OPTIMASI KETAHANAN WATERMARKING AUDIO DIGITAL MENGGUNAKAN ALGORITMA RSA DAN MSB

Resianta Perangin-angin[1], Benget Rumahorbo[2]

[1] Komputerisasi Akuntansi, Universitas Methodist Indonesia
[2] Teknik Informatika, Universitas Methodist Indonesia

[1]resianta88@gmail.com, [2]benget888@gmail.com

ABSTRACT

Copyright is a serious problem in the digital world, the process of sending and distributing digital media is so easy nowadays, copyright in the digital world is very detrimental to those who feel that their digital rights are copied and pasted or taken without the consent of the creator. Therefore we need a way where when a digital file can be identified as original as a product, one of the right ways is to use a watermark technique. But often this watermark process can be lost or cannot be extracted because the digital file has gone through a compression process, duplicate or something else. So in this study, it will be tried to increase the durability of a watermark in digital audio as a solution for identifying copyrighted digital works. Where the watermark process will use the RSA and MSB algorithms to enter information into a digital audio file, later this information can be extracted to view copyright ownership information from the digital audio. And it is hoped that this watermarking is resistant to various digital audio processes such as compression, duplication and editing carried out on the file. the information that is inserted into is maintained without compromising the quality of the digital audio.

Keywords: robussnest, watermarking, msb, rsa, encryption

I. PENDAHULUAN

Penggunaan format digital terutama pada data suara atau musik masih menimbulkan kontrovers seputar perlindungan hak ciptanya. Kemudahan pengolahan data digital menyebabkan sering terjadi pelanggaran hak cipta data tersebut. Perkembangan teknologi informasi membuat prosespertukaran informasi dapat dilakukan dengan mudah melalui internet. Namun, dengan adanya kemudahan ini terdampakterhadap keaslian informasi tersebut.Seseorang dapat membajak dan memodifikasi informasi dengan mudah [1] Salah satu media digital yang dapat digunakan dalam penyampaian pesan dalam bentuk lambang-lambang auditif adalah audio. Media audio dipakai karena mudahdalam penggunaannya dan diikuti dengan kemudahan dalam pengaksesannya. Berbagai macam file audio sudah diciptakan mulai dari WAV, MP3, WMA, FLAC, MP4, dan AMR[2]

Sering terjadi penduplikasian, pengambilan sebagian atau seluruh isi data, maupun pendistribusian secara ilegal terhadap data digital tanpa melaluui izin dari pemiliknya, sehingga secara otomatis pemilik hak cipta telah dirugikan atas perbuatan tersebut.[1]

Permasalahan tersebut menyebabkan pentingnya suatu pembuktian kepemilikan atas hak cipta dari suatu media digital. [2] Untuk dapat membuktikan kepemilikan atas hak cipta audio dapat digunakan teknik *watermarking*. *Watermarking* merupakan teknik yang digunakan untuk menyembunyikan tanda atau informasi hak cipta seperti waktu atau tanggal, dan pemilik hak cipta ke dalam suatu media digital. Penyisipan informasi ke dalam suara digital dilakukan sedemikian rupa sehingga tidak merusak kualitas suara yang disisipi informasi hak cipta.

Informasi hak cipta ini harus dapat diekstrak untuk membuktikan kepemilikan atas produk suara digital tersebut. Hasil dari proses ekstraksi kemudian dibandingkan dengan informasi asli dari pemegang hak cipta. Jika informasi hasil ekstraksi sama dengan informasi asli maka dialah pemegang hak cipta atas produk suara digital tersebut.

II. KAJIAN PUSTAKA

Watermarking

Watermarking adalah proses penambahan sekumpulan kode identifikasi secara permanen ke dalam sebuah data digital. Dimana kode identifikasi tersebut dapat berupa teks, suara, gambar, atau video. Selain tidak merusak data digital induknya, kode identifikasi seharusnya memiliki ketahan/*robustness* terhadap berbagai pemrosesan lanjutan seperti pengubahan, kompresi, enkripsi, dan lain sebagainya. [2]

Digital watermarking didasarkan pada ilmu steganografi, yaitu ilmu yang mengkaji tentang penyembunyian data. Istilah steganografi berasal dari bahasa Yunani, yang berarti *covered-writing*, atau tulisan tersembunyi. Teknik ini mengambil keuntungan dari keterbatasan indera manusia, khusunya penglihatan dan pendengaran, sehingga *watermark* yang dibubuhkan pada dokumen tidak akan disadari kehadirannya oleh manusia.[9]

MOST SIGNIFICANT BIT (MSB)

Suatu sistem komputasi dinamakan real-time jika sistem tersebut dapat mendukung eksekusi program / aplikasi

dengan waktu yang memiliki batasan, atau dengan kata lain suatu sistem real-time harus memiliki :

1. Batasan waktu dan memenuhi deadline, artinya bahwa aplikasi harus menyelesaikan tugasnya dalam waktu yang telah dibatasi atau ditentukan
2. Dapat diprediksi, artinya bahwa sistem harus bereaksi terhadap semua kemungkinan kejadian selama kejadian tersebut dapat diprediksi.
3. Proses bersamaan, artinya jika ada beberapa proses yang terjadi bersamaan, maka semua deadline nya harus terpenuhi.
4. Dapat mengerjakan hal-hal yang penting saja, mengatur strategi task-task mana yang harus dikerjakan lebih dahulu.
5. Membuat processor agar bekerja lebih cepat, sehingga dapat ditingkatkan jumlah taskyang diselesaikan
6. Menemukan tingkat effisiensi waktu.
7. Waktu proses merupakan sesuatu yang vital dan dianggap penting
8. Suatu sistem dimana respon tepat waktu oleh komputer merupakan hal yang dianggap vital[6].

ALGORITMA RSA

Dari sekian banyak algoritma kriptografi kunci-publik yang pernah dibuat, algoritma yang paling populer adalah algoritma RSA. Algoritma RSA dibuat oleh 3 orang peneliti dari MIT pada tahun 1976, yaitu : Ron (R) ivest, Adi (S) hamir, dan Leonard (A) dleman. Kemanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima. Pemfaktoran dilakukan untuk memperoleh kunci privat. Selama pemfaktoran bilangan besar menjadi faktor-faktor prima belum ditemukan algoritma yang mangkus, maka selama itu pula keamanan algoritma RSA tetap terjamin [8]

Algoritma RSA memiliki besaran-besaran sebagai berikut:

1.	p dan q bilangan prima	(rahasia)
2.	n = p.q	(tidak rahasia)
3.	φ(n) = (p-1)(q-1)	(rahasia)
4.	e(kunci enkripsi)	(tidak rahasia)
5.	d(kunci dekripsi)	(rahasia)
6.	m(plainteks)	(rahasia)
7.	c(cipherteks)	(tidak rahasia)

Algoritma Membangkitkan Pasangan Kunci

1. Pilih dua buah bilangan prima sembarang, p dan q
2. Hitung n = p.q (sebaiknya p≠q, sebab jika p=q maka n = p^2 sehingga p dapat diperoleh dengan menarik akar pangkat dua dari n).
3. Hitung φ(n) = (p-1)(q-1).
4. Pilih kunci publik, e, yang relatif prima terhadap φ(n)
5. Bangkitkan kunci privat dengan menggunakan persamaan e.d ≡ 1 (mod φ(n)). Perhatikan bahwa e.d ≡ 1 (mod φ(n)) ekivalen dengan e.d = 1 + k φ(n), sehingga secara sederhana d dapat dihitung dengan

$$d=\frac{1+k\varphi n}{e}$$

Hasil dari algoritma di atas :

- Kunci publik adalah pasangan (e,n)
- Kunci privat adalah pasangan (d,n)

Catatan : n tidak bersifat rahasia, sebab ia diperlukan pada perhitungan enkripsi/dekripsi.

Selama ini, baik kunci publik maupun kunci privat adalah sebuah angka. Hal ini bisa dikembangkan dengan menggunakan suatu citra digital. Dengan demikian, pasangan bilangan prima merupakan representasi digital dari dua buah citra. Lalu kunci enkripsi e disisipkan menjadi *watermark* bagi citra yang satu, sedangkan kunci dekripsi disisipkan menjadi *watermark* bagi citra lainnya.

AUDIO DIGITAL

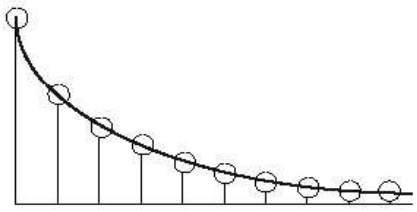
Musik Digital adalah reproduksi suara dari sinyal digital yang telah dirobah keasalnya menjadi sinyal analog, perekaman suara digital dengan cara pengkodean angka biner hasil dari perobahan sinyal suara analog dengan bantuan frekuensi sampling. Musik digital bisa juga berasal dari suara sintetis, contoh peralatan sumber suara sintetis MIDI merupakan sumber suara digital berbagai instrumen musik yang bisa dimainkan oleh pemusik[4].

Bentuk penyimpanan sinyal digital dalam media berbasis teknologi komputer. Format digital dapat menyimpan data dalam jumlah besar, jangka panjang dan berjaringan luas. Musik Digital menggunakan sinyal digital dalam proses reproduksi suaranya. Sebagai proses digitalisasi terhadap format rekaman musik analog, lagu atau musik digital mempunyai beraneka ragam format yang bergantung pada teknologi yang digunakan.

III. METODE PENELITIAN

Penyisipan *Watermarking*

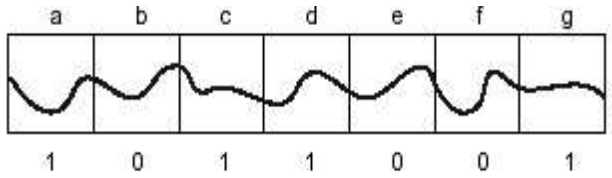
Proses penyisipan *watermark* dapat dinyatakan sebagai sebuah system yang menggunakan satu dari dua kemungkinan system. Dalam domain waktu fungsi dari system merupakan *Discrete Time Exponential* dimana yang membedakan adalah delay antara masing-masing *impulse*[6]. Sebagai contoh misalnya digunakan dua sinyal, sinyal pertama merupakan sinyal asli dari audio dan kedua merupakan RSA. Gambar 2(A) merupakan kernel yang menyatakan fungsi system untuk menyisipkan bit 1 dan gambar 2(B) merupakan fungsi system untuk menyisipkan bit 0. hasil pemrosesan sinyal menggunakan kernel 1 maupun menggunakan kernel 0 akan menghasilkan sinyal seperti gambar 3[6].



Gambar 1. Discrete Time Exponential

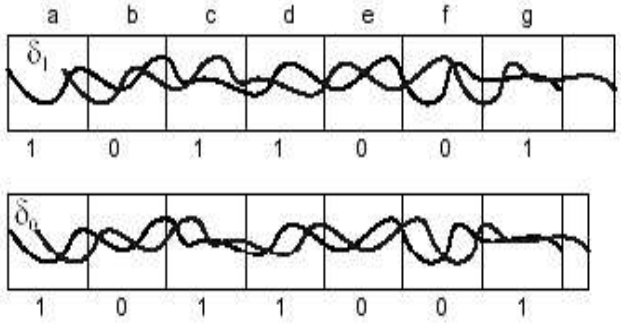
Jarak (δb) antara sinyal asli dengan RSA tergantung dari kernel atau fungsi system mana yang digunakan pada gambar 2. Kernel satu menggunakan jarak (δ1), sedangkan kernel nol memiliki jarak (δ0). Pada penyisipan *watermark* yang terdiri lebih dari 1 bit, sinyal asli dapat dipecah menjadi beberapa bagian kecil. Setiap bagian dapat dilakukan penyisipan dengan bit yang diinginkan dengan

menganggap bahwa bagian kecil tersebut sebagai sinyal independent. Setelah dilakukan proses *encoding RSA* maka bagian-bagian sinyal tersebut digabungkan kembali untuk menghasilkan sinyal awal.



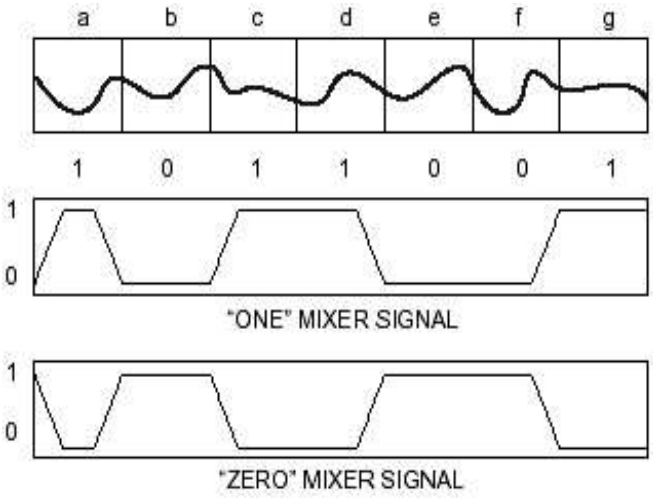
Gambar 2. Sinyal awal yang dipecah menjadi beberapa bagian

Sebagai contoh pada gambar 4 sinyal asli dibagi menjadi tujuh bagian yang diberi label a, b, c, d, e, f, dan g. PAda bagian a, c, d dan g akan disisipkan bit 1. Untuk itu akan digunakan kernel 1 sebagai fungsi system pada setiap bagian tersebut. Demikian sebaliknya bit 0 akan disisipkan pada bagian b, e, dan f maka akan digunakan kernel 0 sebagai fungsi system pada bagian tersebut. Untuk mencapai hasil yang tidak dapat didengar oleh pendengaran manusia, maka dapat dibuat sinyal RSA 1 dengan melakukan pembuatan RSA pada sinyal asli menggunakan kernel 1 dan membuat sinyal RSA 0 dengan menggunakan kernel 0 sebagai fungsi system terhadap sinyal asli. Hasil dari sinyal-sinyal tersebut dapat dilihat pada gambar 5.

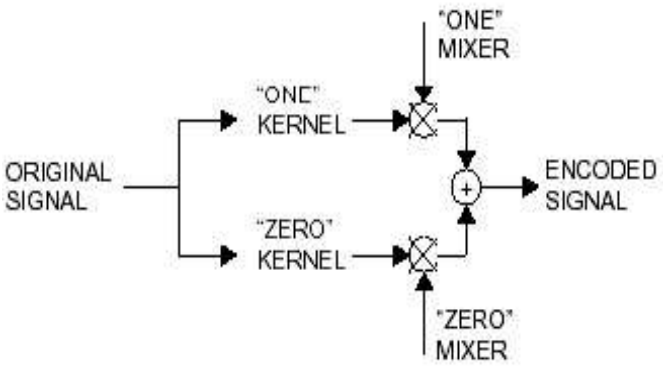


Gambar 3.Pembuatan sinyal RSA 1 dan sinyal RSA 0

Untuk menggabungkan dua sinyal tersebut, maka dibuat dua sinyal *mixer*. Sinyal *mixer* terdiri dari nol dan satu tergantung dari bit yang ingin disembunyikan pada bagian sinyal asli.Sinyal *mixer* 0 kemudian dikalikan dengan sinyal RSA 0 sedangkan sinyal *mixer* 1 dikalikan dengan sinyal RSA 1., kemudian kedua hasil tersebut dijumlahkan. Sebagai catatan bahwa sinyal *mixer* 0 merupakan komplemen dari sinyal *mixer* 1 dan transisi antara masing-masing sinyal adalah bertahap atau melandai. Jumlah antara dua sinyal *mixer* tersebut selalu 1. Ini akan memberikan transisi yang halus antara masing-masing bagian yang dikodekan dengan bit yang berbeda, dan mencegah perubahan yang mencolok pada hasil gabungan sinyal.



Gambar 4. Sinyal *mixer*

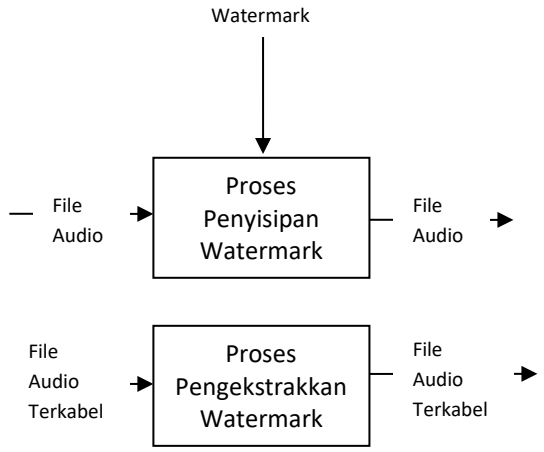


Gambar 5. Proses *encoding*

Gambaran Umum Sistem

Sistem *watermarking* terbagi atas dua bagian yaitu proses penyisipan *watermark* dan proses pengekstrak *watermark*. Penyisipan watermark adalah proses pelabelan file audio dimana pada file audio tersebut akan dimasukkan watermark, sedangkan pengekstrakkan watermark merupakan proses pengambilan watermark dari file audio sesuai dengan metode watermarking yang digunakan pada satu penyisipan watermark.

Pada bagian penyisipan watermark sebagai masukan adalah berkas audio dengan format WAV dan pesan watermark, dimana proses ini akan menghasilkan berkas audio yang telah berisi watermark atau dapat disebut berkas audio terlabel, sedangkan pada proses ekstraksi watermark sebagai masukkannya adalah berkas audio terlabel atau yang memliki watermark dan keluaran adalah pesan atau watermark yang terdapat dalam berkas audio tersebut. Dan dapat dilihat pada gambar dibawah



Gambar 6. Gambaran umum sistem perangkat lunak watermarking

IV. HASIL DAN PEMBAHASAN

Pengujian Penyisipan Menggunakan RSA Dan MSB

Pengujian penyisipan dan ekstraksi watermark menggunakan metode RSA dilakukan dengan cara melakukan proses penyisipan watermark pada berkas suara kemudian dilakukan pengekstrakkan kembali terhadap watermark yang disisipkan sebelumnya. Proses *watermarking* menggunakan metode RSA dipengaruhi oleh nilai amplitude yang digunakan pada saat penyisipan, sehingga untuk membuktikan hak tersebut, pada pengujian ini dilakukan penyisipan *watermark* dengan menggunakan nilai amplitudo yang berbeda yaitu dari pembangkitan robustness menggunakan RSA pada audio digital adalah:

1. Memilih sembarang dua bilangan prima untuk dienkripsi terkebih dahulu sebelum disisipkan ke dalam audio digital, lalu ambil representasi nilainya sebagai bilangan prima. Contoh

   17 dan 11

   Didapatkan hasil :

   n = a x b
   =17 x 11
   = 187
   m = (a-1) x (b-1)
   = 16 x 10
   = 160
   Sebuah bilangan bulat untuk kunci public (e) yang relative prima terhadap m (GCD e, m = 1)

   (e, 160) = 1
   e = 3
   Kunci dekripsi, d, dengan kekongruenan ed ≡ 1 (mod m).

   3 (?) mod 160 = 1
   3 (107) mod 160 = 1
   d = 107

   Masukkan kata yang akan di enkripsi yaitu ABCD

   Representasi nilainya adalah [67 73 78 79]

   C1 = P1e mod n
   = 673 mod 187
   = 67
   = C
   C2 = P2e mod n
   = 733 mod 187
   = 57
   = 9
   C3 = P3e mod n
   = 773 mod 187
   = 66
   = B
   C4 = P4e mod n
   = 793 mod 187
   = 107
   = k

   Hasil kata yang sudah dienkripsi adalah C9Bk diambil nilai bit untuk disisipkan ke audio melalui MSB.

   Pesan ABCD --> C9Bk

   MSB (Most Significant Bit)

   C = 0100 0011

   9 = 0011 1001

   B = 0100 0010

   k = 0110 1010

   Diasumsikan sebuah file audio dengan kumpulan bit sebagai berikut.

   01000101001001001111010110111010010101001010101001010100100010100100111101011011010010101001010100101010010101010010

   Bagi menjadi 4 bit per bagian.

   0100 0101 0010 0100 1111 0101 1011 1010 0101 0100 1010 1010 0101 0101 0100 1010

   0100 0101 0010 0100 1111 0101 1011 1010 0101 0100 1010 1010 0101 0101 0100 1010

   Lakukan penyisipan pada awal bit-bit.

   bit 1 = 0100 --> 0100
   bit 2 = 0101 --> 1101
   bit 3 = 0010 --> 0010
   bit 4 = 0100 --> 0100
   bit 5 = 1111 --> 0111
   bit 6 = 0101 --> 0101
   bit 7 = 1011 --> 1011
   bit 8 = 1010 --> 1010
   bit 9 = 0101 --> 0101
   bit 10 = 0100 --> 0100
   bit 11 = 1010 --> 1010
   bit 12 = 1010 --> 1010
   bit 13 = 0101 --> 1101
   bit 14 = 0101 --> 0101

bit 15 = 0100 --> 0100
bit 16 = 1010 --> 1010
bit 17 = 0100 --> 0100
bit 18 = 0101 --> 1101
bit 19 = 0010 --> 0010
bit 20 = 0100 --> 0100
bit 21 = 1111 --> 0111
bit 22 = 0101 --> 0101
bit 23 = 1011 --> 1011
bit 24 = 1010 --> 0010
bit 25 = 0101 --> 0101
bit 26 = 0100 --> 1100
bit 27 = 1010 --> 1010
bit 28 = 1010 --> 0010
bit 29 = 0101 --> 1101
bit 30 = 0101 --> 0101
bit 31 = 0100 --> 1100
bit 32 = 1010 --> 0010

Dari proses kriptografi dan watermarking sebelumnya, diperoleh deret biner audio digital baru sebagai berikut : 0100 1101 0010 0100 0111 0101 1011 1010 0101 0100 1010 1010 1101 0101 0100 1010 0100 1101 0010 0100 0111 0101 1011 0010 0101 1100 1010 0010 1101 0101 1100 0010

V. KESIMPULAN

Didapat kesimpulan dari perhitungan diatas yaitu meningkatnya *robustness* watermarking pada audio digital dengan memanfaatkan metode kriptografi RSA dan disisipkan kedalam file audio menggunakan metode MSB atau *Most Significant Bit*. Hal ini terbukti dapat meningkatkan *robustness* pada *watermarking* audio digital, dimana hal ini dapat menjadi salah satu cara untuk menentukan kepemilikan audio digital yang pertama kali tanpa harus merusak kualias dari audio itu sendiri

DAFTAR PUSTAKA

[1]. Deltika, C. A., Budiman, G., & Novamizanti, L. (2017). Perancangan Audio Watermarking Dengan Teknik Dwt-Histogram Yang Diterapkan Pada Aplikasi Web.

[2]. Patil, M., & Chitode, J. S. (n.d.). Improved Technique for Audio Watermarking Based on Discrete Wavelet Transform. 2(5),

[3]. Piarsa, I. N., & Dharmadi, I. M. A. (2010). IMPLEMENTASI WATERMARKING PADA SUARA DIGITAL DENGAN METODE DATA ECHO HIDING.

[4]. Pradana, G. K., & Ardian, Y. (n.d.). PENERAPAN TEHNOLOGI SOUNDFONT PADA MIDI KEYBOARD.

[5]. Pratiwi, F. (2018). PENGAMANAN FILE AUDIO DENGAN MENGGUNAKAN ALGORITMA RIVEST SHAMIR ADLEMAN DAN METODE MODIFIED LEAST SIGNIFICANT BIT RED CHANNEL.

[6]. Reddy, P. R. (2009). Robust Digital Watermarking of Color Images under Noise attacks.

[7]. Sihotang, H. T., Efendi, S., Zamzami, E. M., & Mawengkang, H. (2020). Design and Implementation of Rivest Shamir Adleman's (RSA) Cryptography Algorithm in Text File Data Security. Journal of Physics: Conference Series, 1641, 012042. https://doi.org/10.1088/1742-6596/1641/1/012042

[8]. Sitorus, S. H., & Ristian, U. (2020). PERBANDINGAN STEGANOGRAFI METODE LEAST SIGNIFICANT BIT+3 (LSB+3) DENGAN MOST SIGNIFICANT BIT (MSB). 08(01).

[9]. Wong, N. P., Cahyadi, W., Mikroskil, S., & No, J. T. (2012). RANCANG BANGUN APLIKASI WATERMARKING PADA GAMBAR DENGAN ALGORITMA DIGITAL SEMIPUBLIC. 13(2).

[10]. Y.Jani, Y., J. Parmar, Y., & J. Kavathiya, C. (2014). A Review on New Technique for Embedding Image into Audio as a Watermark using DCT. International Journal of Computer Applications, 88(9), 19–22. https://doi.org/10.5120/15381-3812