Terbit *online* pada laman web jurnal : http://innovatics.unsil.ac.id

Innovation in Research of Informatics (INNOVATICS)

| ISSN (Online) 2656-8993 |

Digital Watermarking Using Advanced Encryption Standard (AES) And Steganography Methods to Increase The Level Of Security Of User Data In The Image Files On Internet Network

Khoerul Umam[1]

[1]*Ilmu Komputer, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Semarang*
[1]*khoerulumam@students.unnes.ac.id*

INFORMASI ARTIKEL

Sejarah Artikel:
Diterima Redaksi: 06-06-2020
Revisi Akhir: 06-10-2020
Diterbitkan *Online*: 20-10-2020

KATA KUNCI

Digital Watermarking,
Advanced Encryption Standard,
Steganography

KORESPONDENSI

Telepon: +62 823 2506 9441

E-mail: khoerulumam@studentns.unnes.ac.id

A B S T R A C T

The spread of digital media on the internet was very broad, fast, and cannot be monitored in a structured manner about what media has been uploaded and distributed on the internet network. The spread of digital media like this was very difficult to detect whether the media that shared was privately owned or that of others that is re-shared by media theft or digital media piracy. One step to overcome the theft of digital works is to give them a watermark, which is an identity that is placed on top of the work. However, this is still considered unsafe because the identity attached can be cut and manipulated again until it is not visible. In addition, the use of Steganography method to hide messages in an image can still be manipulated by adding messages continuously so that it accumulates and damages the original owner of the image. In this article, the author provides a solution called Digital Watermarking, a step of encrypting the data of the original owner of the work and putting it into the image of his work. This watermark cannot be seen clearly, but actually in the media there is encrypted data with a strong Advanced Encryption Standard (AES) method. As a result, a tool that can improve the security of media owner data by combining the AES and Steganography methods in the formation of new media that cannot be changed anymore. So, when the media is stolen and used by others and has been edited, the owner's personal data can never be changed.

1. PENDAHULUAN

Penyebaran media terutama media gambar sangat cepat terjadi di dunia internet. Hal ini tidak dapat di cegah karena hampir semua orang mempunyai akses terhadapnya. Hal ini sangat rentan terjadi pembajakan media gambar yang diunggah ke jaringan internet dan merugikan pemilik asli dari media gambar tersebut.

Gambar yang dibajak dapat disalahgunakan, seperti penyebaran berita palsu yang terus meningkat dari tahun 2014 hingga 2016, dimana pengaruh berita palsu ini sangat besar dampaknya di masyarakat[5].

Selain penyebaran berita palsu, pembajakan gambar juga dapat mempengaruhi bisnis yang terjadi. Maksudnya, ketika pemilik asli dari suatu gambar menjual karyanya, dan suatu ketika karya di bajak oleh orang yang tidak bertanggung jawab, pemilik karya tentu akan merasa dirugikan oleh kejadian tersebut.

Salah satu cara untuk menandai bahwa suatu gambar memiliki suatu hak cipta, biasanya pemilik gambar asli akan menempelkan watermark pada sebuah gambar. Namun, hal ini masih kurang aman karena dengan alat editor media, watermark tersebut dapat dihapus dengan mudah dengan cara memanipulasinya.

Kemudian, langkah pengamanan data berkembang menjadi penyembunyian data dengan metode steganography. Suatu data dapat disembunyikan di file media sehingga data pemilik asli tidak terlihat. Namun, hal tersebut masih bisa dimanipulasi kembali dengan cara mengekstrak data yang ada kemudian menggantinya dengan yang baru. Hal ini terjadi karena penggunaan metode End Of File, dimana metode tersebut memiliki kelemahan yaitu dapat dengan mudah diekstrasi[3].

Jika hal tersebut tidak diantisipasi, pembajakan akan terus meningkat dan penyalahgunaan gambar orang lain tanpa ada tanggung jawab juga akan terus meningkat,

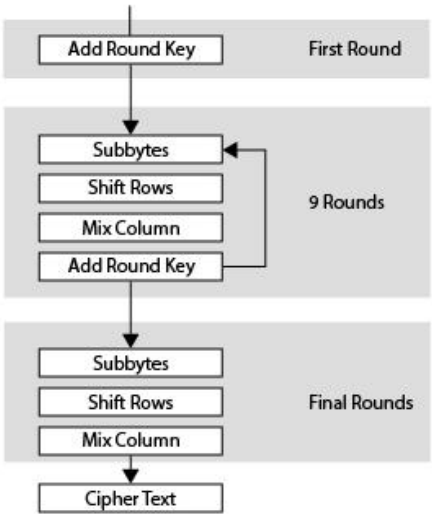
sementara itu di sisi keamanan data masih belum ada alat dan metode yang dapat mencegah hal itu terjadi, artinya perlu adanya sebuah alat dan metode yang dapat mencegah terjadinya pembajakan media gambar yang ada di internet. Alat dan media gambar tersebut dapat diciptakan dengan metode enkripsi data Advanced Encryption Standard (AES) untuk mengenkripsi data pemilik yang asli dan metode Steganography untuk menyembunyikan hasil enkripsi di dalam gambar.

1.1 Advanced Encryption Standard

Algoritma enkripsi dan dekripsi data pertama kali diperkenalkan pada tahun 1977 yang bernama Data Encryption Standard (DES). Pada tahun tersebut, DES menjadi metode enkripsi dan dekripsi data yang popular, akan tetapi seiring berjalannya waktu, semakin terlihat bahwa DES mempunyai kelemahan dalam hal keamanan data karena masih menggunakan 56 bit kunci[1].

Kemudian DES diganti oleh Advanced Encryption Standard (AES) yang sampai sekarang masih digunakan dan masih kuat dalam mempertahankan keamanan data.

AES adalah sebuah metode enkripsi data yang termasuk ke dalam algoritma kriptografi simetrik dimana pada metode AES menggunakan mode chiper blok dalam mengenkripsi dan mendekripsi data. AES menjadi metode yang kuat karena proses cipher blok nya menggunakan 128-bit, 192-bit, atau 256-bit kunci[1]. Ada empat tahapan di dalam proses enkripsi data dengan AES yaitu Add Round Key, Subbytes, Shift Rows, dan Mix Column yang prosesnya digambarkan pada Gambar 1.



Gambar 1. Proses Enkripsi Data dengan AES

Data yang akan dienkripsi, pertama kali dilakukan Add Round Key, kemudian dilakukan perulangan dari Subbytes, Shift Rows, Mix Column, dan Add Round Key kembali sebanyak 9 putaran dan putaran ke 10 tidak melalui Add Round Key.

1.2 Steganography

Steganography adalah sebuah teknik menyembunyikan data di dalam sebuah media sehingga data tersebut tidak dapat dilihat oleh mata[3].

Salah satu jenis Steganography adalah end of file steganography, di mana data disembunyikan pada akhir pixel gambar seperti yang diperlihatkan di Gambar 2.

103	84	87	
109	88	99	
178	131	154	
127	230	81	
78	78	80	
111	87	105	
156	32	88	
98	90	88	
90	92	71	
255	45	111	
194	182	195	
148	11	49	
7	39	52	
195	130	26	Hidden data
195	143	197	
160	127	93	
99	255	255	

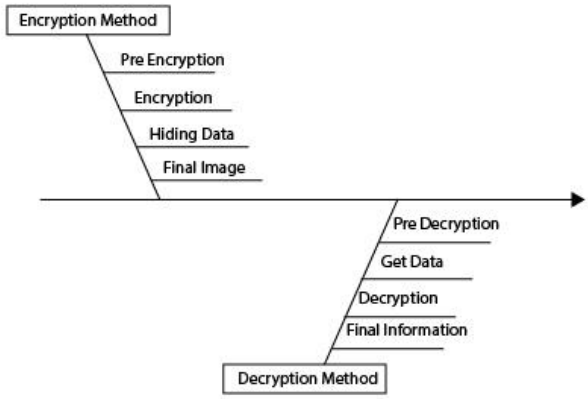
Gambar 2. Contoh Penempatan Data dalam End Of File Steganography

Namun, penggunaan steganography jenis tersebut sangat rentan dimanipulasi dan dapat dengan mudah diekstrasi data. Sehingga data dapat hilang dan dapat digantikan oleh data lain. Tentu, hal ini tetap tidak aman.

2. Metodologi

2.1 Metode Penelitian

Metode penelitian ini dilakukan sebagaimana diperlihatkan dalam flowchart pada Gambar 3.

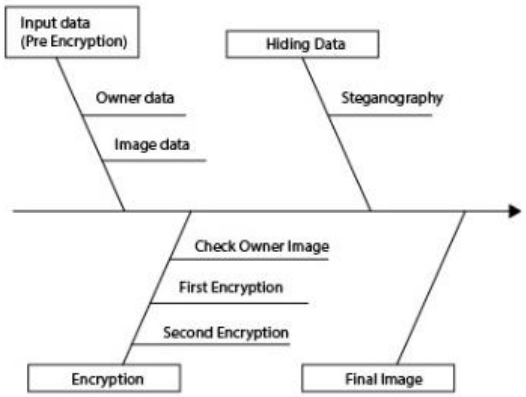


Gambar 3. Flowchart Metode Penelitian

Metode yang digunakan dalam penelitian ini tersusun dari dua proses, yaitu enkripsi dan dekripsi. Masing-masing proses memiliki langkah yang digunakan untuk meningkatkan keamanan data dalam memberikan hak cipta pada sebuah gambar.

2.2 Metode Enkripsi

Metode enkripsi adalah metode yang digunakan untuk mengenkripsi data sekaligus menyembunyikan data ke dalam file gambar sehingga data semakin aman. Metode enkripsi dijelaskan dalam Gambar 4.



Gambar 4. Proses Dari Metode Enkripsi

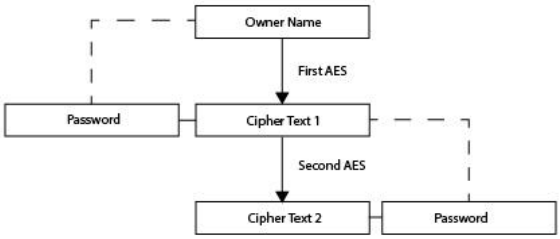
Ada empat langkah dalam melakukan enkripsi, keempat langkah tersebut yaitu:

a) Input Data (Pre Encryption)

Ini merupakan langkah awal di mana data disiapkan untuk dilakukan enkripsi. Data yang disiapkan hanya berupa nama pemilik media gambar dan gambar yang akan dienkripsi.

b) Enkripsi Data (Encryption)

Pada proses ini dilakukan proses enkripsi. Data berupa nama akan dienkripsi dengan metode AES. Data akan dienkripsi sebanyak dua kali. Metode enkripsi data digambarkan di dalam Gambar 5.



Gambar 5. Proses *Double Encryption Methods*

Data nama yang masuk akan dienkripsi dengan AES dengan 256 bit key, di mana data nama ini sekaligus menjadi password di enkripsi yang pertama. Kemudian hasil enkripsi akan dienkripsi kembali dengan AES dengan 256 bi key dan sekaligus cipher text pertama akan menjadi password untuk cipher text kedua.

Hal ini dilakukan kerena ketika pertama kali akan dilakukan enkripsi, gambar akan dicek terlebih dahulu apakah sudah ada data pemiliknya atau belum. Jika sudah ada, maka gambar tidak bisa dienkripsi kembali.

c) Hiding Data

Setelah data sudah siap untuk disembunyikan, selanjutnya masuk ke dalam proses steganography. Proses stegnaography ini menggunakan algoritma memasukkan data ke setiap piksel gambar. Sehingga, sebelum dilakukan proses ini, pesan akan dikonversi menjadi bilangan biner dan kemudian akan dimasukkan ke setiap bit warna di setiap gambar. Berikut algoritmanya:

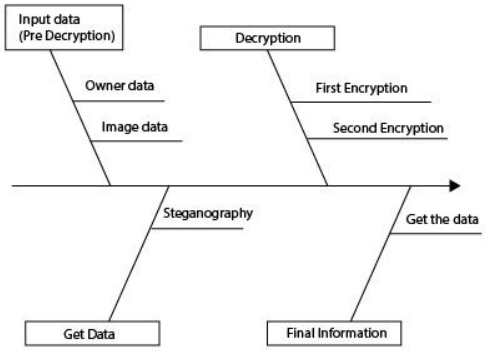
```
Data = Data (in Binner)
Length_of_data ← data

For x from 0 to Length_of_data:
  New_bit_of red ← bit_red <<
  Length_of_data[x]
  New_bit_of green ← bit_green <<
  Length_of_data[x]
  New_bit_of blue ← bit_blue <<
  Length_of_data[x]
Endfor

New_image = image_from(New_bit_of red,
New_bit_of green, New_bit_of blue)
```

d) Final Image

Gambar yang sudah dienkripsi dapat diunduh dan diunggah di internet dengan hak cipta milik pengguna.

2.3 Metode Dekripsi

Metode dekripsi adalah metode untuk mendekrip data yang ada di dalam sebuah gambar. Metode ini memiliki serangkaian proses seperti yang digambarkan pada Gambar 6.



Gambar 6. Flowchart Metode Dekripsi

Metode ini juga terbagi menjadi empat proses, empat proses tersebut yaitu:

a) Input Data (Pre Decryption)

Dalam metode dekripsi, hal pertama adalah memasukkan data berupa gambar yang akan didekripsi dan nama pemilik gambar tersebut, yang kemudian akan dicek apakah benar orang tersebut yang mempunyai gambar.

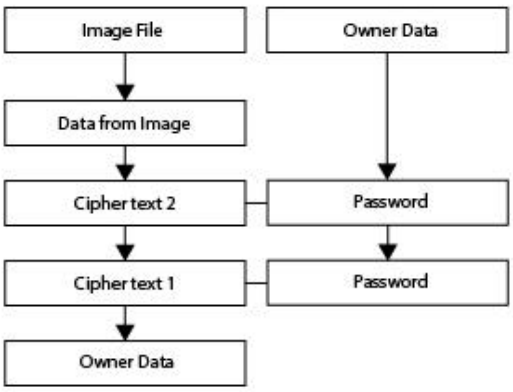
b) Get Data (Ekstrak Data)

Data diambil dari gambar dengan metode steganography lagi, dimana data diambil dari tiap piksel warna gambar yang ada sesuai dengan panjang hasil enkripsi dari nama pemilik yang dimasukkan. Algoritma pengambilan data dari gambar tersebut adalah sebagai berikut:

```
Data = Data (in Binner)
Length_of_data ← data

For x from 0 to Length_of_data:
bit_of    red    ←    bit_red    >>
Length_of_data[x]
bit_of   green   ←   bit_green   >>
Length_of_data[x]
bit_of    blue    ←    bit_blue    >>
Length_of_data[x]
ownerData                          =
bit_of_red+bit_of_green+bit_of_blue;
Endfor

ownerData = toString(ownerData)
```

c) Decryption (Dekripsi Data)

Proses dekripsi dilakukan sesuai dengan yang telah disesuaikan pada metode enkripsi. Metode dekripsi akan mendekrip hasil data dari proses pengambilan data dengan steganography. Jika password sesuai dengan tahap dekripsi pertama, akan dilakuakn tahap dekripsi kedua. Jika tahap dekripsi kedua passwordnya juga sesuai, maka akan ditampikan pemilik gambar tersebut. Namun, jika password tidak sesuai, gambar tidak bisa didekrip dan nama yang dimasukkan bukan pemilik dari gambar tersebut. Keseluruhan proses dekrip dapat dilihat pada Gambar 7.



Gambar 7. Proses Dekripsi Data

d) Final Information

Setelah dilakukan dekripsi, maka akan terlihat apakah benar gambar tersebut milik pemilik asli atau bukan. Jika bukan gambar tidak dapat didekripsi.

3. HASIL

Hasilnya, gambar yang sudah dienkripsi mengalami peningkatan warna menjadi sedikit lebih gelap. Hal ini terjadi karena gambar diberikan piksel baru sehingga warnanya berubah menjadi lebih gelap. Akan tetapi, dengan hal tersebut, gambar tidak akan dapat dienkrip berkali-kali karena akan merusak kualitas gambar. Gambar yang enkrip berkali-kali akan mengalami peningkatan warna lebih banyak sehingga warna akan berbeda dari awalnya.

Gambar yang sudah memiliki data di dalamnya tidak dapat dienkrip lagi, serta gambar yang akan didekrip dan tidak sesuai dengan pemilik aslinya, gambar tidak dapat didekrip dan data pengguna tidak dapat dilihat.

Kelemahan yang ada dalam penelitian ini adalah ukuran gambar harus relatif besar, minimal 500 piksel persegi dan gambar harus berwarna, jika hitam putih gambar tidak dapat diproses karena dalam penilitan ini, hasil enkripsi dimasukkan ke dalam tiap piksel warna gambar yakni merah, hijau, dan biru.

4. KESIMPULAN

Gambar yang dienkripsi jauh lebih aman karena menggunakan double encryption method, serta penggunaan pixel steganography akan membuat gambar susah untuk diekstrasi jika tidak sesuai panjang data dan nama pemilik berbeda. Gambar akan buram jika terus dipaksa untuk dienkrip..

.

DAFTAR PUSTAKA

[1] Alamsyah., Bejo, A., Adji, T.B,. "The replacement of irreducible polynomial and affine mapping for the construction of a strong S-box". Nonlinear Dynamics Journal, vol. 93, pp. 2105–2118. 2018.

[2] Gueron, S., Feghali, W.K., Gopal, V., Makaram, R., Dixon, M.G., Chennupaty, S. and Kounavis, M.E., Intel Corp. "Flexible architecture and instruction for advanced encryption standard (AES)". U.S. Patent Application 10/158,478. 2018.

[3] Rahim, R., Napitulu, D., Nurdiyanto. H., Sari, U.F., Rizky, F., Nofriansyah, D.,...Ihwani, M. "Pixel image steganography using EOF method and modular multiplication block cipher algorithm". Dalam IOP Conference Series: Materials Science and Engineering. IOP Publishing. 2018.

[4] Rashmi, N. and Jyothi, K. "An improved method for reversible data hiding steganography combined with cryptography". Dalam 2018 2nd International Conference on Inventive Systems and Control (ICISC) (pp. 81-84). IEEE, 2018.

[5] Vargo, C.J., Guo, L., Amazeen, M.A. "The agenda-setting power of fake news: A big data analysis of the online media landscape from 2014 to 2016". New Media & Society, vol. 20, pp. 2028-2049, 2017.

BIODATA PENULIS

Khoerul Umam

Penulis merupakan mahasiswa program studi Teknik Informatika, Jurusan Ilmu Komputer, Universitas Negeri Semarang. Mempunyai hobi Programming dan Debugging program.