PROTOKOL KEAMANAN DOKUMEN IJAZAH PENDIDIKAN TINGGI DENGAN INTEGRASI *DIGITAL WATERMARKING* DAN METODE ANALISIS STATIS

SKRIPSI

Diajukan untuk memenuhi sebagian syarat untuk memperoleh Gelar Sarjana Komputer

Oleh:

MUHAMAD FIRMANSYAH

2010021

PROGRAM STUDI ILMU KOMPUTER

FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS PENDIDIKAN INDONESIA

2025

LEMBAR HAK CIPTA

PROTOKOL KEAMANAN DOKUMEN IJAZAH PENDIDIKAN TINGGI DENGAN INTEGRASI *DIGITAL WATERMARKING* DAN METODE ANALISIS STATIS

Oleh:
Muhamad Firmansyah

Sebuah skripsi yang diajukan untuk memenuhi salah satu syarat memperoleh gelar Sarjana Komputer pada Program Studi Ilmu Komputer Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam

Universitas Pendidikan Indonesia
Agustus 2025

MUHAMAD FIRMASNYAH

PROTOKOL KEAMANAN DOKUMEN IJAZAH PENDIDIKAN TINGGI DENGAN INTEGRASI *DIGITAL WATERMARKING* DAN METODE ANALISIS STATIS

Disetujui dan disahkan oleh pembimbing:

Pembimbing 1

Rizky Rachman J.Putra , M.Kom.

NIP. 197711252006041002

Pembimbing 2

Dr. Eddy Prasetyo Nugroho, M.T.

NIP. 197505152008011014

Mengetahui

Ketua Program Studi Ilmu Komputer

Dr. Muhammad Nursalman, M.T.

NIP.197909292006041002

PERNYATAAN

Dengan ini penulis menyatakan bahwa skripsi dengan judul "Protokol Keamanan Dokumen Ijazah Pendidikan Tinggi dengan Integrasi *Digital Watermarking* Dan Metode Analisis Statis" ini beserta seluruh isinya adalah benar-benar karya penulis sendiri. Penulis tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika ilmu yang berlaku dalam masyarakat keilmuan. Atas pernyataan ini, penulis siap menanggung risiko/sanksi apabila di kemudian hari ditemukan adanya pelanggaran etika keilmuan atau ada klaim dari pihak lain terhadap keaslian karya penulis ini.

Bandung, 31 Juli 2025

Yang Membuat Pernyataan,

Muhamad Firmansyah

2010021

KATA PENGANTAR

Segala puji dan syukur penulis panjatkan kehadirat Allah Subhanahu Wata'ala, atas berkat dan rahmat-Nya penulis dapat menyelesaikan proposal skripsi dengan judul "**Protokol Keamanan Dokumen Ijazah Pendidikan Tinggi dengan Integrasi *Digital Watermarking* Dan Metode Analisis Statis**". Tidak lupa shalawat serta salam semoga selalu tercurah limpah kepada Nabi Muhammad Shallallahu 'Alaihi Wasallam. beserta keluarganya hingga akhir zaman. Tidak lupa pula penulis mengucapkan terimakasih kepada seluruh pihak yang telah membantu penyelesaian penulisan proposal seminar ini.

Proposal skripsi ini disusun untuk memenuhi salah satu syarat menyelesaikan mata kuliah seminar pada program studi Ilmu Komputer, Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam, Universitas Pendidikan Indonesia.

Bandung, 6 Juli 2025 Penulis,

Muhamad Firmansyah

UCAPAN TERIMAKASIH

Segala puji bagi Allah Subhanahu Wata'ala, yang telah melimpahkan rahmat, karunia, dan hidayah-Nya sehingga penulis diberikan kelancaran dalam menyelesaikan penulisan skripsi ini. Penulis menyadari bahwa penyusunan skripsi ini tidak terlepas dari banyak dukungan, bantuan, dan do'a dari berbagai pihak yang terlibat secara langsung maupun tidak langsung selama penyusunan skripsi ini dilakukan. Oleh karena itu, penulis ingin menyampaikan rasa terimakasih yang sebesar-besarnya kepada:

1. Kedua orang tua penulis yang senantiasa mendo'akan, dan memberikan kasih sayang, arahan serta dukungan yang tidak pernah terputus kepada penulis baik berupa dukungan moral maupun materiil sedari kecil, hingga selama kuliah dan dalam proses penyusunan skripsi ini.
2. Fani Riskawanti selaku kakak dari penulis yang telah memotivasi untuk menyelesaikan skripsi ini.
3. Bapak Rizky Rachman Judhie Putra, M.Kom., sebagai pembimbing I, atas semua ilmu, waktu, motivasi, serta dukungan yang telah dicurahkan kepada penulis selama penyusunan skripsi ini.
4. Bapak Dr. Eddy Prasetyo Nugroho, M.T., sebagai pembimbing II dan juga pembimbing akademik penulis, atas semua ilmu, waktu, motivasi, serta dukungan yang telah dicurahkan kepada penulis selama penyusunan skripsi.
5. Bapak Dr. Muhammad Nursalman, M.T., selaku ketua Program Studi Ilmu Komputer.
6. Andum, Aryo, Rafli, Ray, Ghiyats, Vega, Amim, Febri, Atta, Irfan, Hagai, Nyoman, Pinan, V, Trian, Yosafat, dan seluruh rakyat C2 2020 yang telah menjadi rekan, sahabat, dan saudara baur bagi penulis.

PROTOKOL KEAMANAN DOKUMEN IJAZAH PENDIDIKAN TINGGI DENGAN INTERGRASI *DIGITAL WATERMARKING* DAN METODE ANALISIS STATIS

ABSTRAKSI

Perkembangan teknologi menyebabkan adanya transformasi dari penggunaan dokumen fisik menjadi dokumen digital, termasuk dalam penerbitan ijazah pada jenjang pendidikan tinggi. Penggunaan dokumen ijazah digital sering berbentuk dalam format Portable Document Format (PDF), hal ini memiliki kelemahan, seperti rentan terhadap tindakan manipulasi, penyalinan tanpa izin, serta distribusi ilegal. Hal ini berdampak pada terancamnya tiga aspek penting dalam keamanan informasi, yaitu kerahasiaan (*confidentiality*), integritas (*integrity*), dan otentikasi (*authentication*) data akademik. Oleh karena itu, penelitian ini bertujuan untuk merancang, mengimplementasikan, serta menguji suatu protokol keamanan dokumen ijazah digital dengan integrasi *digital watermarking* dan metode *analisis statis*. Protokol yang dikembangkan dalam penelitian ini menggunakan metode *digital watermarking* untuk menyisipkan informasi identitas dokumen ijazah yang telah dienkripsi menggunakan algoritma Advanced Encryption Standard (AES) 128-bit dengan mode Cipher Block Chaining (CBC) ke dalam metadata dan *content stream* dokumen PDF. Metode *analisis statis* digunakan untuk memverifikasi keaslian dokumen melalui pemeriksaan metadata dan struktur PDF tanpa perlu membuka atau menjalankan file tersebut. Pengujian dilakukan terhadap empat jenis skenario dokumen, yaitu dokumen asli, dokumen yang telah dimodifikasi, dokumen hasil pemindaian ulang, dokumen asli yang diduplikasi. Berdasarkan hasil pengujian, *digital watermark* yang disisipkan bersifat tidak terlihat (*imperceptible*), hanya menambah ukuran file secara rata-rata sebesar 0,195% (*capacity*), serta bersifat rapuh (*fragile*), di mana jika terjadi modifikasi terhadap dokumen, maka watermark tidak dapat diambil kembali secara utuh. Sementara itu, metode *analisis statis* mampu membedakan metadata serta struktur PDF antara dokumen asli dan dokumen yang telah dimanipulasi. Dengan demikian, kombinasi kedua metode tersebut dapat meningkatkan keamanan dokumen ijazah digital dan memberikan solusi preventif terhadap praktik pemalsuan dokumen pendidikan tinggi.

Kata Kunci : Protokol Keamanan, Keamanan Informasi, Dokumen Ijazah Digital, *Digital Watermarking*, Metode Analisis Statis.

SECURITY PROTOCOL FOR HIGHER EDUCATION DIPLOMA DOCUMENTS WITH THE INTEGRATION OF DIGITAL WATERMARKING AND STATIC ANALYSIS METHOD

ABSTRACT

Technological advancements have driven the transformation from physical to digital documents, including in the issuance of higher education diplomas. The use of digital diploma documents, often in Portable Document Format (PDF), presents vulnerabilities such as susceptibility to manipulation, unauthorized copying, and illegal distribution. This consequently threatens three crucial aspects of information security: the confidentiality, integrity, and authentication of academic data. Therefore, this research aims to design, implement, and test a security protocol for digital diploma documents by integrating digital watermarking and static analysis methods. The protocol developed in this study utilizes a digital watermarking method to embed diploma identity information—encrypted using the Advanced Encryption Standard (AES) 128-bit algorithm with Cipher Block Chaining (CBC) mode—into the metadata and content stream of the PDF document. The static analysis method is used to verify the document's authenticity by examining its metadata and PDF structure without needing to open or execute the file. Testing was conducted on four document scenarios: an original document, a modified document, a rescanned document, and a duplicated original document. Based on the test results, the embedded digital watermark is imperceptible, increases the file size by an average of only 0.195% (capacity), and is fragile, meaning that if the document is modified, the watermark cannot be fully retrieved. Meanwhile, the static analysis method was able to distinguish the metadata and PDF structure between original and manipulated documents. Thus, the combination of these two methods can enhance the security of digital diploma documents and provide a preventive solution against the practice of higher education document forgery.

Keywords: Security Protocol, Information Security, Digital Diploma Document, Digital Watermarking, Static Analysis Method.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR PUSTAKA

Abdullayev, V., & Chauhan, A. S. (2023). SQL Injection Attack: Quick View. Dalam *Mesopotamian Journal of CyberSecurity* (Vol. 2023, hlm. 30–34). Mesopotamian Academic Press. https://doi.org/10.58496/MJCS/2023/006

Abu Al-Haija, Q., Odeh, A., & Qattous, H. (2022). PDF Malware Detection Based on Optimizable Decision Trees. *Electronics (Switzerland)*, *11*(19). https://doi.org/10.3390/electronics11193142

Adityas, R., & Munir, R. (2015). Skema Fragile Watermarking dengan Fungsi Hash dan Ketergantungan Blok Tak Deterministik. Dalam *Jurnal Cybermatika* | (Vol. 3, Nomor 1).

Amirtharajan R., & Rayappan J.B.B. (2012). Inverted pattern in inverted time domain for icon steganography. *Information Technology Journal*, *11*, 587–595.

Arnold, M., Schmucker, M., & Stephen D. Wolthusen. (2003). *Techniques and Applications of Digital Watermarking and Content Protection*. http://www.esecurity.ch/serieseditor.html

Buckland, M. K. (1997). What is a "document"? *Journal of the American Society for Information Science*, *48*(9), 804–809. https://doi.org/10.1002/(SICI)1097-4571(199709)48:9<804::AID-ASI5>3.0.CO;2-V

Castiglione, A., De Santis, A., & Soriente, C. (2010). Security and privacy issues in the Portable Document Format. *Journal of Systems and Software*, *83*(10). https://doi.org/10.1016/j.jss.2010.04.062

Chen', T., Wang'", J., & Zhou', Y. (2001). *Combined Digital Signature and Digital Watermark Scheme for Image Authentication*.

Donaldson, J. P., & Dinolt, G. W. (2013). *SOURCE FINGERPRINTING IN ADOBE PDF FILES*.

Dworkin, M. J. (2001). *Recommendation for block cipher modes of operation*. https://doi.org/10.6028/NIST.SP.800-38a

Eka Purnama, K., Rozikin, C., & Ali Ridha, A. (2023). ANALISIS FORENSIC CITRA DIGITAL MENGGUNAKAN TEKNIK ERROR

LEVEL ANALYSIS DAN METADATA BERDASARKAN METODE NIST. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *7*(2), 1100–1107. https://doi.org/10.36040/jati.v7i2.6660

Ferguson, N., Schneier, B., & Kohno, T. (2015). Cryptography Engineering: Design Principles and Practical Applications. Dalam *Cryptography Engineering*. John Wiley & Sons, Ltd. https://doi.org/https://doi.org/10.1002/9781118722367.ch8

Housley, R. (2009). *Cryptographic Message Syntax (CMS)*. http://trustee.ietf.org/license-info

Irawan, D. (2020). MENCURI INFORMASI PENTING DENGAN MENGAMBIL ALIH AKUN FACEBOOK DENGAN METODE PHISING. *JIKI (Jurnal llmu Komputer & lnformatika)*, *1*(1). https://doi.org/10.24127/jiki.v1i1.671

Jang, Y. S., & Choi, J. Y. (2014). Detecting SQL injection attacks using query result size. *Computers and Security*, *44*. https://doi.org/10.1016/j.cose.2014.04.007

Kantor Arsip USU. (2022, Januari 7). *Ijazah: Arsip Vital yang Harus Dijaga*. https://arsip.usu.ac.id/index.php/21-tips-arsip/232-ijazah-arsip-vital-yang-harus-dijaga#:~:text=Selain%20sebagai%20bentuk%20pengakuan%20yang,untuk%20mendapatkan%20pekerjaan%2Fmelamar%20pekerjaan.

Khadim, U., Munwar Iqbal, M., & Awais Azam, M. (2022). A Secure Digital Text Watermarking Algorithm for Portable Document Format (PDF). *Mehran University Research Journal of Engineering and Technology*, *41*(1), 100–110. https://doi.org/10.22581/muet1982.2201.10

LeBeau, B. (2018). pdfsearch: Search Tools for PDF Files. *Journal of Open Source Software*, *3*(27). https://doi.org/10.21105/joss.00668

Mahjabin, T., Xiao, Y., Sun, G., & Jiang, W. (2017). A survey of distributed denial-of-service attack, prevention, and mitigation techniques. *International Journal of Distributed Sensor Networks*, *13*(12). https://doi.org/10.1177/1550147717741463

Nilamsari, N. (2014). MEMAHAMI STUDI DOKUMEN DALAM PENELITIAN KUALITATIF. *Wacana*, *13*(2), 177–181. https://journal.moestopo.ac.id/index.php/wacana/article/view/143/88

Nugrahantoro, A., Fadlil, A., & Riadi, I. (2020). Optimasi Keamanan Informasi Menggunakan Algoritma Advanced Encryption Standard (AES) Mode Chiper Block Chaining (CBC). *Jurnal Ilmiah FIFO*, *12*(1), 12. https://doi.org/10.22441/fifo.2020.v12i1.002

Nur'aini, S. (2019). Steganografi Pada Digital Image Menggunakan Metode Least Significant Bit Insertion. *Walisongo Journal of Information Technology*, *1*(1), 73. https://doi.org/10.21580/wjit.2019.1.1.4025

Purnowo. (2014). Konsep dan Definisi Dokumentasi. Dalam Purnowo (Ed.), *Dasar-dasar Dokumentasi* (2 ed., hlm. 1.1-1.16). Universitas Terbuka.

Rafique, M., & Khan, M. N. A. (2013). Exploring Static and Live Digital Forensics: Methods, Practices and Tools. *International Journal of Scientific & Engineering Research*, *4*(10), 1048–1056. http://www.ijser.org/researchpaper%5CExploring-Static-and-Live-Digital-Forensic-Methods-Practices-and-Tools.pdf

Raghavan, S. (2013). Digital forensic research: current state of the art. *CSI Transactions on ICT*, *1*(1), 91–114. https://doi.org/10.1007/s40012-012-0008-7

Rahardjo, B. (2013). Sekilas Mengenai Forensik Digital. *Jurnal Sosioteknologi FSRD-ITB*, *12*, 384–387. https://doi.org/10.5614/sostek.itbj.2013.12.29.3

Ramadhan, P. S., Syahril, M., Kustini, R., Winata, H., & Gea, R. D. (2023). Transaction Data Security Using AES and RC4. *CESS (Journal of Computer Engineering, System and Science)*, *8*(1). https://doi.org/10.24114/cess.v8i1.41212

Renier, G. J. (1997). *HISTORY Its Purpose and Methode* (Vol. 34).

Muhamad, S. F. (2025). *Kemdiktisaintek gandeng Peruri percepat digitalisasi ijazah*. Antara. https://www.antaranews.com/berita/4788005/kemdiktisaintek-gandeng-peruri-percepat-digitalisasi-ijazah

Rosana, A. S. (2010). Kemajuan Teknologi Informasi dan Komunikasi dalam Industri Media di Indonesia. *Gema Eksos*, *5*(2).

Schneiner, B. (1996). *Protocols, Algoritms, and Source Code in C. John Wiley & sons, Inc.* .

Son, J., Kim, Y. W., Oh, D. Bin, & Kim, K. (2022). Forensic analysis of instant messengers: Decrypt Signal, Wickr, and Threema. *Forensic Science International: Digital Investigation*, *40*. https://doi.org/10.1016/j.fsidi.2022.301347

Stallings, William. (2023). *CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE EIGHT EDITION*. Pearson/Prentice Hall.

Subramanian, N., Elharrouss, O., Al-Maadeed, S., & Bouridane, A. (2021). Image Steganography: A Review of the Recent Advances. *IEEE Access*, *9*. https://doi.org/10.1109/ACCESS.2021.3053998

Supangkat, S. H., Kuspriyanto, & Juanda. (2000). Watermarking sebagai Teknik Penyembunyian Label Hak Cipta pada Data Digital. Dalam *TEKNIK ELEKTRO* (Vol. 6, Nomor 3).

Systems Incorporated, A. (1985). *PDF Reference fifth edition Adobe® Portable Document Format Adobe Systems Incorporated*.

Systems Incorporated, A. (2006). *PDF Reference sixth edition Adobe® Portable Document Format*. http://www.adobe.com/go/developer_legalnotices.

Tanjung, I., & Arief, T. M. V. A. (2022, Juni 16). Kades di Riau yang Pakai Ijazah Palsu Ditangkap, Sudah Menjabat 2 Tahun. *Kompas.com*. https://regional.kompas.com/read/2023/06/16/144922678/kades-di-riau-yang-pakai-ijazah-palsu-ditangkap-sudah-menjabat-2-tahun

Truică, C. O., & Apostol, E. S. (2023). It's All in the Embedding! Fake News Detection Using Document Embeddings. *Mathematics*, *11*(3). https://doi.org/10.3390/math11030508

Umam, C., & Handoko, L. B. (2024). *PREDIKSI EMAIL PHISING MENGGUNAKAN SUPPORT VECTOR MACHINE*.

Zhang, F., Dubasi, Y., Bao, W., & Li, Q. (2023). Detection and Localization of Data Forgery Attacks in Automatic Generation Control. *IEEE Access*, *11*, 95999–96013. https://doi.org/10.1109/ACCESS.2023.3311393