Management of Information System Journal
Vol 1, No 1, November, Hal 19 - 28
ISSN 2964-9455 (media online)
Website https://journal.fkpt.org/index.php/mis

Penerapan Digital Signature Untuk Identitas File Audio Dengan Metode Snefru

Muhammad Fajri Manullang

Program Studi Teknik Informatika, Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Budi Darma Medan, Medan, Indonesia
Jl. Sisingamangaraja No.338, Siti Rejo I, Kec. Medan Kota, Kota Medan, Sumatera Utara, Indonesia
Email: [1]muhammadfazri2021@gmail.com

Abstrak−Dalam era teknologi informasi yang berkembang sangat pesat, penggunaan tanda tangan sudah banyak diterapkan secara digital melalui tanda tangan digital. Tanda tangan digital seiring berkembangnya zaman memunculkan kebutuhan otentifikasi suatu data atau berkas yang digunakan secara digital. Penggunaanya juga bertujuan untuk menghindari pemalsuan ataupun gangguan. Saat ini, pemanfaatan tanda tangan digital sudah banyak diterapakan pada distribusi perangkat lunak, transaksi keuangan, pengiriman berkas. Kejahatan dalam pemalsuan file audio menjadi masalah serius pada beragam bidang. Pengujian keaslian audio menjadi hal yang penting dan signifikan di semuah wilayah sosial, terutama ketika audio digunakan sebagai pembuktian kesimpulan dalam sidang, landasan pengambilan kebijakan peradilan, dan laporan perusahaan. Pemalsuan file audio akan menyebabkan kerugian yang tidak dapat diperkirakan.Salah satu solusi penyelesaian masalah tersebut diatas adalah dengan melakukan proses pemberian identitas pada file audio, sehingga dapat diketahui audio tersebut tidak dapat dimanipulasi. Metode SNEFRU salah satu fungsi hash untuk mengetahui adanya perubahan terhadap audio digital. SNEFRU memiliki beberapa varian, bervariasi dalam jumlah operan dan ukuran hash. Itu ukuran hash yang didukung adalah 128 dan 256 bit. Jumlah lintasan dalam sumber varian inal 2-pass dari SNEFRU adalah dua pass, sedangkan versi 4-pass yang lebih aman juga tersedia. Setelah serangan sebelumnya diterbitkan, versi 8-pass adalah diperkenalkan juga Versi 8-pass ini masih dianggap aman.

Kata Kunci: Keamanan, Tanda Tangan Digital, Fungsi hash snefru, Audio

Abstract−In the era of information technology that is developing very rapidly, the use of signatures has been widely applied digitally through digital signatures. Digital signatures along with the times have led to the need for authentication of data or files that are used digitally. Its use also aims to avoid counterfeiting or interference. Currently, the use of digital signatures has been widely applied to software distribution, financial transactions, file transfers. The crime of falsifying audio files is a serious problem in various fields. Audio authenticity testing is important and significant in all social areas, especially when audio is used as evidence for conclusions in courts, the basis for judicial decision-making, and corporate reports. Forgery of audio files will cause losses that cannot be estimated. One solution to the problems mentioned above is to perform the process of assigning an identity to the audio file, so that it can be seen that the audio cannot be manipulated. The SNEFRU method is a hash function to detect changes in digital audio. SNEFRU has several variants, varying in number of operands and hash size. The supported hash sizes are 128 and 256 bits. The number of passes in the final 2-pass variant source of SNEFRU is two passes, while a more secure 4-pass version is also available. After the previous attack was published, the 8-pass version was introduced as well. This 8-pass version is still considered safe.

Keywords: Keamanan, Tanda Tangan Digital, Fungsi hash snefru, Audio

1. PENDAHULUAN

Keamanan dan kerahasiaan file audio perlu diperhatikan untuk menghindari tindakan-tindakan pemanipulasian yang dilakukan oleh orang yang tidak berkepentingan. Berbagai macam teknik saat ini banyak digunakan untuk melihat identitas dari sebuah file audio yang diperlukan. Dengan mengetahui file audio yang diterima asli atau tidak tentu berpengaruh pada tingkat kepercayaan pada orang tertentu. Kejahatan dalam pemalsuan file audio menjadi masalah serius pada beragam bidang. Pengujian keaslian audio menjadi hal yang penting dan signifikan di semuah wilayah sosial, terutama ketika audio digunakan sebagai pembuktian kesimpulan dalam sidang, landasan pengambilan kebijakan peradilan, dan laporan perusahaan. Pemalsuan file audio akan menyebabkan kerugian yang tidak dapat diperkirakan.

Dalam hal ini akan dibahas mengenai bagaimana proses pembuatan identitas dari sebuah audio. Dengan memasukkan identitas seperti tanda tangan digital. Tanda tangan digital yang dimaksud bukanlah tanda tangan yang didijitasi dengan alat scanner, tetapi suatu nilai kriptografis yang bergantung pada pesan dan pengirim pesan (Munir, 2005). Tanda tangan digital yang akan diproses akan menjadi identitas file audio tersebut. Hal inilah yang membuat tanda tangan digital atau *digital signature* ini disebut sebagai multi *digital signature*. Salah satu teknik keamanan yang dapat memastikan file audio adalah teknik *kriptografi*. *Kriptografi* adalah ilmu yang bersandarkan pada teknik matematikan untuk berurusan dengan keamanan informasi seperti kerahasiaan file, keutuhan data dan otentikasi entitas (Bruce, 1996). *Metode SNEFRU* salah satu fungsi *hash* untuk mengetahui adanya perubahan terhadap teks digital. *SNEFRU* memiliki beberapa varian, bervariasi dalam jumlah operan dan ukuran *hash*. Itu ukuran hash yang didukung adalah 128 dan 256 bit. Jumlah lintasan dalam sumber varian inal 2-pass dari *SNEFRU* adalah dua pass, sedangkan versi 4-pass yang lebih aman juga tersedia. Setelah serangan sebelumnya diterbitkan, versi 8-pass adalah diperkenalkan juga Versi 8-pass ini masih dianggap aman (Biham, n.d.). *SNEFRU* adalah fungsi hash yang berulang mengikuti konstruksi *Merkle-Damg˚ard*, itu dirancang untuk menjadi fungsi *hash kriptografi* yang *hash* pesan dengan panjang sewenang-wenang menjadi nilai 128-bit (berbasis varian 256-bit pada desain yang sama juga diperkenalkan).

Pada proses penggunaan metode *SNEFRU*, nilai yang dihasilkan disisipkan meggunakan teknik steganografi yang mana teknik ini dipergunakan untuk penyisipan nilai kedalam sebuah file audio yang akan digunakan. Teknik steganografi yang digunakan adalah metode LSB (*Least Signigicant Bit*). Metode penyisipan LSB adalah menyisipkan

Management of Information System Journal
Vol 1, No 1, November, Hal 19 - 28
ISSN 2964-9455 (media online)
Website https://journal.fkpt.org/index.php/mis

pesan degan cara mengganti bit LSB pada representasi biner file audio dengan representasi biner dari pesan rahasia yang akan disembunyikan (Arifin & Oktoviana, 2013). Media yang digunakan untuk teknik steganografi adalah file audio.

2. METODOLOGI PENELITIAN

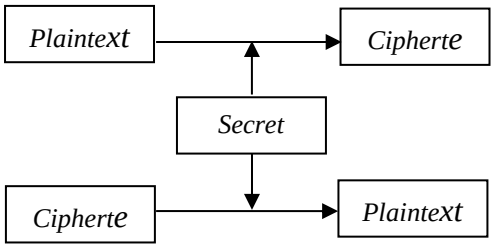
2.1 Tahapan Penelitian

Metode pengumpulan data yang digunakan dalam pembahasan penelitian ini adalah sebagai berikut:

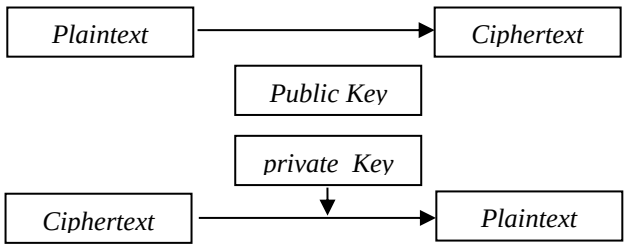
1. Studi Literatur
   Mengumpulkan dan mempelajari referensi baik dari buku, internet, jurnal maupun sumber-sumber lainnya mengenai identitas file audio sebagai tahap untuk melakukan penelitian implementasi kriptografi dengan Metode SNEFRU.
2. Analisa
   Tahap ini akan melaksanakan analisa masalah, analisa data dan proses penyelesaian masalah.
3. Perancangan sistem dan pengujian
   Melakukan perancangan tampilan (interface) untuk proses identitas pada file audio. Kemudian dilakukan uji coba program, menangani dan memperbaiki kesalahan yang ada pada program aplikasi.
4. Implementasi
   Tahap ini dilakukan pembuatan program untuk aplikasi identitas pada file audio.
5. Dokumentasi
   Membuat dokumentasi sistem dari tahap awal sampai pengujian sistem, kemudian untuk disusun dalam format penelitian

2.2 Kriptografi

Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan. Namun pada pengertian *modern* kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berusan dengan keamanan informasi seperti kerahasian, keutuhan data dan otentikasi entitas(Zebua, 2018).



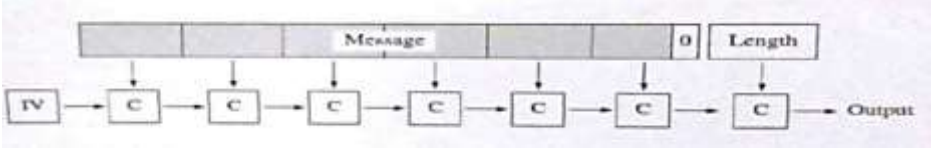
Gambar 1. Diagram enkripsi dan dekripsi simetri



Gambar 2. Diagram enkripsi dan dekripsi kunci asimetri

2.3 Fungsi *Hash Snefru*

Snefru adalah fungsi *hash* berulang yang mengikuti konstruksi *Merkle-Damg˚ard*. Itu dirancang untuk menjadi fungsi *hash* kriptografi yang *hash* pesan dengan panjang sewenang-wenang menjadi nilai 128-bit (berbasis varian 256-bit pada desain yang sama juga diperkenalkan).



Gambar 3. Mode Pengoperasian *Snefru*

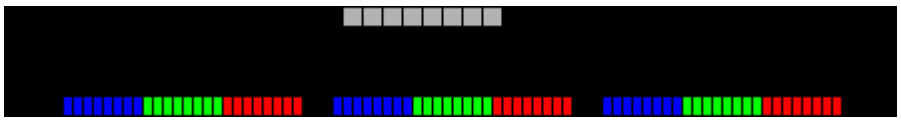
Management of Information System Journal
Vol 1, No 1, November, Hal 19 - 28
ISSN 2964-9455 (media online)
Website https://journal.fkpt.org/index.php/mis

2.4 *File Audio*

MPEG-1 audio layer III atau yang lebih dikenal dengan MP3, adalah salah satu dari pengkodean dalam *digital audio* dan juga merupakan format kompresi audio yang memiliki sifat " menghilangkan". Istilah menghilangkan yang dimaksud adalah kompresi audio kedalam format MP3 menghilangkan aspek-aspek yang tidak signifikan pada pendengaran manusia untuk mengurangi besarnya *file audio*(Aleisa, 2015).Sejarah MP3 dimulai dari tahun 1991 saat proposal dari phillips *(Belanda), CCET (Perancis),* dan istitut *Fur Rundfunktechnik (Jerman)* memenangkan proyek untuk DAB *(Digital Audio Broadcast).*

2.5 LSB

LSB (Least Signification Bit) adalah metode yang cukup sederhana dalam melakukan proses *steganografi*. Selain itu, proses penyisipan dan ekstraksi dari metode ini juga relative cukup cepat. Metode *LSB* menyisipkan pesan ke dalam *cover image* pada bit yang paling kurang berarti. Untuk *LSB* 1 bit, bit yang disisipkan adalah bit ke 8 untuk setiap *byte*, perubahan nilai desimal dari satu *byte* menjadi satu nilai lebih tinggi, atau satu nilai lebih rendah, atau sama dari nilai desimal dari satu *byte* sebelum penyisipan. Sedangkan untuk metode *LSB* 2 bit, bit yang disisipkan adalah bit ke 7 dan bit ke 8 untuk setiap *byte*. Sehingga perubahan nilai pada 2 bit terakhir berkisar antara nol sampai dengan tiga dari nilai *byte* sebelum terjadi penyisipan(Djuwitaningrum & Apriyani, 2016).



Gambar 4. *Least Significant Bit*

3. HASIL DAN PEMBAHASAN

Identitas data file audio rahasia sangat rentan terhadap modifikasi yang digunakan dengan menambah maupun mengurangi isi dari file audio tersebut. Apalagi file audio rahasia didistribusikan melalui jaringan internet, dimana internet merupakan jaringan public yang dapat diakses oleh siapa saja. Berdasarkan hal tersebut dibutuhkan sebuah teknik kriptografi untuk melihat apakah file audio yang akan diterima benar merupakan file asli yang telah dikirim dengan mengandalkan teknik kriptografi untuk melihat nilai hash dari file audio.

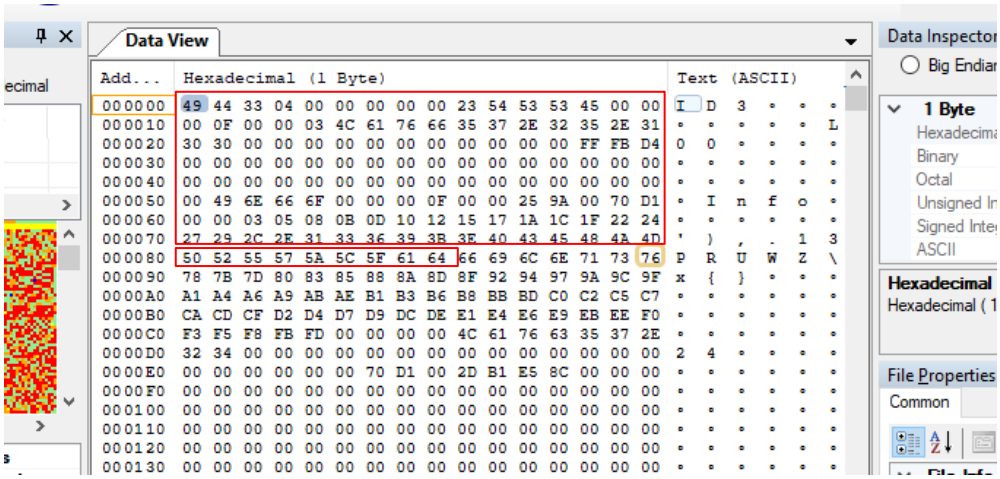
Berdasarkan rumusan masalah pada bab sebelumnya dan paparan di atas, masalah yang terjadi adalah bagaimana sebuah file audio dapat di identifikasi keasliannya dengan teknik kriptografi sebelum didistribusikan kepada penerima dengan memasukkan sebuah tanda tangan digital kedalam file audio. Teknik kriptografi dapat membantu memasukkan tanda tangan digital ke dalam file audio. Metode yang digunakan dalam pembahasan ini adalah metode SNEFRU dengan teknik penyisipan Least Significant Bit (LSB).

3.1 Contoh Kasus

Gambar 5. *File Audio* Sampel

Dari gambar file audio sampel di atas, dilakukan proses pencarian nilai hexa dengan menggunakan aplikasi BinnaryViewer.exe. Adapun nilai hexa yang diperoleh dari file audio dapat dilihat pada gambar di bawah ini :

Management of Information System Journal
Vol 1, No 1, November, Hal 19 - 28
ISSN 2964-9455 (media online)
Website https://journal.fkpt.org/index.php/mis



Gambar 6. Nilai *Hexa* yang digunakan untuk sampel pada *file* audio

Tahap selanjutnya adalah menentukan tanda tangan yang akan disisipkan kedalam file audio di atas, adapun tanda tangan yang digunakan berupa teks adalah sebagai berikut:
M U H A M M A D F A Z R I M A N U L L A N G M U H A M M A D F A Z R I M A N U L L A N G A A A A
Sehingga didapat tabel nilai biner dari sampel tanda tanga digital yaitu sebagai berikut:

Tabel 1. Nilai biner pada tanda tangan digital

Huruf	Decimal	*Biner*
M	77	01001101
U	85	01010101
H	72	01001000
A	65	01000001
M	77	01001101
M	77	01001101
A	65	01000001
D	68	01000100
F	70	01000110
A	65	01000001
Z	90	01011010
R	82	01010010
I	73	01001001
M	77	01001101
A	65	01000001
N	78	01001110
U	85	01010101
L	76	01001100
L	76	01001100
A	65	01000001
N	78	01001110
G	71	01000111
M	77	01001101
U	85	01010101
H	72	01001000

Huruf	Decimal	*Biner*
A	65	01000001
M	77	01001101
M	77	01001101
A	65	01000001
D	68	01000100
F	70	01000110
A	65	01000001
Z	90	01011010
R	82	01010010
I	73	01001001
M	77	01001101
A	65	01000001
N	78	01001110
U	85	01010101
L	76	01001100
L	76	01001100
A	65	01000001
N	78	01001110
G	71	01000111
A	65	01000001
A	65	01000001
A	65	01000001
A	65	01000001

Tabel 2. *S-Box*

1ABC10EF	0A5BEC2C	1B5AE2DC	BE8DC77A
5B4DC3AE	2AA3BCD4	53DBAC31	C7B25AED
F5B33CD4	4E5FFB67	4B5CCAD3	DDB89AD
3B37B7A5	EF4B56AC	B3DCA45A	9A6DBE1

Menggabungkan bit-bit H_0 di depan X_1 sehingga menghasilkan 524 bit, sehingga X_1=

Management of Information System Journal
Vol 1, No 1, November, Hal 19 - 28
ISSN 2964-9455 (media online)
Website https://journal.fkpt.org/index.php/mis

00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000001001101010101010010000100000101001101010011010100000101000100
10001100100000101011010010100100100100101001101010000010100111001010101010011000100110001000001 0
10011100100011101001101010101010010000100000101001101010011010100000101000100010001100100000010
10110100101001001001001010011010100000101001110010101010100110001001100010000010100111001000111 0
10000010100000101000000101000001

Bit 0 dengan jumlah 128 bit sebelah kiri (awal) adalah biner H_0 sedangkah nilai biner selanjutnya adalah biner dari X_1 sejumlah 384 bit. Jumlah bit H_0 dengan bit X_1 secara keseluruhan adalah 512 bit (128 bit + 384 bit = 512 bit).
Proses pengelompokan biner X_1 menjadi 16 bagian.

3.2 Tampilan program Aplikasi

Adapun tampilan keseluruhan program terdiri dari tampilan menu utama, tampilan form fungsi hash snefru, tampilan form cara pemakaian, tampilan form about me. Berikut tampilan program aplikasi beserta dengan penjelesanya pada aplikasi yang telah dibangun:

a. Tampilan Menu Utama

Gambar 7. Tampilan menu utama

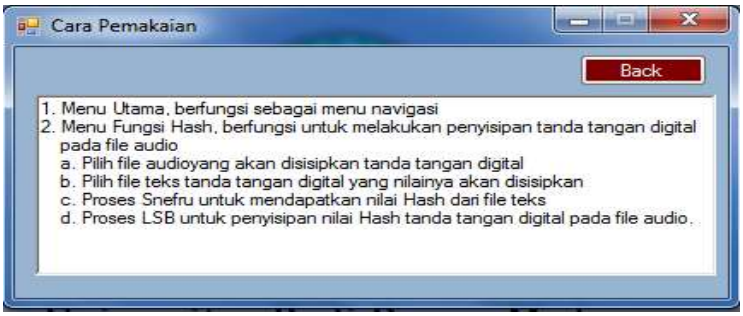
Berdasarkan pada gambar 7, terdiri dari beberapa StripButton yang memiliki fungsi masing-masing. StripButton form fungsi hash snefru berfungsi untuk menampilkan form proses tanda tangan digital. StripButton cara pemakaian berfungsi untuk menampilkan form cara pemakaian aplikasi. StripButton about me berfungsi untuk menampilkan form tentang penulis, sedangkan StripButton exit berfungsi untuk keluar dari aplikasi.

b. Tampilan *Form* Fungsi *Hash Snefru*

Gambar 8. *Form* fungsi *hash snafru*

Management of Information System Journal
Vol 1, No 1, November, Hal 19 - 28
ISSN 2964-9455 (media online)
Website https://journal.fkpt.org/index.php/mis

c. Tampilan *Form* Cara Pemakaian



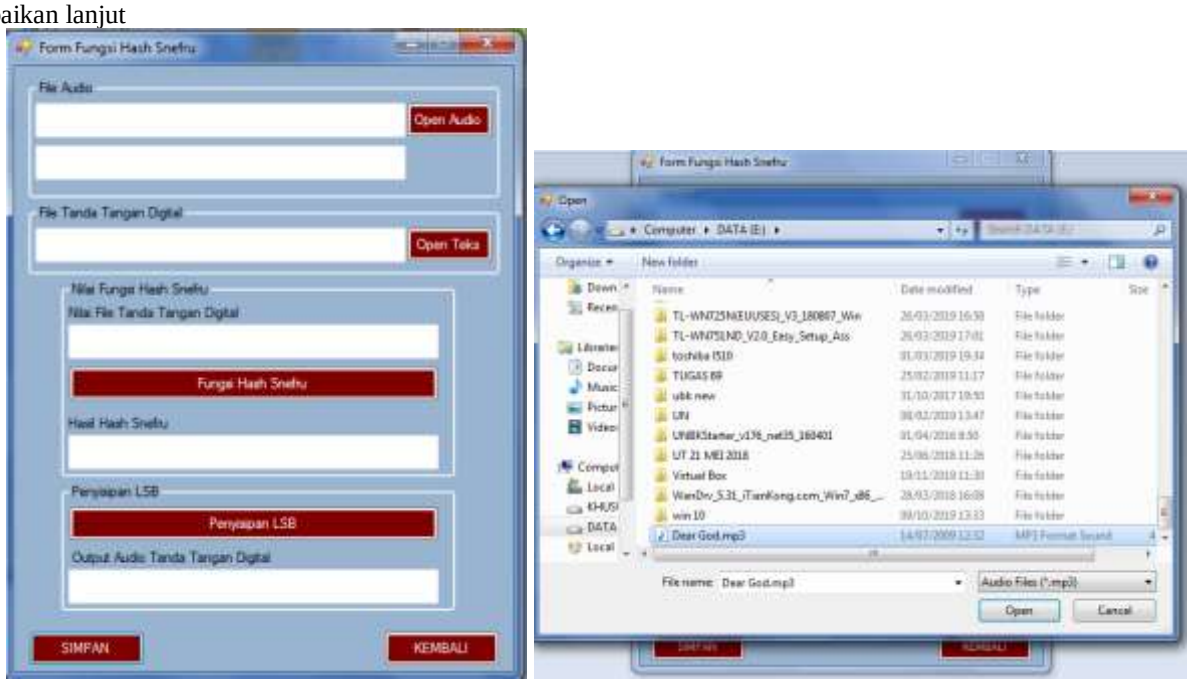
Gambar 8. *Form* cara pemakaian

d. Tampilan *About Me*

Gambar 9. *Form about me*

3.3 Implementasi dan Hasil pengujian

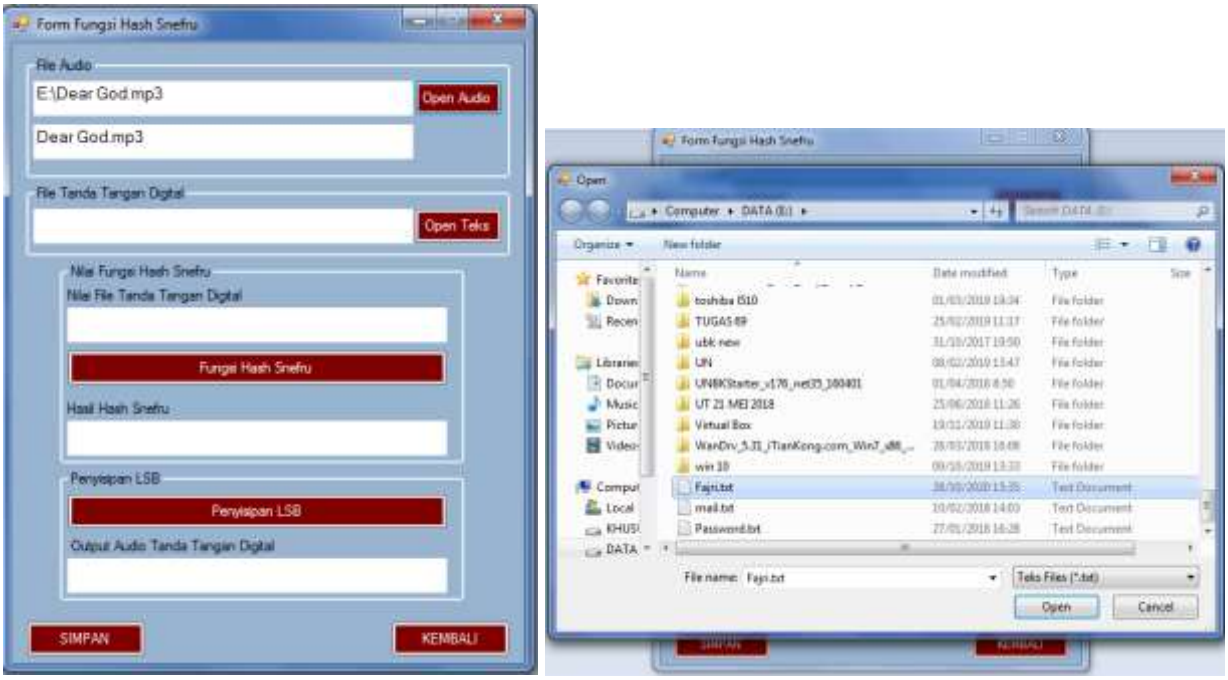
Bab ini akan melakukan pembahasan tentang pengujian dan analisa hasil dari program aplikasi yang telah dibuat. Tujuan dari pengujian ini adalah untuk mengetahui apakah aplikasi yang telah dibuat sesuai dengan perancanganya. Selain itu juga, untuk mengetahui detail dari jalanya aplikasi serta kesalahan yang ada untuk jadikan pengembangan dan perbaikan lanjut



Gambar 10. Proses pemilihan *file* audio

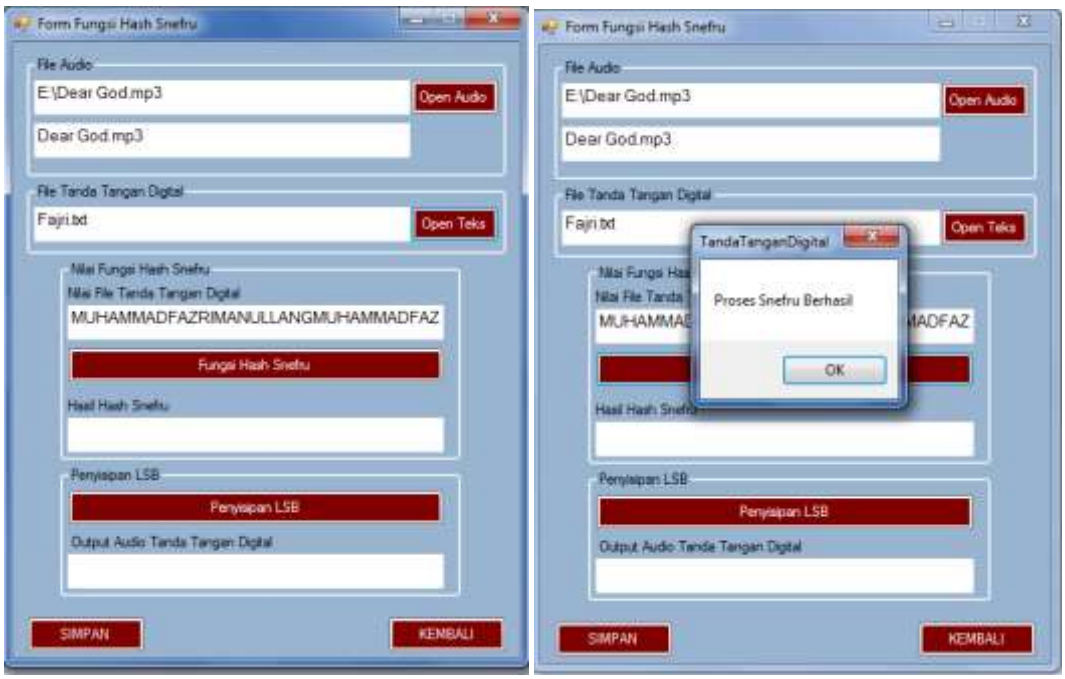
Berdasarkan pada gambar di atas, untuk melakukan pemilihan file audio, user dapat menekan button “Open Audio” sehingga menampilkan direktori pencarian file audio dengan format .mp3, user dapat menentukan file audio yang akan disisipkan tanda tangan digital, jika sudah dipilih user dapat menekan button “Open” sehingga menampilkan informasi file audio pada aplikasi seperti pada gambar di bawah ini:

Management of Information System Journal
Vol 1, No 1, November, Hal 19 - 28
ISSN 2964-9455 (media online)
Website https://journal.fkpt.org/index.php/mis



Gambar 10. Proses pemilihan *file* teks tanda tangan *digital*

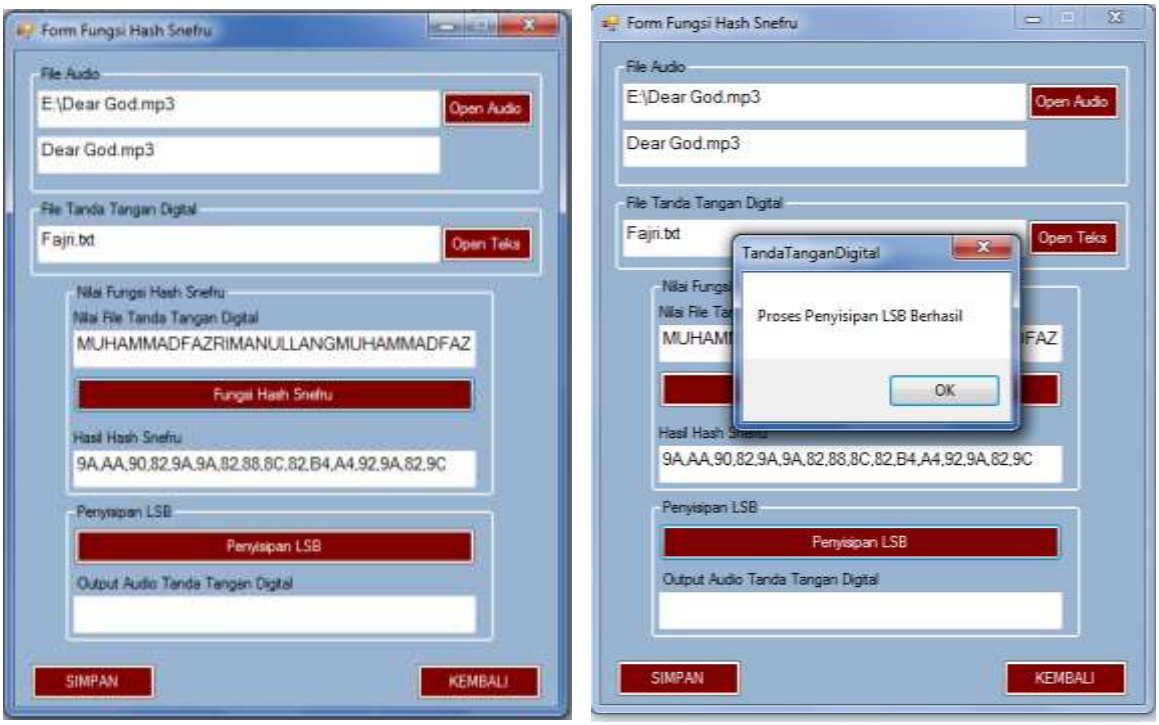
Berdasarkan pada gambar di atas, selanjutnya adalah memilih file tanda tangan digital yang nilainya akan dihash menggunakan snefru. Adapun proses pemilihan file tanda tangan digital dengan format .txt dimulai dengan user menekan button "Open Teks" sehingga menampilkan menu pencarian, user dapat menentukan file teks tanda tangan digital yang akan di hash menggunakan snefru, jika sudah dipilih user dapat menekan button "Open" sehingga menampilkan informasi file teks tanda tangan digital pada aplikasi seperti pada gambar di bawah ini:



Gambar 11. Proses *hash senfru*

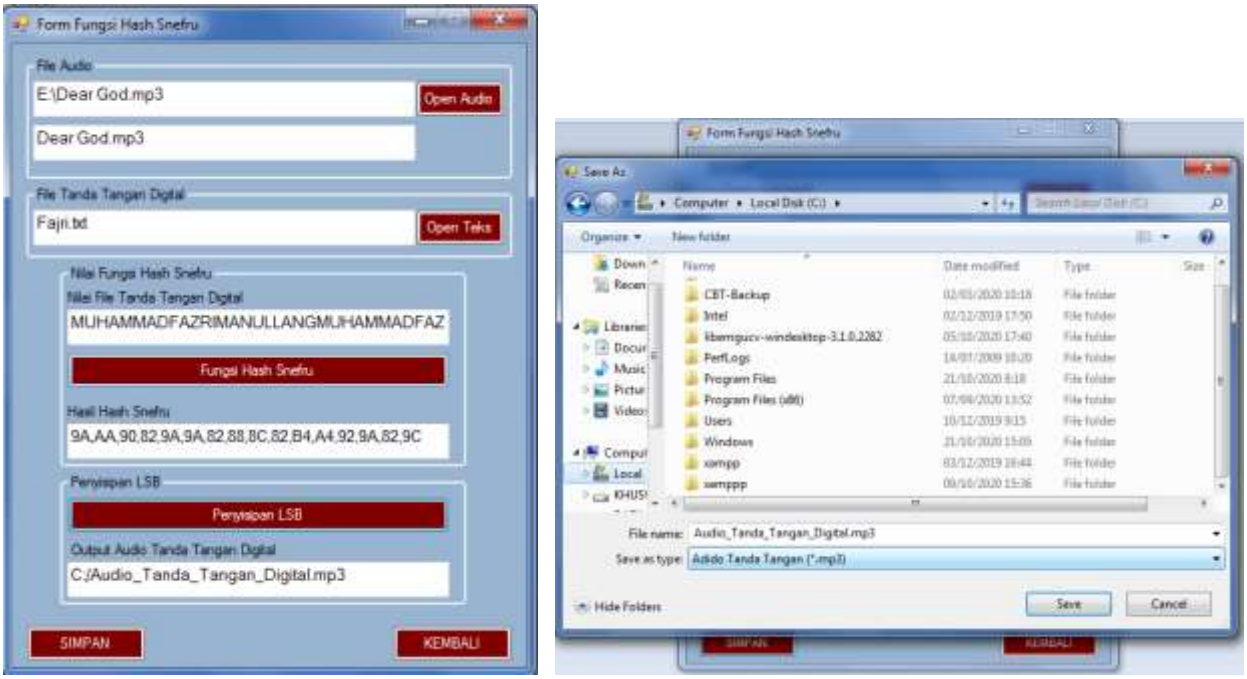
Berdasarkan pada gambar diatas, informasi yang ditampilkan adalah nama file teks tanda tangan digital beserta dengan karakter teks. Selanjutnya adalah mencari nilai Hash teks tanda tangan digital dengan memilih button "Fungsi Hash Snefru" sehingga menampilkan hasil proses, proses melakukan hash pada nilai teks tanda digital berhasil dilakukan, user menekan button "OK", sehingga aplikasi menampilkan nilai hash teks tanda tangan digital seperti pada gambar di bawah ini:

Management of Information System Journal
Vol 1, No 1, November, Hal 19 - 28
ISSN 2964-9455 (media online)
Website https://journal.fkpt.org/index.php/mis



Gambar 12. Proses penyisipan *hash senfru*

Berdasarkan pada gambar di atas, selanjutnya adalah melakukan penyisipan nilai hash teks tanda tangan digital pada audio yang telah dipilih. Adapun prosesnya dengan menekan button "Penyisipan LSB" sehingga menampilkan hasil proses berhasil, proses penyisipan nilai hash teks tanda tangan digital berhasil dilakukan, user menekan button "OK" sehingga menampilkan hasil output audio hasil penyisipan tanda tangan digital seperti pada gambar di bawah ini:



Gambar 13. Simpan *output audio* hasil penyisipan tanda tangan *digital*

Berdasarkan pada gambar di atas, hasil output audio kemudian dapat disimpan dengan menekan button "Simpan", sehingga menampilkan direktori penyimpanan pada komputer, , user menekan button "Save", sehingga pada aplikasi menampilkan informasi sukses seperti pada gambar di bawah ini:

Management of Information System Journal
Vol 1, No 1, November, Hal 19 - 28
ISSN 2964-9455 (media online)
Website https://journal.fkpt.org/index.php/mis

Gambar 14. Simpan *output audio* hasill penyisipan tanda tangan *digital*

Berdasarkan pada proses pengujian sistem aplikasi, adapun hasil pengujian tersebut dapat dilihat pada gambar di bawah ini :

Gambar 15. Perbandingan *file* audio

Berdasarkan pada gambar 4.15, tidak terdapat perbedaan antara audio sebelum disisipkan identitas tanda tangan digital dengan sesudah disisipkan. Hal ini dikarenakan proses penyisipan hanya menukar nilai bit akhir audio dengan nilai bit Hash Snefru teks tanda tangan digital, sehingga perbedaan nilai 0 dan 1 pada bit akhir audio tidak mempengaruhi bit suara audio.

4. KESIMPULAN

Berdasarkan hasil dari implementasi sistem yang telah dilakukan pada bab sebelumnya, dapat diambil kesimpulan bahwa dari prosedur metode Snefru, didapatkan nilai *hash* karakter tanda tangan digital yang akan disisipkan pada file audio, sehingga file audio memiliki identitas. Pada proses penyisipan LSB dengan menukar bit akhir audio berdasarkan bit hash tanda tangan digital berhasil dilakukan tanpa mengubah suara, ukuran dan format dari file audio hasil tanda tangan digital. Perancangan aplikasi tanda tangan digital pada file audio dapat mempermudah mengenali identitas audio.

REFERENCES

[1] Munir, R. (2005). Penggunaan Tanda-Tangan Digital untuk Menjaga Integritas Berkas Perangkat Lunak. In *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*.
[2] Bruce, S. (1996). Applied cryptography. *2nd John Wiley and Sons, Inc*.
[3] Biham, E. (2008, February). New techniques for cryptanalysis of hash functions and improved attacks on Snefru. In *International Workshop on Fast Software Encryption* (pp. 444-461). Springer, Berlin, Heidelberg.
[4] Arifin, R., & Oktoviana, L. T. (2013). Implementasi Kriptografi dan Steganografi menggunakan Algoritma RSA dan metode LSB. *Universitas Malang*.
[5]Zebua, T. (2018). Encoding the record database of computer based test exam based on spritz algorithm. Lontar Komput. J. Ilm. Teknol. Inf, 9(1), 52-62.c
[6] Aleisa, N. (2015). A Comparison of the 3DES and AES Encryption Standards. *International Journal of Security and Its Applications*, *9*(7), 241-246.
[7] Thakur, J., & Kumar, N. (2011). DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis. *International journal of emerging technology and advanced engineering*, *1*(2), 6-12.
[8] Mohtashim, (2015,apr.9). *Cryptografy Hash Functions* [online]. Available:https://www.tutorialspoint.com/cryptography/cryptography.htm
[9] Indrawan, R. (2004). *Penerapan metode enkripsi IDEA dan fungsi hash SNEFRU untuk keamanan dokumen* (Doctoral dissertation, Petra Christian University).
[10] Kusuma, I. J. (2017). ANALISIS TEKNIK STEGANOGRAFI PADA AUDIO MP3 MENGGUNAKAN METODE PARITY CODING DAN ENKRIPSI CIPHER TRANSPOSITION. *Jurnal Elektronik Sistem Informasi dan Komputer*, *3*(2), 1-8.
[11] Setyaningsih, E., & Si, S. (2015). Kriptografi & Implementasinya Menggunakan Matlab. *Yogyakarta: Andi*.
[12] Munir, R. (2005). Penggunaan Tanda-Tangan Digital untuk Menjaga Integritas Berkas Perangkat Lunak. In *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*.
[13] Iswahyudi, C., & Risgianto, I. (2008). Penyisipan Pesan Rahasia pada Teks Digital dengan Teknik Steganografi. *Jurnal Teknologi*, *1*(1), 24-29.

[14] Djuwitaningrum, E. R., & Apriyani, M. (2017). Teknik Steganografi Pesan Teks Menggunakan Metode Least Significant Bit dan Algoritma Linear Congruential Generator. *JUITA: Jurnal Informatika*, *4*(2), 79-85.
[15] Arini, G. M., & Widyawan, T. I. (2012). Pengamanan Pesan Steganografi dengan Metode LSB Berlapis Enkripsi dalam PHP. *Pengamanan Pesan Steganografi dengan Metod. LSB Berlapis Enkripsi dalam PHP*, *3*, 11.
[16] Sukamto, R. A., & Shalahuddin, M. (2011). Modul pembelajaran rekayasa perangkat lunak (terstruktur dan berorientasi objek). *Bandung: Modula*.
[17] Nugroho, A. (2010). *Rekayasa perangkat lunak berorientasi objek dengan metode USDP*. Penerbit Andi.
[18] Hendrayudi, V. B. (2009). untuk Berbagai Keperluan Programming. *Jakarta: PT Elex Media Komputindo*.