ENKRIPSI DATA COCKPIT VOICE RECORDER PADA PESAWAT MILITER DENGAN MENGGUNAKAN ALGORITMA SIMETRIS

Ema, ST., MT
Ketua Program Studi Avionika Fakultas Teknik Universitas Nurtanio Bandung
Jl. Pajajaran No 219 Bandung
Email : demadiena@gmail.com

ABSTRACT

Information confidentiality issues in the military institution is a must, so far the military aircraft should not be equipped with Blackbox as information storage media data plane (FDR, Flight Data Recorder) and information on the cockpit voice (CVR, Cockpit Voice Recorder). On the other hand, the information is needed for the investigation of an accident, but it also Blackbox can be used as guidance in detecting damage of the aircraft systems at the time of treatment. In this thesis was discussed about alternative solutions for problems that are opposite to each other, especially in the media Cockpit Voice Recording (CVR).

Solutions offered in this thesis is the application of encryption on the cockpit voice recording systems. The model chosen is encrypted symmetric encryption streamchiper because its strength lies in the confidentiality of password used. After doing some experiments on the type of password that is used, optimal results obtained by applying the password in the form of sound files with audio frequencies.

The encryption method became one of the methods chosen for the security of information on the Cockpit Voice Recorder (CVR) with the settings and key generation algorithm will determine the level of encryption security. Information security management system data on the Cockpit Voice Recorder (CVR) military aircraft can be applied in a manner keeping the password to decrypt. Decrypt the voice data is used to determine the cause of the accident and taken as a lesson to improve the safety of military aircraft.

PENDAHULUAN

Kotak hitam atau *black box* adalah sekumpulan alat yang digunakan pada pesawat terbang untuk menyimpan semua data aktivitas selama penerbangan. Data tersebut dibutuhkan oleh para penyelidik dalam mengungkap penyebab sebuah kecelakaan penerbangan. Kotak hitam ini terdiri dari dua bagian utama yaitu *Flight Data Recorder* (FDR) dan *Cockpit Voice Recorder* (CVR). FDR mencatat berbagai parameter yang terkait dengan operasi dan karakteristik penerbangan pesawat seperti kecepatan, percepatan, ketinggian, posisi kontrol *cockpit*, parameter mesin, aliran bahan bakar, status *auto pilot* dan berbagai parameter lainnya. Sedangkan CVR merekam suara awak pesawat, bunyi mesin dan bunyi lainnya di *cockpit.* [8]Kebijakan pada pesawat militer tidak mengizinkan adanya FDR dan CVR, karena ditakutkan jika FDR dan CVR jatuh di daerah musuh, maka kerahasiaan militer akan

terbongkar. Tetapi disisi lain kecelakaan pesawat militer tidak mudah diketahui penyebabnya dikarenakan tidak adanya rekaman data atau suara yang bisa di analisa.

Berdasarkan faktor-faktor tersebut diperlukan adanya suatu sistem yang dapat membantu investigasi kecelakaan pada pesawat militer dengan tetap menjaga kerahasiaan data tersebut terhadap pihak yang tidak berwenang mengetahuinya.Alternatif solusi yang dibahas pada tesis ini adalah penerapan sistem enkripsi pada salah satu dari sistem *blackbox* yaitu pada perekaman suara *cockpit* (CVR). Maka ada ide untuk mengadakan perangkat *cockpit voice recorder* terenkripsi pada pesawat militer dimana di dalamnya terdapat suatu perangkat yang membuat peroses enkripsi, jadi proses pemograman enkripsi dilakukan pada perangkat keras.

Dalam dunia pendidikan, tidak banyak publikasi penelitian mengenai CVR atau *Blackbox*. Diantara tesis yang ditemukan di internet adalah dari [11]*Naval Graduate School Monterey California* yang berjudul *"Secure Ground-BasedRemote Recording And Archiving Of Aircraft Black Box Data"*. Tesis tersebut memaparkan *feasibility* sistem yang dapat mentransmit data Blackbox ke darat selama terbang dengan dilengkapi sistem keamanan, jaminan aliran informasi, sehingga kerahasiaan, keutuhan, ketersediaan, dan keaslian data akan terjamin. Tesis tersebut memfokuskan keamanan data transmisi selama penerbangan sebelum terjadi kecelakaan, sedangkan pada tesis ini ditekankan pada keamanan data yang disimpan pada *Blackbox*.Perbedaan dengan penelitian yang sudah ada pada penekanan media yang dienkripsi menggunakan jaringan yang aman dengan metode *Virtual Private Network* (VPN) sedangkan pada tesis ini perangkat *hardware* yang dienkripsi.

KAJIAN MASALAH

Kajian diawali dengan pemilihan teknik enkripsi yang sesuai dengan karakteristik sistem CVR.Dibahas juga hasil percobaan pada penerapan *password* yang berbeda jenisnya, hal ini dilakukan pada simulasi perangkat lunak. Kajian dilanjutkan pada pembuatan *prototype* sistem enkripsi pada CVR berupa *embedded system* yang terdiri dari mikropon sebagai sensor suara, ADC (*Analog to Digital Converter*) sebagai pengubah sinyal analog ke data digital, mikrokontroler sebagai pengolah data dan penerapan sistem enkripsi, dan SD*card* sebagai media penyimpan *file* suara yang telah dienkripsi.

Batasan Masalah

1. Teknik enkripsi dengan metode *stream chipper* dibuat dalam sekala laboratorium untuk dapat di terapkan pada CVR pesawat militer dengan asumsi CVR secara fisik mempunyai ketahanan terhadap benturan, suhu tinggi, dll.
2. Lama perekaman diasumsikan 30 menit, dengan menggunakan media SD*card*

berkapasitas lebih dari ukuran tersebut.

3. Tokoh berbicara : pilot.
4. Simulasi dilakukan pada beberapa jenis *password* yang digunakan pada sistem enkripsi simetris dengan mengunakan *software*. Yaitu *password text* pendek, *password text* panjang, *password file* suara.
5. Tipe pesan yang disembunyikan adalah *voice*dalam format *file wav.*
6. *Prototype* implementasi menggunakan mikropon sebagai sensor *audio*, mikrokontroler sebagai data *processing* dan SD*card* sebagai media penyimpanan.

Metode Penelitian

Pada tesis ini dilakukan metodologi penelitian sebagai berikut :

1 Identifikasi permasalahan

2 Studi Literatur, mengumpulkan data - data dari beberapa opini tentang alasan tidak dipasang *blackbox* pada pesawat militer.

3 Mempelajari teori – teori yang berhubungan dengan teori enkripsi dan *Cockpit Voice Recorder* pada pesawat terbang.

4 Analisis kebutuhan sistemfungsionalitas utama sistem dan proses kerja sistem.

5 Simulasi penggunaan beberapa jenis *password.*

6 Implementasiakan diterapkan pada perangkat keras dan perangkat lunak sedangkan proses pengujian berisi tentang analisis perubahan data suara baik data suara sebelum proses enkripsi, data suara setelah proses enkripsi maupun setelah di dekripsi

7 Kesimpulan proses penerapan teknik enkripsi pada *Cockpit Voice Recorder.*

Sistematika Penulisan

Tesis ini dibagi menjadi 5 bab yang terdiri dari:

1. Bab Pertama Pendahuluan, berisi Latar Belakang, Kajian Masalah, Tujuan, Batasan Masalah, Metode Penelitian dan Sistematika Penulisan tesis.
2. Bab kedua, Dasar Teori, berisi tentang sistem CVR pada pesawat udara dan teori enkripsi.
3. Bab ketiga, Perancangan Sistem enkripsi pada CVR, berisi analisa kebutuhan sistem, pemilihan sistem enkripsi, dan simulasi proses enkripsi.
4. Bab keempat, Implementasi Sistem Enkripsi CVR, berisi penjelasan bagian-bagian sistem dimulai dari mikropon, *pre-amp*, ADC, mikrokontroler, dan SD*card* beserta pengujiannya.
5. Bab kelima, Kesimpulan dan Saran, berisi kesimpulan dari penelitian yang dilakukan pada tesis ini dan saran untuk penelitian selanjutnya.

COCKPIT VOICE RECORDER & KRIPTOGRAFI

***Cockpit Voice Recorder* (CVR)**

Sebelum Perancangan sistem enkripsi CVR dibahas, pada bagian ini dibahas terlebih

dahulu sistem CVR yang sebenarnya ada pada saat ini sebagai bahan perbandingan dengan sistem yang akan dirancang pada tesis ini.

CVR adalah bagian dari sistem *blackbox* pada pesawat udara.*Blackbox* terdiri dari 2 bagian yaitu :

1. FDR (*Flight Data Recorder*), sistem perekam data-data sensor pesawat udara.
2. CVR (*Cockpit Voice Recorder*), adalah alat perekam yang digunakan untuk merekam percakapan dan komunikasi antar *crew* yang bersangkutan yang disimpan dalam *SOLID STATE MEMORY*.

Data – data CVR disimpan pada *memory boards* yang terdapat pada C*rash Survivability Memory Unit* (CSMU) yang berlapis-lapis. Masing-masing lapisan terdiri dari aluminium tipis silika dan baja tahan karat atau juga titanium, yang amat kuat dan tahan terhadap berbagai kondisi ekstrim. Beberapa hal yang harus mampu ditahan oleh CSMU diantaranya, *crash impact* yang harus mampu menahan benturan sampai 3.400 G (percepatan gravitasi bumi), *static crash* mampu menahan beban seberat 5.000 lb (2.500 kg) selama 5 menit pada semua sumbunya. *Firetest* mampu bertahan pada suhu 20.000 F (11.000 derajat celcius) selama satu jam, mampu bertahan di kedalaman laut selama 30 hari, berbagai macam bahan kimia dan sebagainya. CVR disimpan di bagian ekor pesawat, tempat yang diduga paling aman jika pesawat mengalami kecelakaan. Karena seringkali ekor pesawat lebih utuh kondisinya pada saat terjadi kecelakaan dibandingkan bagian depan, sehingga akan lebih melindungi keutuhan kotak hitam. Kotak hitam yang lebih modern memiliki kemampuan *self-eject* serta mudah dideteksi oleh SONAR atau RADAR.

Untuk memudahkan pencariannya, terutama pencarian di bawah air, kotak hitam dilengkapi pula dengan *Underwater Locator Beacon* yang kerjanya adalah ketika terguncang karena benturan, alat ini akan terus-menerus memancarkan perekam ultrasonik dan sinyal yang dapat mencapai permukaan dari kedalaman 14.000 ft. Sinyal inilah yang bisa ditangkap radar untuk menunjukkan lokasi pesawat. Namun kekuatan sinyal terbatas, biasanya sampai seminggu sebelum menghilang.Saat kecelakaan terjadi dan kotak hitam ditemukan, maka kotak itu segera di kirim ke organisasi yang netral (bukan bagian dari perusahaan pesawat yang terkena musibah) untuk dilakukan "pembacaan" dan analisa.Untuk dapat dianalisis, data dan FDR dan CVR dibaca dengan menggunakan peralatan dan piranti lunak khusus.

Tujuan dari *blackbox* adalah mengkoleksi data audio dan data dari sensor dan merekamnya ke dalam media yang akan selamat dari kecelakaan. Saat ini pesawat-pesawat militer tidak dilengkapi kotak hitam dengan alasan khawatir data-data yang terekam akan diambil oleh musuh ketika

terjadi kecelakaan. Gambar *blackbox* dapat dilihat

Penempatan CVR dan FDR diposisikan pada tempat yang paling mungkin untuk selamat ketika terjadi kecelakaan yaitu dibagian belakang pesawat.

Gambar Penempatan FDR dan CVR Pada Pesawat Udara

CVR memiliki 4 *track* untuk merekam suara. Penggunaan *track audio* yang dianjurkan adalah sebagai berikut:

Track 1: *copilot headset* dan *live boom microphone*

Track 2: *pilot headset* dan *live boom microphone*

Track 3: *area microphone*

Track 4: *Time reference* atau *Crew* yang lain

Lamanya perekaman

a. 2 jam untuk pesawat dengan MTOW (*Maximum Take Off and Landing Weight*) lebih dari 5,7 ton
b. 30 menit untuk tipe MTOW kurang dari 5,7 ton

PERANCANGAN MANAJEMEN DAN IMPLEMENTASI SISTEM ENKRIPSI CVR

Managemen keamanan yang diterapkan pada angkatan udara yang merupakan salah satu instansi militer, dalam hal ini kerahasiaan informasi untuk itu ada penyelamatan data keamanan yang berkaitan dengan teknologi yang digunakan, kebijakan yang ada, kebutuhan yang muncul yaitu jika diruang suatu rencana maka banyak faktor yang mendukung SDM, teknologi maka harus ada persiapannya. Contohnya : Pelatihan dan kepedulian dari SDM nya.

Teknologi yang digunakan adalah teknologi keamanan data berupa enkripsi yang dikaitkan dengan kerahasiaan dan pengaturan hak akses. Enkripsi yang diterapkan pada sistem CVR, selain itu untuk hak akses akan diimplementasikan teknologi autentikasi menggunakan *password*.

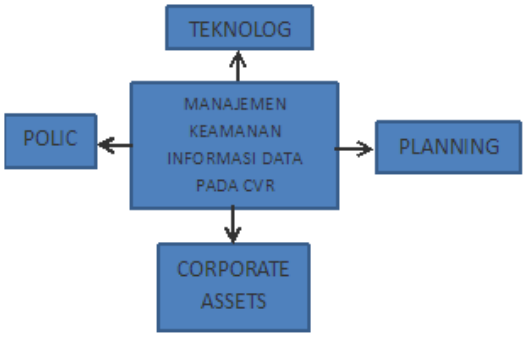
Kebijakan dan strategi yang dibuat memperhatikan masalah siapa yang berhak mengetahui informasi, jenis *password* yang digunakan dan mekanismepenanyamasalah, selain itu kebijakannya harus memperhatikan resiko yang mungkin terjadi, dalam hal ini pengelolaan resiko adalah suatu hal yang ditekankan.

Teknik enkripsi yang digunakan cenderung bersifat simetris mengingat tidak diperlukannya manajemen distribusi kunci yang rumit. Teknik enkripsi disesuaikan dengan media yang akan dienkripsikan yaitu

media suara yang akan dikonversi dalam format yang sesuai dengan proses enkripsi.

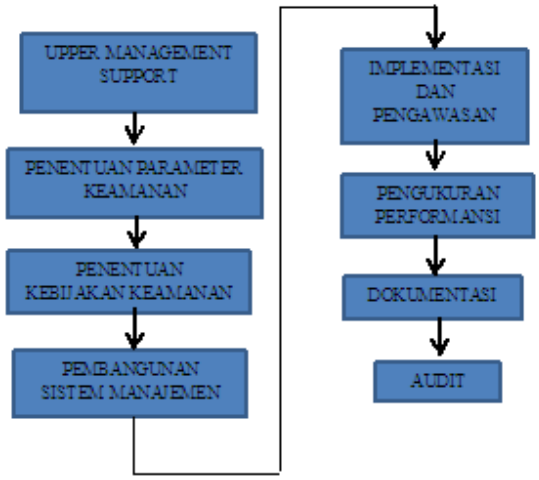
Pada Pesawat militer jika terjadi kecelakaan, untuk forensik pertanggungjawaban dan investigasi sulit jika tidak ada *blackbox*. Tetapi keadaan *blackbox* dalam kondisi apa adanya akan memungkinkan kebocoran informasi sehingga diketahui oleh pihak yang tidak berwenang.

Berawal dari kondisi tersebut muncul suatuide dan pemikiran untuk menerapkan enkripsi sebagai saran keamanan informasi data. Tetapi hal ini harus sesuai dengan kaidah dalam manajemen dan pengelolaan keamanan (*Security Management*), dimana banyak faktor yang harus diperhatikan, diantaranya : kebijakan institusi, tingkat keamanan yang diinginkan, persiapan teknologi dan dana adalah yang sangat berpengaruh dalam usaha pengaman data. Untuk lebih lengkapnya hal yang berkaitan dengan pengolahan keamanan dapat dijelaskan pada blok diagram dibawah ini.



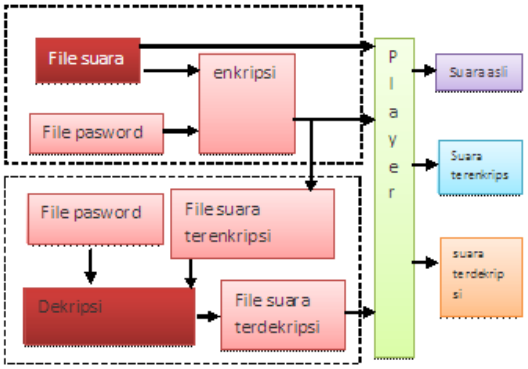
Gambar Blok Diagram Rancangan Manajemen Keamanan Informasi Data CVR.

Berdasarkan butir- butir acuan ISO di atas maka dibuat alur manajemen keamanan CVR sebagai berikut :

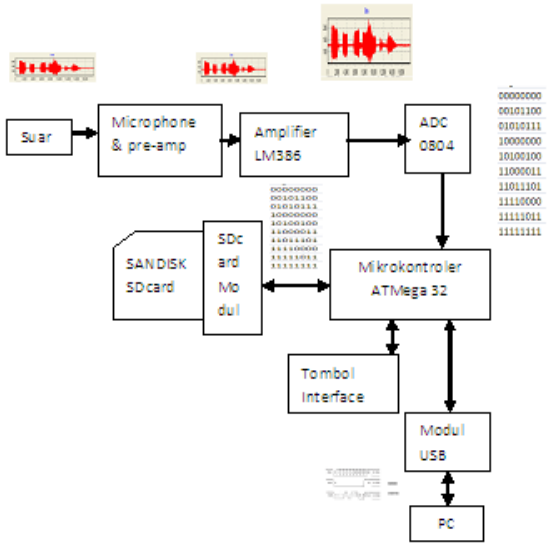


Gambar Blok Diagram Pembangunan Manajemen sistem Keamanan Informasi CVR

Blok diagram *system* simulasi pada *software* dan *prototype*implementasi yang akan dibuat secara sederhana.



Gambar Diagram Blok simulasi Pada Software



Gambar Diagram Blok *prototype* implementasi

Pemilihan Sistem Enkripsi

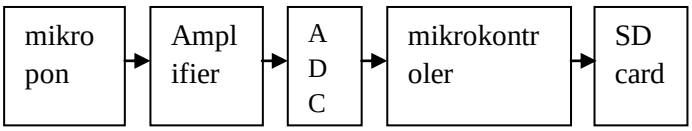
Sistem enkripsi yang dipilih pada implementasi tesis ini adalah enkripsi algoritma simetris dengan teknik pembangkitan kunci enkripsi *stream* yaitu dengan menerapkan operasi XOR pada tiap *byte* data dengan *bytepassword*.Percobaan yang dilakukan menggunakan 3 jenis *password* untuk diketahui seberapa efektif penyembunyian suara dapat dilakukan dengan teknik enkripsi simetris, yaitu:

1. *Password text*pendek : Text dalam format ASCII yang berupa kumpulan huruf yang membentuk satu sampai sepuluh kata dalam bahasa indonesia.
2. *Password text*panjang : Text dalam format ASCII yang berupa kumpulan kata-kata berjumlah 1000 kata atau lebih dalam bahasa indonesia atau bahasa inggris.
3. *Pasword file* data suara

Implementasi Fisik Sistem Enkripsi

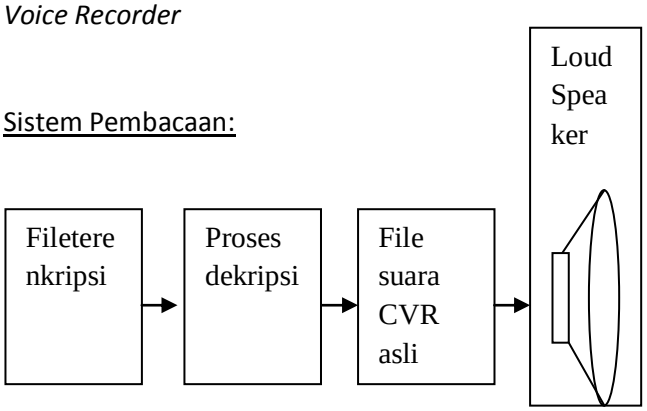
Perancangan Sistem yang akan dibuat dapat dilihat pada diagram dibawah ini:

Sistem Perekaman :



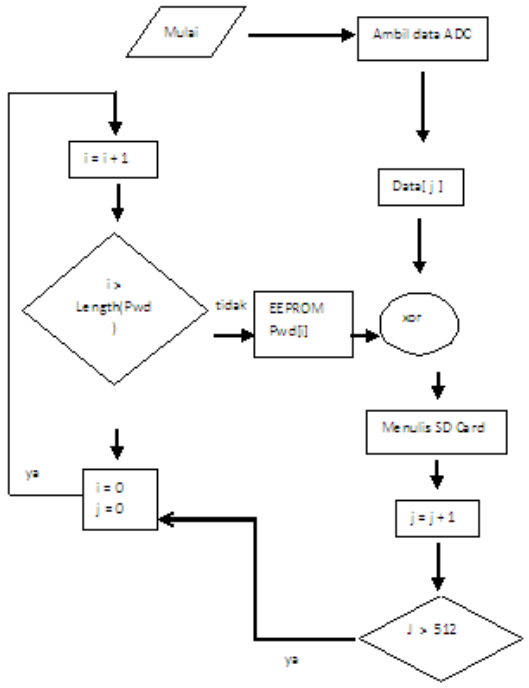
Gambar Diagram Sistem Enkripsi *Cockpit Voice Recorder*

Sistem Pembacaan:



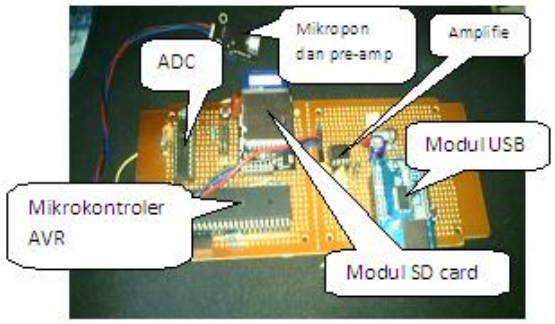
Gambar Diagram Sistem Pembacaan *Cockpit Voice Recorder*

Pengkodean Enkripsi Dalam *Processor*



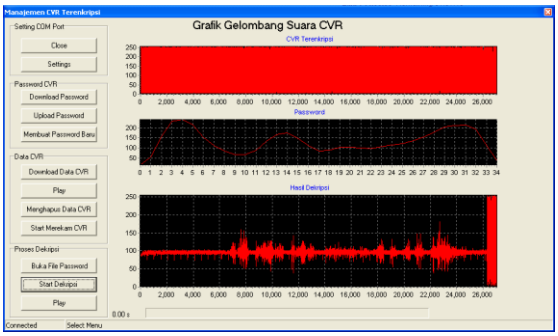
Gambar 3.13 Diagram Enkripsi.

Prototype sistem ini dapat dilihat pada gambar



Gambar *Prototype* Sistem Perekam CVR Terenkripsi

Rancangan *Software* Pembaca *Encrypted* CVR



Gambar 3.19 Rancangan GUI (*Graphical User Interface*) *Software* Manajemen CVR Terenkripsi

HASIL IMPLEMENTASI ENCRYPTED CVR DAN PENGUJIAN FUNGSIONALNYA

Realisasi manajemen sistem keamanan CVR

Untuk terimplementasinya system keamanan CVR ini maka dibutuhkan dukungan dari Pihak TOP manajemen lembaga angkatan udara berupa sarana prasarana, kebijakan, regulasi, dan arahan. Pihak TOP manajemen akan menentukan hak akses, wewenang, tingkat keamanan, dan kendali asset terkait pengamanan CVR.

Berikutnya TOP manajemen akan menentukan pihak yang terlibat dalam pemilihan teknologi, implementasi, dokumentasi dan pengujian performansi *system* keamanan yang diterapkan.

Pihak TOP manajemen juga memiliki estimasi dan prediksi performansi *system* jika dilakukan audit.

Pemilihan teknologi disertai dengan pertimbangan mengenai kemampuan sumber daya dalam membangun, merawat dan

pengembangan *system*, semua ini juga menjadi *focus* dari TOP manajemen.

Pada TNI Angkatan Udara yang memiliki wewenang terbesar tentang *control asset* terkait keselamatan penerbangan adalah Kadislambangjaau. Kadislambangjaau melaksanakan fungsi manajerial terkait keamanan dan keselamatanpenerbangan.Kadislambangjaau mencari strategi untuk meningkatkan keamanan dan keselamatan pesawat terbang dengan menambahkan CVR yang terenkripsi.

Pesawat terbang sebagai *corporate asset* pada TNI AU akan selalu dalam pengawasan dan pengendalian, suatu standar kelayakan diterapkan tetapi terkadang ada error yang mengakibatkan kecelakaan penerbangan dan pihak angkatan udara akan melakukan investigasi terhadap insiden tersebut. CVR sebagai sumber data dalam *forensic*akan membantu mengungkap sebab terjadinya kecelakaan sehingga diharapkan tidak terulang kembali dikemudian hari.

Teknologi keamanan terhadap informasi pada CVR adalah hal yang harus dipikirkan karena setiap beroperasinya pesawat TNI AU pastinya memiliki misi dan kerahasiaan misi adalah hal krusial.Pada era sekarang ini metode enkripsi dapat menjadi opsi teknologi yang dapat digunakan. Parameter keamanan yang ditentukan akan menentukan jenis algoritma enkripsi yang digunakan, dan setiap penerapan suatu teknologi pasti membutuhkan sarana dan prasarana serta kebijakan, ataupun regulasi. Performasi penerapan suatu teknologi dapat diprediksi dari awal, dan harus dilakukan pengujian setelah diimplementasikan. Tingkat deviasi antara apa yang direncanakan dan setelah diimplementasikan menjadi kajian untuk penyempurnaan sistem.

Implementasi Encrypted CVR

Pada Tesis ini pengimplementasian CVR terenkripsi dilakukan secara bertahap agar setiap tahapnya dapat diketahui kinerja dan fungsionalnya dengan baik. Tahapan yang dilakukan adalah sebagai berikut:

1. Pengujian algoritma enkripsi menggunakan simulasi pada *software*
   a. Enkripsi data *text* dengan password *text* pendek
   b. Enkripsi *file* suara (format wav) dengan *password text* pendek (1 sampai 10 kata)
   c. Enkripsi *file* suara dengan *password text* panjang (*file text* ukuran 6kb)
   d. Enkripsi *file* suara dengan *password* berupa suara lain
   e. Dekripsi *file* suara dengan *password* berupa suara lain
2. Pengujian *hardware*
   a. Pengujian fungsional modul *microphone* dan *pre-Amplifier*
   b. Pengujian ADC
   c. Pengujian fungsional modul SD *card reader/writer*

No	Password	Hasil Enkripsi	Kesimpulan
1	Text 1 kata	Suara asli asih terdengar	Tidak bisa digunakan
2	Text 2 kata	Suara asli asih terdengar	Tidak bisa digunakan
3	Text 3 kata	Suara asli asih terdengar	Tidak bisa digunakan
4	Text 4 kata	Suara asli asih terdengar	Tidak bisa digunakan
5	Text 5 kata	Suara asli asih terdengar	Tidak bisa digunakan
6	Text 6 kata	Suara asli asih terdengar	Tidak bisa digunakan
7	Text 7 kata	Suara asli asih terdengar	Tidak bisa digunakan
8	Text 8 kata	Suara asli asih terdengar	Tidak bisa digunakan
9	Text 9 kata	Suara asli asih terdengar	Tidak bisa digunakan
10	Text 10 kata	Suara asli asih terdengar	Tidak bisa digunakan
11	Text 1000 kata	Suara asli asih terdengar	Tidak bisa digunakan
12	Text 10000 kata	Suara asli asih terdengar	Tidak bisa digunakan
13	File suara	Suara tersembunyi	Bisa digunakan lebih sulit pembuatan prototypenya
14	Satu Periode Gelombang	Suara tersembunyi	Bisa digunakan lebih mudah pembuatan prototypenya

d. Pengujian fungsional enkripsi suara pada Software Simulasi
e. Pengujian *software* pembaca data CVR terenkripsi.
f. Pengujian fungsional Mikrokontroler
g. Pengujian fungsional managemen CVR terenkripsi

Hasil:

Hasil yang diperoleh dari dekripsi menggunakan *password file* suara menunjukkan hasil yang sama dengan data aslinya, terlihat pada gambar 2.24. dari hasil tersebut sehingga teknik enkripsi simetrik (menggunakan *password* yang sama) dapat terbukti.

Tabel Pengujian Enkripsi Pada Beberapa Password

Analisis :

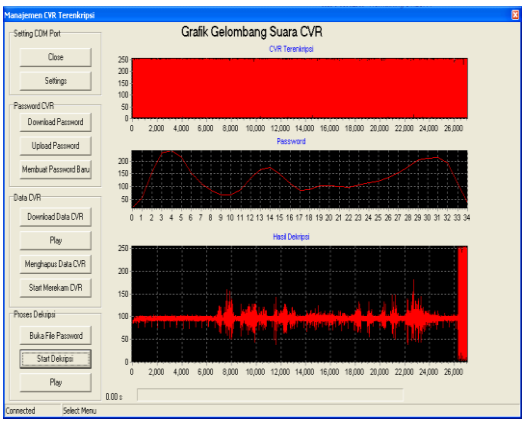
1. Secara visual data terlihat bahwa enkripsi menggunakan *password text* pendek, dan *text* panjang sudah dapat diterapkan terbukti dengan bentuk gelombang (*amplitude)* yang tidak lagi berbentuk seperti semula. Namun ketika diperdengarkan ternyata suara orang mengucapkan *"tes.."* masih terdengar suara tersebut diantara *noise* yang banyak, ini menunjukkan *password text* pendek dan *text* panjang tidak mampu menyembunyikan data suara. Hal ini dibuktikan dengan menggunakan

software audio (Cool Edit) *file* suara terenkripsi tadi di filter (dibuang *noise* nya) menghasilkan suara *"tes.."* yang makin jelas

2. Percobaan berikutnya digunakan *password* berupa *file* suara lain. Hasil enkripsi simetris menggunakan *file* suara menunjukkan hasil yang baik, artinya suara asli dapat disembunyikan sampai tidak terdengar lagi, sehingga

teknik ini dapat menjadi satu *alternative* bagi penerapan sistem keamanan suara pada CVR militer.

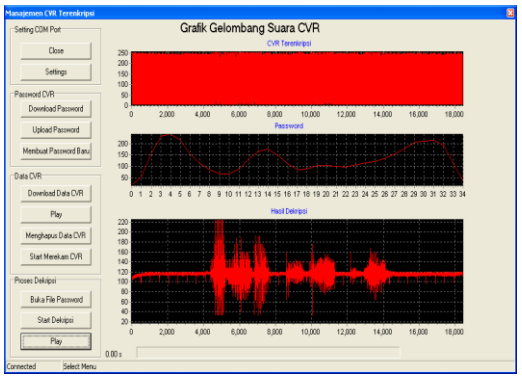
Percobaan berikutnya digunakan *password* berupa *file* berisi satu gelombang dari suara manusia yang berukuran hanya 35 *byte*. Hasil enkripsi menunjukkan bahwa suara asli tidak dapat terdengar lagi, sehingga teknik ini dapat menjadi pilihan untuk penerapan sistem keamanan pada CVR militer. Bahkan dengan *tipepassword* ini pembuatan *prototype* jadi lebih mudah.



Gambar *Software* Manajemen CVR Terenkripsi (Grafik menunjukkan CVR terenkripsi, *Password*, dan Hasil Dekripsi).

Percobaan pada alat prototype CVR terenkripsi terdapat empat percobaan yaitu:

1. Kasus Enkripsi CVR dengan *Password Text* Pendek (35 huruf)
2. Kasus Enkripsi CVR dengan *Password Text* Panjang (511 huruf)
3. Kasus Enkripsi CVR dengan potongan Suara (511 byte)
4. Kasus Enkripsi CVR dengan satu periode gelombang suara (35byte)



Gambar Hasil percobaan Enkripsi CVR *Password* Berupa Suara Pendek.

CONCLUSION

1. CVR voice cipher encryption result by using a short text password and the long text password still has value of information, because the original sounds can still be heard.
2. Password encryption techniques with a number of sound waves that can hide a lot of the original sound data but difficult to implement in hardware using a relatively large memory
3. Password encryption techniques with a wave of sound with a little amount of data able to hide the original sound and can be implemented in hardware as a prototype system of data security at military CVR.
4. Information security management system CVR data on military aircraft can be applied in a manner keeping the password to decrypt. Decryption of the voice data is used to determine the cause of the accident and taken as a lesson to improve the safety of military aircraft.

SUGGESTION

1. This study still needs refinement to reproduce the experiment with other types of passwords.
2. Prototype manufacture was still using audio input sample rate by 8000 and using 16bit resolution, but it still contains noise that needs to be improved quality.
3. Encryption techniques can be developed in this thesis point by using a more complex encryption.

DAFTAR PUSTAKA

1. AMM (Aircraft Maintenance Manual). From http://www.1-3ar.com
2. *Analog Sound Sensor*. From http://www.centralelectro.com/catalog.php?cat=1&page=2ATMEL
3. ATMEL (2011). *ATMega 32 8-bit AVR Microcontroller with 32KBytes In-System Programmable Flash*. USA: Atmel Corporation.
4. Brown, Burr. ADS 7822 12-Bit High Speed 2.7V microPower Sampling Analog to Digital Converter datasheet.
5. Dharmani, CC. *microSD ATmega32 Data-Logger.* From http://www.dharmanitech.com
6. Dharmani, CC. *Design with Microcontroller*. From http://www.dharmanitech.com
7. FN3094.4, Data Sheet (August 2002). *ADC0803, ADC0804.*Intersil.
8. Gigih Prastawa, Hannan. My Crypt Program enkripsi – dekripsi. Gigih's Net Zone.
9. Intersil (2002). *ADC0804 8-Bit Microprocessor-CompatibleA/D Converters.* Americas: Intersil Inc.

10. *RIFF Format Reference.* From http://www.lightlink.com/tjweber/StripWav/WAVE.html
11. R. Schoberg, Paul (Sep 2003). *Secure Ground - Based Remote Recording And Archiving Of Aircraft "Black Box" Data*. Monterey California AMM: Naval Post Graduate School.
12. SanDisk Manual. From http://www.cs.ucr.edu/%7Eamitra/sdcard/ProdManualSDCardv1.9.pdf
13. Semiconductor, National (August 2000). *LM386 Low Voltage Audio Power Amplifier*. Texas: Texas Instrument Dallas.
14. *WAV format.* From http://netghost.narod.ru/gff/graphics/summary/micriff.htm
15. *Wilson, Scott (jan 20,2003). WAVE PCM SOUND FILE FORMAT* From http://www.spies.com/sox
16. http;//www.hajsmy.us/2012/06/inilah alas an-fokker-27-tak dilengkapi.html