengan cara membandingkannya dengan berkas audio asli sehingga dapat diketahui nilai distorsi yang disebabkan oleh proses penyisipan *watermark* tersebut menggunakan pengukuran *peak signal to noise ratio* (PSNR). Hasil pengukuran nilai PSNR dilakukan pada semua berkas audio dengan berbagai nilai alpha (α).

Pemilihan nilai alpha ini diharapkan memperhatikan faktor *trade-off* antara ketahanan dan kualitas. Semakin tinggi nilai alpha maka semakin rendah pula kualitas audio yang dihasilkan, tapi sebaliknya mempertinggi ketahanan audio terhadap serangan berbasis frekuensi. Hasil perhitungan nilai PSNR dari *watermarked audio* dan audio asli pada berbagai nilai alpha dapat dilihat pada Tabel 1.

Tabel 1. Nilai PSNR watermarked audio dan audio asli.

Nilai Alpha	Jenis Audio			
	Speech	Instru-mental	Instrument mix	Full Song
0.1	55.80	49.30	59.16	59.11
0.2	49.78	43.28	53.14	53.09
0.3	46.26	39.76	49.62	49.57
0.4	43.76	37.26	47.12	47.07
0.5	41.82	35.32	45.18	45.15
0.6	40.24	33.74	43.60	43.62
0.7	38.90	32.24	42.23	42.39
0.8	37.74	31.24	41.19	41.46
0.9	36.76	30.22	40.34	40.71

Berdasarkan hasil pada Tabel 1, *watermarked audio* yang dihasilkan memiliki kualitas yang baik karena nilai PSNR yang dihasilkan rata-rata di atas 30 dB. PSNR biasanya dipresentasikan sebagai logaritmik desibel (dB) dan kualitas audio yang baik berada pada kisaran di atas 30 dB [10]. Selain itu nilai PSNR tertinggi untuk setiap jenis musik yang diujikan pada Tabel 1 menunjukkan nilai α optimal untuk setiap jenis musik tersebut.

7. Pengujian Robustness Watermark

Untuk melakukan pengujian tingkat ketahanan (*robustness*) *watermark*, dilakukan operasi-operasi manipulasi audio terhadap *watermarked audio.* Operasi-operasi manipulasi audio yang digunakan dalam pengujian robustness watermarked audio adalah *resampling*, *cropping*, penambahan derau, dan *time stretching*. Pada proses pengujian ini dilakukan perbandingan antara watermark asli dengan watermark hasil deteksi setelah diujikan dengan serangan–serangan yang diberikan.

7.1 Operasi Resampling

Untuk melihat tingkat robustness *watermark,* akan dilihat apakah nilai watermark hasil ekstraksi dari *watermarked audio* setelah mengalami proses *resampling* mengalami perubahan atau tidak. Pada serangan resampling, *sample rate* yang digunakan adalah 22050 Hz dan 48000 Hz sedangkan *sample rate* berkas audio asal keseluruhan adalah 44100 Hz. Hasil pengujian menunjukkan bahwa watermark robust/kokoh terhadap operasi *resampling* karena nilai *watermark* hasil deteksi selalu sama. Hal ini bisa terjadi dikarenakan operasi *resampling* hanya mengubah jumlah *sample* per-detik dari *watermarked audio* sehingga tidak mempengaruhi nilai blok–blok transformasi ataupun nilai *carrier signal* dari *watermarked audio.*

7.2 Operasi Cropping

Untuk melihat apakah watermark robust terhadap serangan cropping, watermark dari watermarked audio hasil cropping dideteksi kembali dan dibandingkan dengan watermark aslinya. Operasi cropping dilakukan dengan memotong 1/2 bagian dari *watermarked audio* baik dari 1/2 bagian awal, tengah maupun akhir dengan menggunakan tools *Audacity*. Hasil pengujian menunjukkan semua nilai watermark dari *watermarked audio* yang mendapatkan operasi *cropping tidak* dapat diperoleh kembali atau dapat dikatakan bahwa watermark tidak *robust* terhadap operasi cropping. Operasi cropping memotong beberapa bagian dari *watermarked audio*, sehingga menghilangkan beberapa bagian dari *carrier signal*. Oleh karena itu, nilai watermark tidak dapat dikembalikan seperti semula.

7.3 Operasi Penambahan Derau

Derau merupakan suara–suara yang tidak dinginkan. Operasi penambahan derau pada *watermarked audio* di domain frekuensi dilakukan melalui transformasi Fourier dan menambahkan sinyal Fourier dengan sinyal random carrier yang dimultiplikasi dengan amplitude yang kurang dari watermark amplitude yang digunakan untuk penyisipan. Hasil pengujian menunjukkan bahwa semua nilai watermark dari *watermarked audio* yang mendapatkan penambahan derau dapat dideteksi kembali dan bernilai sama dengan watermark aslinya. Sehingga dapat dikatakan bahwa watermark tersebut robust terhadap operasi penambahan derau dengan amplitude yang kecil. Operasi ini tidak mempengaruhi nilai blok-blok transformasi karena amplitude untuk random noise signal yang digunakan kurang dari nilai watermark amplitude yang digunakan untuk menyisipkan pesan

7.4 Operasi time stretching

Metode operasi *time stretching* yang digunakan adalah metode Phase Vocoder yang bekerja dengan mengimplementasikan resampling pada data, lalu memanipulasi fase sinyal pada domain STFT (*Short Time Fourier Transform*). Hasil uji robustness watermark terhadap serangan ini menunjukkan bahwa watermark tidak tahan terhadap operasi *time stretching*, karena nilai watermark dari *watermarked audio* tidak dapat diperoleh kembali Operasi *time stretching* menggunakan metode *phase vocoder* yang melakukan *overlapping* serta memanipulasi fase sinyal pada domain STFT. Dengan kata lain *phase vocoder* menciptakan sinyal yang hampir mirip dengan sinyal aslinya untuk melakukan pemecahan pada sinyal untuk mendapatkan perubahan *speed*. Sehingga ketika dideteksi kembali nilai blok –blok transformasi mengalami perubahan begitu pula untuk nilai *carrier signal watermark.*

8. Pengujian Skema Shamir's Secret Sharing

Pengujian skema *shamir's secret sharing* dilakukan untuk membuktikan apakah *secret* dapat

diperoleh jika jumlah *shares* kurang dari *threshold*. Pada pengujian digunakan nilai *secret* yaitu 1234 yang dibagi menjadi 5 *shares* dengan *threshold* sebanyak 3, dimana bilangan prima p yang dipilih adalah 1237 sehingga koefisien a_1 dan a_2 persamaan polinom yang digunakan merupakan bilangan *integer* random $1 \leq a_j < 1236$ dan *shares* yang dihitung merupakan $S_i=f(i)$ dimana $1 \leq i \leq 5$. Pasangan kunci (*shares*) yang dihasilkan adalah (1, 48), (2, 1122), (3, 745), (4, 154), dan (5, 586). Dari kelima pasangan kunci tersebut dilakukan skenario uji untuk membentuk kembali *secret* seperti yang terlihat pada Tabel 2.

Tabel 2. Hasil pembentukan *secret* pada berbagai jumlah dan kondisi *shares*

Jumlah shares	Kondisi nilai *shares*		
	Semua benar	Tidak semua benar	Semua benar, tapi *redundant*
Kurang (n < t)	211	877	NaN
Sama dengan (n = t)	1234	1167	NaN
Lebih besar (n > t)	1234	28	NaN

Dari Tabel 2 diatas menunjukkan bahwa *secret* hanya akan terbentuk kembali dengan benar jika jumlah *shares* yang benar sama dengan atau lebih besar dari threshold (t) tanpa ada nilai yang *redundant*.

Jika terdapat *t-1 shares* (nilai benar semua) maka dibutuhkan sebuah *share* (i, $f(i)$) lagi untuk mendapatkan *secret* yang benar. Jika dimisalkan nilai bilangan prima $p = 1237$, maka terdapat 1236 kemungkinan kunci $f(i)$, sehingga peluang untuk mendapatkan pasangan *share* (i, $f(i)$) yang benar adalah $\frac{1}{1236} = 0{,}0008$. Dengan demikian, secara umum jika nilai $p=M$ dan jumlah *shares* sebanyak $t-r$, dengan $1 \leq r \leq t-1$, maka peluang untuk mendapatkan *secret* yang benar adalah:

$$P(s) = \left(\frac{1}{(M-1)}\right)^r$$

9. Penutup

Penerapan skema *shamir's secret sharing* pada *joint ownership watermarking* untuk audio digital dapat menjadi salah satu solusi untuk mengatasi permasalahan kepemilikan hak cipta audio digital yang dipegang oleh lebih dari satu pihak. Untuk melakukan *joint ownership watermarking*, dapat dicobakan dengan perapan jenis teknik watermarking domain transformasi yang lainnya, sehingga diharapkan bisa lebih tahan terhadap proses *manipulasi cropping* dan *time stretching*.

Daftar Pustaka:

[1] Gottesman D. 1999. "*Quantum Secret Sharing*", DOI=://perimeterinstitute.ca/people/researchers/dgottesman/QSS.html. [9 Maret 2004]

[2] Menezes A, Oorschot PV, Vanstone S. 1996. *Handbook of Applied Cryptography*. CRC Press.

[3] Kesiman MWA, Munir R. 2004. *Penerapan Secret Sharing Scheme pada Joint Ownership Watermarking Untuk Citra Digital*. Departemen Teknik Informatika, Institut Teknologi Bandung.

[4] Guo H, Georganas N. 2003. *Joint ownership verification for an image using digital watermarking*. Proceedings. International Conference on Information Technology: Coding and Computing (ITCC) 2003.

[5] Guo H, Georganas N. 2003. *Digital image watermarking for joint ownership verification without a trusted dealer*. Proceedings. International Conference on Multimedia and Expo (ICME'03).

[6] Sun HM dan Shieh SP. 1999. *Constructing Perfect Secret Sharing Schemes for General And Uniform Access Structures*. Department of Computer Science and Information Engineering National Cheng Kung University Tainan, Taiwan.

[7] Petitcolas F, Katzenbeisser S, dan Hyeon L. 2002. *Watermarking FAQ*. DOI= http://watermarkingworld.org/faq. [28 April 2008]

[8] Bender W, Gruhl D, Lu A, Morimoto N. 1996. *Techniques For Data Hiding*. IBM Systems Journal Vol. 35, No. 3&4, MIT Media Lab. G321-5608.

[9] Cvejic N. 2004. *Algorithms for Audio Watermarking and Steganography*. Oulu: University of Oulu Publications.

[10] Pelton G. 1993. *Voice Processing*. Singapore: McGraw-Hill.