



JURNAL **TEKNOLOGI INFORMASI** **DAN KOMUNIKASI**

Vol 5 No 1 Juni 2016



KEMENTERIAN KOMUNIKASI DAN INFORMATIKA RI
BADAN PENELITIAN DAN PENGEMBANGAN SUMBER DAYA MANUSIA
BALAI BESAR PENGKAJIAN DAN PENGEMBANGAN KOMUNIKASI DAN INFORMATIKA MEDAN



JURNAL TEKNOLOGI INFORMASI DAN KOMUNIKASI

Vol 5 No 1 Juni 2016

Jurnal Teknologi Informasi dan Komunikasi (TIK) adalah jurnal ilmiah, dengan visi menjadi media informasi dan komunikasi bagi pengembangan ilmu pengetahuan serta sebagai rekomendasi dalam penyusunan kebijakan pemerintah di bidang TIK

Pengarah

Kepala Badan Litbang SDM Kementerian Kominfo

Penanggungjawab

Kepala BBPPKI Medan

Ketua Dewan Redaksi

Jarudo Damanik, S.Kom (*Teknologi Informasi dan Komunikasi Lainnya*)

Anggota Dewan Redaksi

Yusrizal, S.Kom, M.Eng (*Manajemen Sistem Informasi*)
Marudur Pandapotan Damanik, ST, M.Eng (*Manajemen Sistem Informasi*)
Meilinia Diakonia Br. Ginting, S. Kom (*Teknologi Informasi dan Komunikasi Lainnya*)

Ketua Redaksi Pelaksana

Moh. Muttaqin, ST, M.Eng (*Teknik Sistem Informasi*)

Anggota Redaksi Pelaksana

Vita Puspita, St, M.Eng (*Teknik Sistem Informasi*)

Desain Grafis

Fachri Auliansyah Siregar, S.Kom

Sekretaris

Laili Fahlia, S.Pd

Peer Reviewer/Mitra Bestari

Prof. Dr. Muhammad Zarlis, M. Sc
(*Ilmu Komputer dan Teknologi Informasi*)

Prof. Dr. Opim Salim Sitompul, M. Sc
(*Data Warehouse*)

Dr. Poltak Sihombing, M.Kom
(*Artificial Intelligence dan Information Retrieval*)

Dr. Erna Budhiarti Nababan, MIT
(*Artificial Intelligence*)

Dr. Ester S.M. Nababan, M.Sc
(*Pemodelan Matematika (Operation Research)*)

Sekretariat Redaksi

Balai Besar Pengkajian dan Pengembangan Komunikasi dan Informatika Medan
Badan Penelitian dan Pengembangan Sumber Daya Manusia
Kementerian Komunikasi dan Informatika
Jl. Tombak No. 31 Medan 20222, Sumatera Utara – **Telp/Fax.** (061) 6639817

Email: jtik.kominfo@gmail.com



Puji dan syukur kehadiran Allah SWT karena atas rahmat dan kuasaNya, Jurnal Teknologi Informasi dan Komunikasi Balai Besar Pengkajian dan Pengembangan Komunikasi dan Informatika (BBPPKI) Medan ini dapat terbit untuk yang ke delapan kalinya. Untuk penerbitan volume 5 no.1, akan disajikan 6 (enam) tulisan dari rekan rekan peneliti, akademisi dan praktisi dari berbagai wilayah dan instansi yang ada di Indonesia.

Beberapa karya ilmiah yang terbit dalam jurnal ini diantaranya penelitian yang dilakukan oleh Fifin Sonata dan kawan kawan yang menerapkan metode *optimasi multi-objective A Fast Elitist Non-Dominated Sorting Genetic Algorithm for Multi-Objective Optimazitaion : NSGA-II* pada penyusunan penjadwalan mesin untuk dua objek yaitu makespan dan total tardiness yang tertuang dalam naskah berjudul ***Optimasi Maskespan dan Total Tardiness Dalam Penjadwalan Mesin Produksi Type Flow Shop Menggunakan Metode Non -Dominated Sorting Genetik Algorithm (NSGA-II)***. Yusrizal menulis dalam karya tulis ilmiah berjudul ***Survei Penggunaan Teknologi Informasi dan Komunikasi di Wilayah Perbatasan*** menyimpulkan bahwa mayoritas responden di lokasi penelitian, dalam hal ini dikawasan perbatasan telah memiliki akses internet. Kepemilikan akses internet pada wilayah urban jauh lebih besar dari pada wilayah rural. Sementara itu sebesar 65,2% responden di wilayah urban dan 26,11% di wilayah rural telah menggunakan internet untuk berbagai kepentingan. Sementara itu, Seniman dan kawan kawan mencoba memberi solusi alternatif dalam pengukuran jarak tempuh dan posisi kendaraan melalui sebuah penelitian berjudul ***Pemantauan Jarak Tempuh Kendaraan Menggunakan Modul General Packet Radio Service (GPRS), Global Positioning System (GPS) dan Ardiono***. Implementasi dari hasil penelitian ini dapat diterapkan pada pengontrolan pemakaian kendaraan pada sebuah institusi maupun pemantauan keberadaan pengemudi pada bisnis transportasi. Pada terbitan jurnal ini juga memuat naskah berjudul ***Implementasi Algoritma Two Sliding Windows Untuk Mempercepat Pencarian Dokumen*** yang ditulis oleh Dedy Arisandi dan kawan kawan. Penelitian ini bertujuan untuk mengoptimalkan sistem pencarian dokumen dengan menerapkan algoritma Two Sliding Windows yang dikolaborasi dengan metode Steming Porter untuk mengubah kata berimbunan dasar dalam sebuah pencarian dengan menggunakan kata kunci. Hasil uji coba penerapan algoritma ini mampu mempercepat proses pencarian dokumen hingga 97,93%. Moh. Muttaqin mencoba merancang sebuah Data Flow Diagram (DFD) untuk Pengembangan Information Retrieval System (IRS) Dokumen Penelitian yang dapat diterapkan untuk mengoptimalkan pengaksesan terhadap informasi dalam dokumen-dokumen beragam tipe dalam sebuah tulisan berjudul ***Rancangan Data Flow Diagram (DFD) untuk pengembangan Information Retrieval System (IRS) Dokumen Penelitian Menggunakan Basis Data Non-Relational***. Hasil penelitian berupa rancangan Data Flow Diagram (DFD) hingga level 2 yang dapat dikembangkan dalam sistem pengelolaan dokumen penelitian sesuai dengan kebutuhan. Terbitan jurnal ini diakhiri dengan naskah Ratnawati Simbolon berjudul ***Pengamanan Transkrip Nilai Mahasiswa Menggunakan Kriptografi Playfair Chiper dan Steganografi Dengan Teknik Least Significant Bit (LSB)***. Penelitian ini membahas tentang solusi meningkatkan tingkat keamanan data yang dirahasiakan dengan kombinasi antara kriptografi dan steganografi dengan teknik Playfair Chiper, dimana hasil penelitian menunjukkan file citra bitmap grayscale 8 bit per pixel dengan skala 0 sampai 255, atau dengan format biner yang terbangun dalam bentuk enkripsi dalam dikembalikan menjadi pesan asli dengan proses dekripsi.



Seluruh hasil penelitian dan kajian yang dipublikasikan ini diharapkan dapat menjadi tambahan khazanah ilmu pengetahuan, khususnya bidang teknologi informasi dan komunikasi, sekaligus melengkapi diseminasi hasil hasil penelitian di bidangnya yang diharapkan dapat bermanfaat bagi seluruh stakeholder pemerintah, khususnya Kementerian Komunikasi dan Informatika Republik Indonesia. Apresiasi dan kontribusi dari seluruh pihak diharapkan, khususnya dari para akademisi, praktisi Teknologi Informasi dan Komunikasi berupa masukan dan pemikiran dinamis, sehingga peningkatan kualitas penerbitan berikutnya menjadi lebih baik lagi.

Akhir kata kami sadari, “tak ada gading yang tak retak”, dengan segala kerendahan hati kami mengharapakan kritik dan saran yang membangun dari semua dewan pembaca untuk perbaikan dan kesempurnaan jurnal ini dimasa mendatang

Salam,

Redaksi

UCAPAN TERIMA KASIH

Sege nap Dewan Redaksi Jurnal Teknologi Informasi dan Komunikasi mengucapkan terima kasih kepada :

1. Prof. Dr. Muhammad Zarlis, M.Sc (Universitas Sumatera Utara)
2. Prof. Dr. Opm Salim Sitompul, M.Sc (Universitas Sumatera Utara)
3. Dr. Poltak Sihombing, M.Kom (Universitas Sumatera Utara)
4. Dr. Erna Budhiarti Nababan, M.IT (Universitas Sumatera Utara)
5. Dr. Ester Nababan, M.Sc (Universitas Sumatera Utara)

Selaku Mitra Bestari Jurnal Teknologi Informasi dan Komunikasi Volume 5 No. 1 Juni 2016 atas kerjasamanya dalam meluangkan waktu dan memberikan sumbangan pemikiran dalam rangka meningkatkan kualitas karya tulis ilmiah.

Medan, Juni 2016

Dewan Redaksi



| | |
|---|--------|
| Pengantar Redaksi | i-ii |
| Ucapan Terimakasih | iii |
| Daftar Isi | iv |
| Lembar Abstrak | v-viii |
| Optimasi Makespan dan Total Tardiness Dalam Penjadwalan Mesin Produksi Type Flow Shop Menggunakan Metode Non-Dominated Sorting Genetic Algorithm (NSGA-II) Fifin Sonata, dkk | 1-12 |
| Survey Penggunaan Teknologi Informasi dan Komunikasi di Wilayah Perbatasan Yusrizal | 13-28 |
| Pemantauan Jarak Tempuh Kendaraan Menggunakan Modul GPRS GPS dan Arduino Seniman, dkk | 29-38 |
| Implementasi Algoritma <i>Two Sliding Windows</i> Untuk Mempercepat Pencarian Dokumen Dedy Arisandi, dkk | 39-48 |
| Rancangan <i>Data Flow Diagram(DFD)</i> Untuk Pengembangan <i>Information Retrieval System(IRS)</i> Dokumen Penelitian Menggunakan Basis Data <i>Non- Relational</i> Moh. Muttaqin, dkk | 49-58 |
| Pengamanan Transkrip Nilai Mahasiswa Menggunakan Kriptografi <i>Playfair</i> Cipher dan Steganografi Dengan Teknik <i>Least Significant Bit</i> (LSB) Ratna Wati Simbolon | 59-70 |



JURNAL TEKNOLOGI INFORMASI DAN KOMUNIKASI

Vol. 5 No. 1 Juni 2016

Kata kunci yang dicantumkan merupakan istilah bebas. Lembaran abstrak ini boleh dikopi tanpa izin dan biaya.

**Fifin Sonata, Muhammad Zarlis, Tulus | STIKOM
Medan, Universitas Sumatera Utara
JTIK Vol.5 No.1 Juni 2016**

OPTIMASI MAKESPAN DAN TOTAL TARDINESS DALAM PENJADWALAN MESIN PRODUKSI TYPE FLOW SHOP MENGGUNAKAN METODE NON- DOMINATED SORTING GENETIC ALGORITHM (NSGA-II)

Permasalahan optimasi dua objek yaitu makespan dan total tardiness pada penjadwalan mesin produksi flow shop berkaitan dengan penyusunan penjadwalan mesin secara teratur. Optimasi kedua permasalahan tersebut merupakan optimasi yang bertolak belakang sehingga diperlukan metode optimasi multi-objective A Fast Elitist Non-Dominated Sorting Genetic Algorithm for Multi-Objective Optimization: NSGA-II yang dapat mengintegrasikan permasalahan tersebut. Penyelesaian penjadwalan mesin produksi flow shop dengan algoritma NSGA-II mampu membangun jadwal dengan meminimalkan makespan dan total tardiness. NSGA-II dapat membantu memberikan solusi penjadwalan mesin produksi flow shop yang efisien berupa solusi pareto optimal yang dapat memberikan sekumpulan solusi alternatif bagi pengambil keputusan dalam membuat penjadwalan mesin produksi yang diharapkan. Nilai solusi yang diperoleh akan terlihat dengan cara melakukan perbandingan antara dominasi solusi Agregat Of Function (AOF) dengan solusi NSGA-II.

Kata Kunci : Makespan, NSGA-II, Penjadwalan, Tardiness.

MAKESPAN AND TOTAL TARDINESS OPTIMIZATION IN FLOW SHOP TYPE FOR PRODUCTION MACHINE SCHEDULING USING NON-DOMINATED SORTING GENETIC ALGORITHM (NSGA-II)

The problem of optimization two objects, i.e makespan and total tardiness on flow shop production machine scheduling are related to regularly scheduling machine. Both optimization problems is a contradictory

optimization that require a multi-objective optimization method A Fast elitist Non-dominated Sorting Genetic Algorithm for Multi-Objective Optimization: NSGA-II which can integrates these problems. The main purpose of the completion the flow shop production machine scheduling with NSGA-II algorithm is to provide a solution to flow shop production machine scheduling, an efficient of pareto optimal solutions achieved an alternative for decision makes in making the expected production of machine scheduling. Value of solutions obtained will be seen by comparison between Aggregate of Function (AOF) solutions with NSGA-II solutions.

Keywords : Makespan, NSGA-II, Scheduling, Tardiness

**Yusrizal | BBPPKI Medan
JTIK Vol.5 No.1 Juni 2016**

SURVEY PENGGUNAAN TEKNOLOGI INFORMASI DAN KOMUNIKASI DI WILAYAH PERBATASAN

Pembangunan TIK di wilayah perbatasan, selain untuk menyediakan media bagi masyarakat agar tidak terisolasi dari perkembangan informasi global, juga untuk membantu memperlancar berbagai upaya dan aktivitas produktif masyarakat melalui penyediaan jaringan komunikasi yang lancar. Penelitian yang dilaksanakan secara survei dengan menggunakan teknik kuota sampling dan instrument berupa kuesioner dan dianalisis secara deskriptif dilakukan untuk mengetahui kekuatan dan kemampuan sosial masyarakat perbatasan dalam penggunaan Teknologi Informasi dan Komunikasi (TIK) kepada 180 responden yang berada di 7 (tujuh) wilayah prioritas perbatasan yaitu, Kabupaten Bengkalis; Kabupaten Natuna; Kabupaten Sanggau; Kabupaten Bengkayang; Kabupaten Kapuas Hulu; Kabupaten Nunukan dan Kabupaten Malinau. Hasil penelitian menemukan bahwa sekitar 76,2% responden di wilayah urban dan 42,3% untuk wilayah rural di perbatasan telah memiliki akses internet dalam keluarga. Dan sebesar 65,2% responden di wilayah urban dan 26,11% di

wilayah rural telah menggunakannya. Kepemilikan akses internet merupakan kepemilikan melalui jaringan tetap (*fixed*) maupun jaringan bergerak (*mobile*), dalam hal ini termasuk penggunaan internet dengan menggunakan peralatan yang memungkinkan akses internet selain komputer seperti telepon selular, PDA/ Smart Phone maupun tablet.

Kata Kunci : Wilayah perbatasan, Teknologi Informasi dan Komunikasi, internet, broadband.

SURVEY OF THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGY IN THE BORDER REGION

ICT development in the border regions, in addition to providing a medium for people to not be isolated from the development of global information, as well as to help facilitate the efforts and activities of productive community through the provision of smooth communication networks. Research conducted the survey by using the technique of quota sampling and instrument in the form of questionnaires and descriptive analysis was conducted to determine the strength and social skills of border communities in the use of Information and Communication Technology (ICT) to 180 respondents in seven (7) priority areas border that is , Bengkalis; Natuna; Sanggau; Bengkayang; Kapuas Hulu; Nunukan and Malinau. The study found that about 76.2% of respondents in urban areas and 42.3% for rural areas on the border had to have internet access in the family. And amounted to 65.2% of respondents in urban areas and 26.11% in rural areas has been used. Ownership is a proprietary internet access via fixed networks and mobile networks, in this case including the use of the Internet by using equipment that enables Internet access in addition to a computer such as mobile phones, PDA / Smart Phone or tablet.

Keywords : Borders area, Information and Communication Technology, internet, broadband.

Seniman, Irzal Sofyan, Syahril Efendi | Universitas Sumatera Utara

JTIK Vol.5 No.1 Juni 2016

PEMANTAUAN JARAK TEMPUH KENDARAAN MENGGUNAKAN MODUL GENERAL PACKET RADIO SERVICE (GPRS), GLOBAL POSITIONING SYSTEM(GPS) DAN ARDUINO

Sistem pemantauan kendaraan yang berbasis pelacakan Global Positioning System (GPS) umumnya hanya menggunakan data posisi garis lintang dan garis bujur (*latitude* dan *longitude*) sebagai acuan pemantauan lokasi kendaraan tersebut. Informasi jarak tempuh kendaraan diperlukan misalnya sebagai pengontrolan pemakaian kendaraan pada suatu

instansi/perusahaan, atau sebagai penentuan tarif jasa transportasi berdasarkan jarak tempuhnya. Untuk itu, diperlukan sebuah solusi dalam pengukuran jarak tempuh dan posisi kendaraan. Dalam penelitian ini, penentuan jarak tempuh kendaraan menggunakan prinsip percepatan pada kinematika gerak, dengan memanfaatkan data kecepatan dan waktu yang diperoleh menggunakan GPS pada modul SIM908. Sementara Arduino sebagai mikrokontroler yang bekerja mengatur system secara keseluruhan termasuk memproses data dari modul SIM908. Sehingga, diperoleh informasi jarak tempuh dan koordinat posisi kendaraan. Hasil pengujian menunjukkan bahwa sistem yang diajukan mampu bekerja stabil untuk menentukan jarak tempuh kendaraan yang paling mendekati dengan yang sebenarnya dan posisi kendaraan yang sesuai dengan lokasi sebenarnya.

Kata Kunci : pengukuran , GPS SIM908, arduino uno, percepatan, kinematika gerak.

VEHICLE DISTANCE MONITORING BASED ON GENERAL PACKET RADIO SERVICE (GPRS), GLOBAL POSITIONING SYSTEM(GPS)AND ARDUINO

Vehicle monitoring system based on Global Positioning System (GPS) tracking commonly just uses latitude and altitude data as reference to determine vehicle location. Vehicle mileage information can be used for vehicle controlling usage in company, or can be used as fare calculation of transportation based on the distance. This required a solution in measure the distance and position of vehicle. In this research, vehicle mileage measuring uses acceleration principle in motion kinematic, by using speed and time data which is extracted from SIM908 GPS module. In other hand, Arduino is used as microcontroller which manage all system work, including process data from SIM908 module. Then it can be acquired information of vehicle mileage and position. The result of testing shows that system is able to work stable to measure vehicle mileage to the closest real distance, and vehicle position shows the real location.

Keywords : measuring, SIM908 GPS, arduino uno, acceleration, kinematic motion.

Dedy Arisandi, Erna Budhiarti Nababan, Frans Octavianus | Universitas Sumatera Utara

JTIK Vol.5 No.1 Juni 2016

IMPLEMENTASI ALGORITMA TWO SLIDING WINDOWS UNTUK MEMPERCEPAT PENCARIAN DOKUMEN

Salah satu metode yang umum digunakan dalam pencarian dokumen adalah dengan menggunakan kata dasar atau kata berimbuhan sebagai kata kunci. Kata-kata tersebut kemudian akan dicocokkan dengan seluruh dokumen yang tersimpan. Pencarian dilakukan

dengan mencocokkan kata yang sama terhadap seluruh isi dokumen tersebut. Metode ini kurang efektif dan cenderung lambat. Oleh karena itu, pencarian dokumen perlu menggunakan algoritma yang dapat mempercepat proses tersebut. Perubahan kata berimbuhan menjadi kata dasar dilakukan dengan menggunakan Metode Stemming Porter. Proses berikutnya adalah dengan menggunakan algoritma Two Sliding Windows (TSW) untuk mempercepat pencarian pola. TSW menggunakan jendela dua sisi secara paralel untuk mencari kata atau sinonim yang cocok. Berdasarkan hasil uji coba, algoritma ini dapat mempercepat proses pencarian dokumen dengan tingkat kebenaran 97.93%.

Kata Kunci : Two Sliding Windows, Pencarian dokumen, Sinonim kata, Stemming Porter.

TWO SLIDING WINDOWS ALGORITHM IMPLEMENTATION TO INCREASE DOCUMENTS SEARCHING PERFORMANCE

A common method to perform document searching is to use the root or inflected words as keywords. Those keywords is then matched to all stored documents. The search is performed through all the document's content to find word with exact similarity. This is not an effective solution and tend to be slow. A new algorithm is needed to speed up the performance of document-searching. Stemming Porter Method is used to reduce the inflected words to it's root form. The next step is to use Two Sliding Windows (TSW) Algorithm to speed up pattern finding. TSW uses two-sided windows parallely to find matched word or synonym. Based on the results, this algorithm speeds up the performance of document searching with 97.93% accuracy.

Keywords : Two Sliding Windows, Document Searching, Synonym, Porter Stemming.

**Moh. Muttaqin, Eko Nugroho, Eko Adi Nugroho | Universitas Gadjah Mada
JTIK Vol.5 No.1 Juni 2016**

RANCANGAN DIAGRAM ALIR DATA (DAD) UNTUK PENGEMBANGAN INFORMATION RETRIEVAL SYSTEM (IRS) DOKUMEN PENELITIAN MENGGUNAKAN BASIS DATA NON-RELATIONAL

Dokumen penelitian memiliki jenis dan format data yang sangat beragam. Penanganan dokumen dengan kompleksitas tinggi seperti ini membutuhkan sistem khusus sehingga pengaksesan terhadap informasi dalam dokumen-dokumen tersebut dapat dilakukan dengan optimal. Information Retrieval System (IRS) diciptakan untuk melakukan manajemen dokumen dari proses penyimpanan, pemberian indeks hingga pengaksesan kembali dengan cepat. Arsitektur IRS yang dibangun akan beragam juga, mengingat pihak

pengguna memiliki standar dan kebiasaan sendiri dalam menggunakan dokumen untuk kepentingan penelitian. Artikel ini menyajikan rancangan Diagram Alir Data (DAD) untuk pengembangan IRS dokumen penelitian berdasarkan observasi proses bisnis penelitian di Unit Pelaksana Teknis(UPT) Bidang Pengkajian dan Pengembangan Komunikasi dan Informatika (BPPKI) Badan Penelitian dan Pengembangan Sumber Daya Manusia Kementerian Komunikasi dan Informatika (Balitbang SDM Kominfo) RI. Metode perancangan menggunakan tahapan rekayasa informasi sesuai Software Development Life Cycle (SDLC) model Waterfall. Penelitian ini menghasilkan DAD-DAD untuk pengembangan IRS dengan basis data non-relational sehingga menghasilkan rancangan yang sederhana dan umum sebagai dasar bagi pengembangan beragam jenis arsitektur IRS yang lebih kompleks.

Kata Kunci : DAD, IRS, SDLC, model Waterfall, basis data non-relational

DATA FLOW DIAGRAM(DFD)DESIGN FOR THE DEVELOPMENT OF INFORMATION RETRIEVAL SYSTEM(IRS) OF RESEARCH DOCUMENT USING NON-RELATIONAL DATABASE

Research Documents have a large variety of type and format. Handling these high-complexity documents needs special system for optimal acces of informations within documents. Information Retrieval System (IRS) created for document management from storing process, indexing, until retrieving it quickly. Developed IRS architecture maybe vary depends on user standard and using behaviour of the document for the research purpose. This article propose Data Flow Diagram (DFD) design to develop IRS of research document based on the observation result of research bussiness processin Unit Pelaksana Teknis (UPT) Bidang Pengkajian dan Pengembangan Komunikasi dan Informatika (BPPKI) of Badan Penelitian dan Pengembangan SDM Kementerian Komunikasi dan Informatika (Balitbang SDM Kominfo) RI. Design method using information engineering stage according to Software Development Life Cycle (SDLC) in Waterfall model. This research results the DFDsfor IRS development using non-relational database, so its design is simple and generalto fit as a template for the development of more complex types of IRS architecture.

Keywords : DFD, IRS, SDLC, Waterfall model, non-relational database

**Ratna Wati Simbolon | Universitas Sumatera Utara
JTIK Vol.5 No.1 Juni 2016
PENGAMANAN TRANSKRIP NILAI MAHASISWA MENGGUNAKAN KRIPTOGRAFI PLAYFAIR CIPHER**

DAN STEGANOGRAFI DENGAN TEKNIK LEAST SIGNIFICANT BIT (LSB)

Jika kita menyampaikan pesan kepada orang lain, tentu pesan yang dimaksud adalah penting dan diupayakan segera sampai kepada orang yang tepat. Pesan yang dikirim sudah tentu adalah hal yang penting untuk disampaikan. Supaya pesan tersebut aman hingga diterima oleh orang yang tepat, maka perlu dijaga kerahasiaannya dan dihindarkan dari kecurigaan orang lain. Kombinasi antara kriptografi dan steganografi dapat dilakukan untuk lebih meningkatkan keamanan pada pesan yang hendak disembunyikan. Teknik kriptografi yang digunakan dalam penelitian ini adalah playfair cipher. Playfair cipher termasuk dalam Polygram Cipher. Algoritma ini mengenkripsi pasangan alfabet (bigram) pada plaintext. Dalam penelitian ini tabel matriks playfair yang digunakan yaitu matriks 6x6. Steganografi yang digunakan adalah metode spasial domain dengan teknik Least Significant Bit (LSB) yang terdiri dari 2 bagian yaitu LSB Embedding Process dan LSB Extracing Process. Penelitian ini menggunakan metode penelitian kuantitatif yang bersifat pengembangan. Tujuan penelitian ini adalah untuk merahasiakan pesan, dalam hal ini transkrip nilai mahasiswa, yang dilakukan dengan kriptografi, juga supaya menghindarkan pesan tersebut dari kecurigaan, yang kemudian dilakukan dengan proses steganografi. Hasil yang diperoleh adalah berupa file citra bitmap grayscale 8 bit per piksel dengan skala 0 sampai 255, atau dengan format biner. Pesan rahasia berhasil sepenuhnya dikembalikan menjadi pesan asli dengan proses dekripsi.

Kata Kunci : Kriptografi, Playfair, Bigram, Steganography, Least-Significant-Bit

PROTECTING THE STUDENT ACADEMIC TRANSCRIPT USING PLAYFAIR CIPHER CRYPTOGRAPHY AND STEGANOGRAPHY WITH THE LEAST SIGNIFICANT BIT (LSB) TECHNIQUES

If we convey the message to others, certainly the message in question is important and sought immediately to the right people. Messages sent is of course the important thing to be delivered. In order to secure the message is received by the right person, then it needs to be kept confidential and avoided the suspicion of others. The combination of cryptography and steganography can be done to further improve security in the message that would be hidden. Cryptographic techniques used in this study is the Playfair cipher. Playfair cipher is included in the Cipher Polygram. This algorithm encrypts a couple alphabet (Bigram) in plaintext. In this study Playfair matrix table used is the 6x6 matrix. Steganography is the method of spatial domain by using Least Significant Bit (LSB), which consists of two parts, namely LSB and LSB Embedding Process extracing Process. This study used quantitative research methods development. The purpose of this study was to conceal the message, in this case the transcripts of students, which is done with cryptography, also in order to avoid the message of suspicion, which is then conducted with steganography. The results obtained are in the form of bitmap image files grayscale 8 bits per pixel scale of 0 to 255, or binary format. Secret messages succeed fully restored to the original message with the decryption process.

Keywords : Cryptography, Playfair, Bigram, Steganography, Least-Significant-Bit

ISSN 2338-5839



9 772338 583913