JATIKOM: Jurnal Aplikasi dan Teori Ilmu Komputer | ISSN: 2615-577X (Online)

https://ejournal.upi.edu/index.php/JATIKOM

IMPLEMENTASI ALGORITMA BLOCK CIPHER 3 DAN RSA DALAM MENGENKRIPSI DATA HAK CIPTA YANG DISISIPKAN PADA AUDIO MP3 MENGGUNAKAN METODE *LEAST SIGNIFICANT BIT*

Judul Inggris

Ariswara[1], Rizky Rachman Judhie[2], Muhamad Nursalman[3]

Prodi Ilmu Komputer Departemen Ilmu Komputer Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam

Universitas Pendidikan Indonesia

Bandung, Indonesia

[1]ariswara@student.upi.edu, [2]rizky_rjp@upi.edu, [3]mnursalman@upi.edu

Abstrak— **Penyalahgunaan data hak cipta sering terjadi pada era digital sekarang, dimana mendapatkan informasi sangat mudah sehingga untuk memanipulasi informasi sangat mudah juga, terutama penyalahgunaan data hak cipta pada media yang sering dipakai seperti lagu. Oleh karena itu dibutuhkan sebuah *software* atau alat yang dapat mengamankan data hak cipta, salah satunya adalah *software* yang memiliki fungsi dalam mengenkripsi data hak cipta menggunakan metode kriptografi. Pada penelitian ini metode yang dipakai dalam mengenkripsi data hak cipta adalah metode kriptografi RSA dan BC3, dimana RSA merupakan metode kriptografi asimetris yang menghasilkan dua kunci berbeda yatu kunci publik dan privat, pada metode ini data hak cipta akan di proses menggunakan dua buah bilangan prima, sedangkan BC3 merupakan metode kripografi simetris yang menghasilkan kunci privat saja, dengan menggunakan dua buah metode kriptografi maka data hak cipta memiliki keamanan ganda sehingga dapat menjamin kemanan data hak cipta, setelah dienkripsi data hak cipta akan lebih aman dan mudah di akses jika data hak cipta di masukan kedalam media yang memiliki data hak cipta tersebut, maka dari itu metode LSB sangat memudahkan untuk fungsi tersebut, dimana metode LSB akan menyisipkan data hak cipta kedalam media. Hasil pengujian enkripsi dan dekripsi data hak cipta lagu menggunakan metode BC3 dan RSA menunjukan bahwa data sangat sensitif terhadap perubahan,sehingga menjamin kerahaisaan data, begitupun data hak cipta dapat diekstrak dari *Stegano File* yang berupa *file* audio menggunakan metode LSB. Dapat disimpulkan bahwa *software* yang dibangun dapat mengamankan data hak cipta lagu.**

Kata Kunci: *RSA , BC3 , LSB , kriptografi*

I. PENDAHULUAN

Pemanfaatan Teknologi Informasi dan Komunikasi semakin berkembang pesat pada abad 21, hal itu ditandai dengan dimana pada abad ini informasi dan komunikasi bukan suatu hal yang sulit untuk didapatkan [1]. Salah satu pemanfaatan Teknologi Informasi dan Komunikasi adalah pemanfaatan data digital baik yang berupa teks,gambar,video.

Hak cipta yang merupkan salah satu data digital yang sering digunakan oleh masyarakat, dan biasanya berupa sebuah berkas teks. Penggunaan data digital sebenarnya rawan terkena penyalahgunaan ,hal itu disebabkan karena dengan mudahnya konten digital yang dapat dipertukarkan melalui Internet sehingga mengakibatkan masalah pelanggaran, termasukan pelanggaran hak cipta [2]. Salah satu pelanggaran hak cipta adalah penyalinan tidak resmi dalam skala besar, dan ini menjadi perhatian besar bagi industri musik, penerbitan film, buku, dan perangkat lunak [3] . Ditambah dengan perkembangan Teknologi Informasi yang kian pesat mengakibatkan lebih banyak perangkat lunak pengolah media yang kuat dan komputer pribadi yang lebih cepat, hal tersebut menghadirkan tantangan untuk melindungi data hak cipta yang mana biasanya permasalahannya adalah tentang penyalinan dan distribusi digital tanpa izin [4].

Salah satu pemanfaatan hak cipta yang paling banyak adalah di industri musik,hal itu ditandai dengan dimulainya penggunaan hak cipta pada tahun 1980an, yang mana pada saa itu Perusahaan musik tidak lagi terorganisir untuk

menghasilkan suatu karya cipta dengan sembarang,tetapi bergantung pada pertimbangan pembuatan hak cipta,karena pada waktu itu karya musik mulai identik dengan hak cipta [5]. Namun sama hal nya dengan hak cipta pada umumnya,hak cipta pada industri musik sangat rentan sekali dengan penyalahgunaan,hal itu dapat dilihat mengapa pada tahun 1980an dimulainya era hak cipta pada industri musik,karena itu disebabkan oleh peristiwa dimana pada tahun 1985 yaitu negara -negara seperti Brasil, Columbia, Meksiko dan Taiwan dilaporkan mempunyai kaset bajakan yang terdiri dari 100% total pasar industri musik mereka [6], kenapa bisa seperti itu,hal tersebut tidak terlepas dari lemahnya keamanan hak cipta pada penggunaan kaset yang mana pada tahun 1985 masih banyak masyarakat yang menggunakan kaset sebagai media musik dibandingkan media lain seperti CD [7]. Apalagi pada era sekarang yang mana konsumsi musik sangat berpengaruh degan penggunaan internet,bahkan pada tahun-tahun sebelumnya,sebelum pengguna internet tahun lalu yang mencapai 3,6 miliar [8] ,pada tahun 2005 pengguna internet yang masih ratusaan juta yaitu 533 juta [9] ,pada waktu itu penjualan musik rugi US$ 3,1 miliar(tiga koma 1 milar dollar Amerika) pada tahun 2005,hal itu disebabkan karena pelanggaran hak cipta [10] , bahkan pelanggaran hak cipta musik sangat besar bagi negara-negara berkembang seperti negara Indonesia dimana penyalahgunaan musik secara ilegal pada tahun 2017 mencapai 84% [11]. Salah satu pelanggaran hak cipta pada industri musik adalah proliferasi klaim pelanggaran hak cipta terhadap musisi seperti Robin Thicke, Justin Bieber, dan Bruno Mars,dimana kasus-kasus mereka adalah jeleknya regulasi dalam penanganan hak cipta musik yang menjadi pengingat betapa buruknya penggunaan hak cipta pada media yang satu ini,dan ada juga Gilbert O'Sullivan, yang menuntut hak cipta kepada Rapper Biz Markie untuk penggunaan tiga kata dan sebagian dari musik dari lagunya "Alone Again (Naturally)," [12].

Untuk mengatasi kelemahan pada penggunaan hak cipta, maka dibutuhkan sebuah teknik atau metode yang aman. Salah satu metode yang paling terkenal adalah metode dimana data atau informasi dapat disisipkan pada sebuah format multimedia atau biasa disebut dengan metode Steganografi. Steganografi (steganography) adalah teknik atau seni untuk menyembunyikan sebuah pesan rahasia di dalam sebuah *file* multimedia sehingga keberadaan pesan rahasia tersebut tidak dapat di akses oleh orang lain yang tidak mempunyai kewenangan [13]. Atau bisa dikatakan Steganografi adalah sebuah metode dimana data penting (misalnya. pin identitas) dapat diimplementasikan kedalam sebuah media yang pada umumnya digunakan masyarakat(mis. fingerprint) tanpa pihak ketiga ,yang mana media tersebut dapat dibagikan kesiapapun tanpa memperlihatkan bahwa informasi tersembunyi itu ada [14] .Dalam metode Steganografi yang berbasis audio terdapat beberapa teknik dalam penyisipan pesan, salah satunya adalah metode Least Significant Bit atau biasa dikenal LSB yang merupakan cara paling sederhana untuk menanamkan informasi dalam sebuah *file* audio digital dengan mengganti bit paling tidak berpengaruh dari setiap titik pengambilan sampel dengan mengubah biner pada *file* tersebut [15].

Tetapi hanya dengan penyisipan data hak cipta pada MP3 atau berkas audio saja tidak akan menjamin pesan tersebut aman dari luar. Yang nantinya berakibat akan penyalahgunaan hak cipta ,hal itu bisa saja terjadi karena steganografi rentan terhadap serangan analisis statistik dan proses steganalisis [16]. Untuk mencegah hal tersebut penulis menggunakan metode Blok Cipher untuk mengenkripsi data pesan tersebut sebelum disisipkan kedalam *file* MP3. Blok Cipher adalah algoritma deterministik pada kumpulan atau sekelompok bit dengan panjang tetap, yang mana sekumpulan bit ini disebut Blok [17]. Namun dengan pesatnya perkembangan teknologi informasi, Blok Cipher mudah akan serangan dari luar,salah satunya adalah karena Blok Cipher versi awal (DES) hanya mendukung kunci dengan panjang 64 bit [17].

Oleh karena itu dalam proposal ini menggunakan Blok Cipher versi terbaru sebagai metode enkripsinya,yaitu Blok Cipher 3.Blok Cipher 3 adalah algoritma Blok Cipher yang cukup mirip dengan AES dan Camellia ,hal itu karena Blok Cipher 3 dikembangkan dengan dua pertimbangan,pertama pertimbangan akan keamanan atau ketahanan Blok Cipher terhadap serangan dari luar dan yang kedua adalah efisiensi implementasi dari Blok Cipher 3 [18].Blok Cipher 3 mendukung kunci sampai 128 bit atau lebih [18],oleh karena itu dalam proposal ini menggunakan Blok Cipher versi ini karena lebih aman dan efisien digunakan.

Setelah dienkripsi data tersebut,dan disisipkan kedalam *file* MP3,itu tidaklah cukup untuk mengamankan data pesan/hak cipta ,maka diperlukan lah perlindungan ganda menggunakan sebuah metode dimana kunci dari data tersebut dapat diamankan ,salah satunya adalah dengan metode enkripsi asimetris RSA. RSA adalah salah satu metode enkripsi asimetris yang paling banyak digunakan di seluruh dunia, algoritma ini pada awalnya dikembangkan oleh Ron Rivest, Adi Shamir dan Leonard Adleman [19], pada tahun 1987 dan nama RSA muncul dengan menggunakan nama keluarga mereka [20],metode ini juga dikenal sebagai algoritma kunci publik, dimana menjadi sangat populer karena kesederhanaannya dalam perhitungan [21].Kelebihan dari metode ini adalah perhitungan untuk meng generate kunci dengan mudah namun sulit dipecahkan hal itu membuat metode ini sangat banyak digunakan karena dengan keadaan seperti itu keamanan sebuah data akan terjaga,karena sulitnya komputasi memfaktorkan produk dari dua bilangan bulat utama besar (jika ingin membobol algoritma ini) [22] ,RSA juga merupakan salah satu algoritma kriptografi yang handal melawan malware pada sebuah sistem komputer [23],adapun tahapan enkripsi Algoritma ini secara garis besar adalah dimulai dari pembangkitan kunci, enkripsi kunci publik, dan kunci pribadi /*Private* Key [24].

Setelah selesai menggunakan semua metode yang ada diatas maka data pesan atau hak cipta pun sangat aman. Pada proposal kali ini mengapa membahas tentang mengamankan hak cipta,hal itu karena seperti dikatakan diatas MP3 adalah salah satu format multimedia paling populer terutama untuk mengkonsumsi musik . Ada miliaran MP3 yang tersebar di laptop, ponsel, tablet, dan pemutar MP3 lainnya di Dunia. Pada tahun 2014, di di Amerika saja, 1,1 miliar lagu yang berformat MP3 dibeli berdasarkan bayar per unduh dan 164 miliar dialirkan melalui langganan berbayar bulanan dan langganan yang didanai iklan [25]. Bayangkan saja jika ada orang yang curang memanipulasi hak cipta lagu seseorang

,maka bisa dipastikan orang tersebut mendapatkan keuntungan yang sangat besar.

II. PENELITIAN TERKAIT

Penelitian terkait pertama adalah penelitian yang berjudul "Implementation of Low Bit Coding Algorithm and Cipher Block with Electronic Code Book Mode for Data Legality in Audio Steganographic Streaming " yang mana mengamankan data hak cipta buku pada format mp3 menggunakan Block Cipher [26] ataupun penelitian yang kedua berjudul "IMPLEMENTASI ALGORITMA KRIPTOGRAFI RC4 DAN METODE STEGANOGRAFI AUDIO 2LSB PADA SISTEM KEAMANAN INFORMASI" dimana pada penelitian ini yang menjadi fokus utamanya adalah melihat bagaimana pesan apapun itu, aman dengan di enkripsi terlebih dahulu menggunakan algorimta RC4 dan disisipkan menggunakan 2LSB yang nantinya dimasukan kedalam berkas audio [27].

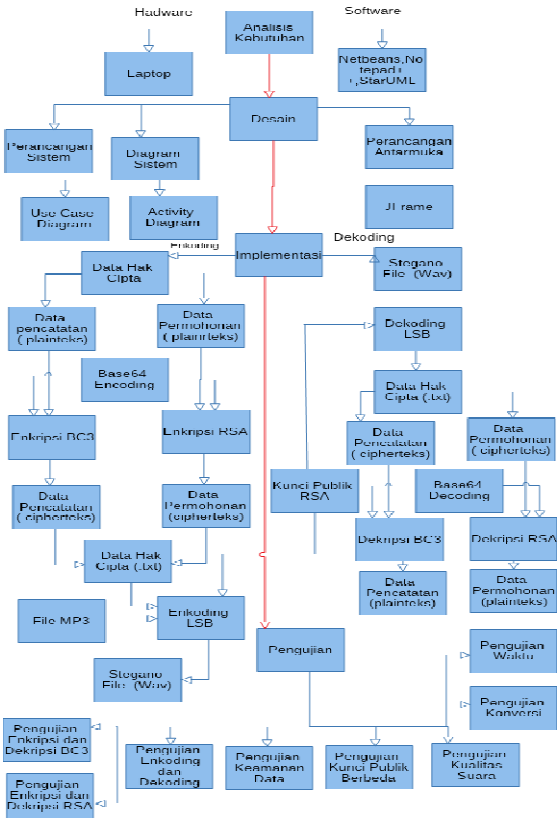
Adapun dalam penelitian ini menggunakan dua metode kriptografi yaitu RSA dan BC3 dan untuk menyisipkan pesan atau hak cipta yang terenkripsinya tersebut menggunakan metode steganografi yaitu LSB,jika dibandingkan dengan dua penelitian yang diatas,penelitian ini memiliki kelebihan yaitu dari yang penelitian pertama penelitian ini sangat jauh lebih aman karena menggunakan dua teknik kriptografi dalam pengenkripsiannya, adapaun versi block cipher nya pun sudah versi yang mana merupakan versi terbaru setelah block cipher 2 [18], untuk penelitian kedua pun hampir sama penelitian ini menggunakan satu teknik kriptografi simetris yaitu RC4 yang mana masih lebih baik BC3 karena BC3 efisiensi algoritmanya 4x lebih cepat dari pada AES sedangkan untuk RC4 hanya 20% lebih cepat dibandingkan AES [28] ditambah dengan keamanan RSA yang mana lebih aman daripada RC4 (Akinyele A Okedola, 2015) sedangkan untuk teknik 2LSB lebih bagus daripada LSB karena daya tampungnya lebih besar [28], namun karena penelitian ini menggunakan data hak cipta lagu yang mana tidak terlalu besar maka LSB lebih cocok karena lebih efisien penggunaannya dibandingkan 2LSB.

III. METODE PENELITIAN

Metode penelitian yang dipakai dalam peneltiian ini adalah metode penelitian studi literatur dan metode pengembangan sistem.

Metode penelitian studi literatur dilakukan setelah menganalisis metode yang akan dipakai dalam penelitian ini seperti proses enkripsi RSA,BC3 ataupun proses dekripsi RSA,BC3 hingga bagaiamana proses penyispan data menggunakan metode LSB,ditambah juga refrensi dari skripsi yang temanya sama,dan ada juga beberapa buku,website,atau di forum-forum yang ada di internet dengan tema keamanan data digital.

Metode pengembangan sistem yang dipakai untuk penelitian ini adalah dengan metode *Waterfall* dimana tahapan-tahapannya adalah dimulai dari analisis kebutuhan,desain,implementasi dan terakhir adalah pengujian. Hal itu bisa dilihat pada gambar 1 dibawah ini :



Gambar 1. Alur Sistem

A. *Analisis Kebutuhan*

Tahap awal adalah menganalisis kebutuhan apa saja yang dibutuhkan selama penelitian ini berlangsung,dimulai dari bagian Software ada :

1. Neatbens ,aplikasi ini untuk implementasi algoritma dan membuat aplikasi.
2. StarUML , untuk membuat diagram-diagram UML.
3. Notepad++ ,untuk pengecekan algoritma,lebih tepatnya untuk efisiensi pengecekan.

Adapun untuk Hadware yang dibutuhkan untuk implementasi penelitian ini yaitu :

1. Laptop dengan spesifikasi (Prosesor min i3 dengan kecepatan Min 2.00Ghz,dan RAM 4GB).

B. *Desain*

Tahapan ini merupakan tahapan yang mana menggambarkan bagaiamana sistem bekerja dan bagaiamana alur kerjanya . Untuk penjabaran dari tahapan ini akan dibagai menjadi 3 yaitu dimulai dari perancangan sistem,diagram sistem dan perancangan antarmuka sistem.

1.) Perancangan Sistem

Perancangan sistem penelitian ini mempunyai tujuan bagaiamana caranya mengamankan data hak cipta kedalam *File* audio MP3,terutama data hak cipta lagu. Dari masalah tersebut maka dibuatlah suatu sistem yang mana

menggunakan dua buah algoritma dalam mengenkripsi data hak cipta lagu.

Dua algorimta kriptografi yang digunakan adalah BC3 dan RSA, yang merupakan jenis kriptografi berbeda satu sama lain yaitu simetris (BC3) dan asimetirs (RSA), kedua buah algoritma digunakan dalam mengenkripsi data hak cipta lagu yang mana untuk data permohonan akan dienkripsi menggunakan RSA dan data pencatatan akan menggunakan algoritma BC3, setelah semua data di enkripsi maka *user* harus membuat sebuah *file* text yang mana nantinya akan diisikan data permohonan dan data pencatatan yang telah dienkripsi. Setelah membuat data hak cipta (.txt) maka langkah selanjutnya adalah menyisipkan data tersebut kadalam *file* mp3 menggunakan algoritma LSB.

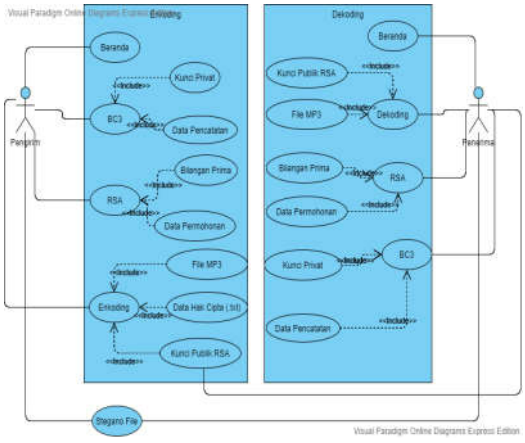
Dimana pada proses penyisipan user diminta untuk memasukan *password* yang mana bisa berupa kunci publik RSA. Setelah proses enkoding maka akan menghasilkan *file* stegano yang berformat wav. Langkah selanjutnya adalah mengekstrak stegno *file* tadi menggunakan algoritma LSB, dan menggunakan kunci publik RSA, setelah di ekstrak atau didekoding maka akan menghasilkan data hak cipta(.txt) setelah itu dilakukun proses dekripsi pada masing-masing algoritma kriptografi.

2.) Diagram Sistem

Pada pembuatan diagram sistem pada penelitian ini menggunakan *use case* diagram dan *activity diagram*.

- *Use case Diagram*

  Dalam *Use Case Diagram* akan menjalaskan bagaimana pengguna menggunakan sistem. Pada sistem ini ada dua skema proses yaitu skema untuk pengirim sebagai yang mengenkripsi pesan dan skema untuk penerima,yang mana sebagai pendekripsi data hak cipta, hal itu dapat terlihat pada Gambar 2.



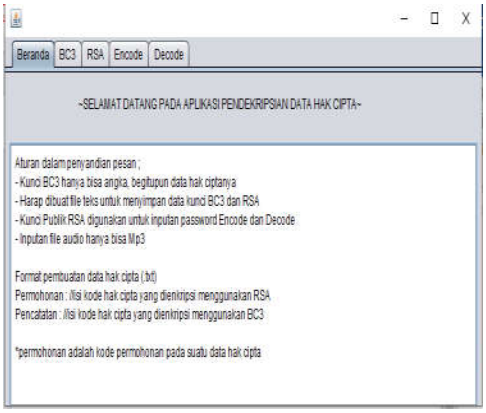
Gambar 2. *Use Case Diagram*

- *Activity Diagram*

  Pada diagram ini merupakan diagram yang berfungsi untuk menggambarkan aliran kerja dari proses yang ada di *Use Case Diagram* pada Gambar 2 Diagram ini terdapat dua bagian yaitu bagian pengirim dan penerima.

3.) Perancangan antarmuka

Perancangan antarmuka pada penelitian menggunakan aplikasi Jframe yang ada pada Netbeans, pada aplikasi ini terdapat 5 menu utama yaitu beranda,BC3,RSA,Enkoding,dan terakhir Dekoding. Adapun salah satu contoh menu antarmuka pada Beranda dapat dilihat pada Gambar 3.



Gambar 3. Antarmuka Beranda

C. Implementasi

Implementasi penelitian ini adalah menggunakan metode steganografi kritografi dimana untuk mengamankan data hak cipta yang terutama untuk mengamankan data hak cipta sebuah lagu jadi penggunaan formatnya dalam aplikasi ini adalah MP3,karena lagu banyak menggunakan format ini.

Adapaun dalam implementasinya pengguna harus memiliki dulu data hak cipta yang kemudia nanti setelah di enkripsi menggunakan BC3 dan RSA dibuat *File* (.txt) yang nantinya akan disisipkan kedalam *File* Audio (.mp3) dimana akan menghasilkan Stego Audio dan setelah itu baru di dekripsi kembali dengan algoritma BC3 dan RSA.

Untuk implementasi algoritmanya penelitian menggunakan bahasa Java yang diimplementasikan menggunakan *Software* Notepad ++ dan Neatbens ,dimana jika Notepad++ guna untuk efisiensi implementasi algoritma,karena dengan Neatbens biasanya lebih lama memuat data nya,dan setelah bekerja algoritmanya baru kemudian di implementasikan di Neatbens sekalian dengan pembuatan Interface aplikasinya.

Adapun implementasi pada penelitian ini ada dua skema secara garis besar, yaitu skema untuk pengirim dan skema untuk penerima.

Skema pertama yaitu skema pengirim bisa disebut juga skema enkripsi karena pada proses ini data akan di enkripsi dan dimasukan kedalam *stego file*, pada awal proses pengirim akan mengenkripsi data hak cipta yang mana dibagi menjadi dua yaitu data hak cipta pencatatan yang akan di enkripsi menggunakan algoritma BC3, dan data hak cipta permohonan yang menggunakan algoritma RSA.

Pada proses enkripsi dengan algoritma BC3 pengirim akan memasukan 4 buah kunci privasi dan setelah

memasukan data hak cipta pencatatan. Hasil proses enkripsi BC3 akan di enkripsi kembali oleh Base64, begitupun dengan proses enkripsi RSA, yang membedakan adalah pada saat proses enkripsi RSA yang dibutuhkan adalah bilangan prima untuk membentuk kunci privat,kunci publik dan modulus,selebihnya hampir sama dengan proses BC3.

Setelah di enkripsi maka pengirim wajib membuat *file* teks untuk menampung data hak cipta tersebut, atau kunci privasi,kunci publik dan modulus, setelah dibuat data hak cipta yang berupa teks, maka langkah selanjutnya adalah memasukan data hak cipta kedalam *file* audio menggunakan algoritma LSB. Pada proses ini pengrim akan memasukan *file* audio yang berformat (.mp3) dan *file* hak cipa yang berformat (.txt) setelah itu pengirim akan memasukan *password* yang mana merupakan kunci publik RSA. Setelah itu pengirim akan mengklik tombol enkoding dan akhirnya menghasilkan *stego file* yang berformat (.wav)

Skema kedua adalah skema penerima atau bisa disebut juga kema dekripsi, karena pada skema ini penerima akan mendekripsi *stegano file* ataupun data hak cipta.

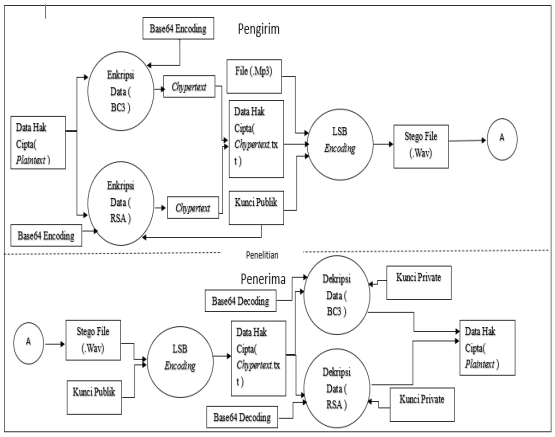
Langkah awal adalah penerima akan memasukan *stegano file* dan kemudaian memasukan *password* kembali yang berupa kunci publik RSA. Setelah itu barulah menghasilkan data hak cipta (.txt), jika *password* yang dimasukan benar maka proses enkripsi data hak ciptanya akan benar dan data hak cipta yang ditampilkan dalam *file* sama dengan sebelumnya, namun jika salah maka yang akan ditampilkan adalah data yang salah.

Langkah kedua setelah mendapatkan data hak cipta (.txt) pengirim dapat mengenkripsi data yang ada pada *file* teks tersebut sesuai dengan nama data hak cipta, jika pencatatan maka dekripsi menggunakan BC3 yang mana harus memasukan kunci privasi kembali,namun jika data permohonan maka akan menggunakan RSA yang membutuhkan kunci privasi dan modulus untuk proses dekripsi, jika kedua data hak cipta sudah di dekripsi maka akan menghasilkan data hak cipta yang asli.

D. Pengujian

Tahap pengujian adalah tahap akhir untuk memastikan seluruh kebutuhan sistem telah terpenuhi dan diimplementasikan,dalam tahap ini selain menguji akan mengidentifikasi kekurangan pada aplikasi atau sistem ataupun melihat bagaimana implementasi berjalan dengan baik dan sesuai dengan rumusan masalah yang ada dalam penelitian. Adapaun rencana pengujian pada sistem ada 8 yaitu pengujian enkripsi dan dekripsi BC3, pengujian enkripsi dan dekripsi RSA, pengujian penyisipan dan ekstrasi pesan menggunakan LSB, pengujian kemanan data yang mana akan memodifikasi hasil enkripsi oleh kedua buah algoritma dan dicek apakah jika dimodifikasi data hak cipta tersebut yang mana berupa cipherteks apakah akan tetap aman, pengujian dekoding menggunakan kunci publik RSA yang berbeda, pengujian kualitas suara, pengujian konversi, dan pengujian waktu untuk berapa lama proses enkripsi dan dekripi pada algoritma BC3 dan RSA dan berapa lama proses untuk enkoding dan dekoding menggunakan algoritma LSB.

IV. HASIL DAN PEMBAHASAN



Gambar 4. Proses implementasi algoritma BC3,RSA dan LSB

Gambar 4 merupakan skema dalam proses implementasi algoritma BC3,RSA,dan LSB dalam mengamankan data hak cipta sebuah lagu. Pada penelitian ini data hak cipta dibagi dua, yaitu data pencatatan dan data permohonan, untuk data pencatatan yang mana bisa di lacak Online sehingga mudah di manipulasi maka pada penelitian pengamanan data itu menggunakan algoritma BC3 karena memiliki keunggualan terhadap serangan, sedangkan untuk data permohonan akan menggunakan algoritma RSA.

Dalam proses enkripsi BC3, algoritma BC3 membutuhkan 4 buah kunci dimana semua inputan harus berupa angka,tidak boleh huruf ataupun simbol,sedangkan untuk proses enkripsi algoritma RSA tidak perlu inputan kunci,karena nanti akan di Generate kunci secara otomatis. Hasil dari enkripsi BC3 akan menghasilkan suatu cipherteks yang mana data tersebut akan di enkode menggunakan metode Base64 sama juga dengan algoritma RSA yang membedakan hanya pada algoritma RSA kunci publik akan dipakai kembali selain dari nanti proses dekripsi, yaitu akan digunakan pada input password untuk mengamankan data Stegano.

Algoritma LSB dalam penelitian ini berfungsi dalam menyisipkan pesan data hak cipta yang berupa cipherteks hasil dari proses enkripsi BC3 dan RSA pada media *file* audio Mp3, namun sebelum disisipkan menggunakan algoritma LSB, *file* data hak cipta yang berformat (.txt) akan di enkripsi menggunakan password yang inputannya merupakan kunci publik dari hasil enkripsi RSA sebelumnya, setelah data hak cipta di enkripsi maka proses selanjutnya adalah penyisipan data pada bit yang tidak signifikan kedalam *file* audio menggunakan algoritma LSB, setelah itu akan menghasilkan Stegano *File* yang berformat (.wav).

Pada proses dekoding Stegano *File* akan diekstrak menggunakan algoritma LSB dimana untuk mengesktrak *file* tersebut membutuhkan password yang berupa kunci publik RSA, setelah selasai mengekstrak maka akan menghasilkan data hak cipta yang berformat teks. Selanjutnya adalah proses dekripsi,untuk data pencatatan akan didekripsi menggunakan algoritma BC3 dan 4 buah kunci, sedangkan untuk data permohanan akan menggunakan algoritma RSA dan kunci *private*.

A. Pengujian Enkripsi dan Dekripsi.

Pengujian ini bertujuan untuk mengetahui apakah implementasi algoritma RSA dan BC3 berjalan dengan baik dalam mengamankan data hak cipta, hal tersebut bertujuan untuk melihat apakah algoritma RSA dan BC3 dapat memenuhi salah satu tujuan dari kriptografi yaitu kerahasian. Pada penelitian ini dilakukan 30 kali percobaan menggunakan algoritam RSA dan 30 kali percobaan menggunkan algoritma BC3. Pengujian ini dilakukan dengan menggunakan kunci publik RSA (3,1081) , kunci privat RSA (675,1081) dan kunci privat BC3 (1993,2007,1006,2020) . Pada penelitian ini hasil dari proses enkripsi dan dekripsi akan menghasilakan cipherteks atau plainteks dengan panjang 32 bit. Adapun hasil pengujian untuk artikel hanya mengambil data dari data 1-3 saja, untuk hasil pengujian algoritma RSA dapat dilihat pada Tabel 1.

Tabel 1.
Hasil Enkripsi dan Dekripsi RSA

No	Plainteks	Bit	Cipherteks	Bit	Hasil Dekripsi	Bit
1	11928491448	34	010011110101 010001011001 011110000100 111101010100 011010110011 000101001110 010101000101 100100110010 010011010111 101001001101 01110111	128	11928491448	34
2	24871249219	35	010011110100 010001001001 001111010100 110101111010 011010110111 011101001110 011010100100 110100110011 010011010111 101001100011 01111010	128	24871249219	35
3	24627841992	35	010011100100 010001100111 001100010100 111001111010 011000110011 110101001101 010101000110 001101111000 010011010111 101001011001 00110100	128	24627841992	35

Pada Tabel 1 dapat terlihat bahwa proses enkripsi dan dekripsi pada algoritma RSA sudah berjalan sangat baik dengan hasil dekripsi sama dengan plainteks. Adapun untuk BC3 dapat dilihat pada Tabel 2.

Tabel 2.
Hasil Enkripsi dan Dekripsi BC3

No	Plainteks	Bit	Cipherteks	Bit	Hasil Dekripsi	Bit
1	1167829173	32	0100101100101 1110010100111 0011001110011 1101001111010 1001100010101 0001000101011 1100101001110 0110101001010 0010111101001 0011010100010	256	1167829173	32
			0010000010111 1000010011100 1111010010110 0100111101			
2	1167829172	32	0100110001010 1000100010100 1100110100110 1010101000100 0001001100000 1001111010101 0001100011011 1011101001111 0100010001000 0010011110101 0011110100010 0010001010111 1001010011110 1000100010110 0101110111010 0111101010100 0100100101111 010	250	1167829172	32
3	1167829171	32	0100111001111 0100101010100 1100100100110 1010001000100 0001001100000 1001101010001 0001101011001 1000101001100 0101010001010 0010111100101 0011100110101 0010001010011 0010010011010 1010100010101 0100110000	192	1167829171	32

Pada Tabel 2. dapat terlihat bahwa pada hasil pengujian algoritma BC3 berjalan baik hal itu ditandai dengan hasil enkripsi yang berbeda dan hasil dekripsi yang sama dengan masukan.

B. Pengujian Proses Enkoding dan Dekoding

Dalam pengujian enkoding dan dekoding menggunakan algoritma LSB, data yang dipakai adalah data hasil enkripsi algoritma BC3 dan RSA yang mana data ke-1 sampai data ke-8 pada masing-masing hasil pengujian enkripsi kedua buah algoritma tersebut, untuk data hak cipta yang menggunakan algoritma RSA adalah data hak cipta pada nomor permohonan sedangkan untuk BC3 adalah data hak cipta nomor pencatatan, data yang dipakai akan dibedakan untuk panjang datanya dan saat dekoding harus memasukan kunci publik RSA yang mana pada penilitian ini menggunkan kunci publik RSA (3,1081). Adapun hasilnya dapat dilihat pada Tabel 3 yang mana data yang ditampilkan adalah hasil pengujian sampai data ke 3.

Tabel 3.

Hasil Enkoding dan Dekoding LSB

No	Data Hak Cipta	Bit	Hak Cipta setelah di Enkoding	Bit	Hasil Dekoding	Bit
1	Permohonan : BAOTYxOTk1NTY2MzMw	248	Sfqnlklmbm#9#ABLWZ{LWh2MWZ1NyNt	248	Permohonan : BAOTYxOTk1NTY2MzMw	248
2	Nomor Permohonan : BAODI=Mz	296	Mlnlq#Sfqnlklmbm#9#ABLGJ>NyhtMiN0Ny`y	296	Nomor Permohonan : BAODI=Mz	296

	kwNjM3Mzcz				kwNjM3Mzcz	
3	Data Permohon : BA NDg1Nzc= MTcxMzY4	272	Gbwb#Sfqnl klm#9#AB# MGd2My`> NW`{NyZ7	280	Data Permohon : BA NDg1Nzc=M TcxMzY4	272

Pada Tabel 3. Terlihat bahwa data hak cipta setalah di dekoding sama dengan data hak cipta setelah di enkoding , yang menandakan berhasilnya proses penyisipan data karena dapat mengambil data yang spesifik pada *file* audio sehingga menghasilkan hasil yang sama dengan data hak cipta sebelumnya, adapun untuk kunci publik RSA berhasil dalam implementasinya, hal itu terlihat bahwa data hak cipta yang ada pada *file* audio berbeda dengan data aslinya,dikarenakan dienkripsi menggunakan kunci publik RSA.

C. Pengujian Keamanan Data

Pada pengujian ini dilakukan modifikasi cipherteks dan cipherkey pada kedua algoritma kriptografi. Dalam modifikasi cipherteks yang dilakukan adalah mengubah 1 bit pertama pada tiap data, dan nanti akan dilihat apakah data sensitif terhadap perubahan tersebut.

Misalkan data ke-1 cipherteks pada hasil enkripsi algoritama RSA adalah “OTYxOTk1NTY2MzMw“ dengan nilai biner “11011111111110110110011101101100111111010” maka nilai biner nya akan diubah 1 bit paling depan jadi : “01011111111110110110011101101100111111010” yang menghasilkan cipherteks : “NDEyMjM5NzUyNDQy”.

Sedangkan untuk modifikasi cipherkey yang diubah adalah kunci pada algoritma RSA dan BC3, pada penelitian ini kunci RSA yang asalnya dari bilangan prima (23,47) diubah menjadi (19,43) sedangkan BC3 dari (1993,2007,1006,2020) menjadi (10,6,19,197).

Adapun hasil pengujian modifikasi cipherteks dapat dilihat pada Tabel 4.

Tabel 4.
Hasil Modifikasi Cipherteks

No	Algoritma	Jumlah Data	Hasil Pengujian	Keterangan	Tujuan
1	RSA	29 dari 29	100%	Sensitif	Terpenuhi
2	BC3	30 dari 30	100%	Sensitif	Terpenuhi
Rata-rata		59 dari 59	100%	Sensitif	Terpenuhi

Ada satu data pada RSA yaitu data ke-9 yang tidak bisa diubah karena jika diubah cipherteks maka nilai biner lebih kecil daripada 11 angka. Sedangkan untuk hasil modifikasi cipherkey dapat dilihat pada Tabel 5.

Tabel 5.
Hasil Modifikasi Cipherkey

No	Algoritma	Jumlah Data	Hasil Pengujian	Keterangan	Tujuan
1	RSA	29 dari 29	100%	Sensitif	Terpenuhi
2	BC3	30 dari 30	100%	Sensitif	Terpenuhi
Rata-rata		59 dari 59	100%	Sensitif	Terpenuhi

D. Penggunaan kunci publik yang berbeda saat dekoding

Pada pengujian ini kunci publik yang digunakan dalam proses dekoding berbeda. Dalam pengujian kunci publik rsa yang digunakan adalah kunci publik(3,1081), namun kali ini akan menggunakan kunci publik rsa(5,817) , hal ini berasal dari masukan bilangan prima yang berbeda yaitu 19 dan 43 yang sebelumnya 23 dan 47. Maka menghasilkan modulus yang berbeda sehingga kunci publiknya pun berbeda, unuk hasilnya dapat dilihat pada Tabel 6.

Tabel 6.
Hasil Pengujian Dekoding denga Kunci Publik RSA berbeda

No	Data Hak Cipta	Dekripsi Asli	Dekripsi Setelah Modifikasi	Keterangan	Tujuan
1	Permohonan : BAOTYxOTk1NTY2MzMw	53 66 71 6E 6C 6B 6C 6D 62 6D 23 39 23 41 42 4C 57 5A 7B 4C 57 68 32 4D 57 5A 31 4E 79 4E 74	56 63 74 6B 69 6E 69 68 67 68 26 3C 26 44 47 49 52 5F 7E 49 52 6D 37 48 52 5F 34 4B 7C 4B 71	Sensitif	Terpenuhi
2	Nomor Permohonan : BAODI=MzkwNjM3Mzcz	4D 6C 6E 6C 71 23 53 66 71 6E 6C 6B 6C 6D 62 6D	4B 6A 68 6A 77 25 55 60 77 68 6A 6D 6A 6B 64 6B	Sensitif	Terpenuhi
3	Data Permohon : BA NDg1Nzc=MTcxMzY4	47 62 77 62 23 53 66 71 6E 6C 6B 6C 6D 23 39 23	48 69 6B 69 74 26 56 63 74 6B 69 6E 69 68 67 68	Sensitif	Terpenuhi

Pada Tabel 6. Terlihat bahwa perubahan pada kunci publik akan mengubah seluruh data . Adapaun hasil pada Tabel 6. hanya menampilkan tiga data.

E. Pengujian Kualitas Suara

Pada pengujian ini dilakukan bertujuan untuk mengetahui apakah *file* audio sama dengan *file* audio yang asli, hal itu dilihat dari nilai LUFS. LUFS (Loudness Unit Full Scale) adalah pengukuran tingkat kenyaringan pada suatu lagu, oleh karena itu jika suatu lagu memiliki tingkat kenyaringan yang sama maka lagu itu jika didengarkan akan terdengar sama. Pengujian dilakukan dengan menggunakan 31 data hak cipta, pada dua audio *file* yaitu lagu Katy Perry – Daises.mp3 dan Katy Perry – Last Friday Night.mp3. Parameter yang digunakan ada tiga yaitu:

1). Momentary Max , yang merupakan pengukuran nilai kenyaringan maksimum selama 400ms.

2). Short Term Max , menunjukan nilai kenyaringan yang diukur selama 3 detik.

3). Integrated , menunjukan kenyaringan rata-rata yang diukur dari awal lagu hingga selesai.

Adapun hasil pengujian dapat dilihat pada Tabel 7. Untuk lagu Daises

Tabel 7.
Hasil Pengujian LUFS 1

Data	*Stegano File*			*File Asli*			Kecocokan
	Momenraty Max	Short Term Max	Integrated	Momenraty Max	Short Term Max	Integrated	
1	4.99	5.80	8.57	4.97	5.78	8.55	99,7%
2	4.99	5.80	8.57	4.97	5.78	8.55	99,7%
3	4.99	5.80	8.57	4.97	5.78	8.55	99,7%

Adapun untuk lagu Last Friday Night dapat dilihat pada Tabel 8.

Tabel 8.
Hasil Pengujian LUFS 2

Data	*Stegano File*			*File Asli*			Kecocokan
	Momenraty Max	Short Term Max	Integrated	Momenraty Max	Short Term Max	Integrated	
1	9.85	10.78	13.92	9.83	10.76	13.92	99,82 %
2	9.85	10.78	13.92	9.83	10.76	13.92	99,82 %
3	9.85	10.78	13.92	9.83	10.76	13.92	99,82 %

Pada Tabel 7 dan Tabel 8 dapat terlihat bahwa kedua buah lagu memiliki keakuratan yang hampir 100% dalam kualitas suara jika dibanidingkan *file* asli.

F. *Pengujian Konversi File*

Pada pengujian ini dilakukan untuk mengetahui apakah jika *file* audio di konversi kedalam format audiolainnya apakah jika nanti di dekoding akan menghasilkan *file* data hak cipta yang sama. Dalam pengujian ini menggunakan dua buah lagu yang nantinya akan dikonversi ke mp3 lalu dikonversikan kembali ke wav dan terakhir di dekoding. Hasil pengujian dapat terlihat pada Tabel 9.

Tabel 9.
Hasil Konversi Audio

No	*Stegano File* (.wav)	Data hak cipta (.txt)	*Stegano File* setelah di konversi (.mp3)	*Stegano File* setelah di konversi (.wav)	Hasil
1.	Katy Perry – Daises.wav	Hc1.txt	Test1.mp3	Test3.wav	Gagal
2.	Katy Perry – Last Friday Night.wav	Hc1.txt	Test2.mp3	Test4.wav	Gagal

Gagal dalam Tabel 9 dimaksud adalah data tidak bisa diproses dalam aplikasi, akan muncul error "java.lang.OutOfMemoryError: Java heap space" hal itu menandakan bahwasannya alokasi memori pada *file* baru dan *file* tidak sama, hal itu dikaranekan proses konversi menyebabkan perubahan pada bit LSB dari *file* stego audio. Perubahan pada bit LSB di mana pesan berada disimpan menyebabkan kerusakan sehingga pesan tidak dapat diekstraksi, yang enyebabkan kesalahan membaca jumlah bit pesan yang dimasukkan sehingga program mendapati kesalahan dan menghentikan proses.

G. *Pengujian Waktu*

Pengujian waktu dilakukan pada proses enkripsi dan dekripsi pada algoritma BC3 dan algoritma RSA, sedangkan pengujian waktu yang lainnya adalah proses enkoding dan dekoding menggunakan algoritma LSB, pengujian waktu ini dilakukan di Netbeans jadi keakuratan waktu pertama tidak 100% karena ada proses aplikais yang cukup lama waktu awal proses.

Adapun data ke-1 pengujian waktu enkripsi RSA dan BC3 dapat dilihat pada Tabel 10 dan Tabel 11.

Tabel 11.
Hasil pengujian lama waktu enkripsi RSA

No	Ukuran Data		Waktu (Milidetik)
	Input	Output	
1	34	128	22,24
2	34	128	2,2061
3	34	128	0,6144
4	34	160	1,6024
5	34	128	0,604
6	34	128	0,5359
7	34	128	0,5363
8	34	128	0,6353
9	34	128	0,7147
10	34	128	0,7226
11	34	128	0,6741
12	34	128	0,5568
13	34	128	0,5274
14	34	128	0,6084
15	34	128	0,6275
16	34	128	0,6656
17	34	128	0,5034
18	34	128	0,4923
19	34	128	0,5038
20	34	128	0,4839
21	34	128	0,6248
22	34	128	0,5418
23	34	128	0,4774
24	34	128	0,4609
25	34	128	0,5968
26	34	128	0,5453
27	34	128	0,4689
28	34	128	0,4911
29	34	128	0,4658
30	34	128	0,4949
Rata-Rata kecepatan enkripsi RSA			1,374087

Tabel 12.
Hasil pengujian lama waktu enkripsi BC3

NO	Ukuran data		Waktu(milidetik)
	Input	Output	
1	32	256	29,49
2	32	250	0,5748
3	32	192	0,4541
4	32	104	0,5117
5	32	96	0,4288
6	32	224	0,4935

7	32	256	0,5459
8	32	256	0,4303
9	32	256	0,6812
10	32	224	0,4441
11	32	256	0,4583
12	32	256	0,4421
13	32	224	0,4299
14	32	256	0,4487
15	32	256	0,4193
16	32	224	0,5042
17	32	256	0,3929
18	32	224	0,533
19	32	256	0,5614
20	32	256	0,3918
21	32	224	0,4419
22	32	192	0,4138
23	32	192	0,4039
24	32	224	0,4091
25	32	256	0,3772
26	32	224	0,6254
27	32	256	0,4108
NO	Ukuran data		Waktu(milidetik)
	Input	Output	
28	32	224	0,3963
29	32	192	0,4077
30	32	256	0,437
Rata-Rata kecepatan enkripsi BC3			1,43197

Pada Tabel 11 dan 12 dapat terlihat bahwa lama waktu enkripsi pada penlitian ini walaupun inputannya sama yaitu 32 bit pada BC3 dan 34 bit pada RSA, tetapi memiliki waktu yang berbeda, karena hal itu disebabkan dalam proses enkripsi yang ke-1 sistem akan memerlukan waktu untuk memproses inputan kunci publik atau privat dan plainteks sehingga memerlukan waktu lebih banyak daripada proses data ke-2 dan selanjutnya , walaupun begitu proses enkripsi pada dua algoritma rata-rata sangat cepat yaitu dibawah 1 milidetik, begitu juga dengan hasil dekripsi pada RSA yang memiliki rata-rata waktu 0,783243 dan untuk lama waktu dekripsi BC3 yaitu 0,530083, pada proses dekripsi waktu yang diperlukan lebih sedikit, hal itu dikarenakan dalam pengujian waktu pada implementasi ini, kunci privasi, kunci publik ataupun modulus tidak dihapus pada *jTextField* yang mengakibatkan proses untuk mendapatkannya lebih sebentar daripada enkripsi yang mana ada proses masukan.

Adapun data ke-1 untuk proses enkoding dan dekoding menggunakan algoritma LSB dapat dilihat pada Tabel 13 dan 14 .

Tabel 13.
Hasil pengujian lama waktu Enkoding

No	Ukuran Data		Waktu (Milidetik)
	Input	Output	
1	248	248	7
2	296	296	52
3	272	280	57
4	280	288	27
5	304	304	56
6	208	208	13
7	264	264	29
8	144	144	47
9	408	408	10
10	328	328	27
11	344	344	45
12	219	219	9
13	416	416	32
14	288	288	53
15	376	376	13
16	256	256	32
17	720	720	58
18	640	640	22
19	656	656	44
20	624	624	57
21	728	728	13
22	608	608	35
23	688	688	56
24	568	568	16
25	672	672	38
26	704	704	2
27	720	720	19
28	736	736	41
29	704	704	0
30	688	688	19
Rata-Rata kecepatan enkoding			30,97

Tabel 14.
Hasil pengujian lama waktu Dekoding

NO	Ukuran data		Waktu(milidetik)
	Input	Output	
1	248	248	6085,7734
2	296	296	465,9885
3	280	272	584,1145
4	288	280	525,9252
5	304	304	511,9027
6	208	208	530,8366
7	264	264	506,2928
8	144	144	471,4423
9	408	408	1184,9649
10	328	328	478,3403
11	344	344	477,0766
12	219	219	456,8016
13	416	416	507,3472
14	288	288	500,9293
15	376	376	578,1175
16	256	256	540,2952
17	720	720	525,6751
18	640	640	437,517
19	656	656	453,633
20	624	624	470,9783
21	728	728	434,3915
22	608	608	529,0052
23	688	688	431,3103
24	568	568	430,3114
25	672	672	435,4891
26	704	704	459,3645
27	720	720	456,9564
28	736	736	684,6805
29	704	704	491,4078
30	688	688	454,9158
Rata-Rata kecepatan dekoding			703,392817

Pada Tabel 13 dan 14 dapat terlihat pada proses enkoding dan dekoding memiliki lama waktu yang lebih lama daripada proses enkripsi, hal itu dikaranekan pada proses ini memeliki

proses berlapis saat berlangsung, dalam proses enkoding ada proses enkripsi data hak cipta dan proses konversi *file* menjadi wav, maka waktu yang diperlukan lebih lama, adapun dalam proses enkoding memerlukan yang lebih banyak daripada proses lainnya karena pada proses ini terdapat proses, dimulai dari dekripsi menggunakan kunci publik dan proses ekstrasi *file* audio menjadi text.

V. KESIMPULAN

Berikut kesimpulan dari Implementasi Algoritma BC3 dan RSA Dalam mengamankan data hak cipta lagu yang disisipkan pada *file* aduio mp3 menggunakan Algoritna LSB adalah sebagai berikut :

A. Implementasi Algoritma BC3 dan RSA dapat berjalan dengan baik dalam mengenkripsi data hal tersebut terlihat dalam pengujian bahwa setiap masukan data yang berupa plainteks akan berubah sepenuhnya menjadi cipherteks, hal itu didukung juga dari jumlah bit yang sama semua, yaitu untuk RSA masukannya adalah 11 karakter yang mana sedangkan di BC3 adalah 10 karakter,namun hasil dari tiap enkripsi berbeda-beda.

B. Kinerja Algoritma BC3 dan RSA dalam mengamankan data hak cipta sangat baik hal itu didukung dengan adanyanya modifikasi pada chiperteks dan chiperkey pada kedua buah algoritma dan menghasilkan bahwa semua data sangat sensitif terhadap perubah bahkan untuk 1 bit saja, walaupun tidak 100% sensitif tiap blok data, hal itu dikarenakan jumlah karakter pada Base64 terbatas hanya berkisar 64 karakter dan ditambah lagi masukan hanya berupa angka yang mana hanya 9 karakter unik, oleh karena ada kemungkinan satu blok pada data sama nilainya, tapi kesamaan itu sangat acak,jadi bisa saja blok ke 1 pada data ke 1 yang sama tapi ketika dimasukan ke data ke 2 maka blok yang sama tidak akan di posisi blok yang sama seperti data sebelumnya, hal itu dapat dilihat pada modifikasi BC3 yang mana masukannya hanya beda satu angka saja,namun kesamaan blok berbeda-beda posisinya,maka dari itu terlihat bahwa kedua buah algoritma dalam mengamankan data hak cipta sangat terjamin.

C. Pengaruh implementasi BC3,RSA dan LSB dalam tujuan kriptografi pada pengamanan data hak cipta memenuhi hal tersebut yaitu :

1). Kerahasiaan

Implementasi BC3 dan RSA sangat aman dalam mengamankan data hak cipta lagu, hal itu dapat dilihat pada pengujian bahwa 100% data sangat sensitif baik itu ada perubah 1 bit ataupun perubah cipherkey, apalagi jika sudah menggunakan LSB dan di enkoding menggunakan kunci publik RSA, yang mana hasil modifikasi kunci menunjukan 100% data berbeda tiap blok nya yang menandakan data sangat sensitif terhadap perubahaan sehingga data sangat terjamain kerahasiaannya karena hanya orang-orang tertentu saja yang bisa mengakses data dengan benar

2). Integritas data

Pada implementasi ini hasil pengujian menunjukan jika kunci yang berbeda saat mendekripsi maka 100% data plainteks hasil enkripsi akan berbeda dengan plainteks asli, hal itu menandakan bahwa data memiliki integritas.

D. Dalam pengujian Stegano *file* , data asli dan data audio yang telah disisipkan data hak cipta memiliki kemiripan yang sama,sehingga ketika diputar lagunya orang tidak akan tahu bahwa lagu tersebut didalamnya ada data enkripsi, sedangkan jika data yang telah disisipkan kemudian di konverisi ke format yang lain lalu dikonversi ke format seperti yang awal maka akan terjadi perubahaan pada tiap bit didalam data sehingga saat menggunakan algoritma lsb, data tidak bisa ditemukan.

E. Lama waktu enkripsi dan dekripsi, karena dalam penelitian ini memiliki inputan yang sama, maka tidak heran dalam penghitung waktu tidak berbeda satu dengan yang liannya, yang membedakan adalah proses ke-1 pada saat menenkripsi, hal itu dikarenakan waktu awal-awal sistem harus memerlukan waktu dalam memproses masukan,kunci,dsb tidak seperti proses enkpsi kedua sampai terakhir,maka dapat disimpulkan bahwa walaupun jumlah inputan yang sama tapi waktu memproses data berbeda-beda, namun semuanya sangat cepat, tidak lebih dari 1 milidetik.

F. Lama waktu enkoding dan dekoding lebih lama dibandingkan dengan proses enkripsi dan dekripsi, pada enkoding saja rata-rata memerlukan waktu lebih dari 30 milisecond, apalagi jika dekoding yang mana rata-rata impelementasinya 0,7 detik, hal itu dikarenakan ada proses pembuatan *file* teks.

REFERENSI

[1] A. B. Utama, "Pemanfaatan Teknologi Informasi di Kalangan Mahasiswa Universitas Negeri," *Jurnal Universitas Airlangga Surabaya* , p. 1, 2016.

[2] S. H. E. C. Vidyasagar M. Potdar, "A Survey of Digital Image Watermarking Techniques," in *2005 3rd IEEE International Conference on Industrial Informatics*, Perth, 2005.

[3] F. Petitcolas, R. Anderson and M. Kuhn, "Information hiding-a survey," *PROCEEDINGS OF THE IEEE,* pp. 1062 - 1078, 1999.

[4] Y. Wang, J. Doherty and R. V. Dyck, "A wavelet-based watermarking algorithm for ownership verification of digital images," *IEEE Transactions on Image Processing,* pp. 77-88, 2002.

[5] S. Frith, "Copyright and the music business," *Popular Music,* pp. 57-75, 1988.

[6] T. O'Regan, "From piracy to sovereignty: International video cassette," *Continuum: Journal of Media & Cultural Studies,* pp. 112-135, 1991.

[7] J. Ullman, "The Development and Testing of Potential Music," *UNLV Theses, Dissertations, Professional Papers, and Capstones,* pp. 1-314, 2017.

[8] M. C. a. M. Commission, Internet Users Survey 2018, Cyberjaya: Malaysian Communications and Multimedia Commission, 2018.

[9] C. R. S. Enrique Bigne, "THE IMPACT OF INTERNET USER SHOPPING PATTERNS AND DEMOGRAPHICS ON CONSUMER MOBILE BUYING BEHAVIOUR," *Journal of Electronic Commerce Research,* pp. 193-209, 2005.

[10] R. D. G. a. G. L. S. Sudip Bhattacharjee, "DIGITAL MUSIC AND ONLINE SHARING: SOFTWARE PIRACY 2.0?," *COMMUNICATIONS OF THE ACM,* pp. 107-111, 2003.

[11] J. P. Q. v. d. E. Y. H. Joost Poort, Global Online Piracy Study, Amsterdam: Institute for Information Law, 2018.

[12] K. B. Kennedy, "Copyright Infringement in Sound Recording: How Courts and Legislatures Can Get in Vogue in a Post-Ciccone World," *Journal of Law and Policy,* pp. 723-755, 2017.

[13] N. Anwar, "Hidden Message Steganography Design with Matlab-based Least," *Jurnal Algoritma, Logika dan Komputasi,* vol. 1, no. 1, p. 25, 2018.

[14] K. B. M. L. C. Mandy Douglas, "An overview of steganography techniques applied," *Journal Multimed Tools Application,* vol. 13, no. 77, p. 17334, 2017.

[15] D. B. K. B.-h. K. Ratul Chowdhury, "A View on LSB Based Audio Steganography," *International Journal of Security and Its Applications,* vol. 10, no. 2, p. 52, 2016.

[16] B. A. A. M. H. Fatiha Djebbar, "Comparative study of digital audio," *Journal on Audio, Speech, and Music Processing,* p. 1, 2012.

[17] Q. D. Hai Cheng, "Overview of the Block Cipher," *International Conference on Instrumentation & Measurement, Computer, Communication and Control,* p. 1628, 2012.

[18] H. K. S. Arif Sasongko, "Architecture for the Secret-Key BC3 Cryptography," *ITB Journal of ICT Research and Applications ,* vol. 5, no. 2, pp. 125-140, 2011.

[19] P. Chaudhury, S. Dhang, M. Roy, S. Deb, J. Saha, A. Mallik, S. Bal, S. Roy, M. K. Sarkar, S. Kumar and R. Das, "ACAFP: Asymmetric Key based Cryptographic Algorithm using Four Prime Numbers to Secure Message Communication A review on RSA algorithm," in *2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON)*, Bangkok, 2017.

[20] Y. Liu, W. Gong and W. Fan, "Application of AES and RSA Hybrid Algorithm in E-mail," in *2018 IEEE/ACIS 17th International Conference on Computer and Information Science (ICIS)*, Singapore, 2018.

[21] W. Rui, C. Ju and D. Guangwen, "A k-RSA algorithm," in *2011 IEEE 3rd International Conference on Communication Software and Networks*, Xi'an, 2011.

[22] W. F. S. S. F. A. F. C. Fausto Meneses, "RSA Encryption Algorithm Optimization to Improve," *International Journal of Computer Science and Network Security,* vol. 16, no. 8, pp. 55-62, 2016

[23] J.-C. L. a. C.-C. L. Chu-Hsing Lin, "Speeding Up RSA Encryption Using GPU Parallelization," in *2014 Fifth International Conference on Intelligent Systems, Modelling and Simulation*, Taichung, 2014.

[24] R. K. Sarika Khatarkar, "A Survey and Performance Analysis of Various RSA," *International Journal of Computer Applications,* vol. 114, no. 7, pp. 30-33, 2015.

[25] J. Denegri-Knott, "MP3," *Journal Consumption Markets & Culture,* vol. 18, no. 5, pp. 397-401, 2015.

[26] R. R. J. F. S. Muhamad Nursalman, "Implementation of Low Bit Coding Algorithm and Cipher Block with Electronic Code Book Mode for Data Legality in Audio Steganographic Streaming," in *2018 International Conference on Information Technology Systems and Innovation (ICITSI)*, Padang, 2018.

[27] E. S. A. P. E. Apriyani, "IMPLEMENTASI ALGORITMA KRIPTOGRAFI RC4 DAN METODE STEGANOGRAFI AUDIO 2LSB PADA SISTEM KEAMANAN INFORMASI," *Jurnal Teknologi Informatika dan Terapan ,* pp. 81-88, 2017.

[28] Prabhudesai KevalKetan, V. V. (2012). An Amalgam Approach using AES and RC4 Algorithms for Encryption and Decryption. International Journal of Computer Applications, 29-36.