

# Mendeteksi Orisinalitas Hasil Scan Citra Ijazah Menerapkan Metode Blake

Robert Laia

Program Studi Teknik Informatika, Universitas Budi Darma, Medan, Indonesia

Email: robertlaia87@gmail.com

**Abstrak**—Pesatnya perkembangan teknologi sekarang menyebabkan sering terjadinya penyalahgunaan sistem kinerja komputer yang banyak dimanfaatkan sebagai salah satu tindak kejahatan memanipulasi *file* dokumen yang merugikan orang lain. Untuk melakukan penelitian ini, penulis menggunakan metode BLAKE untuk mendeteksi keaslian *file* dokumen adalah dengan membandingkan *file* asli, sehingga dapat diketahui *file* tersebut asli atau tidak jika hasilnya sama maka *file* tersebut dikatakan asli, dan jika hasilnya tidak sama maka *file* tersebut dikatakan tidak asli. Dengan aplikasi yang dirancang menggunakan *Microsoft Visual basic 2008*, dapat mempermudah untuk pengujian keaslian *file* dokumen agar dapat membedakan mana *file* yang asli dan *file* yang tidak asli.

**Kata Kunci:** Kriptografi; Keaslian File; BLAKE

**Abstract**—The rapid development of technology now causes frequent abuse of computer performance systems which are widely used as one of the crimes of manipulating document files that harm others. it can be known whether the file is original or not if the results are the same then the file is said to be original, and if the results are not the same then the file is said to be not original. original and non-original files.

**Keywords:** Cryptography; File Authenticity; BLAKE

## 1. PENDAHULUAN

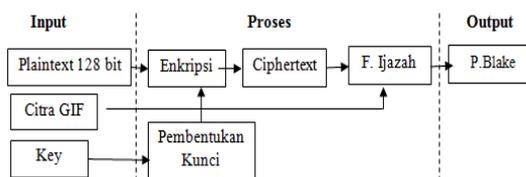
Ijazah adalah sebuah sertifikat atau dokumen yang diberikan oleh suatu instansi sebagai dokumen resmi tentang orang, santri, siswa atau mahasiswa. Ijazah biasanya diperoleh sesudah tamat belajar oleh sekolah atau universitas baik di dalam negeri atau mahasiswa luar negeri kepada siswanya atau mahasiswanya. Hal ini biasanya berarti bahwa siswa telah belajar pengetahuan ini melalui tatap muka interaksi "di kaki" dari guru. Ijazah biasanya diterbitkan oleh satuan pendidikan yang sudah terakreditasi, misalnya, Pendidikan Anak Usia Dini (PAUD) Sekolah Dasar (SD) Sekolah Menengah Pertama (SMP) Sekolah Menengah Atas (SMA) dan Perguruan Tinggi. Berita tentang ijazah palsu sering kita dengar di TV, koran, media sosial dan lain-lain. Kalau ada ijazah palsu, dalam undang-undang pemegang ijazah palsu (ancaman hukuman) 5 tahun. Yang mengeluarkan 10 tahun.

*File scan* ijazah dihasilkan dari proses *scan* dokumen ijazah dengan menggunakan alat mesin *scan*. *File* hasil *scan* ijazah pada umumnya digunakan untuk melengkapi administrasi pada saat melamar pekerjaan baik itu di instansi swasta maupun di instansi negeri. Mendeteksi orisinalitas *file scan* ijazah tentunya sangatlah penting, mengingat banyak permasalahan yang berkaitan dengan pemalsuan data. Pelanggaran terhadap pemalsuan dokumen ijazah merupakan bentuk tindak pidana pemalsuan surat sebagaimana diatur dalam Pasal 263 Kitab Undang-Undang Hukum Pidana ("KUHP")

## 2. METODOLOGI PENELITIAN

### 2.1 Tahapan Penelitian

Berikut merupakan tahapan dari enkripsi.



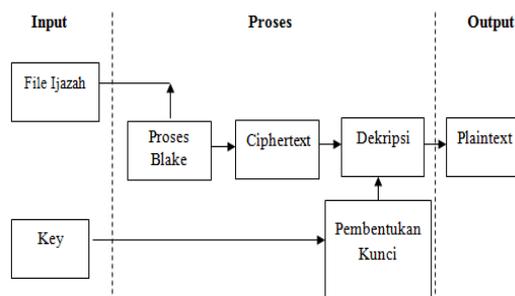
Gambar 1. Gambar Tahapan Enkripsi dan Blake

Keterangan dari gambar di atas adalah sebagai berikut:

1. Memasukkan *input* berupa citra, *plaintext*, dan *key*
2. Proses pembentukan kunci
3. Mengenkripsi *Plaintext* dengan algoritma *Blake*
4. Hasil keluaran berupa *Ciphertext*, *Ciphertext* tersebut yang nantinya akan disisipkan pada media citra
5. Melakukan proses *Blake* dengan file ijazah algoritma *Blake*

### 3. HASIL DAN PEMBAHASAN

Pada tahap analisa dilakukan pengumpulan informasi dan penguraian mengenai proses yang akan digunakan untuk membangun sistem peningkatan keamanan data teks terenkripsi algoritma *Blake* menggunakan file ijazah *Blake*. Dalam hal ini akan diuraikan tentang proses penyisipan data teks terenkripsi algoritma *Blake* ke suatu media menggunakan file ijazah dengan algoritma *Blake*. Sebelum dilakukannya proses penyisipan, terlebih dahulu dilakukan proses enkripsi pada pesan atau data teks menggunakan algoritma *Blake* untuk menjaga keaslian dari pesan tersebut. Sehingga pesan atau data teks yang telah dienkripsi tersebut akan disisipkan ke suatu media citra GIF menggunakan file ijazah *Blake*. Hasil keluaran berupa *file* ijazah, selesai.



**Gambar 2** Gambar Tahapan *Blake* dan Dekripsi

Keterangan dari gambar di atas adalah sebagai berikut :

1. Memasukkan *input* berupa *Stegoimage*, dan *Key*
2. Melakukan proses *Blake* menggunakan algoritma *Blake*
3. Hasil keluaran berupa *ciphertext*, *ciphertext* ini yang nantinya akan dikembalikan menjadi teks awal atau *plaintext*
4. Mendekripsi *ciphertext* menjadi *plaintext* menggunakan kriptografi algoritma *Blake*
5. Hasil keluaran berupa *plaintext*, selesai.

**Tabel 1.** Hasil Nilai Palet Warna Setiap *Pixel*

182	146	150	146	182	146	150	146	182	146
146	150	140	187	146	150	139	150	146	181
182	146	150	146	182	146	150	146	182	146
150	145	182	146	150	140	150	140	150	146
182	146	150	146	182	146	150	146	145	182
146	150	140	187	146	182	146	182	146	146
140	150	146	150	140	146	150	140	145	182
150	145	182	146	150	139	146	182	146	140
140	150	146	150	140	150	181	146	139	150
150	146	182	145	146	182	146	181	146	140
140	182	146	182	146	150	146	150	140	150
150	146	150	146	150	139	150	140	146	150
150	140	150	140	150	146	150	146	150	140

#### 3.1 Hasil Pengujian

Proses pengujian dalam penelitian ini dilakukan terhadap beberapa file ijazah yang berbeda, dengan menggunakan aplikasi yang telah dibangun dengan menggunakan bahasa pemrograman visual Microsoft VB. Net 2008. Berikut tabel hasil pengujian yang telah dilakukan:

**Tabel 2.** Hasil Pengujian

Spesifikasi File Ijazah Asli	Kode Hash File Ijazah Asli	Perubahan yang dilakukan	Spesifikasi File Ijazah Palsu	Kode Hash File Ijazah Asli
NamaFile: Robert Date modified: 24/07/2019 14:39 Ukuran: 1.726 Kb	E4A40F15AE54 AAE07B72B2E 0611ADCF	Mendeteksi keaslian file ijazah	NamaFile: Robert Date modified: 24/07/2019 14:45 Ukuran: 1.724 Kb	A4E40F15AE542 AE32B72345061 1A5CCB

### 4. KESIMPULAN

Setelah menyelesaikan penelitian ini, penulis berkesimpulan panjang atau pendek dari *plaintext* yang akan disandikan tidak berpengaruh terhadap kecepatan karena setiap *plaintext* harus dalam bentuk *block-block* 512 *bit*. Mendeteksi menggunakan metode *Blake* membutuhkan 64 operasi dan setiap operasi mengalami pergeseran secara sikuler.

Mendeteksi secara manual harus memiliki ketelitian yang tinggi karena kesilafan 1 *bit* saja menyebabkan kesalahan fatal kecuali diulangi dari awal. Struktur metode yang digunakan tidak terlalu rumit, cukup dengan pemahaman operasi sitem bilangan. Alat bantu bisa dilakukan dengan menggunakan *matlab* dan *microsoft visual studio 2008*. Untuk ini juga diperlukan konsistensi terhadap tampilan, struktur dari *database* disesuaikan dengan ukuran data yang akan disimpan, dalam hal ini *blake* memerlukan ukuran *record* yang tetap.

## **REFERENCES**

- [1] S. Emy Setyaningsih, Kriptografi & implementasinya menggunakan matlab, Yogyakarta: ANDI, 2015.
- [2] Schneir, "Pengamanan basis data sistem penjualan dengan menggunakan teknik enkripsi kriptografi," *Jurnal Teknologi Informasi dan Komunikasi*, no. 6, pp. 2252-4517, 2018.
- [3] Sarineen, "Pengamanan basis data sistem penjualan dengan menggunakan teknik enkripsi kriptografi gost," *Jurnal teknologi informasi dan komunikasi*, no. 6, pp. 2252-4517, 2018.
- [4] Leurent, G.: ARXtools: A toolkit for ARX analysis. In: The Third SHA-3 Candi-date Conference. (March 2012).