JNATIA Volume 1, Nomor 1, November 2022
Jurnal Nasional Teknologi Informasi dan Aplikasinya

Implementasi Steganografi Citra Gambar pada Sertifikat Hak Kekayaan Intelektual (HKI)

Ni Putu Anita Dewi[a1], Made Agung Raharja[a2]

[a]Informatics Departement, Faculty of Math and Sience, Udayana University
Jimbaran, Bali, Indonesia
[1]anitadewi20177@gmail.com
[2]made.agung@unud.ac.id

Abstract

Information based technology in the digital era 4.0 currently has a very high influence on life. Many activities are carried out online, for example: meetings, lectures, ordering food, ordering transportation, applying for jobs and sending important files. Not a few of these online activities require image file transactions such as sending Intellectual Property Right (IPR) image files. There are irresponsible people who can misuse someone's copyrighted work to carry out certain interests. Therefore, the IPR file used must be inserted with a message so that if something unexpected happens, it can quickly identify the culprit. Steganography is a method of inserting information into digital data to protect data ownership. This system will run in website, create using JavaScript Framework that is React.js.

Keywords: *Steganography, Intellectual Property Right (IPR), JavaScript Framework, React.js.*

1. Introduction

Teknologi berbasis informasi di era digital 4.0 saat ini memiliki pengaruh yang sangat tinggi terhadap kehidupan. [3]. Mengirim data rahasia melalui internet adalah tugas yang beresiko. Perhatian utama adalah untuk melindungi data dari penyusup. Seperti data ditransmisikan melalui media digital, memiliki kelemahan seperti gangguan, mudah diakses, penggunaan ilegal, hak cipta, pelanggaran dll. Penyembunyian informasi adalah cabang ilmu komputer yang berhubungan dengan penyembunyian data, objek, atau fungsi [2]. Privasi dan kerahasiaan data menjadi lebih mendasar keberadaannya daripada sebelumnya, terutama dengan meningkatnya ketergantungan pada layanan online dan transfer informasi, baik untuk kenyamanan atau pengaruh pandemi COVID. Langkah-langkah keamanan tradisional seperti kriptografi dan steganografi sangat penting [2].

Steganografi adalah seni komunikasi tak terlihat [1]. Menggunakan steganografi, informasi rahasia ditransfer secara aman dengan menyematkan informasi. Dengan demikian, data berjalan dalam penyamaran, tidak terdeteksi oleh penyadap. Selanjutnya, jika seseorang mendapatkan akses ke sampul tersebut, mereka tidak mengetahui fakta bahwa informasi sensitif sebenarnya tersembunyi di dalam sampul itu atau bahwa komunikasi rahasia sedang berlangsung [2]. Data yang akan dilindungi adalah Sertifikat HKI. HKI termasuk kedalam benda bergerak yang tidak terihat. Hak kekayaan intelektual dilindungi karena berguna untuk melindungi reputasi, mendorong dan menghargai setiap inovasi serta penciptaannya, dan mencegah duplikasi. Kurangnya perlindungan terhadap HKI mengakibatkan banyaknya kekayaan intelektual milik masyarakat dan bangsa Indonesia diambil dan dimanfaatkan bahkanmemberikan keuntungan ekonomi bagi negara lain [4].

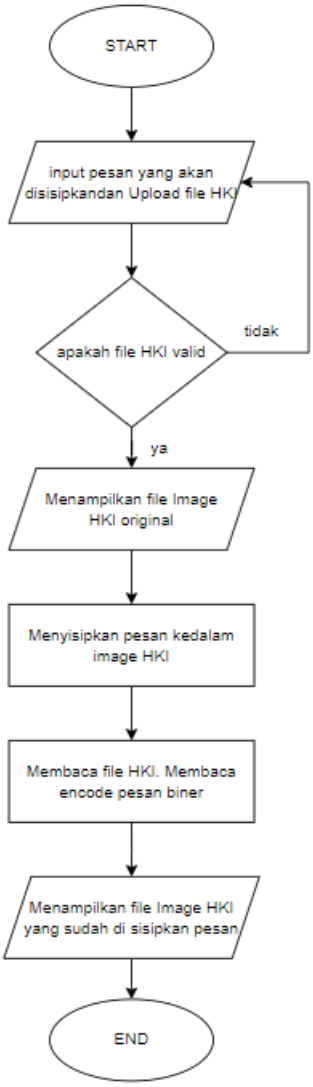
2. Reseach Methods

2.1. Gambaran Aplikasi

Implementasi pengamanan sertifikat HKI menggunakan steganografi memiliki kategori utama yaitu penyisipan pesan kedalam citra gambar. Dalam paper ini dilakukan penyisipan pesan rahasia kedalam sertifikat HKI. File yang digunakan menggunakan format jpg atau png.

2.2 Desain Aplikasi

Aplikasi yang dibuat menggunakan framework dari JavaScript yaitu React.js dan tampilan antarmuka menggunakan html, css, dan bootstraps. Berikut merupakan *flowchart* yang digunakan dalam implementasi pengamanan sertifikat HKI menggunakan steganografi.



Gambar 1. Diagram Alur Penyisipan Pesan

Penjelasan diagram alur penyisipan pesan :

1. *Input* berupa file sertifikat HKI yang berekstensi gambar (jpg, png)
2. Dilakukan pengecekkan apakah *file* sertifikat HKI sudah valid, jika tidak maka akan diminta untuk mengimputkan ulang *file* sertifikat HKI yang benar. Jika valid maka menuju proses selanjutnya.
3. Menampilkan *output file image* HKI yang original sebelum di sisipkan pesan.

4. Proses menyisipkan pesan kedalam *image* HKI.
5. Membaca *file* HKI mdan membaca file dari encode biner.
6. Menghasilkan *output file image* HKI yang sudah di sisipkan pesan.

Gambar 2. Diagram Alur Pembacaan Pesan

Penjelasan diagram alur pembacaan pesan :

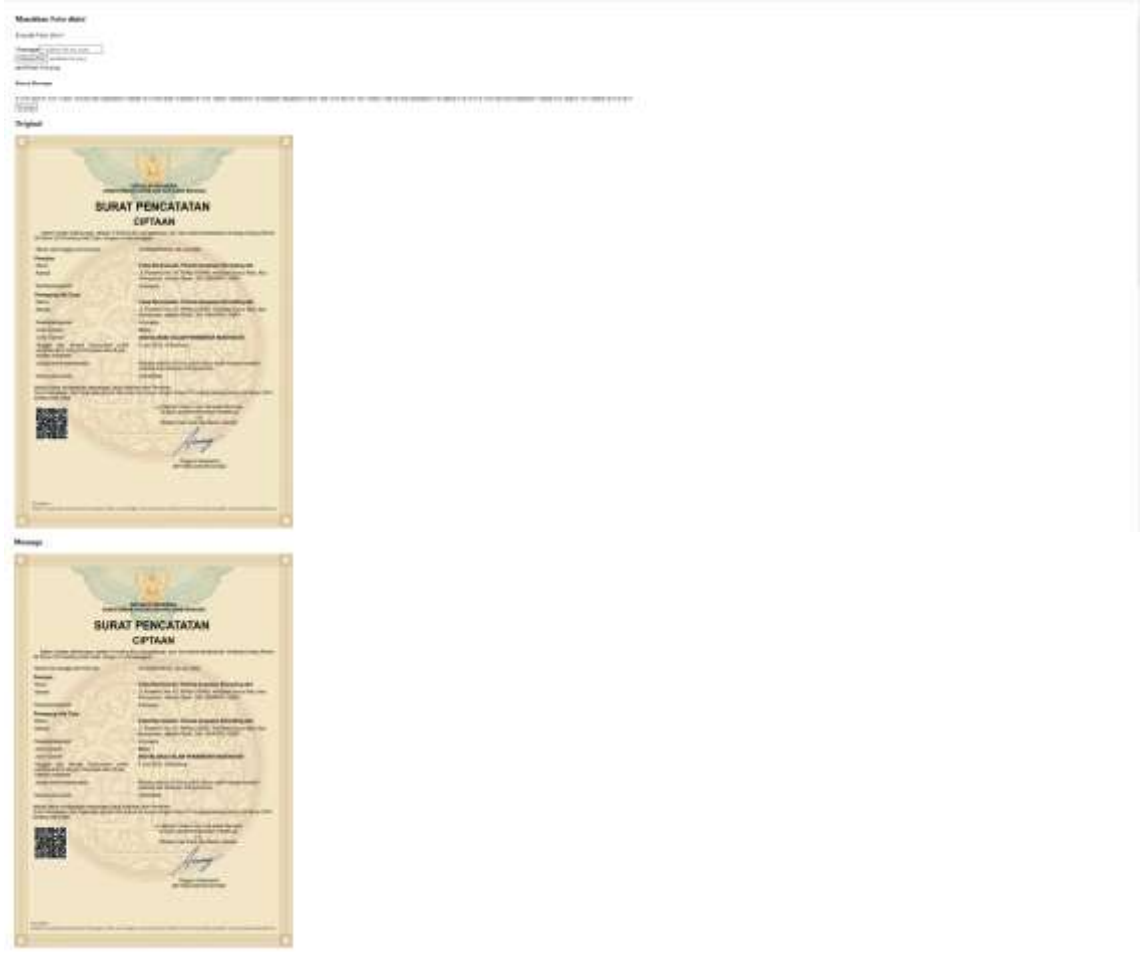
1. Input berupa *file* HKI yang berekstensi gambar (jpg, png) yang sudah disisipkan pesan sebelumnya.
2. Proses membaca *image* HKI dan membaca pesan yang disisipkan.
3. Menghasilkan *output* pesan yang telah disisipkan pada *file image* HKI.

3. Result and Discussion

3.1. Tampilan Awal Aplikasi

Pada tampilan awal aplikasi seperti pada gambar 3. Terdapat dua bagian dalam satu halaman yaitu yang pertama pada bagian atas untuk mengupload gambar sertifikat HKI yang akan disisipkan pesan rahasia dan yang kedua pada bagian bawah untuk melakukan pembacaan pesan rahasia dari file HKI yang di download. Pada halaman atas terdapat form untuk mengetikkan pesan, form yang berisikan file HKI. User mengisikan pesan yang akan disisipkan dan juga mengupload file HKI, jika file HKI valid maka sistem akan menampilkan file HKI yang sudah diisisipkan pesan dan bisa di download seperti gambar 4. Pada halaman bagian bawah yaitu membaca pesan yang telah disisipkan, terdapat form yang hanya berisikan upload file HKI yang sudah di sisipkan pesan, jika valid maka sistem akan menampilkan pesan yang ada pada file tersebut seperti gambar 5.

Gambar 3. Tampilan Awal Website



Gambar 4. Tampilan Penyisipan Pesan

Gambar 5. Tampilan Pembacaan Pesan

3.2. Pengujuan Sistem

Metode pengujian sistem menggunakan metode *blackbox.* Hasil pengujian *blackbox*:

Table 1. Pegujian Penyisipan Pesan

No.	Sekenario Pengujian	Test Case	Hasil yang Diharapkan	Hasil Pengujian	Kesimpulan
1	Input pesan menggunakan tulisan dan gambar berekstensi jpg atau png	Mengisi inputan dengan tulisan Klik tombol untuk menginput file dan masukkan file gambar berekstensi jpg atau png. Klik tombol upload	File gambar berhasil di upload dan sisipkan tulisan	Sesuai harapan	Valid
2	Input pesan menggunakan tulisan dan file selain gambar berekstensi jpg atau png	Mengisi inputan dengan tulisan Klik tombol untuk menginput file dan masukkan file selain gambar Klik tombol upload	Program akan menampilkan peringatan file bukan gambar	Tidak sesuai harapan	Invalid
3	Klik tombol encode	Klik tombol encode ketika gambar sudah di upload	Program berhasil menampilkan apa yang kita input pada input field sebelumnya	Sesuai harapan	Valid

Table 2. Pengujiap Pembacaan Pesan

No.	Sekenario Pengujian	Test Case	Hasil yang Diharapkan	Hasil Pengujian	Kesimpulan
1	Upload file berekstensi jpg atau png	Upload file jpg atau png yang sudah disisipkan pesan	Program berhasil menampilkan gambar yang sudah disisipkan pesan	Sesuai harapan	Valid
2	Upload file berekstensi selain jpg atau png	Upload file selain jpg atau png yang sudah disisipkan pesan	Program akan menampilkan peringatan file yang di upload bukan gambar	Tidak sesuai harapan	Invalid
3	Klik tombol decode	Klik tombol decode Ketika gambar sudah di upload	Program berhasil menampilkan isi pesan pada file gambar.	Sesuai harapan	Valid

4. Conclusion

Dapat disimpulkan pada rancangan sistem steganografi ini dapat menyisipkan pesan ke dalam *file* HKI dan pesan yang disisipkan tidak tampak pada *file* tersebut. *File* HKI yang sudah disisipkan pesan dapat di download kemudian dicek bahwa *file* tersebut berisi pesan. Lama waktu yang diperlukan untuk menyisipkan *file* HKI tergantung dari berapa panjang teks yang disisipkan,

References

[1] Alanazi, N., Khan, E., Gutub, A. “Involving spaces of unicode *stfile andard* within irreversible Arabic text steganography for practical implementations in press Arab. J. Sci. Eng. 46 (9), 8869–8885. https://doi.org/10.1007/s13369-021-05605-8. Accessed 28 September 2022.

[2] Al-Shaarani, F., & Gutub, A. “Securing matrix counting-based secret-sharing involving crypto steganography.“ Journal of King Saud University - Computer and Information Sciences, 34(9), 6909–6924. 16 September 2021 https://doi.org/10.1016/j.jksuci.2021.09.009. Accessed 26 September 2022.

[3] Ramalingam, M., Mat Isa, N. A., & Puviarasi, R. (2020). “A secured data hiding using affine transformation in video steganography.” Procedia Computer Science, 171, 1147–1156. https://doi.org/10.1016/j.procs.2020.04.123. Accessed 29 September 2022.

[4] Staff, A. (2021, April 26). “PENTINGNYA PERLINDUNGAN HAK KEKAYAAN INTELEKTUAL (HKI) DALAM DUNIA BISNIS.” 26 April 2021, https://fh.unair.ac.id/en/pentingnya-perlindungan-hak-kekayaan-intelektual-hki-dalam-dunia-bisnis/. Accessed 24 September 2022.