



PROSIDING

SEMINAR NASIONAL INFORMATIKA DAN APLIKASINYA SNIA - TAHUN 2017

📅 Rabu, 27 September 2017

📍 Hotel Mason Pine Kota Baru Parahyangan Bandung Barat



TEMA

Computer Crime & Digital Evidence

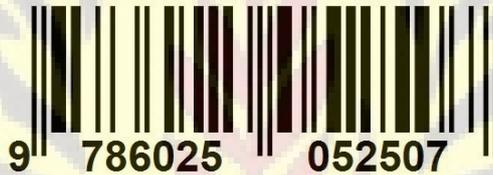


JURUSAN INFORMATIKA

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN
UNIVERSITAS JENDERAL ACHMAD YANI

Dipublikasikan Tahun 2017 oleh:
Jurusan Informatika
Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Jenderal Achmad Yani
Cimahi - Jawa Barat

ISBN 978-602-50525-0-7



Panitia tidak bertanggung jawab terhadap isi paper dari peserta



PROSIDING SEMINAR NASIONAL

“COMPUTER CRIME AND DIGITAL EVIDENCE”

Cimahi, 27 September 2017

Editor

Dr. Esmeralda C. Djamal, S.T., M.T.

Layout Editor

Wina Witanti, S.T., M.T.

Agus Komarudin, S.Kom., M.T.

Puspita Nurul Sabrina, S.Kom., M.T.

Penerbit dan Redaksi:

Jurusan Informatika Fakultas MIPA

Universitas Jenderal Achmad Yani (Unjani)

Jl. Terusan Jenderal Sudirman Cimahi, 40533

Telp./Fax : 022-6631302

Website : <http://snia.unjani.ac.id>

Email : sniaunjani@gmail.com

Cetakan Pertama: September 2017

ISBN : 978-602-50525-0-7

Hak Cipta © 2017 pada penulis

Dilarang memperbanyak sebagian atau seluruh isi buku ini dalam bentuk apa pun tanpa izin tertulis dari penulis atau penyelenggara SNIA 2017.



KOMITE SNIA 2017

PELINDUNG

Hernandi Sujono, S.Si., M.Si.

Dekan Fakultas MIPA Universitas Jenderal Achmad Yani (Unjani)

PENASEHAT

Yulison H. Chrisnanto, S.T., M.T. – Wakil Dekan I Fakultas MIPA Unjani

Senadi Budiman, Drs., M.Si. – Wakil Dekan III Fakultas MIPA Unjani

PENANGGUNG JAWAB

Gunawan Abdillah, S.Si., M.Cs. – Ketua Jurusan Informatika

KETUA PELAKSANA

Asep Id Hadiana, S.Si., M.Kom.

STEERING COMMITTEE

Dr. Esmeralda C. Djamal, S.T., M.T. (Universitas Jenderal Achmad Yani)

Yulison H. Chrisnanto, S.T., M.T. (Universitas Jenderal Achmad Yani)

Gunawan Abdillah, S.Si., M.T. (Universitas Jenderal Achmad Yani)

Hernandi Sujono, S.Si., M.Si. (Universitas Jenderal Achmad Yani)

Tacbir Hendro P., S.Si., M.T. (Universitas Jenderal Achmad Yani)

Senadi Budiman, Drs., M.Si. (Universitas Jenderal Achmad Yani)

Kridanto Surendro, Ir., M.Sc., Ph.D. (Institut Teknologi Bandung)

Prof. Dr. Iping Supriana, DEA (Institut Teknologi Bandung)

Dr. Savitri Galih, S.Si., M.T. (Universitas Widyatama)

REVIEWER

Dr. Rer. Nat. Cecilia Esti Nugraheni, S.T., M.T. (Universitas Katholik Parahyangan)

Dr. Esmeralda Contessa Djamal, S.T., M.T. (Universitas Jenderal Achmad Yani)

Dr. Asep Najmurokhman, S.T., M.T. (Universitas Jenderal Achmad Yani)

Gunawan Abdillah, S.Si., M.Cs. (Universitas Jenderal Achmad Yani)

Kridanto Surendro, Ir., M.Sc., Ph.D. (Institut Teknologi Bandung)

Retantyo Wardoyo, Drs., M.Sc., Ph.D. (Universitas Gadjah Mada)

Wina Witanti, S.T., M.T. (Universitas Jenderal Achmad Yani)

Dr. Rila Mandala, Ir., M.Eng. (Institut Teknologi Bandung)

Dr. Tedjo Darmanto, S.Si., M.T. (STIMK AMIK Bandung)

Dr. Rinaldi Munir, Ir., M.T. (Institut Teknologi Bandung)

Dr. Savitri Galih, S.Si., M.T. (Universitas Widyatama)

Dr. Asep Sholahuddin, M.T (Universitas Padjadjaran)

Dr. Ayi Purbasari, S.T., M.T. (Universitas Pasundan)

PANITIA

Wakil Ketua

Fajri Rakhmat Umbara, S.T., M.T.

Sekretaris

Agus Komarudin, S.Kom., M.T.

Puspita Nurul Sabrina, S.Kom., M.T.

Meryana Putri R.

Wawa Nurazizah

Bendahara

Wina Witanti, S.T., M.T.

Tacbir Hendro P., S.Si., M.T.

Sri Wahyuningsih, A.Md.

Dion Christian

Divisi Acara

Dian Nursantika, S.Kom., M.Cs.

Erna Piantari, S.Komp., M.T.

Deka Panca Gustiawan

Else Lies Ibanez

Erry Fuadilah

Asti Fath

Divisi Makalah dan Persidangan

Dr. Esmeralda C. Djamal, S.T., M.T.

Dr. Eddie Krishna Putra, Drs., M.T.

Yulison H. Chrisnanto, S.T., M.T.

Kartika Nur Oktaviani

Ira Oktavia

Divisi Publikasi dan Dokumentasi

Rezki Yuniarti, S.Si., M.T.

Asri Maspupah, S.ST., M.T.

Rizky Alimansyah

Rizkia Ilham Ramadhan

M. Fauzan Ar Rasyid

Kholidah Syadiah

Divisi Humas dan Dana Usaha

Faiza Renaldi, S.T., M.Sc.

Ridwan Ilyas, S.Kom., M.T.

Irma Santikarama, S.Kom., M.T.

Firman Haidy

Khanif Azhar Anas Waluyo

Diah Hasna Salsabila

Ankky Suchiadilla

Digital Repository Universitas Jember

Divisi Konsumsi

Ade Kania Ningsih, S.Si., M.Stat.

Komariah

Yulia Puspita

M. Abdul Dwiyanto Suyudi

Rikhsainy Sekar Vinanjung

Fauzi Maulana Kusuma

Ranny Anggraeni

Resa Anida

Divisi Perlengkapan dan Transportasi

Rustandi, S.Ip.

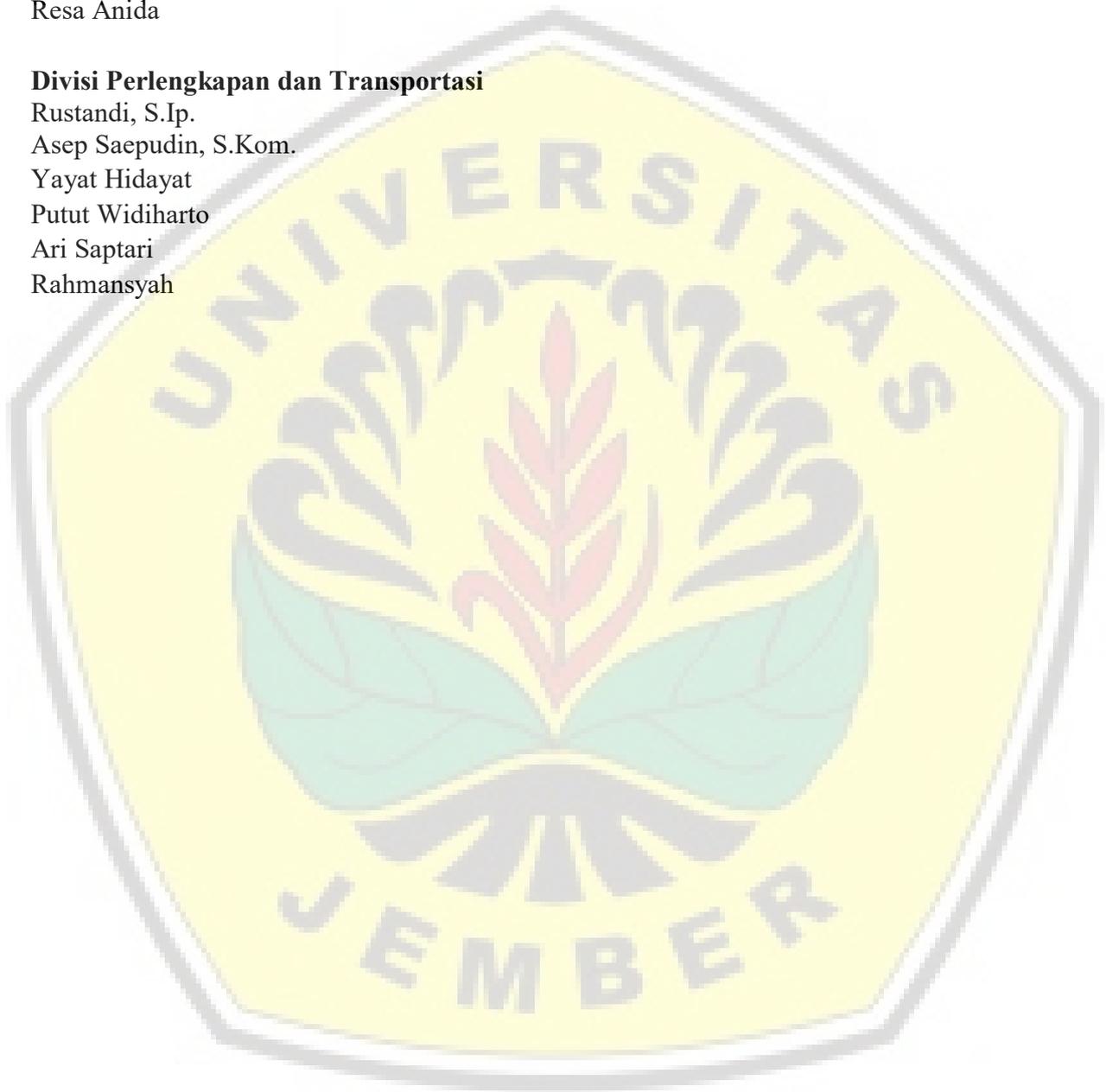
Asep Saepudin, S.Kom.

Yayat Hidayat

Putut Widiharto

Ari Saptari

Rahmansyah





SAMBUTAN KETUA PELAKSANA

Assalammu'alaikum wa rahmatullaahi wa barakaatuh.
Salam sejahtera bagi kita semua.

Segala puji dan syukur kita panjatkan ke hadirat Allah SWT, atas berkat dan rahmat serta hidayah-Nya maka Seminar Nasional Informatika dan Aplikasinya (SNIA) 2017 dengan tema “*Computer Crime and Digital Evidance*” yang diselenggarakan pada tanggal 27 September 2017 di Jurusan Informatika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Jenderal Achmad Yani (Unjani) dapat terlaksana.

Seminar Nasional Informatika dan Aplikasinya 2017 merupakan seminar nasional ketiga yang dilaksanakan oleh Jurusan Informatika Fakultas Matematika dan Ilmu Pengetahuan Alam (FMIPA) Unjani dan kegiatan ini rutin diadakan 2 (dua) tahun. Seminar ini menjadi sarana bagi para akademisi, peneliti, praktisi dan pengguna teknologi informasi di Indonesia, untuk menuangkan ide/penelitian dalam bentuk tulisan.

Prosiding yang diterima berasal dari seluruh Indonesia. Paper yang dimuat dalam Prosiding SNIA 2017 telah melalui tahapan evaluasi oleh reviewer yang berkompeten di bidangnya. Besar harapan kami, Prosiding SNIA 2017 akan memberikan manfaat, terutama tentang bagaimana berbagi informasi antar peneliti, berbagi antara peneliti dan industri, serta bagaimana cerita membangun sukses bersama.

Dalam kesempatan ini, panitia SNIA 2017 mengucapkan terima kasih yang sebesar-besarnya kepada steering committee, para reviewer, panitia pelaksana, pembicara utama (*keynote speaker*), humas Unjani, para sponsor dan peserta yang telah berpartisipasi serta memberikan dukungan hingga acara ini dapat terlaksana.

Akhir kata kami terima kasih bagi para pemakalah dan peserta yang telah berpartisipasi pada Seminar Nasional Informatika dan Aplikasinya (SNIA) 2017 yang bertempat di Mason Pine Hotel, Bandung Barat dan semoga Allah SWT selalu memberi rahmat, hidayah dan perlindungan-Nya kepada kita semua.

Wassalamu'alaikum wa rahmatullaahi wa barakaatuh.
Ketua Pelaksana SNIA 2017

Asep Id Hadiana, S.Si., M.Kom.



SAMBUTAN KETUA JURUSAN INFORMATIKA

Assalammu'alaikum warahmatullaahi wabarakaatuh.

Seminar Nasional Informatika dan Aplikasinya (SNIA) merupakan agenda dua tahunan yang diselenggarakan oleh Jurusan Informatika FMIPA Universitas Jenderal Achmad Yani. SNIA sudah dilaksanakan sebanyak dua kali yaitu pada tahun 2013 dan 2015. Setiap pelaksanaannya, SNIA selalu mengangkat tema ilmu informatika yang sedang berkembang pada masanya. Saat ini tema yang diangkat dalam SNIA 2017 adalah "*Computer Crime and Digital Evidence*". Pengangkatan tema ini dilatarbelakangi oleh penggunaan internet di Indonesia yang semakin berkembang. Berdasarkan hasil survey Kominfo (Kementerian Komunikasi dan Informatika), pengguna internet di Indonesia telah mencapai 63 juta orang. Hal ini, menandai bahwa era digitalisasi sudah mulai merambah di Indonesia. Tak dapat dipungkiri, bahwa perkembangan era digitalisasi disertai juga dengan banyaknya kejadian kejahatan digital atau dikenal sebagai *cybercrime*. *Cybercrime* atau kejahatan digital merupakan tindak kejahatan yang dilakukan dengan menggunakan media berbasis komputer baik secara *offline* maupun *online*.

Contoh kasus *cybercrime* yang sedang marak sekarang ini adalah banyaknya pemberitaan yang tidak benar (berita hoax). Dampak pemberitaan hoax ini sangat besar, bahkan dapat memecah belah persatuan NKRI dan merusak politik serta perekonomian Indonesia. *Digital forensic* merupakan salah satu cabang ilmu yang mempelajari investigasi, analisa, *recovery* dan *management* data dari media digital yang muncul akibat adanya *cybercrime*. Mekanisme *digital forensic* dalam membuka tabir *cybercrime* akan dibahas dalam SNIA 2017 yang diselenggarakan di Hotel Mason Pine, pada tanggal 27 September 2017. Dengan diselenggarakannya seminar ini, diharapkan dapat memberikan wawasan dan meningkatkan kesadaran masyarakat terutama sivitas akademika, terhadap ancaman *cybercrime* dan penanggulangannya dengan *digital forensic*. Selain itu, tujuan lainnya dari penyelenggaraan SNIA 2017 adalah untuk menjadi suatu ajang media diskusi dan publikasi berbagai hasil penelitian di bidang Teknologi Informasi dan Komunikasi (TIK).

Wassalamu'alaikum wa rahmatullaahi wa barakaatuh.

Ketua Jurusan Informatika Unjani

Gunawan Abdillah, S.Si., M.Cs.



JADWAL ACARA SNIA 2017 Mason Pine Hotel, 27 September 2017

Waktu			Keterangan
08:00	-	09:00	Pendaftaran ulang peserta dan pemakalah
09:00	-	09:15	Opening SNIA 2017
09:15	-	09:25	Sambutan dari Rektor Unjani
09:25	-	09:35	Sambutan dari Ketua Jurusan Informatika Unjani
09:35	-	09:45	Sambutan dari Ketua Panitia SNIA 2017
09:45	-	10:00	Foto bersama Rektor, Ketua Jurusan dan Ketua Panitia
10:15	-	10:30	Coffee break
10:30	-	11:00	Pembicara 1
11:00	-	11:30	Pembicara 2
11:30	-	12:00	Pembicara 3
12:00	-	12:20	Diskusi dan tanya jawab
12:20	-	12:30	Foto bersama seluruh pembicara, pemakalah dan peserta
12:30	-	13:00	Istirahat, shalat dan makan siang
13:00	-	15:15	Sesi paralel 1
15:15	-	15:30	Istirahat, shalat
15:30	-	17:00	Sesi paralel 2
17:00	-	17:10	Penutupan dari ketua panitia
17:10	-	17:20	Foto bersama seluruh panitia
17:20	-	17:30	Closing

JADWAL SESI PARALEL

Keterangan Bidang Ilmu:

- A. Sistem Cerdas dan Sistem Pendukung Keputusan
- B. Sistem Informasi dan Arsitektur Informasi
- C. Security, Internet of Things, Audit Sistem Informasi, Human Computer Interaction dan Animasi
- D. Aplikasi Mobile, Website, dan Komputasi

Sesi Paralel *Call For Paper 1*

Waktu	R-A	R-B	R-C	R-D
13:00-13:15	A-01	B-01	C-01	D-01
13:15-13:30	A-02	B-02	C-02	D-02
13:30-13:45	A-03	B-03	C-03	D-03
13:45-14:00	A-04	B-04	C-04	D-04
14:00-14:15	A-05	B-05	C-05	D-05
14:15-14:30	A-06	B-06	C-06	D-06
14:30-14:45	A-07	B-07	C-07	D-07
14:45-15:00	A-08	B-08	C-08	D-08
15:00-15:15	A-09	B-09	C-09	D-09
ISTIRAHAT, SHALAT				

Sesi Paralel *Call For Paper 2*

Waktu	R-A	R-B	R-C	R-D
15:30-13:45	A-10	B-10	C-10	D-10
15:45-16:00	A-11	B-11	C-11	D-11
16:00-16:15	A-12	B-12	C-12	D-12
16:15-16:30	A-13	B-13	C-13	D-13
16:30-16:45	A-14	B-14	C-14	D-14
16:45-17:00	A-15	B-15	C-15	D-15

SESI PARALEL PERTAMA

Sesi Paralel Call For Paper 1: 13:00 – 15:15

Ruang A

Moderator: Dr. Esmeralda C. Djamal

Waktu	Kode	Judul, Pemakalah, Asal Institusi
13:00-13.15	A-01	Desain dan Implementasi Robot Heksapoda dengan Misi Pemadaman Api Asep Najmurokhman, Kusnandar, Bambang HSR Wibowo dan Nizwar A. R. Program Studi Teknik Elektro Unjani
13.15-13.30	A-02	Expert System: Rekomendasi System Gadget Menggunakan Forward Chaining dan Pendekatan Berbasis Aturan Sulis Setiowati Departemen Teknik Elektro dan Teknologi Informasi, UGM
13.30-13.45	A-03	Evaluasi Sentence Extraction pada Peringkasan Dokumen Otomatis Kania Evita Dewi dan Nelly Indriani Widiastuti Program Studi Teknik Informatika Unikom
13.45-14.00	A-04	Aksi Game Berbasis Brain Computer Interface dengan Spektral Daya dan Learning Vector Quantization Aditya Setiawan Putra, Esmeralda C. Djamal, dan Rezki Yuniarti Program Studi Informatika Unjani
14.00-14.15	A-05	Sistem Pendukung Keputusan Penentuan Uang Kuliah Tunggal dengan Menggunakan Metode Wighted Product Rusdi Efendi, Desi Andreswar, dan Imanuel Barus Program Studi Teknik Informatika Universitas Bengkulu
14.15-14.30	A-06	Perbandingan Jumlah Pinalti Alokasi Task pada Penjadwalan Kerja dengan Perhitungan Manual dan Algoritma Genetika Asri Maspupah dan Ani Rahmani Program Studi Informatika Unjani
14.30-14.45	A-07	Perancangan Sistem Pendukung Keputusan Penempatan Kecabangan TNI AD Menggunakan Metode Analytic Hierarchy Process dan Simple Additive Weighting Kreshna Arya Prasetya, Wina Witanti dan Ridwan Ilyas Program Studi Informatika Unjani
14.45-15.00	A-08	Sistem Rekomendasi Program Pelatihan untuk Masyarakat Menggunakan Metode Profile Matching Fariz Yusran Baehaki, Gunawan Abdillah, dan Ridwan Ilyas Program Studi Informatika Unjani
15.00-15.15	A-09	Klasifikasi Aksi NPC Berdasarkan Kondisi Karakter Eko Nurdiyanto, Wina Witanti dan Rezki Yuniarti Program Studi Informatika Unjani

Sesi Paralel Call For Paper 1: 13.00 – 15.15

Ruang B

Moderator: Faiza Renaldi, S.T., M.Sc.

Waktu	Kode	Judul, Pemakalah, Asal Institusi
13.00-13.15	B-01	Sistem Informasi Monitoring Wiraniaga Kholid Haryono, Fahmy Abida Asa Firdausi dan Hendrik Program Studi Informatika Universitas Islam Indonesia
13.15-13.30	B-02	Pemodelan Sistem Informasi Pengajuan Pengambilan Data Penelitian pada Bankesbangpol Kota Palembang Arsia Rini dan Fatmariansi Program Studi Management Informatika Politeknik PalComTech
13.30-13.45	B-03	Pemodelan Perangkat Lunak Pemilihan Ketua Program Studi Berprestasi Berbasis Object Oriented Herlinda Kusmiati dan D. Tri Octafian Program Studi Sistem Informasi Politeknik PalComTech
13.45-14.00	B-04	Sistem Informasi Bale Adat dan Beruqaq Suku Sasak Lombok Berbasis Konten Bergerak Dadang Priyanto dan Raesul Azhar Program Studi Teknik Informatika STMIK Bumigora Mataram
14.00-14.15	B-05	Pemodelan Enterprise Architecture di Sekolah Tinggi Kesehatan Irma Santikarama dan Diana Trivena Yulianti Program Studi Informatika Unjani
14.15-14.30	B-06	Implementasi Executive Information System pada Aplikasi Sistem Informasi Akademik Berbasis Web Cecep Muhamad Sidik dan Andi Nur Rachman Program Studi Teknik Informatika Universitas Siliwangi
14.30-14.45	B-07	Penerapan Modul Enterprise Resource Planning dan Supply Chain Management pada Proses Bisnis Rodliatum Mardliyyah AlHadi dan Galih Suprayitno Program Studi Sisten Informasi Universitas Trilogi
14.45-15.00	B-08	Perancangan Sistem Informasi Koperasi dan UMKM Berbasis Technopreneur, Daya Saing dan Pemasaran Dony Waluya Firdaus dan Dimas Widayasastrena Program Studi Komputerisasi Akuntansi Unikom
15.00-15.15	B-09	Purwarupa Perangkat Lunak Pendeteksi Pola Jawaban Siswa Menggunakan Algoritma Apriori Sandi Fajar Rodiyansyah dan Ardi Mardiana Program Studi Teknik Informatika Universitas Majalengka

Digital Repository Universitas Jember

Sesi Paralel Call For Paper 1: 13:00 – 15:15

Ruang C

Moderator: Dr. Savitri Galih, S.Si., M.T.

Waktu	Kode	Judul, Pemakalah, Asal Institusi
13:00-13:15	C-01	Model Enkripsi XML pada Output DFXML untuk Pengamanan Metadata Bukti Digital Danar Cahyo Prakoso dan Yudi Prayudi Program Studi Informatika Forensik Digital Universitas Islam Indonesia
13:15-13:30	C-02	Implementasi Steganografi Citra Digital Pemberkasan Arsip Menggunakan Metode Least Significant Bit (LSB) Yanuar Nurdiansyah dan Ayu Lusya Fitrasari Riftana Program Studi Sistem Informasi Universitas Jember
13:30-13:45	C-03	Konsep Lemari Penyimpanan Bukti Digital Menggunakan Struktur Bahasa XML Krisna Widatama dan Yudi Prayudi Program Studi Teknik Informatika Universitas Islam Indonesia
13:45-14:00	C-04	Pemodelan Perangkat Lunak Audit Mutu Akademik Internal Berbasis Object Oriented Adelin dan Hendra Efendi Program Studi Sistem Informatika STMIK PalComTech
14:00-14:15	C-05	Implementasi Algoritma Twofish pada Sistem Informasi Pengarsipan Yanuar Nurdiansyah dan Agil Bi Aviv Taufiqi Program Studi Sistem Informasi Universitas Jember
14:15-14:30	C-06	Penerapan Teknologi M-Commerce di Kampung Kue Indra Budi Trisno, Yulius Hari, Andrean Novan dan Minny Elisa Yanggah Program Studi Teknik Informatika Universitas Widya Kartika Surabaya
14:30-14:45	C-07	Pengembangan dan Usability Testing Aplikasi Semi-Immersive Virtual Reality untuk Pembelajaran Sejarah Faizal I., Febryani P. P., Fahmi S. N., Eka Q. M. S, Mira S., Erick P., Ino S. Program Studi Teknik Informatika Universitas Padjadjaran
14:45-15:00	C-08	Pengujian Perangkat Lunak Rudi Setiawan Program Studi Sistem Informasi Universitas Trilogi
15:00-15:15	C-09	Perancangan Sistem Keamanan Rumah dengan Mikrokontroler ATmega16 pada Perumahan di Kabupaten Majalengka Deffy Susanti dan Whydiantoro Program Studi Teknik Informatika Universitas Majalengka

Digital Repository Universitas Jember

Sesi Paralel Call For Paper 1: 13:00 – 15:15

Ruang D

Moderator: Yulison Herry Chrisnanto, S.T., M.T.

Waktu	Kode	Judul, Pemakalah, Asal Institusi
13:00-13:15	D-01	Klasifikasi Objek Kode Tangan pada Pengenalan Isyarat Alphabet Bahasa Isyarat Indonesia (Bisindo) Rohmat Indra Borman, Bentar Priopradono dan Abdul Rahman Syah Program Studi Informatika Universitas Teknokrat Indonesia
13:15-13:30	D-02	Akurasi Algoritma C4.5 dalam Klasifikasi Data 5K2S Des Suryani, Ause Labellapansa, dan Cahaya Fitri Program Studi Teknik Informasi Universitas Islam Riau
13:30-13:45	D-03	Aplikasi Forecasting untuk Prediksi Jumlah Penderita Penyakit Menggunakan Metode Regresi Linier Andi Nur Rachman, Alfi Nijamul B., dan Cecep Muhamad SR. Program Studi Informatika Universitas Siliwangi
13:45-14:00	D-04	Data Mining dengan Teknik Clustering Menggunakan Algoritma K-Means pada Data Transaksi Superstore Priati dan Ahmad Fauzi Program Studi Sistem Informasi Universitas Buana Perjuangan Karawang
14:00-14:15	D-05	Evaluasi K-Means dan K-Medoids pada Dataset Kecil Rima Dias Ramadhani dan Dwi Januarita AK. Program Studi Informatika Sekolah Tinggi Teknologi Telematika Telkom
14:15-14:30	D-06	Aplikasi Manajemen Keuangan Sekolah dengan Notifikasi Berbasis SMS Gateway Aldy Putra Aldya dan Heni Sulastri Program Studi Teknik Informatika Universitas Siliwangi
14:30-14:45	D-07	Evaluasi Penggunaan Animasi dengan Blender pada Materi Komputasi Paralel Leonard Goeirmento Program Studi Informatika Universitas Mercu Buana
14:45-15:00	D-08	Prediksi Rating Drama Korea Menggunakan Algoritma Iterative Dichotomiser 3 Hidayatin Novi Nurfajriah, Wina Witanti dan Rezki Yuniarti Program Studi Informatika Unjani
15:00-15:15	D-09	Rancang Bangun Aplikasi Keluhan Mahasiswa Berbasis Android Salman Jaya Sempurna dan Abi Arfianoris Program Studi Sistem Informasi Universitas Trilogi

SESI PARALEL KE DUA

Sesi Paralel Call For Paper 2: 15:30 – 17:00

Ruang A

Moderator: Dr. Esmeralda C. Djamal, S.T., M.T.

Waktu	Kode	Judul, Pemakalah, Asal Institusi
15:30-15:45	A-10	Perancangan Motif Batik dengan Model Fraktal IFS Tedjo Darmanto Program Studi Teknik Informatika STMIK AMIK Bandung
15:45-16:00	A-11	Optimalisasi Penjadwalan Jaga Dokter dan Tenaga Medik di Rumah Sakit Dustira Menggunakan Algoritma Genetika Yuli Yudriani, Esmeralda C. Djamal dan Ridwan Ilyas Program Studi Informatika Unjani
16:00-16:15	A-12	Sistem Pendukung Keputusan Pemilihan Dokter Kandungan Menggunakan TOPSIS Nureni Firdianti, Gunawan Abdillah dan Agus Komarudin Program Studi Informatika Unjani
16:15-16:30	A-13	Optimalisasi Menu Makan Diet Sehat Menggunakan Algoritma Genetika William Faisal Mustafa, Esmeralda C. Djamal, dan Rezki Yuniarti Program Studi Informatika Unjani
16:30-16:45	A-14	Penerapan Algoritma C45 untuk Penilaian Karyawan pada Restoran Cepat Saji Harry Dhika dan Fitriana Destiawati Program Studi Informatika Universitas Indraprasta PGRI
16:45-17:00	A-15	Analytic Hierarchy Process dengan Multi-Level Kriteria pada Sistem Pemilihan Hotel Puspita Nurul Sabrina Program Studi Informatika Unjani

Sesi Paralel Call For Paper 2: 15:30 – 17:00

Ruang B

Moderator: Faiza Renaldi, S.T., M.Sc.

Waktu	Kode	Judul, Pemakalah, Asal Institusi
15:30-15:45	B-10	Perancangan Arsitektur Aplikasi Open Source untuk Koperasi Generasi Baru Estiyan Dwipriyoko dan Yiyi Supendi Program Studi Informatika Universitas Langlangbuana
15:45-16:00	B-11	Analisa dan Perancangan Aplikasi Transaksi Elektronik untuk Transportasi Menggunakan Fingerprint (E-Transportation) Lani Fitria Damayanti dan Azka Taufiq Program Studi Sistem Informasi Universitas Trilogi
16:00-16:15	B-12	Disain dan Analisis Pengembangan Program Aplikasi IDMS dengan Metodologi Scrum Framework O. Ginanjar, Asep Sholahudin, dan Erick Paulus Program Studi Teknik Informatika Universitas Padjadjaran
16:15-16:30	B-13	Perencanaan Strategis Sistem Informasi Manajemen di Politeknik Praktisi Bandung Ponsen Sindu Prawito Program Studi Management Informatika Politeknik Praktisi Bandung
16:30-16:45	B-14	Kajian Sebuah Sistem Informasi Eksekutif Universitas Jenderal Achmad Yani dengan Pendekatan Online Analytical Processing Wina Witanti, Faiza Renaldi dan Iwan Ridwan Program Studi Informatika Unjani
16:45-17:00	B-15	Pembangunan Sistem Informasi Perkembangan Studi Mahasiswa Berbasis Mobile Irma Santikarama, Puspita Nurul Sabrina, dan Faiza Renaldi Program Studi Informatika Unjani

Sesi Paralel Call For Paper 2: 15:30 – 17:00

Ruang C

Moderator: Dr. Savitri Galih, S.Si., M.T.

Waktu	Kode	Judul, Pemakalah, Asal Institusi
15:30-15:45	C-10	Manajemen Risiko Teknologi Informasi Berbasis National Institute of Standards and Technology SP800-30 di Universitas Jenderal Achmad Yani Ae Saepul, Yulison Herry C. dan Asep Id Hadiana Program Studi Informatika Unjani
15:45-16:00	C-11	Penilaian Tata Kelola Keamanan Informasi Perpustakaan dengan Framework Cobit 5 Yoki Muchsam Program Studi Teknik Komputer STMIK AMIK Bandung
16:00-16:15	C-12	Prototipe Kendali Lampu Jarak Jauh untuk Home Automation Systems Berbasis Arduino Mega dan Android Application Handoko R. Iskandar, Indra Bayu Prasetya, Imam Arifin dan Akhmad Triaji Program Studi Teknik Elektro Unjani
16:15-16:30	C-13	Implementasi Internet of Things (IoT) pada Sistem Pencegahan Dini Potensi Kebakaran Aditya Wibowo, Rudi Setiawan dan Depi Yulyanti Program Studi Sistem Informasi Universitas Trilogi
16:30-16:45	C-14	Implementasi Internet of Things (IoT) pada Sistem Penanganan Banjir Ilham Abdulrachman, Bayu Trianto dan Doni Kurniawan Program Studi Sistem Informasi Universitas Trilogi
16:45-17:00	C-15	Program Animasi sebagai Media Interaktif Mardhiatul Husna Program Studi Administrasi Niaga Universitas Politeknik Negeri Medan

Digital Repository Universitas Jember

Sesi Paralel Call For Paper 2: 15:30 – 17:00

Ruang D

Moderator: Yulison Herry Chisnanto, S.T., M.T.

Waktu	Kode	Judul, Pemakalah, Asal Institusi
15:30-15:45	D-10	Implementasi Web Service NuSOAP pada Pengembangan Akses SIM Akademik Falahah Suprpto dan Rizky Dwi Saputra Program Studi Teknik Informatika Universitas Widyatama
15:45-16:00	D-11	Rancang Bangun Sistem Informasi Perpustakaan Universitas Trilogi Berbasis Website Galih Wahyu Baskoro Program Studi Sistem Informasi Universitas Trilogi
16:00-16:15	D-12	Social Network Service dan Web Mapping pada Situs Pariwisata Herdi Ashaury dan Mira Kania Sabariah Program Studi Informatika Unjani
16:15-16:30	D-13	Komparasi Farthest First dan K-Mean pada Clustering Huruf Alphabet Dian Nursantika dan Eddie Krishna Putra Program Studi Informatika Unjani
16:30-16:45	D-14	Rancang Bangun Sistem Informasi Manajemen Peternak Ayam di Koperasi Sinar Mulya Menggunakan Microsoft Visual Basic 2010 .Net Ade Bastian, Tri Ferga Prasetyo dan Nia Kurniati Program Studi Teknik Informatika Universitas Majalengka
16:45-17:00	D-15	Aplikasi Monitoring Hasil Studi Mahasiswa Teknik Informatika Politeknik Negeri Tanah Laut Berbasis Web Mobile dan SMS Gateway Herpendi dan Wan Yuliyanti Program Studi Teknik Informatika Politeknik Negeri Tanah Laut

DAFTAR ISI

	Halaman
IDENTITAS PROSIDING	i
JUDUL PROSIDING	ii
KOMITE SNIA 2017	iii
SAMBUTAN KETUA PELAKSANA	vi
SAMBUTAN KETUA JURUSAN INFORMATIKA	vii
JADWAL ACARA SNIA 2017	viii
JADWAL SESI PARALEL	ix
SESI PARALEL PERTAMA	x
SESI PARALEL KE DUA	xiv
DAFTAR ISI	xviii
DAFTAR PEMAKALAH	xix



DAFTAR PEMAHALAH

	Halaman
A. SISTEM CERDAS DAN SISTEM PENDUKUNG KEPUTUSAN	
Desain dan Implementasi Robot Heksapoda dengan Misi Pemadaman Api Asep Najmurokhman, Kusnandar, Bambang HSR Wibowo dan Nizwar A. R. Program Studi Teknik Elektro Universitas Jenderal Achmad Yani	A-1
Expert System: Rekomendasi System Gadget Menggunakan Forward Chaining dan Pendekatan Berbasis Aturan Sulis Setiowati Departemen Teknik Elektro dan Teknologi Informasi Universitas Gadjah Mada	A-2
Evaluasi Sentence Extraction pada Peringkasan Dokumen Otomatis Kania Evita Dewi dan Nelly Indriani Widiastuti Program Studi Teknik Informatika Universitas Komputer Indonesia	A-8
Aksi Game Berbasis Brain Computer Interface dengan Spektral Daya dan Learning Vector Quantization Aditya Setiawan Putra, Esmeralda C. Djamal, dan Rezki Yuniarti Program Studi Informatika Universitas Jenderal Achmad Yani	A-13
Sistem Pendukung Keputusan Penentuan Uang Kuliah Tunggal dengan Menggunakan Metode Wighted Product Rusdi Efendi, Desi Andreswar, dan Imanuel Barus Program Studi Teknik Informatika Universitas Bengkulu	A-14
Perbandingan Jumlah Pinalti Alokasi Task pada Penjadwalan Kerja dengan Perhitungan Manual dan Algoritma Genetika Asri Maspupah dan Ani Rahmani Program Studi Informatika Universitas Jenderal Achmad Yani	A-20
Perancangan Sistem Pendukung Keputusan Penempatan Kecabangan TNI AD Menggunakan Metode Analytic Hierarchy Process dan Simple Additive Weighting Kreshna Arya Prasetya, Wina Witanti dan Ridwan Ilyas Program Studi Informatika Universitas Jenderal Achmad Yani	A-21
Sistem Rekomendasi Program Pelatihan untuk Masyarakat Menggunakan Metode Profile Matching Fariz Yusran Baehaki, Gunawan Abdillah, dan Ridwan Ilyas Program Studi Informatika Universitas Jenderal Achmad Yani	A-27
Klasifikasi Aksi NPC Berdasarkan Kondisi Karakter Eko Nurdianto, Wina Witanti dan Rezki Yuniarti Program Studi Informatika Universitas Jenderal Achmad Yani	A-33
Perancangan Motif Batik dengan Model Fraktal IFS Tedjo Darmanto Program Studi Teknik Informatika STMIK AMIK Bandung	A-39

	Halaman
Optimalisasi Penjadwalan Jaga Dokter dan Tenaga Medik di Rumah Sakit Dustira Menggunakan Algoritma Genetika Yuli Yudriani, Esmeralda C. Djamal dan Ridwan Ilyas Program Studi Informatika Universitas Jenderal Achmad Yani	A-40
Sistem Pendukung Keputusan Pemilihan Dokter Kandungan Menggunakan TOPSIS Nureni Firdianti, Gunawan Abdillah dan Agus Komarudin Program Studi Informatika Universitas Jenderal Achmad Yani	A-45
Optimalisasi Menu Makan Diet Sehat Menggunakan Algoritma Genetika William Faisal Mustafa, Esmeralda C. Djamal, dan Rezki Yuniarti Program Studi Informatika Universitas Jenderal Achmad Yani	A-50
Penerapan Algoritma C45 untuk Penilaian Karyawan pada Restoran Cepat Saji Harry Dhika dan Fitriana Destiawati Program Studi Informatika Universitas Indraprasta PGRI	A-55
Analytic Hierarchy Process dengan Multi-Level Kriteria pada Sistem Pemilihan Hotel Puspita Nurul Sabrina Program Studi Informatika Universitas Jenderal Achmad Yani	A-60
 B. SISTEM INFORMASI DAN ARSITEKTUR INFORMASI	
Sistem Informasi Monitoring Wiraniaga Kholid Haryono, Fahmy Abida Asa Firdausi dan Hendrik Program Studi Informatika Universitas Islam Indonesia	B-1
Pemodelan Sistem Informasi Pengajuan Pengambilan Data Penelitian pada Bankesbangpol Kota Palembang Arsia Rini dan Fatmariyani Program Studi Management Informatika Politeknik PalComTech	B-2
Pemodelan Perangkat Lunak Pemilihan Ketua Program Studi Berprestasi Berbasis Object Oriented Herlinda Kusmiati dan D. Tri Octafian Program Studi Sistem Informasi Politeknik PalComTech	B-7
Sistem Informasi Bale Adat dan Beruqaq Suku Sasak Lombok Berbasis Konten Bergerak Dadang Priyanto dan Raesul Azhar Program Studi Teknik Informatika STMIK Bumigora Mataram	B-13
Pemodelan Enterprise Architecture di Sekolah Tinggi Kesehatan Ditinjau dari Designer Perspective Treasury Enterprise Architecture Framework Irma Santikarama dan Diana Trivena Yulianti Program Studi Informatika Universitas Jenderal Achmad Yani	B-17
Implementasi Executive Information System pada Aplikasi Sistem Informasi Akademik Berbasis Web Cecep Muhamad Sidik R. dan Andi Nur Rachman Program Studi Teknik Informatika Universitas Siliwangi	B-18

	Halaman
Penerapan Modul Enterprise Resource Planning dan Supply Chain Management pada Proses Bisnis Rodliatum Mardliyyah AlHadi dan Galih Suprayitno Program Studi Sisten Informasi Universitas Trilogi	B-23
Perancangan Sistem Informasi Koperasi dan UMKM Berbasis Technopreneur, Daya Saing dan Pemasaran Dony Waluya Firdaus dan Dimas Widyasastrena Program Studi Komputerisasi Akuntansi Universitas Komputer Indonesia	B-27
Purwarupa Perangkat Lunak Pendeteksi Pola Jawaban Siswa Menggunakan Algoritma Apriori Sandi Fajar Rodiyansyah dan Ardi Mardiana Program Studi Teknik Informatika Universitas Majalengka	B-33
Perancangan Arsitektur Aplikasi Open Source untuk Koperasi Generasi Baru Estiyan Dwipriyoko dan Yiyi Supendi Program Studi Informatika Universitas Langlangbuana	B-37
Analisis dan Perancangan Aplikasi Transaksi Elektronik untuk Transportasi Menggunakan Fingerprint (E-Transportation) Lani Fitria Damayanti dan Azka Taufiq Program Studi Sistem Informasi Universitas Trilogi	B-43
Analisis dan Disain Pengembangan Program Aplikasi IDMS dengan Metodologi Scrum Framework O. Ginanjar, Asep Sholahudin, dan Erick Paulus Program Studi Teknik Informatika Universitas Padjadjaran	B-47
Perencanaan Strategis Sistem Informasi Manajemen di Politeknik Praktisi Bandung sebagai Optimalisasi Proses Akademik Ponsen Sindu Prawito Program Studi Management Informatika Politeknik Praktisi Bandung	B-53
Kajian Sebuah Sistem Informasi Eksekutif Universitas Jenderal Achmad Yani dengan Pendekatan Online Analytical Processing Wina Witanti, Faiza Renaldi dan Iwan Ridwan Program Studi Informatika Universitas Jenderal Achmad Yani	B-58
Pembangunan Sistem Informasi Perkembangan Studi Mahasiswa Berbasis Mobile Irma Santikarama, Puspita Nurul Sabrina, dan Faiza Renaldi Program Studi Informatika Universitas Jenderal Achmad Yani	B-59
 C. SECURITY, INTERNET OF THINGS, AUDIT SISTEM INFORMASI, HUMAN COMPUTER INTERACTION DAN ANIMASI	
Model Enkripsi XML pada Output DFXML untuk Pengamanan Metadata Bukti Digital Dinar Cahyo Prakoso dan Yudi Prayudi Program Studi Informatika Forensik Digital Universitas Islam Indonesia	C-1

	Halaman
Implementasi Steganografi Citra Digital Pemberkasan Arsip Menggunakan Metode Least Significant Bit (LSB) Yanuar Nurdiansyah dan Ayu Lusita Fitriastari Riftana Program Studi Sistem Informasi Universitas Jember	C-2
Konsep Lemari Penyimpanan Bukti Digital Menggunakan Struktur Bahasa XML Krisna Widatama dan Yudi Prayudi Program Studi Teknik Informatika Universitas Islam Indonesia	C-8
Pemodelan Perangkat Lunak Audit Mutu Akademik Internal Berbasis Object Oriented Adelin dan Hendra Efendi Program Studi Sistem Informatika STMIK PalComTech	C-15
Implementasi Algoritma Twofish pada Sistem Informasi Pengarsipan Yanuar Nurdiansyah dan Agil Bi Aviv Taufiqi Program Studi Sistem Informasi Universitas Jember	C-20
Penerapan Teknologi M-Commerce di Kampung Kue Indra Budi Trisno, Yulius Hari, Andrean Novan dan Minny Elisa Yanggah Program Studi Teknik Informatika Universitas Widya Kartika Surabaya	C-26
Pengembangan dan Usability Testing Aplikasi Semi-Immersive Virtual Reality untuk Pembelajaran Sejarah Faizal I., Febryani P. P., Fahmi S. N., Eka Q. M. S, Mira S., Erick P., Ino S. Program Studi Teknik Informatika Universitas Padjadjaran	C-32
Pengujian Perangkat Lunak Berbasis Flow Graph, Cyclomatic Complexity dan Graph Matrix Rudi Setiawan Program Studi Sistem Informasi Universitas Trilogi	C-37
Perancangan Sistem Keamanan Rumah dengan Mikrokontroler ATmega16 pada Perumahan di Kabupaten Majalengka Deffy Susanti dan Whydiantoro Program Studi Teknik Informatika Universitas Majalengka	C-40
Manajemen Risiko Teknologi Informasi Berbasis National Institute of Standards and Technology SP800-30 di Universitas Jenderal Achmad Yani Ae Saepul, Yulison Herry C. dan Asep Id Hadiana Program Studi Informatika Universitas Jenderal Achmad Yani	C-44
Penilaian Tata Kelola Keamanan Informasi Perpustakaan dengan Framework Cobit 5 Yoki Muchsam Program Studi Teknik Komputer STMIK AMIK Bandung	C-49
Prototipe Kendali Lampu Jarak Jauh untuk Home Automation Systems Berbasis Arduino Mega dan Android Application Handoko R. Iskandar, Indra Bayu Prasetya, Imam Arifin dan Akhmad Triaji Program Studi Teknik Elektro Universitas Jenderal Achmad Yani	C-55

	Halaman
Implementasi Internet of Things (IoT) pada Sistem Pencegahan Dini Potensi Kebakaran Aditya Wibowo, Rudi Setiawan dan Depi Yulyanti Program Studi Sistem Informasi Universitas Trilogi	C-62
Implementasi Internet of Things (IoT) pada Sistem Penanganan Banjir Ilham Abdulrachman, Bayu Trianto dan Doni Kurniawan Program Studi Sistem Informasi Universitas Trilogi	C-67
Program Animasi sebagai Media Interaktif Bahasa Inggris untuk Anak Pra-Sekolah Mardhiatul Husna Program Studi Administrasi Niaga Universitas Politeknik Negeri Medan	C-71
D. APLIKASI MOBILE, WEBSITE DAN KOMPUTASI	
Klasifikasi Objek Kode Tangan pada Pengenalan Isyarat Alphabet Bahasa Isyarat Indonesia (Bisindo) Rohmat Indra Borman, Bentar Priopradono dan Abdul Rahman Syah Program Studi Informatika Universitas Teknokrat Indonesia	D-1
Akurasi Algoritma C4.5 dalam Klasifikasi Data 5K2S Des Suryani, Ause Labellapansa, dan Cahaya Fitri Program Studi Teknik Informasi Universitas Islam Riau	D-5
Aplikasi Forecasting untuk Prediksi Jumlah Penderita Penyakit Menggunakan Metode Regresi Linier Andi Nur Rachman, Alfi Nijamul B., dan Cecep Muhamad SR. Program Studi Informatika Universitas Siliwangi	D-9
Data Mining dengan Teknik Clustering Menggunakan Algoritma K-Means pada Data Transaksi Superstore Priati dan Ahmad Fauzi Program Studi Sistem Informasi Universitas Buana Perjuangan Karawang	D-15
Evaluasi K-Means dan K-Medoids pada Dataset Kecil Rima Dias Ramadhani dan Dwi Januarita AK. Program Studi Informatika Sekolah Tinggi Teknologi Telematika Telkom	D-20
Aplikasi Manajemen Keuangan Sekolah dengan Notifikasi Berbasis SMS Gateway Aldy Putra Aldya dan Heni Sulastri Program Studi Teknik Informatika Universitas Siliwangi	D-25
Evaluasi Penggunaan Animasi dengan Blender pada Materi Komputasi Paralel Leonard Goeirmento Program Studi Informatika Universitas Mercu Buana	D-31
Prediksi Rating Drama Korea Menggunakan Algoritma Iterative Dichotomiser 3 Hidayatin Novi Nurfajriah, Wina Witanti dan Rezki Yuniarti Program Studi Informatika Universitas Jenderal Achmad Yani	D-35

	Halaman
Rancang Bangun Aplikasi Keluhan Mahasiswa Berbasis Android Salman Jaya Sempurna dan Abi Arfianoris Program Studi Sistem Informasi Universitas Trilogi	D-40
Implementasi Web Service NuSOAP pada Pengembangan Akses SIM Akademik Falahah Suprpto dan Rizky Dwi Saputra Program Studi Teknik Informatika Universitas Widyatama	D-45
Rancang Bangun Sistem Informasi Perpustakaan Universitas Trilogi Berbasis Website Galih Wahyu Baskoro Program Studi Sistem Informasi Universitas Trilogi	D-52
Social Network Service dan Web Mapping pada Situs Pariwisata Herdi Ashaury dan Mira Kania Sabariah Program Studi Informatika Universitas Jenderal Achmad Yani	D-56
Komparasi Farthest First dan K-Mean pada Clustering Huruf Alphabet Dian Nursantika dan Eddie Krishna Putra Program Studi Informatika Universitas Jenderal Achmad Yani	D-60
Rancang Bangun Sistem Informasi Manajemen Peternak Ayam di Koperasi Sinar Mulya Menggunakan Microsoft Visual Basic 2010 .Net Ade Bastian, Tri Ferga Prasetyo dan Nia Kurniati Program Studi Teknik Informatika Universitas Majalengka	D-63
Aplikasi Monitoring Hasil Studi Mahasiswa Teknik Informatika Politeknik Negeri Tanah Laut Berbasis Web Mobile dan SMS Gateway Herpendi dan Wan Yuliyanti Program Studi Teknik Informatika Politeknik Negeri Tanah Laut	D-68

Implementasi Steganografi Citra Digital Pemberkasan Arsip Menggunakan Metode Least Significant Bit

Studi Kasus: PT. Angkasa Pura I (Persero) Bandar Udara Internasional Juanda Surabaya

Yanuar Nurdiansyah*, Ayu Lusia Fitrasari Riftana
Program Studi Sistem Informasi, Universitas Jember (UNEJ)
Jl. Kalimantan 37, Jember 68121
yanuar_pssi@unej.ac.id*

Abstrak—Implementasi steganografi citra digital pada pemberkasan arsip menggunakan metode Least Significant Bit (LSB) (Studi kasus: PT. Angkasa Pura I (Persero) Cabang Bandar Udara Internasional Juanda Surabaya) merupakan sistem yang bertujuan untuk memberikan keamanan data pemberkasan arsip. Metode Least Significant Bit (LSB) digunakan untuk menyembunyikan informasi rahasia dari data arsip dengan cara menyisipkan informasi pada media citra. Penyisipan informasi dengan mensubstitusi bit akhir dari informasi dengan bit media citra. Informasi yang sisipkan sebelumnya dienkripsi terlebih dahulu menggunakan Algoritma Twofish untukantisipasi saat informasi yang disisipkan terekstrak oleh pihak tidak berwenang. Metode LSB dipilih karena ukuran informasi yang disisipkan pada metode LSB tidak mengubah media aslinya sehingga metode ini dapat menampung informasi yang tersembunyi tanpa menimbulkan kecurigaan. Sistem pemberkasan arsip yang dibangun berbasis website agar dapat digunakan dengan mudah oleh pengguna. Pembuatan sistem ini dibangun mengadopsi dari model prototipe. Sistem pemberkasan arsip dirancang dan dibangun dengan 2 (dua) hak akses, yaitu admin, dan sekretaris dengan berbagai fitur yang dapat memudahkan penggunaannya. Hasil dari penelitian ini, sistem mampu mengimplementasikan metode LSB untuk memberi keamanan pada data arsip rahasia objek obyek.

Kata kunci—*arsip; steganografi; Least Significant Bit.*

I. PENDAHULUAN

PT. Angkasa Pura I merupakan salah satu perusahaan Badan Usaha Milik Negara (BUMN) yang bergerak pada bidang jasa pengelolaan dan pelayanan penerbangan. Perusahaan berdasar jasa transportasi udara ini telah subur tumbuh dan berkembang di Indonesia. Perusahaan ini membawahi 13 bandara berbasis Internasional, hal ini semakin memantapkan posisinya dalam memberikan pelayanan. PT. Angkasa Pura I sebagai perusahaan komersial kebandaraan memiliki tujuan untuk memberikan pelayanan terbaik, keselamatan dan pelayanan bertaraf internasional.

Bandar Udara Internasional Juanda merupakan salah satu bandar udara yang berada di bawah pengelolaan PT. Angkasa Pura I. Bandar Udara Internasional Juanda sendiri memiliki dua terminal yaitu Terminal 1 (T1) yang melayani penerbangan *domestic*, umroh dan haji sedangkan Terminal 2 (T2) yang melayani penerbangan *domestic* dan internasional. PT. Angkasa Pura I Bandar Udara Internasional Juanda juga

memiliki sebuah kantor yang menangani kegiatan yang ada di bandar udara dan kegiatan administratif perusahaan.

PT. Angkasa Pura I mempunyai tujuan untuk pengoptimalan sumber daya untuk memberikan pelayanan yang bermutu dan meningkatkan nilai perusahaan, serta tingkat kepercayaan masyarakat. Selain meningkatkan nilai tambah yang optimal bagi masyarakat dan lingkungan, perusahaan juga memiliki tujuan untuk meningkat kualitas agar dapat berdaya saing baik dengan perusahaan domestik ataupun internasional.

Hal yang dibutuhkan untuk mewujudkan tujuan perusahaan PT. Angkasa Pura I adalah adanya data pendukung terkait kegiatan dari setiap bagian (*department*) pada PT. Angkasa Pura I. Tujuan kegiatan pada setiap bagian (*department*) dapat berlanjut dengan adanya aktivitas pokok dan aktivitas penunjang. Aktivitas pokok yaitu aktivitas yang secara langsung sedangkan aktivitas penunjang yaitu menunjang aktivitas pokok meliputi kegiatan tata usaha dan administratif.

Kegiatan Tata Usaha merupakan kegiatan yang berhubungan dengan warkat, surat-surat, dan dokumen atau sering disebut arsip. Arsip ini sangat berperan penting bagi sebuah organisasi atau perusahaan karena merupakan pusat atau sumber informasi. Dokumen dalam arsip berperan terhadap perencanaan, penganalisisan, perumusan kebijaksanaan, pengambilan keputusan, pembuatan laporan, penilaian, pengendalian dan pelaksanaan pertanggungjawaban secara tepat, sehingga informasi arsip memiliki hak akses terbatas karena menyimpan rahasia informasi perusahaan.

Informasi tersebut dihimpun secara sistematis dan logis sesuai konteks sehingga menjadi satu konteks yang memiliki hubungan informasi atau biasa disebut pemberkasan arsip. Pemberkasan arsip harus secara benar dan aman agar informasi penting atau rahasia milik perusahaan tidak disalah gunakan oleh pihak yang tak bertanggung jawab. Semakin majunya teknologi dan perkembangan sistem informasi, juga mempengaruhi keamanan sebuah data. Banyaknya peretas yang akan mencoba untuk mendapatkan informasi secara ilegal. Selain itu ancaman juga datang dari pihak dalam atau pekerja dalam organisasi tersebut. Pengamanan data pada pemberkasan arsip untuk menjaga informasi penting atau rahasia, dari ancaman luar atau dalam organisasi itu sendiri. Sehingga pemberkasan arsip pada PT. Angkasa Pura I dapat menerapkan steganografi.

Steganografi merupakan salah satu pengamanan data guna menyamarkan atau menyembunyikan sebuah informasi rahasia. Penerapan steganografi pada pemberkasan arsip dengan memanfaatkan media citra sebagai tempat penyisipannya. Dengan menggunakan media citra akan menghilangkan kecurigaan bahwa tersimpan pesan rahasia di dalamnya. Informasi yang disisipkan di dalam media citra tersebut tidak akan terlihat dengan kasat mata[1].

Banyak metode steganografi yang dapat digunakan untuk pengamanan informasi rahasia di antaranya yaitu metode *Least Significant Bit* (LSB). Metode LSB merupakan metode yang menyisipkan informasi rahasia bukan dengan menambah atau mengurangi melainkan mengganti bit terakhir pada media penyimpanan[2]. Ukuran informasi yang dimasukkan pada metode LSB tidak mengubah media aslinya sehingga metode ini dapat menampung informasi yang tersembunyi tanpa menimbulkan kecurigaan.

Pencegahan sebagai antisipasi ancaman yang mungkin terjadi terhadap informasi dalam gambar stego, maka informasi rahasia tersebut akan diubah sebelum disisipkan pada media. Perubahan informasi yang akan disisipkan dilakukan dengan menggunakan kriptografi algoritma *Twofish*. Algoritma *Twofish* ini digunakan karena di antara algoritma enkripsi yang merupakan finalis dari *Advance Encryption Standard* (AES) pada tahun 1998 di Amerika yaitu *Rijndael*, *Serpent*, *Twofish*, *MARS*, dan *RC6*, algoritma *Twofish* dianggap sebagai algoritma yang memiliki tingkat keamanan yang tinggi.

Berdasarkan paparan di atas, dalam penelitian ini menggunakan steganografi dengan metode LSB pada pemberkasan arsip pada PT. Angkasa Pura I (Persero) Cabang Bandar Udara Internasional Juanda Surabaya, informasi yang akan disisipkan akan diubah terlebih dahulu menggunakan algoritma *Twofish*[3].

Dari latar belakang masalah, tujuan yang ingin dicapai dan manfaat yang ingin diperoleh dalam penelitian ini: (1) untuk merancang dan membangun sistem steganografi citra digital pada pemberkasan arsip menggunakan metode *Least Significant Bit* (LSB) dan (2) untuk mengetahui tingkat *security* dan *robustness* pada sistem.

II. METODE

A. Jenis Penelitian

Penelitian ini menggunakan pendekatan pengembangan (*development research*), dikarenakan penelitian ini bukan untuk membuat atau menguji kebenaran suatu teori maupun hipotesis, melainkan menghasilkan dan mengembangkan produk.

B. Pengumpulan Data

Tahap pengumpulan data dilakukan dengan cara mencari data yang dibutuhkan dalam mengimplementasikan metode LSB pada pemberkasan arsip. Pada tahap ini studi pustaka dan wawancara.

C. Tahapan Penelitian

Tahapan penelitian ini meliputi tahap pengumpulan data dan tahap analisis data. Penelitian dimulai dengan mencari

studi literatur wawancara yang kemudian dilanjutkan ke analisis data untuk merumuskan analisis kebutuhan dari sistem. Setelah analisis kebutuhan terpenuhi, proses selanjutnya yaitu perancangan dan implementasi meliputi desain, *coding* kemudian *testing* aplikasi yang dibangun. Jika terjadi *error* maka akan dilakukan perbaikan sistem. Tahap terakhir yaitu penyusunan laporan.

D. Perancangan Sistem

Tahapan penelitian pengembangan sistem mengadopsi dari model *prototype*. Model *prototype* merupakan model yang harus dievaluasi dan dimodifikasi kembali sesuai dengan kebutuhan pengguna, sehingga memungkinkan pengembangan untuk memahami kebutuhan pengguna[4]. Tahapan penelitian *prototype* meliputi tahap dengan perancangan secara cepat, perancangan *prototype*, evaluasi *prototype*, pengkodean dan pengujian.

1) Perancangan secara Cepat

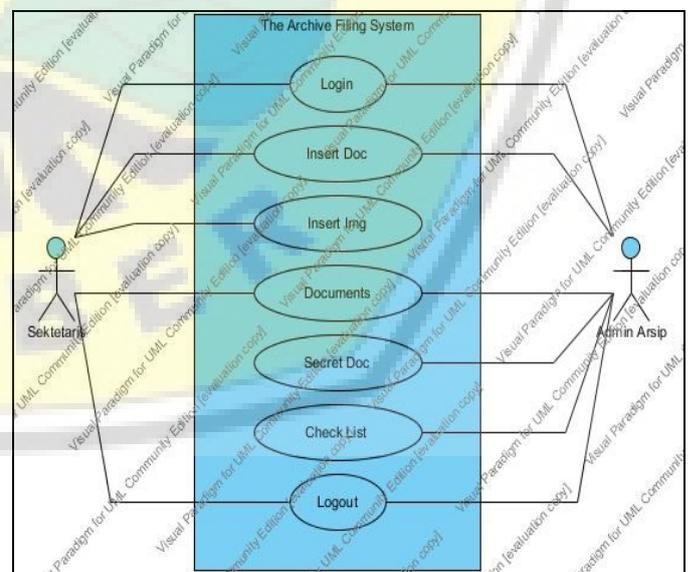
Pada tahap ini dilakukan analisis untuk mendapatkan kebutuhan sistem sesuai dengan keinginan pengguna. Analisis kebutuhan merupakan kegiatan menganalisa hasil informasi yang telah didapat untuk kemudian dikelompokkan menjadi kebutuhan fungsional dan kebutuhan non-fungsional.

2) Perancangan Prototype

Tahap ini merupakan tahap perancangan prototipe dengan membuat perancangan sementara yang digunakan untuk penyajian pada pengguna. Perancangan sementara dibuat dengan membuat tampilan dari sistem. Tampilan yang dibuat berdasarkan hasil dari analisis kebutuhan yang telah didapatkan.

3) Evaluasi Prototype

Evaluasi digunakan untuk mengetahui prototipe yang sudah dibangun telah sesuai dengan keinginan pengguna. Tahap ini peneliti menggunakan *Unified Modeling Language* (UML) yang dirancang menggunakan konsep *Object-Oriented Programming* (OOP). Pemodelan UML yang digunakan antara lain: *Business Process*, *Usecase Diagram* dapat dilihat pada Gambar 1.



Gambar 1. Usecase Diagram

4) Pengkodean

Tahap implementasi dari desain yang telah dibuat menjadi kode program. Hal yang dilakukan dalam implementasi antara lain: penulisan kode program (*coding*) menggunakan bahasa pemrograman *Page Hyper Text Pre-Processor* (PHP) dan manajemen basis data menggunakan MySQL.

5) Pengujian

Pengujian dilakukan terhadap perangkat lunak yang telah dibuat. Tujuan dari tahap ini adalah untuk mengetahui apakah sistem yang dibuat sudah sesuai dengan kebutuhan serta mencari kesalahan atau *bug*. Terdapat dua pengujian yang dilakukan, yaitu pengujian perangkat lunak meliputi; *White Box Testing* dan *Black Box Testing* serta pengujian metode yang meliputi; pengujian visual, Pengujian *Peak Signal to Noise Ratio* (PSNR) dan pengujian *Robustness*[5][6][7].

III. HASIL DAN DISKUSI

Hasil dan diskusi sistem selama dilakukannya penelitian yang mencakup setiap tahap implementasi dan pengujian sistem penilaian konsumen terhadap sistem pemberkasan arsip menggunakan metode LSB.

A. Hasil Pembuatan Sistem Steganografi Citra Digital pada Pemberkasan Arsip Menggunakan Metode LSB

Tahap ini merupakan tahap pengkodean dari perancangan yang telah dibuat ke dalam bahasa pemrograman. Penelitian ini menggunakan bahasa PHP sebagai bahasa pemrograman. Tahap pengkodean akan menghasilkan beberapa *interface* atau tampilan dari sistem steganografi citra digital pada pemberkasan arsip yang dapat diakses oleh dua pengguna, yaitu admin dan sekretaris. Sistem ini memiliki beberapa fitur. Berikut fitur *Insert Doc*, *Insert Img*, dan *Secret Doc*.

1) Insert Doc

Fitur *insert doc* merupakan fitur untuk menambah data arsip baru. Fitur ini dapat diakses oleh dua pengguna admin dan sekretaris. Pada tampilan fitur terdapat perbedaan antara pengguna, tampilan admin lebih kompleks karena dapat menambahkan data arsip rahasia, sedangkan sekretaris hanya dapat menambahkan data arsip yang tidak rahasia. Tampilan lebih lengkapnya dapat dilihat pada Gambar 2 dan Gambar 3.

Gambar 2. Insert Doc Sekretaris

Gambar 3. Insert Doc Admin

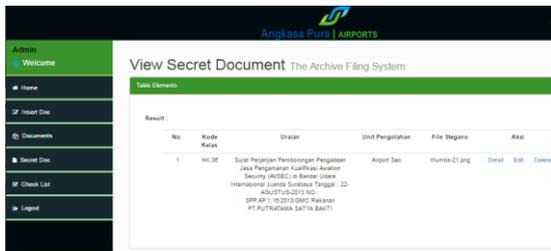
2) Insert Img

Fitur *insert img* merupakan fitur untuk memasukkan gambar baru, yang digunakan sebagai pengajuan arsip rahasia pada admin. Fitur ini diakses oleh sekretaris. Terdapat dua tombol, yaitu *Choose File* yang digunakan untuk memilih *file* yang akan dimasukkan dan *Upload* yang digunakan untuk memasukkan gambar dapat dilihat pada Gambar 4.

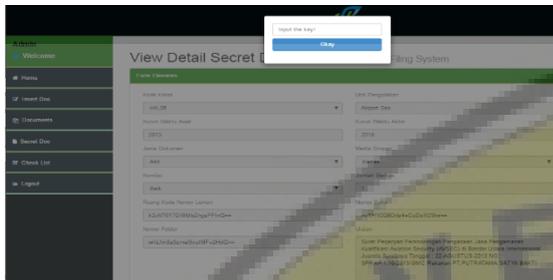
Gambar 4. Insert Img

3) Secret Doc

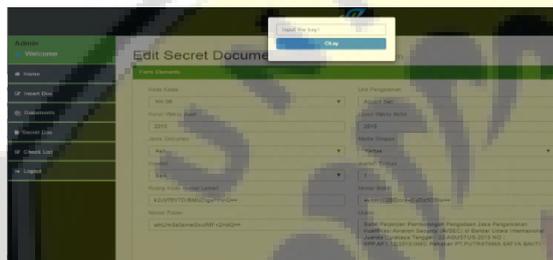
Fitur *secret doc* merupakan fitur untuk mengelola data arsip rahasia yang telah dimasukkan oleh admin berdasarkan pengajuan sekretaris. Fitur ini diakses oleh admin. Pada tampilan fitur ini terdapat tiga tombol, *Detail* digunakan untuk melihat rincian dari data arsip, *Edit* digunakan untuk mengubah data arsip, dan *Delete* digunakan untuk menghapus data, maka akan muncul *popup* untuk melihat dan mengubah data arsip rahasia, lihat pada Gambar 5, Gambar 6 dan Gambar 7.



Gambar 5. Secret Doc



Gambar 6. Detail Secret Doc



Gambar 7. Edit Secret Doc

mendapatkan urutan yang dibutuhkan. Hasil dari *pixel* gambar *cover* tersebut diubah pada bentuk biner, dengan *syntax* “\$pixel = imagecolorat(\$cover, \$x, \$y)” dan “\$red = (\$pixel >> 16) & 0xFF;”, langkah ini dapat dilihat pada Gambar 9.

```
$dimension = getimagesize($cover);
$cover = imagecreatefrompng($cover);
$stego = imagecreatetruecolor($dimension[0], $dimension[1]);
for ($y = 0; $y < $dimension[1]; $y++) {
    for ($x = 0; $x < $dimension[0]; $x++) {
        if (strlen($message) == 0) {
            $message = "00000000";
        }
        $pixel = imagecolorat($cover, $x, $y);
        $red = ($pixel >> 16) & 0xFF;
        $green = ($pixel >> 8) & 0xFF;
        $blue = $pixel & 0xFF;
    }
}
```

Gambar 9. Kode program mengubah pixel menjadi biner

Langkah selanjutnya yaitu memasukkan pesan rahasia gambar *cover*. Pada langkah ini biner dari gambar akan disubstitusi dengan biner pesan rahasia dengan *syntax* “\$red = 2 * floor(\$red / 2) + substr(\$message, 0, 1);”. Hasil dari substitusi biner, diubah kembali dalam bentuk *pixel* untuk mengembalikan gambar, menjadi gambar stego dengan *syntax* “imagecolorallocate” dan “imagestpxel”. Langkah ini dapat dilihat pada Gambar 10.

```
switch ($this->color) {
    case "red":
        $red = 2 * floor($red / 2) + substr($message, 0, 1);
        break;
    case "green":
        $green = 2 * floor($green / 2) + substr($message, 0, 1);
        break;
    case "blue":
        $blue = 2 * floor($blue / 2) + substr($message, 0, 1);
        break;
}
$message = substr($message, 1);
$pixel = imagecolorallocate($stego, $red, $green, $blue);
imagestpxel($stego, $x, $y, $pixel);
```

Gambar 10. Kode program substitusi mengubah biner menjadi pixel

B. Implementasi Metode Least Significant Bit (LSB)

Pada penelitian ini mengimplementasikan steganografi metode LSB. Steganografi metode LSB ini terdiri dari dua proses yaitu *embedding* dan *extracting*. Berikut penjelasan mengenai implementasi metode yang digunakan.

1) Embedding

Proses *embedding* atau proses menyisipkan pesan pada gambar terdapat pada fungsi *submit()*. Pada bahasan ini akan dipaparkan bagaimana proses menyisipkan pesan rahasia pada gambar *cover*. Langkah awal dari proses ini yaitu membaca pesan rahasia dalam bentuk biner dengan *syntax* “str_pad(decbin(ord(\$value)), 7, ‘0’, STR_PAD_LEFT)”. Langkah ini dapat dilihat pada Gambar 8.

```
$message = str_split($message2);
foreach ($message as $key => $value) {
    $message[$key] = str_pad(decbin(ord($value)), 7, '0', STR_PAD_LEFT);
}
$message = implode($message);
```

Gambar 8. Kode Program Membaca Pesan Rahasia dalam Bentuk Biner

Langkah ke dua yaitu mengubah gambar *cover* dalam bentuk biner. Gambar *cover* akan diambil *pixel*nya terlebih dahulu dengan urutan dari atas berjalan ke kanan, *syntax* yang digunakan “getimagesize” dan “imagecreatetruecolor (\$dimension[0], \$dimension[1])” dan perulangan untuk

2) Extracting

Proses *extracting* atau proses mengembalikan pesan yang telah disisipkan dari gambar terdapat pada fungsi *dec()*. Pada bahasan ini akan dipaparkan bagaimana proses pengambilan pesan rahasia dari gambar stego. Langkah pertama yaitu mengubah gambar stego dalam bentuk biner. Gambar stego akan diambil *pixel*nya terlebih dahulu dengan urutan dari atas berjalan ke kanan, *syntax* yang digunakan “getimagesize” dan “imagecreatetruecolor(\$dimension[0], \$dimension[1])” dan perulangan untuk mendapatkan urutan yang dibutuhkan. Hasil dari *pixel* gambar stego tersebut diubah pada bentuk biner, untuk mendapatkan biner dari pesan rahasia dengan *syntax* “\$pixel = imagecolorat(\$cover, \$x, \$y)”, “\$red = (\$pixel >> 16) & 0xFF;”, dan “\$binary .= \$pixel % 2;”. Langkah ini dapat dilihat pada Gambar 11.

```
$dimension = getimagesize($stego);
$stego = imagecreatefrompng($stego);
$binary = "";
for ($y = 0; $y < $dimension[1]; $y++) {
    for ($x = 0; $x < $dimension[0]; $x++) {
        $pixel = imagecolorat($stego, $x, $y);
        switch ($this->color) {
            case "red":
                $pixel = ($pixel >> 16) & 0xFF;
                $binary .= $pixel % 2;
                break;
            case "green":
                $pixel = ($pixel >> 8) & 0xFF;
                $binary .= $pixel % 2;
                break;
            case "blue":
                $pixel = $pixel & 0xFF;
                $binary .= $pixel % 2;
                break;
        }
    }
}
```

Gambar 11. Kode program mengambil biner pesan dari pixel gambar

D. Hasil Pembahasan Sistem Pemberkasan Arsip Menggunakan Metode LSB

Pembahasan ini menjelaskan hasil pengamatan yang dilakukan mengenai sistem pemberkasan arsip telah dibangun. Berdasarkan pengamatan yang dilakukan, diperoleh hasil bahwa sistem pemberkasan arsip menggunakan metode LSB dapat membantu petugas arsip dalam melakukan pemberkasan arsip dan menjaga kerahasiaan serta keamanan informasi arsip.

Hasil analisa dari pengimplementasian steganografi metode LSB didapatkan kelebihan dan kekurangan sistem. Ada pun kelebihan dan kekurangan dari sistem, yaitu:

1) Kelebihan Sistem

Dari hasil pembuatan sistem, peneliti dapat menganalisa kelebihan dari sistem yang dibuat, yaitu:

- Pengguna harus melakukan *login* untuk menggunakan sistem. Hal ini dimaksudkan untuk keamanan data yang dimiliki oleh pengguna.
- Sistem mampu menampilkan pesan ketika terjadi *error*. Hal ini memudahkan pengguna untuk mengetahui bahwa terjadi kesalahan pada saat menjalankan sistem.
- Sistem mampu menampilkan pemberitahuan pada *user* admin, ketika ada pengajuan gambar baru. Hal ini dapat memudahkan *user* admin dalam memasukkan dalam manajemen data.
- Sistem menggunakan steganografi metode LSB dalam proses penyimpanan data. Hal ini dapat menjamin keamanan dan menghilangkan kecurigaan pesan rahasia yang disimpan.
- Hasil gambar dari proses steganografi memiliki kualitas yang baik dan tidak terlihat perbedaan dengan gambar *cover* secara kasat mata.

2) Kelemahan Sistem

Dari hasil pembuatan sistem, penulis dapat menganalisa kekurangan dari sistem yang dibuat, yaitu hasil gambar dari proses steganografi tidak memiliki ketahanan terhadap *image processing*, karena pesan yang disisipkan tidak dapat diekstrak.

Berdasarkan dari kelemahan di atas diperlukan pengembangan metode yang digunakan untuk mempertahankan gambar hasil stego yang telah dilakukan *image processing*. Pengembangan dapat berupa penambahan fitur untuk mengekstrak gambar hasil steganografi berdasarkan *image processing* yang dilakukan, salah satu contohnya *image processing* rotasi 90°. *Image processing* rotasi 90° dapat diatasi dengan mengubah urutan pengambilan *pixel* yang awalnya dari

pojok kiri atas berjalan ke kanan menjadi pojok kanan atas berjalan ke bawah saat akan diubah menjadi biner dan diambil pesan rahasianya pada proses ekstrak dari metode.

IV. KESIMPULAN

Pengimplementasian steganografi metode LSB pada pemberkasan arsip untuk menjamin keamanan dan menghilangkan kecurigaan pesan rahasia yang disimpan. Terdapat dua proses dalam pengimplementasian steganografi metode LSB yaitu penyisipan pesan dan pengestrakan pesan. Proses penyisipan pesan diawali dengan *user* sekretaris memasukkan gambar pada sistem, langkah ini dilakukan untuk menyiapkan gambar *cover*. Langkah selanjutnya yaitu *user* admin memasukkan *key* untuk proses enkripsi, kemudian *chypertext* hasil enkripsi akan disisipkan pada gambar *cover* dengan proses steganografi metode LSB. Gambar hasil dari proses steganografi selanjutnya disimpan pada *database*. Proses pengestrakan pesan diawali dari gambar stego yang tersimpan pada *database* diekstrak menjadi *chypertext*. Langkah selanjutnya *user* admin memasukkan *key* untuk dekripsi, lalu *plaintext* hasil dekripsi akan ditampilkan.

Gambar hasil dari proses steganografi metode LSB tidak memiliki ketahanan terhadap *imageprocessing*. Gambar stego yang melalui tindakan (*resize, rotation, brightness, contrast*) tidak dapat mengembalikan pesan rahasia yang telah disisipkan di dalamnya. Gambar stego yang telah melalui *imageprocessing* dengan tindakan *resize, rotation, dan brightness* tergolong gambar dapat tidak digunakan karena nilai PSNR dihasilkan di bawah 20 db, sedangkan gambar stego yang telah melalui *imageprocessing* dengan tindakan *contrast* tergolong tidak baik karena nilai PSNR di atas 20 db.

DAFTAR PUSTAKA

- [1] Ariyus, D., 2006. Kriptografi: Keamanan Data dan Komunikasi. Yogyakarta: Graha Ilmu.
- [2] Ardhyana, d., 2008. Aplikasi Steganografi pada Mp3 Menggunakan Teknik LSB.
- [3] Randi, A., 2012. Studi Perbandingan Algoritma Blowfish dan Twofish.
- [4] Pressman, R.S., 2012. Rekayasa Perangkat Lunak. Yogyakarta: Andi.
- [5] Cheddad A, C.J.d., 2010. Digital Image Steganography: Survey and Analysis of Current Methods.
- [6] Krisnawati, 2008. Metode Least Significant Bit (LSB) dan End Of File (EOF) untuk Menyisipkan Teks ke dalam Citra Grayscale.
- [7] Saefullah, A.d., 2012. Aplikasi Steganografi untuk Menyembunyikan Teks dalam Media Image dengan Metode LSB.

Implementasi Algoritma Twofish pada Sistem Informasi Pengarsipan

Studi Kasus : PT. Angkasa Pura I

Yanuar Nurdiansyah*, Agil Bi Aviv Taufiqi
Program Studi Sistem Informasi, Universitas Jember (UNEJ)
Jl. Kalimantan 37, Jember 68121
yanuar_pssi@unej.ac.id

Abstrak—Sebuah sistem harus memiliki proteksi untuk mengamankan datanya termasuk sistem informasi pengarsipan. Tanpa adanya sebuah proteksi semua data pada sistem tersebut akan dapat dengan mudah diambil. Salah satu cara untuk memproteksi data adalah dengan mengenkripsinya. Enkripsi adalah sebuah proses mengubah data menggunakan key tertentu sehingga data tersebut tidak dapat dibaca jika tidak didekripsi (kebalikan dari enkripsi). Pada penelitian ini, teknik enkripsi yang digunakan adalah algoritma Twofish. Algoritma Twofish merupakan algoritma kuat yang sampai saat ini dapat dinyatakan aman karena masih belum ada serangan kriptanalisis yang dapat mematahkannya. Algoritma Twofish menggunakan jaringan feistel 16 putaran dan 4 kotak-S yang bergantung pada key. Terdapat empat macam key schedule dalam implementasinya yaitu: full keying, partial keying, minimal keying, dan zero keying dengan perbedaan dalam hal key setup. Selain itu, Twofish memiliki beberapa metode pengacakan yaitu matriks MDS, teknik PHT, dan teknik whitening. Hasil penerapan pada sistem informasi pengarsipan ini dilengkapi dengan proses enkripsi pada saat memasukkan (*input*) data menggunakan algoritma Twofish di mana key akan diubah terlebih dahulu ke dalam bentuk hexadecimal sebelum digunakan untuk enkripsi.

Kata kunci—arsip; kriptografi; enkripsi; dekripsi; algoritma Twofish.

I. PENDAHULUAN

Pengarsipan adalah tata cara penyusunan arsip perusahaan dari awal didirikan sampai saat ini. Arsip dapat berupa laporan dari setiap keputusan atau aturan dari satu perusahaan dapat berupa data keuangan dan data karyawan, sehingga data arsip merupakan data vital dalam satu perusahaan.

Perkembangan teknologi saat ini pada pengarsipan dapat dilakukan secara komputerisasi dengan menggunakan sistem, sehingga manajemen data arsip dapat dilakukan dengan baik. Penyimpanan arsip saat ini tidak hanya dalam bentuk fisik tetapi dalam bentuk *file* digital untuk mempermudah dalam mengelola data arsip.

Risiko perkembangan teknologi yang sangat pesat, memungkinkan seseorang yang tidak memiliki hak akses untuk mengambil dan memanfaatkan informasi tanpa ijin. Risiko tersebut mengancam keamanan data arsip perusahaan yang akan berakibat fatal terhadap perusahaan.

Keamanan informasi data arsip dapat atasi dengan sistem yang memiliki fitur untuk menyamarkan data sehingga informasi arsip tidak mudah dibaca. Fitur keamanan dengan cara menyamarkan data disebut enkripsi. Enkripsi adalah proses yang dilakukan untuk mengamankan sebuah pesan yang disebut *plaintext* menjadi pesan yang tersembunyi yang disebut *ciphertext*[1]. Metode enkripsi memiliki banyak algoritma yang dapat digunakan di antaranya algoritma *rijndael*, *serpent*, *Twofish*, MARS, RC6, *blowfish*, DES dan 3DES.

Algoritma enkripsi yang menjadi finalis dari kompetisi untuk menetapkan Algoritma Enkripsi Standar (AES) antara lain Igoritma *rijndael*, *serpent*, *Twofish*, MARS, dan RC6. Analisa performa dari segi penggunaan memori, algoritma *rijndael* yang paling sedikit, sedangkan dari segi keamanan dan kecepatan algoritma *Twofish* yang lebih unggul dari algoritma lainnya[2]. Sistem pengarsipan lebih mengutamakan keamanan data daripada penggunaan memori. Oleh karena itu, algoritma *Twofish* lebih tepat digunakan dalam sistem pengarsipan.

Algoritma *Twofish* merupakan algoritma kuat yang sampai saat ini dinyatakan aman karena masih belum ada serangan kriptanalisis yang benar-benar dapat mematahkan algoritma ini[3]. Algoritma yang beroperasi dalam mode *block cipher* ini juga tidak dipatenkan sehingga penggunaannya pada alat enkripsi tidak perlu mengeluarkan biaya. Algoritma *Twofish* menggunakan jaringan *feistel* 16 putaran dan 4 kotak-S yang bergantung pada *key*. Terdapat empat macam *key schedule* dalam implementasinya yaitu: *full keying*, *partial keying*, *minimal keying*, dan *zero keying* dengan perbedaan dalam *key setup*. *Twofish* juga memiliki beberapa metode pengacakan yaitu matriks MDS, teknik PHT dan teknik *whitening*.

PT. Angkasa Pura I saat ini dalam proses manajemen arsip memerlukan waktu yang lama dan pencatatannya menggunakan Microsoft Excel tanpa fitur keamanan. Proses manajemen yang lama dikarenakan semua proses pengarsipan harus melalui satu petugas pengarsipan, di mana setiap divisi harus menemui petugas pengarsipan baik dalam pencatatan maupun melihat daftar berkas arsip. Proses manajemen yang lama dapat diatasi dengan menggunakan sistem yang memiliki beberapa hak akses, sehingga dalam proses manajemen arsip setiap divisi tidak perlu menemui petugas pengarsipan.

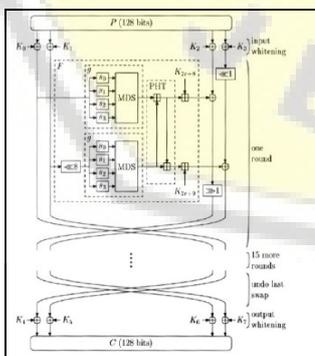
Permasalahan dalam PT. Angkasa Pura I tersebut yaitu manajemen pengarsipan dan keamanan data dapat diatasi dengan membangun sistem yang memiliki hak akses dan mampu menyamarkan data arsip. Penggunaan sistem dalam

proses manajemen pengarsipan akan lebih cepat dan efisien karena setiap divisi dapat mencatat dan melihat daftar arsip tanpa harus melalui petugas pengarsipan. Proses pengamanan data menggunakan enkripsi Algoritma Twofish karena dari segi keamanan algoritma ini lebih unggul dari metode lainnya dan sistem pengarsipan lebih mengutamakan keamanan.

A. Algoritma Twofish

Algoritma *Twofish* menggunakan desain yang mudah dan tidak memiliki kunci lemah[4]. Desain yang mudah akan mempengaruhi kecepatan proses enkripsi dan dekripsi. Tidak adanya kunci lemah pada algoritma ini membuat kunci apa pun yang menjadi masukan oleh pengguna, tingkat keamanannya akan tetap sama. *Key* (kunci) merupakan elemen yang sangat penting dalam enkripsi dan harus dijaga kerahasiaannya. *Key* memberikan cara khusus bagaimana suatu algoritma mengubah *plaintext* menjadi *ciphertext* dan sebaliknya. Algoritma ini menggunakan *key* yang sama pada proses enkripsi dan dekripsinya yang disebut *symmetric key*. *Twofish* menggunakan 16-round struktur seperti jaringan *feistel* dengan penambahan *whitening* pada masukan dan keluaran[5]. Satu-satunya elemen bukan *feistel* adalah pergeseran satu bit. Pergeseran ini dapat dipindahkan ke dalam fungsi *F* untuk membuat sebuah jaringan *feistel* yang sesungguhnya, namun hal ini memunculkan pergeseran tambahan dari *words* sebelum langkah *whitening* keluaran. *Plaintext* dibagi menjadi empat buah 32-bit *words*.

Pada langkah *whitening* masukan, *plaintext* ini diXORkan dengan 4 *words* kunci. Langkah ini dilanjutkan oleh enam belas *round*, yang pada tiap *round*-nya 2 *words* di kiri digunakan sebagai masukan untuk fungsi *g* (salah satunya terlebih dahulu digeser sebanyak 8 bit ke kiri). Fungsi *g* terdiri dari empat kotak-S yang bergantung pada kunci, dan diikuti langkah pencampuran linear berbasis matriks MDS. Hasil dari dua fungsi *g* ini dikombinasikan dengan menggunakan transformasi Pseudo-Hadamard (PHT), dan 2 *keywords* ditambahkan. Dua hasil ini diXORkan dengan *words* di sebelah kanan (salah satunya terlebih dahulu digeser sejauh 1 bit ke kiri, dan satu lagi digeser 1 bit ke kanan setelah diXORkan). Bagian kiri dan kanan lalu dipertukarkan untuk *round* berikutnya. Setelah semua *round* selesai dilakukan, pertukaran terakhir dikembalikan dan empat *words* tersebut diXORkan dengan empat *keywords* menghasilkan *ciphertext* seperti pada Gambar 1.



Gambar 1. Garis Besar Algoritma Twofish

B. Penerapan Algoritma dalam Sistem

Sistem informasi pengarsipan akan mengenkripsi data arsip yang telah dimasukkan oleh admin menggunakan algoritma Twofish. Data yang dienkripsi adalah nama data arsip dan tempat penyimpanan datanya.

II. METODE

Metode yang digunakan dalam merancang dan membangun sistem yaitu metode pengembangan.

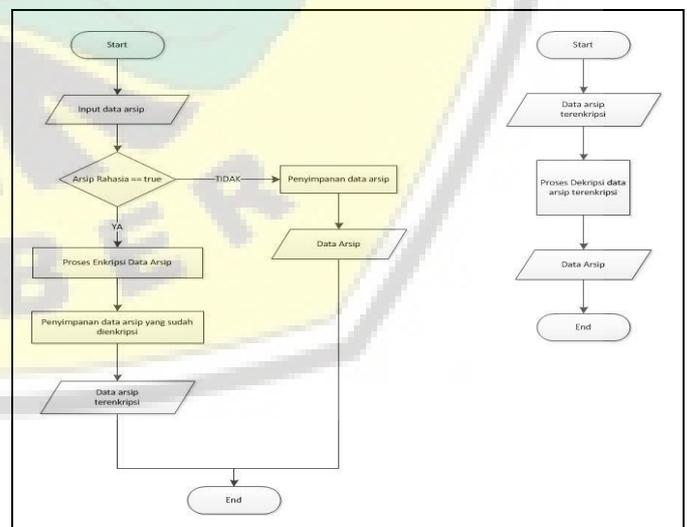
A. Tahap Perancangan

Metode yang digunakan dalam penelitian ini yakni SDLC (System Development Life Cycle) dengan model *prototype*[6]. Model *prototype* dibangun untuk memenuhi kebutuhan klien. Selain tidak menunggu agar kebutuhan klien terdaftar sepenuhnya, model *prototype* ini bisa langsung melanjutkan proses coding dan juga desain. Tujuan dari *prototype* ini adalah mempersilakan *user* untuk mengevaluasi desain *product* dengan menggunakan *prototype* program sementara secara langsung daripada menginstruksikan bayangan program dengan basis desain di atas kertas.

B. Pengembangan Sistem

Pada tahap ini menguraikan mengenai analisis kebutuhan, desain, implementasi, dan pengujian sistem yang digunakan dalam proses pengembangan sistem. Tahapan analisis hingga pengujian dilakukan sesuai dengan metode pengembangan model *prototype*.

Sistem pengarsipan adalah sebuah sistem berbasis web yang digunakan untuk mengelola arsip suatu perusahaan. Arsip perusahaan ada yang bersifat rahasia dan ada yang bersifat umum. Untuk arsip yang bersifat rahasia, sistem akan mengenkripsi data tersebut terlebih dahulu sebelum dimasukkan ke dalam *database*. Kemudian akan dilakukan proses dekripsi untuk menampilkan arsip rahasia tersebut, sedangkan arsip yang bersifat umum akan langsung dimasukkan ke dalam *database* tanpa dienkripsi terlebih dahulu. Dari uraian di atas, gambaran sistem yang dibuat dapat dilihat pada Gambar 2.



Gambar 2. Gambaran Umum Sistem

1) Analisis Kebutuhan

Tahap analisis dilakukan dengan mengamati objek penelitian sehingga didapatkan kebutuhan sistem. Kebutuhan sistem dapat dijabarkan menjadi dua yaitu kebutuhan fungsional dan non fungsional.

2) Kebutuhan Fungsional

Kebutuhan fungsional sistem berisi fitur-fitur inti yang harus dipenuhi dalam sistem agar sistem mampu difungsikan sesuai dengan tujuan dan kebutuhan pengguna terhadap sistem itu sendiri. Kebutuhan fungsional dari sistem informasi pengarsipan PT. Angkasa Pura I menggunakan Algoritma *Twofish* sistem dapat mengelola data arsip (*create, read, update, delete, encrypt and decrypt*).

3) Kebutuhan Non-Fungsional

Kebutuhan non-fungsional merupakan fitur-fitur yang dimiliki untuk mendukung sistem dalam memenuhi fungsionalitasnya untuk dapat memenuhi kebutuhan dari pengguna. Kebutuhan non-fungsional dari sistem informasi pengarsipan PT. Angkasa Pura I menggunakan Algoritma *Twofish* yaitu:

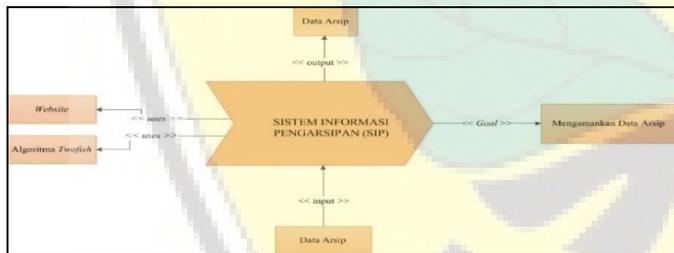
- Sistem berbasis website.
- Sistem menggunakan framework *CodeIgniter*.

4) Quick Desain

Desain yang dibuat meliputi *business process, use case diagram, use case scenario, sequence diagram, activity diagram, class diagram*, dan ERD.

5) Business Process

Business Process adalah suatu kumpulan aktivitas yang terstruktur untuk mencapai suatu tujuan tertentu atau untuk menghasilkan sebuah produk. Ada beberapa komponen di dalamnya, meliputi data yang menjadi masukan (*input*), data masukan yang kemudian diolah menjadi data keluaran (*output*), media yang digunakan (*uses*), dan tujuan yang ingin dicapai (*goal*). *Business Process* aplikasi dapat dilihat pada Gambar 3.



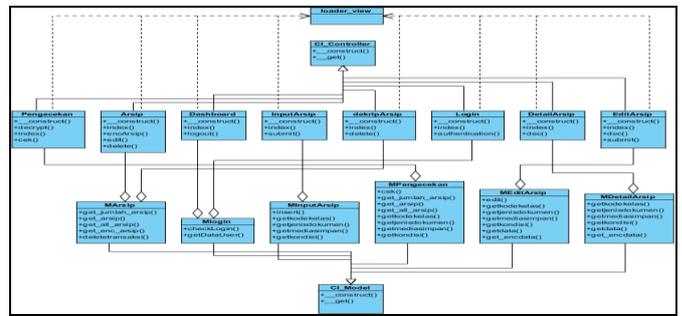
Gambar 3 Business process Sistem Informasi Pengarsipan

6) Use Case Diagram

Use case diagram merupakan pemodelan yang dibuat untuk dapat menggambarkan interaksi antara aktor dengan sistem informasi pengarsipan. Melalui use case diagram dapat diketahui interaksi yang dapat dilakukan aktor terhadap sistem sesuai dengan hak akses yang dimiliki oleh masing-masing aktor atau pengguna.

7) Class Case Diagram

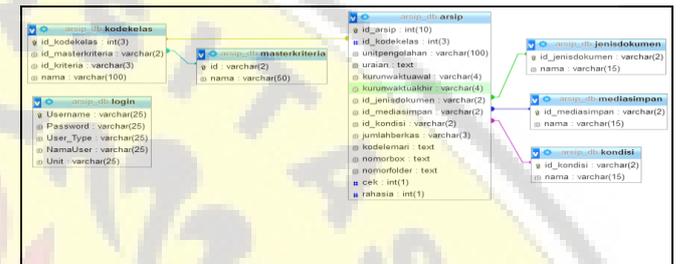
Class Diagram menggambarkan hubungan antar kelas yang digunakan untuk membangun suatu sistem. *Class Diagram* sistem informasi pengarsipan dapat dilihat pada Gambar 4.



Gambar 4 Class Diagram Sistem Informasi Pengarsipan

8) ERD (Entity Relationship Diagram)

ERD merupakan gambaran komponen dan struktur database yang digunakan dalam pembangunan sistem. ERD sistem informasi pengarsipan dapat dilihat pada Gambar 5.



Gambar 5 Entity Relationship Diagram Sistem Informasi Pengarsipan

9) Building Prototype

Building prototype merupakan tahap pembuatan *User Interface* (UI) dari sistem yang dibangun. Pembuatan UI berdasarkan dari *quick design* yang telah dibuat. UI yang dibuat berupa tampilan sistem yang sudah terdapat *link* pada tombol untuk masuk halaman selanjutnya dan mampu menunjukkan proses dari sistem yang akan dibangun. Sistem informasi pengarsipan memiliki empat fitur utama yaitu masukan arsip, *view* daftar arsip, *view* daftar arsip rahasia, dan pengecekan arsip.

10) Customer Evaluation

Pada tahap ini dilakukan testing terhadap aplikasi yang telah dibuat, dan proses testingnya akan dilakukan secara langsung oleh *customer*. Tujuan dari testing adalah untuk menguji apakah aplikasi sudah sesuai dengan kebutuhan, dan keinginan user, serta mencari *bug* atau kesalahan pada aplikasi yang dibangun. Pengujian menggunakan dua metode yakni *WhiteBox* dan *BlackBox*[7].

11) Refining Prototype

Refining Prototype merupakan tahap perbaikan *prototype* dari *costumerevaluation*. Pada tahap ini dilakukan perbaikan *prototype* sesuai dengan keinginan *costumer*.

12) Building Prototype

Engineer Prototype adalah tahap terakhir dalam model *prototype* di mana pada tahap ini desain perancangan yang telah diperbaiki diimplementasikan ke dalam bahasa pemrograman. Implementasi sistem informasi pengarsipan menggunakan *framework codeigniter* dan *MySQL* sebagai tempat penyimpanan datanya (*database*).

III. HASIL DAN DISKUSI

A. Implementasi Algoritma Twofish

Algoritma *Twofish* menggunakan desain yang mudah dan tidak memiliki kunci lemah[4]. Desain yang mudah akan mempengaruhi kecepatan proses enkripsi dan dekripsi. Tidak adanya kunci lemah pada algoritma ini membuat kunci apa pun yang menjadi masukan oleh pengguna, tingkat keamanannya akan tetap sama. *Key* (kunci) merupakan elemen yang sangat penting dalam enkripsi dan harus dijaga kerahasiaannya. *Key* memberikan cara khusus bagaimana suatu algoritma mengubah *plaintext* menjadi *ciphertext* dan sebaliknya. Algoritma ini menggunakan *key* yang sama pada proses enkripsi dan dekripsinya yang disebut *symmetric key*. *Twofish* menggunakan 16-round struktur seperti jaringan *feistel* dengan penambahan *whitening* pada masukan dan keluaran[5]. Satu-satunya elemen bukan *feistel* adalah pergeseran satu bit. Pergeseran ini dapat dipindahkan ke dalam fungsi *F* untuk membuat sebuah jaringan *feistel* yang sesungguhnya, namun hal ini memunculkan pergeseran tambahan dari *words* sebelum langkah *whitening* keluaran. *Plaintext* dibagi menjadi empat buah 32-bit *words*.

Sistem yang dibangun dalam penelitian ini digunakan untuk mengelola dan mengamankan data arsip. Sistem ini berbasis *web* yang dapat mengamankan data arsip rahasia sehingga pihak lain tidak dapat melihatnya. Sistem dibangun menggunakan *framework codeigniter* dan *database MySQL* sebagai tempat penyimpanan datanya. Fitur masukan (*input*) arsip merupakan fitur di mana pengguna dapat memilih apakah arsip tersebut bersifat rahasia atau tidak. Data arsip akan langsung dikirimkan ke server untuk disimpan di *database* jika pengguna memasukkan data arsip yang tidak bersifat rahasia, apabila pengguna memilih arsip bersifat rahasia maka data arsip akan dienkripsi menggunakan algoritma *Twofish*.

Proses enkripsi pada sistem ini diawali dengan mengonversi masukan (*input*) *key* ke dalam bentuk *hexadecimal*, di mana konversi *key* dilakukan untuk menyamakan *key*. Contoh *key* yang dimasukkan untuk enkripsi adalah 'abcdef' dan *plaintext* menggunakan kata 'aku'. Pembagian konversi tersebut dapat dilihat pada Gambar 6, di mana *key* dan *plaintext* dibagi menjadi 4 bagian yang dinamakan *words* menggunakan konversi *little-endian*. Hasil konversi yang didapatkan dapat dilihat pada Gambar 7 dan Gambar 8 di mana *words* dari *plaintext* dan *key* diubah ke dalam bentuk *binary*. Langkah selanjutnya *words* keempat digeser ke kiri sejauh 8-bit sebelum dikonversi kembali ke dalam bentuk persamaan XOR sebanyak 16-round. Hasil dari langkah tersebut didapatkan *ciphertext* per-blok seperti pada Gambar 9 yang kemudian diubah ke dalam bentuk *hexadecimal* seperti pada Gambar 10. Langkah terakhir yaitu mengonversi *ciphertext* menggunakan base64 encode yang dapat dilihat pada Gambar 11, di mana bilangan binary dari *ciphertext* digabungkan. Hasil dari penggabungan binary tersebut kemudian dibagi menjadi 6 bagian bit. Contohnya, binary "00110011" dibagi ke dalam beberapa 6 bagian bit maka akan menjadi "001100", "11". Apabila terdapat bagian yang tidak berjumlah 6 bit, maka akan dilakukan *padding* dengan cara menambahkan binary "00000000" sampai tiap bagiannya berjumlah 6 bit, menghasilkan "001100", "110000",

"000000", "000000". Kemudian dikonversi ke dalam bentuk base64 menggunakan tabel base64 pada Gambar 12 menghasilkan "Mw==".

hex 616263646566

Gambar 6 Hasil Konversi Key Ke dalam Bentuk Hex

4 words key 1684234849,26213,0,0

Gambar 7 Hasil Konversi Key Menggunakan Little-Endian

4 words plaintext
1634432269,218959117,218959117,218959117

Gambar 8 Hasil Konversi Plaintext Menggunakan Little-Endian

ciphertext per blok
-422493356,-335998223,-1111231872,-1320948916

Gambar 9 Hasil Ciphertext Per-Blok

ciphertext hex æÑCTëùñ%Ãö±CèL

Gambar 10 Hasil Konversi Ciphertext Ke dalam Bentuk Hex

Ciphertext (Base64-encoded): 5tFDVOv5EvG9w/KAsUPrTA==

Gambar 11 Hasil Konversi Ciphertext Menggunakan Base64 Encoder

Value	Char	Value	Char	Value	Char	Value	Char
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/
pad	=						

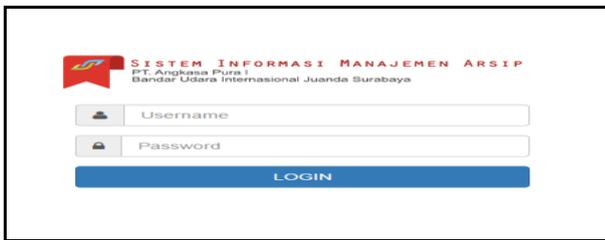
Gambar 12 Tabel Konversi Base64

B. Hasil Implementasi Aplikasi

Hasil implementasi dari sistem informasi pengarsipan yang dibangun pada penelitian ini memiliki dua hak akses yaitu, admin dan sekretaris. Sistem informasi pengarsipan ini memiliki beberapa fitur:

1) Halaman Login

Halaman *Login* adalah halaman yang akan diakses oleh *user* saat pertama kali menjalankan sistem informasi pengarsipan. Sistem akan menampilkan sebuah form masukan untuk mengisi *username* dan *password* seperti pada Gambar 13.



Gambar 13 Halaman Login

2) Halaman Input Arsip

Halaman input arsip merupakan halaman untuk memasukkan data arsip yang bersifat rahasia maupun tidak. Tampilan dari halaman input arsip dapat dilihat pada gambar 14. Jika *user* ingin memasukkan data arsip yang bersifat rahasia, maka *user* harus memilih “ya” pada masukan Gambar 15 setelah itu, sistem akan menampilkan sebuah masukan untuk mengisi *key* yang akan digunakan dalam proses enkripsi seperti pada Gambar 16. Apabila *key* tidak diisi, sistem akan menampilkan pesan seperti Gambar 17.



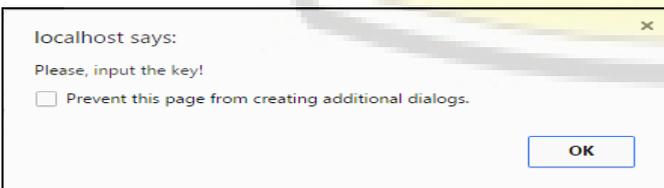
Gambar 14 Halaman Input Arsip



Gambar 15 Masukkan Untuk Memilih Sifat Data Arsip



Gambar 16 Masukkan untuk Mengisi Key yang Digunakan dalam Proses Enkripsi



Gambar 17 Pesan Saat Key Tidak Diisi

C. Pengujian Keamanan Sistem

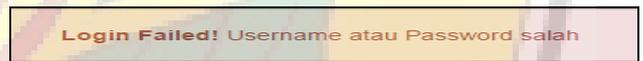
Pengujian keamanan sistem dilakukan untuk melihat tingkat keamanan dari sistem yang dibangun. Pengujian akan dilakukan menggunakan tiga metode yaitu, *SQL injection*, *Cross-site-scripting*, dan *decryptor tools*.

1) SQL Injection Attack

SQL Injection Attack adalah sebuah teknik memasukkan perintah SQL yang menyebabkan penyerang dapat mengakses *database* sistem dan memanipulasinya[8]. Hal tersebut tentunya sangat berbahaya bagi sebuah sistem. Oleh karena itu, penulis menggunakan teknik *SQL Injection Attack* untuk menguji sistem yang dibuat. Penyerang mencoba *login* menggunakan teknik *Bypass SQL Injection* seperti pada Gambar 18 dan hasilnya penyerang tidak dapat *login* seperti pada Gambar 19. Penyerang akan mencoba cara lain untuk *login* lalu mencari *method get* karena *method get* dapat dimanfaatkan untuk melakukan *SQL Injection Attack*. Penyerang akan mengubah *url* dengan menambahkan tanda petik pada akhir *url* seperti pada Gambar 20 untuk melihat apakah akan muncul *error* pada sistem karena *error* pada *url* yang di dalamnya terdapat *method get* akan menampilkan struktur dari *database* sistem seperti pada Gambar 21. Hasilnya sistem tetap menampilkan halaman tersebut tanpa *error* seperti pada Gambar 22.



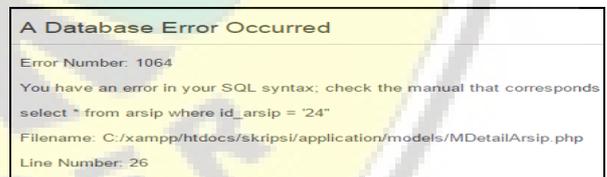
Gambar 18 Percobaan Login Menggunakan Bypass SQL



Gambar 19 Hasil Percobaan Login Menggunakan Bypass SQL



Gambar 20 Percobaan SQL Injection Attack Melalui URL



Gambar 21 Contoh error ketika di akhir URL diberi tanda petik



Gambar 22 Halaman Detail Arsip Rahasia Setelah URL dari Halaman tersebut Diberi Tanda Petik

Hasil percobaan *login* ke dalam sistem menggunakan beberapa teknik *Bypass SQL* dapat dilihat pada Tabel 1.

TABEL 1. HASIL PERCOBAAN BYPASSSQL

No	Teknik <i>Bypass SQL</i>	Hasil
1	" or ""="	Gagal
2	Admin' --	Gagal
3	Admin' or '1'='1	Gagal
4	Admin') or '1'='1	Gagal
5	Admin') or ('1'='1' --	Gagal
6	Or 1=1	Gagal
7	Or 1=1/*	Gagal

menguji tingkat keamanannya. Hasilnya, data arsip rahasia tidak berubah menjadi *plaintext*-nya seperti pada Gambar 26.



Gambar 25 Percobaan Dekripsi Menggunakan DecryptorOnline



Gambar 26 Hasil Percobaan Dekripsi Menggunakan DecryptorOnline

1) Cross Site Scripting

Cross Site Scripting (XSS) adalah sebuah serangan yang dilakukan dengan cara menginputkan HTML, JavaScript, ActiveX, Flash dan bahasa-bahasa pemrograman lain pada sisi *client* melalui *form* yang tidak memiliki validasi pada masukan[7]. *Cross site scripting* (XSS) merupakan salah satu dari beberapa metode penyerangan yang sering digunakan untuk mengambil *cookies* dari komputer korbannya.

Percobaan serangan menggunakan metode ini dapat dilihat pada Gambar 23. Penyerang menginputkan *script>alert* pada *form* masuk arsip.



Gambar 23 Percobaan Serangan Cross Site Scripting

Sistem informasi pengarsipan menggunakan *filter* pada *form* input arsip yang berfungsi untuk menghapus *tag-tag* HTML yang diinputkan oleh *user* sebagai salah satu langkah pencegahan terhadap serangan XSS. Hasil dari inputan pada Gambar 23 akan seperti pada Gambar 24 setelah melalui proses *filter*.



Gambar 24 Hasil Percobaan Serangan Cross Site Scripting

2) Decryptor Online

Decryptor online adalah sebuah *tools* untuk mengubah *ciphertext* menjadi *plaintext* atau biasa disebut dengan dekripsi. Sistem informasi pengarsipan menggunakan algoritma *Twofish* untuk mengenkripsi data arsip yang bersifat rahasia. Penulis akan mencoba mendekripsi data arsip rahasia pada sistem informasi pengarsipan dengan algoritma yang sama menggunakan *decryptor online* seperti pada Gambar 25 untuk

IV. KESIMPULAN

Sistem informasi pengarsipan dilengkapi dengan proses enkripsi pada saat penginputan data menggunakan algoritma *Twofish* di mana *key*akan diubah terlebih dahulu ke dalam bentuk *hexadecimal* sebelum digunakan untuk enkripsi. Hasil enkripsi tersebut akan disimpan ke dalam *database*.

Data yang tersimpan dalam *database* aman karena data tersebut berbentuk *ciphertext* dan tidak dapat didekripsi menggunakan *decryptor online tools*, selain itu sistem yang dibangun tahan terhadap serangan *SQL injection*, *cross site scripting*.

DAFTAR PUSTAKA

- [1] V. d. D. R. Kannan, SQL Injection - Database Attack Revolution And Prevention, 2011.
- [2] L. Pandian, A Survey on Detection and Prevention of Cross-Site Scripting Attack, 2015.
- [3] R. Primartha, Penerapan Enkripsi Dan Dekripsi File Menggunakan Algoritma Data Encryption, 2011.
- [4] B. Schneier dan D. Whiting, A Performance Comparison of the Five AES Finalists., 2000.
- [5] I. Mukmin, Algoritma Twofish : Kinerja dan Implementasinya Sebagai Salah Satu Kandidat Algoritma AES (Advanced Encryption Standard), 2007.
- [6] W. Setiawan, Analisa dan Perbandingan Algoritma Twofish dan Rijndael, 2011.
- [7] A. Randy, Studi dan Perbandingan Algoritma Blowfish dan Twofish, 2010.
- [8] S. Nidhra dan J. Dondeti, Black Box and White Box Techniques - A literature Review, 2012.