

**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

© Muhamad Firmansyah

Universitas Pendidikan Indonesia

Agustus 2025

Hak Cipta dilindungi undang-undang.

Skripsi ini tidak boleh diperbanyak seluruhnya atau sebagian,
dengan dicetak ulang, difotokopi, atau cara lainnya tanpa ijin dari peneliti.

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

Disetujui dan disahkan oleh pembimbing:

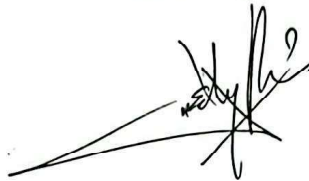
Pembimbing 1



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,

A handwritten signature in dark ink, appearing to read 'Firmansyah', with a stylized flourish at the end.

Muhamad Firmansyah

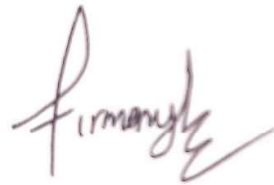
2010021

KATA PENGANTAR

Segala puji dan syukur penulis panjatkan kehadiran 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,

A handwritten signature in dark ink, appearing to read 'Firmansyah', with a stylized flourish at the end.

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

ABSTRAKSI.....	vi
ABSTRACT	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	xi
DAFTAR TABEL	xiv
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	4
1.3 Tujuan Penelitian	5
1.4 Batasan Masalah.....	5
1.5 Manfaat Penelitian	5
1.6 Sistematika Penulisan	6
BAB II TINJAUAN PUSTAKA.....	7
2.1 Keamanan Informasi	7
2.1 Dokumen	9
2.1.1 <i>Portable Document Format (PDF)</i>	11
2.1.1 Ijazah	14
2.3 Kriptografi.....	15
2.4 AES	15
2.4.1 Algoritma Enkripsi AES	16
2.4.2 Algoritma Dekripsi AES	21
2.4.3 Padding pada AES	25
2.4.4 Algoritma AES mode CBC.....	27
2.5 Steganografi	29
2.6 <i>Digital Watermarking</i>	30

2.6 <i>Digital Forensics</i>	32
2.7 Metode Analisis Statis	33
BAB III METODOLOGI PENELITIAN	35
3.1 Desain Penelitian.....	35
3.2 Rancangan Ide	37
3.3 Metode Pengumpulan Data	38
3.4 Alat dan Bahan Penelitian.....	39
3.4.1 Alat Penelitian	39
3.4.2 Bahan Penelitian.....	39
BAB IV PENELITIAN DAN PEMBAHASAN	40
4.1 Arsitektur Sistem.....	40
4.2 Potensi Ancaman Keamanan Pada Dokumen Ijazah Digital.	40
4.3 Proses Protokol Keamanan Dokumen Ijazah	43
4.4 Identifikasi Metadata.....	45
4.5 Implementasi Algoritma AES-128 Mode CBC	46
4.5.1 Proses Enkripsi.....	46
4.5.2 Proses Dekripsi	52
4.6 Proses <i>Digital Watermarking</i>	56
4.6.1 Proses <i>Embedding</i>	56
4.6.2 Proses <i>Extracting</i>	59
4.7 Metode Analisis Statis	61
4.7.1 Analisis Berdasarkan Metadata PDF	62
4.7.2 Analisis Berdasarkan Struktur PDF	69
4.8 Pengujian Protokol Keamanan	71
4.8.1 Implementasi Verifikasi Dokumen Ijazah	76
BAB V KESIMPULAN DAN SARAN	80

5.1 Kesimpulan	80
5.2 Saran.....	81
DAFTAR PUSTAKA.....	82

DAFTAR GAMBAR

Gambar 1.1 Validasi Kemendiktisaintek mengenai inisiatif untuk mengatasi masalah keamanan ijazah (Muhamad, 2025).....	3
Gambar 2.1 Struktur PDF	12
Gambar 2.2 Contoh Struktur <i>Body</i>	12
Gambar 2.3 Struktur <i>Cross-reference table</i>	13
Gambar 2.4 Contoh Struktur <i>Trailer</i>	14
Gambar 2.5 Contoh Blok Bit AES.....	16
Gambar 2.6 Diagram Proses Enkripsi AES	17
Gambar 2.7 Perhitungan <i>AddroundKey</i>	17
Gambar 2.8 Proses <i>SubBytes</i>	18
Gambar 2.9 Proses <i>ShiftRow</i>	19
Gambar 2.10 Contoh pengaplikasiannya pada state	19
Gambar 2.11 Nilai state setelah proses <i>ShiftRow</i>	20
Gambar 2.12 Operasi MixColumns pada kolom	20
Gambar 2.13 Hasil MixColumns terhadap seluruh kolom	20
Gambar 2.14 Nilai Key pada round pertama.....	21
Gambar 2.15 Proses Dekripsi AES.....	22
Gambar 2.16 Proses <i>InverseSubBytes</i>	23
Gambar 2.17 Proses <i>InverseShiftRows</i>	23
Gambar 2.18 Contoh pengaplikasiannya pada state	24
Gambar 2.19 Nilai state setelah proses <i>ShiftRow</i>	24
Gambar 2.20 Operasi MixColumns pada kolom	25
Gambar 2.21 Hasil MixColumns terhadap seluruh kolom	25
Gambar 2.22 Contoh Padding	26
Gambar 2.23 Contoh Unpadding	27

Gambar 2.24 Algoritma enkripsi AES mode CBC	28
Gambar 2.25 Proses Dekripsi Algoritma AES mode CBC	29
Gambar 2.26 Perbedaan Ilmu Steganography dan Cryptography (Supangkat dkk., 2000).....	29
Gambar 2.27 Proses <i>digital watermarking</i> (Supangkat dkk., 2000).....	31
Gambar 2.28 Contoh <i>structural signature</i> pada sebuah dokumen PDF.....	34
Gambar 3.1 Desain Penelitian.....	35
Gambar 3.2 Rancangan Ide Protokol Keamanan Dokumen Ijazah	37
Gambar 4.1 Arsitektur Sistem	40
Gambar 4.3 Skema SQL <i>Injection</i> pada website lembaga pendidikan	42
Gambar 4.4 Alur Proses Protokol Keamanan Dokumen Ijazah	44
Gambar 4.5 Contoh metadata pada sebuah dokumen ijazah digital.....	46
Gambar 4.6 Proses <i>Embedding</i> terhadap Dokumen Ijazah	57
Gambar 4.7 Contoh kunci dan pesan yang akan diembedding.....	57
Gambar 4.8 Penambahan metadata Watermark pada PDF	58
Gambar 4.9 Perbandingan Visual pada file PDF.....	59
Gambar 4.10 Nilai watermark yang terdapat pada Objek baru.....	59
Gambar 4.11 Proses <i>Extracting</i> terhadap Dokumen Ijazah	60
Gambar 4.12 Hasil Dekripsi nilai pada metadata watermark.....	60
Gambar 4.13 Hasil ekstraksi nilai objek pada <i>content stream</i> PDF	61
Gambar 4.14 Contoh Dokumen Ijazah Asli Pendidikan Tinggi.....	63
Gambar 4.15 Contoh dokumen ijazah yang sudah dimodifikasi	65
Gambar 4.16 Contoh dokumen ijazah yang di scan ulang	66
Gambar 4.17 Hasil Struktur PDF pada Dokumen Ijazah Digital	69
Gambar 4.18 Contoh dokumen ijazah yang sudah dimodifikasi	72
Gambar 4.19 Contoh dokumen ijazah yang di scan ulang	73

Gambar 4.20 Hasil Dekripsi pada Dokumen Ijazah Modifikasi	74
Gambar 4.21 Perbandingan Visual Dokumen yang Terwatermark dan yang tidak.....	75
Gambar 4.22 Tampilan Halaman Verifikasi Dokumen Ijazah	76
Gambar 4.23 Hasil Verifikasi Dokumen Ijazah Asli	76
Gambar 4.24 Hasil Verifikasi Dokumen Ijazah Modifikasi.....	77
Gambar 4.25 Hasil Verifikasi Dokumen Ijazah Hasil Scan.....	78
Gambar 4.26 Hasil Verifikasi Dokumen Ijazah Asli yang Diduplikasi	79

DAFTAR TABEL

Tabel 2.2 Tabel S-Box.....	18
Tabel 2.3 Tabel <i>Inverse</i> S-box	23
Tabel 4.1 Metadata pada dokumen ijazah digital.....	45
Tabel 4.2 Hasil <i>KeyExpansion</i> pada Kunci Enkripsi	47
Tabel 4.3 Hasil Enkripsi Algoritma AES mode CBC	50
Tabel 4.3 Hasil Dekripsi Algoritma AES mode CBC	55
Tabel 4.4 Hasil Ekstraksi Metadata Dokumen Ijazah Digital	63
Tabel 4.5 Hasil Ekstraksi Metadata pada Dokumen Ijazah Modifikasi.....	65
Tabel 4.6 Hasil Ekstraksi pada Dokumen Hasil Scan Ulang	67
Tabel 4.7 Hasil Ekstraksi Metadata Dokumen Ijazah Digital	68
Tabel 4.8 Penjelasan Objek beserta Fungsinya.....	70
Tabel 4.9 Struktur PDF pada keempat skenario	70
Tabel 4.10 Hasil Pengujian Ekstraksi Watermark pada Dokumen Ijazah	73
Tabel 4.11 Perubahan Kapasitas pada Dokumen Ijazah Terwatermak.....	75

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](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 Ilmu Komputer & Informatika)*, 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>
- Nugrahanoro, 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 Sositologi 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, Algorithms, 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>