



Analisa Metode Mid Position Value Untuk Menyisipkan Pesan Pada File Video

Abdul Gafur Daulay

Fakultas Ilmu Komputer Dan Teknologi Informasi, Tenik Informatika, Universitas Budi Darma, Medan, Indonesia

Email: abdulgafurdaulay14071996@gmail.com

Abstrak—Masalah keamanan merupakan salah satu aspek yang sangat penting dalam dunia informasi, salah satunya yaitu keamanan pesan teks. Dalam pengiriman pesan sering terjadi pengambilan dan manipulasian pesan dari pihak yang tidak bertanggung jawab. Sehingga tingkat keamanan kualitas keaslian dan kerahasiaan pesan tersebut tidak terjamin. Untuk mengatasi masalah keamanan pesan agar terjaga dari pihak yang tidak bertanggung jawab perlu di buat teknik untuk mengamankan pesan. Salah satu teknik untuk mengamankan pesan yaitu dengan menyisipkannya kedalam sebuah media yaitu video. Dengan disisipkannya pesan kedalam sebuah video maka tingkat kecurigaan pihak yang ingin memanipulasi pesan tersebut berkurang. Salah satu metode untuk menyisipkan pesan adalah metode Mid Position Value. Metode Mid Position Value berfungsi untuk menyisipkan nilai byte di tengah Nilai byte object.

Kata Kunci: Penyisipan, Pesan, File, Video, Mid Position Value.

Abstract—The issue of security is one of the most important aspects in the world of information, one of which is the security of text messages. In sending messages often occurs taking and manipulating messages from parties who are not responsible. So that the security level of the authenticity and confidentiality of the message is not guaranteed. To overcome the message security problem so that it is protected from irresponsible parties, it is necessary to develop techniques to secure the message. One technique for securing messages is by inserting them into a medium, namely video. By inserting a message into a video, the level of suspicion of those who want to manipulate the message is reduced. One method for inserting messages is the Mid Position Value method. The Mid Position Value method functions to insert a byte value in the middle of the object's byte value.

Keywords: Message, Insertion, Video, File, Mid Position Value

1. PENDAHULUAN

Steganografi merupakan salah satu kajian di dalam ilmu komputer yang bertujuan untuk menyisipkan pesan kedalam suatu objek seperti citra, audio, video dan dokumen. Steganografi adalah teknik penyisipan pesan yang berupa penting dan rahasia agar selain yang tidak berpihak tidak dapat mengetahui isi pesan tersebut, jadi pesan lebih terjaga kerahasiannya. Steganografi cukup hebat untuk menyisipkan suatu pesan agar orang ketiga mengetahui apa isi didalam citra, audio, video dan dokumen tersebut[1]. Jadi pesan yang akan kirim tidak akan diketahui orang yang tidak bersangkutan sehingga keaslian pesan tersebut masih terjaga keasliannya. Oleh karena itu maka teknik steganografi ini sangat diperlukan untuk menjaga sebuah orisinalitas pesan tersebut. Masalah yang sering dihadapi adalah begitu banyaknya terjadi suatu pesan yang kerap tersadap dan terjebol oleh pihak-pihak yang tidak berkepentingan mengenai pesan tersebut. Karena mungkin sebagian pihak tidak ingin pesan yang kita kirimkan tidak bisa diketahui oleh orang lain apa isi dari pesan yang kita kirimkan tersebut, sama hal ini berisi rahasia.

Dalam menjaga keamanan pesan, tentunya sangat diperlukan suatu sistem yang menjaga agar pesan tersebut terjamin kerahasiaannya. file yang tidak memiliki keamanan akan mudah disalah gunakan oleh pihak yang tidak berhak. Dalam pengiriman pesan yang melalui jaringan, diperlukan suatu metode agar pesan tersebut tidak hilang atau utuh sampai tujuan. Dalam pengiriman pesan diperlukan suatu keamanan agar pesan yang dikirim tidak dapat dibuka, dibaca bahkan diambil oleh orang yang tidak memiliki hak[2]. Penyembuyian atau penyisipan pesan pada umumnya berupa pesan yang penting dan rahasia sehingga tidak bisa dilihat oleh orang yang tidak berhak. oleh karena itu pesan akan menghasilkan operasi descrambling. Salah satu metode penyisipan pesan pada sebuah media yang akan dibahas adalah Mid Position Value. Pada penelitian yang telah dilakukan oleh Srilekha Mukherjee, Subhajit Roy dan Goutam Sanyal tahun 2018 yaitu membahas mengenai penyisipan pesan menggunakan metode steganografi Mid Position Value. Dan penulis memelihan metode Mid Position Value dikarenakan metode ini cukup baik untuk melakukan penyisipan pesan pada berbagai file, seperti file Gambar, Audio dan file Video[3].

2. METODOLOGI PENELITIAN

2.1 Steganografi

Steganografi merupakan salah satu kajian di dalam ilmu komputer yang bertujuan untuk menyisipkan pesan kedalam suatu objek seperti citra, audio, video dan dokumen. Steganografi adalah teknik penyisipan pesan yang berupa penting dan rahasia agar selain yang tidak berpihak tidak dapat mengetahui isi pesan tersebut, jadi pesan lebih terjaga kerahasiannya. Steganografi cukup hebat untuk menyisipkan suatu pesan agar orang ketiga mengetahui apa isi didalam citra, audio, video dan dokumen tersebut[1].

2.2 Pesan





Pesan adalah setiap pemberitahuan, kata, komunikasi baik secara lisan maupun tulisan yang dikirimkan dari satu orang ke orang lain. Pesan menjadi inti dari setiap komunikasi yang terjalin. Proses pengiriman pesan memerlukan sebuah media perantara agar pesan yang dikirimkan oleh sumber dapat diterima dengan baik oleh penerima. Dalam proses pengiriman tersebut pesan harus dikemas dengan sebaik mungkin untuk mengatasi gangguan yang muncul dalam proses transmisi pesan, agar tidak mengakibatkan perbedaan makna yang diterima oleh penerima[4].

2.3 Mid Position Value

Mid Position value (MVP) merupakan beberapa persamaan untuk melakukan proses *generate key*, proses enkripsi dan proses dekripsi [5]. Algoritma ElGamal memerlukan sepasang kunci yang dibangkitkan dengan memilih bilangan prima p dan dua buah bilangan acak (*random*) g dan x , dengan syarat bahwa nilai g dan x lebih kecil dari p yang memenuhi persamaan. $y = g^x \text{ mod } p$ Dari persamaan tersebut nilai y , g dan p merupakan pasangan kunci public sedangkan x , p merupakan pasangan kunci pribadi. Besaran-besaran yang digunakan dalam algoritma *Mid Value Psition* adalah :

- Bilangan prima p bersifat tidak rahasia.
- Bilangan acak g ($g < p$) bersifat tidak rahasia
- Bilangan acak x ($x < p$) bersifat rahasia.
- Bilangan y bersifat tidak rahasia.
- m (*plaintext*) bersifat rahasia merupakan pesan asli yang digunakan untuk data
- sumber dalam proses enkripsi dan merupakan data hasil pada proses dekripsi.
- a dan b (*ciphertext*) bersifat tidak rahasia.

Algoritma proses enkripsi dilakukan dengan memilih bilangan acak k yang berada dalam himpunan $1 \leq k \leq p-2$.

Setiap blok *plaintext* m dienkripsi dengan persamaan :

$$a = g^k \text{ mod } p \tag{1}$$

$$b = y^k m \text{ mod } p \tag{2}$$

Adapun langkah-langkah enkripsi algoritma Mid Value Psition :

- Susun *plainteks* menjadi blok-blok m_1, m_2, \dots, m_n , dengan setiap blok adalah satu karakter pesan.
- Konversikan masing-masing karakter ke dalam kode ASCII, maka diperoleh *plainteks* sebanyak n bilangan, yaitu $m_1, m_2, \dots, m_n, 3$.
- Untuk i dari 1 sampai n kerjakan :
 - Pilih sembarang bilangan acak rahasia .
 - Hitung $a_i = g^k \text{ mod } p$, $1 \leq k \leq p-2$
 - Hitung $b_i = y^k m_i \text{ mod } p$, $1 \leq k \leq p-2$, jadi ukuran Cipherteks dua kali ukuran= 4 . Diperoleh cipherteks yaitu (a_i, b_i) , i *plainteksnya*.

Proses dekripsi menggunakan kunci pribadi x dan p untuk mendekripsi a dan b menjadi *plaintext* m dengan persamaan :

$$(a^x)^{-1} = a^{p-1-x} \text{ mod } p \tag{3}$$

$$m = b * a^x \text{ mod } p \tag{4}$$

Sehingga *plaintext* dapat ditemukan kembali dari pasangan *ciphertext* a dan b . Adapun langkah-langkah dekripsi Mid Value Psition :

- Cipherteks (a_i, b_i) , $i = 1, 2, \dots, n$, kunci= publik p dan kunci rahasia x .
- Untuk i dari 1 sampai n kerjakan :
 - Hitung $a_i^{-1} = a_i^{p-1-x} \text{ mod } p$
 - Hitung $m_i = b_i / a_i^x \text{ mod } p = b_i (a_i^x)^{-1} \text{ mod } p$
- Diperoleh *plainteks* $m_1, m_2, \dots, m_n, 4$.
- Konversikan masing-masing bilangan m_1, m_2, \dots, m_n ke dalam karakter sesuai dengan kode ASCII-nya, kemudian hasilnya digabungkan kembali.

3. HASIL DAN PEMBAHASAN

Analisa masalah dalam penyisipan pesan pada file video, penulis akan menguraikan bagaimana proses penyisipan pesan kedalam file video dengan menggunakan metode MPV. Adapun pesan yang akan disisipkan adalah pesan teks dan proses enkripsi dilakukan dengan chiperteks. Secara umumnya *plainteks* dienkripsi dengan file video, akan tetapi untuk kunci yang digunakan pada metode Mid Position Value adalah cipherteks hasil dari enkripsi dengan Mid Position Value. Hal ini dilakukan untuk memperumit bentuk karakter kunci yang dilakukan oleh penulis. Untuk didekripsi kebalikan dari enkripsi yaitu cipherteks didekripsi dengan menggunakan metode Mid Position Value. Analisa metode adalah suatu cabang khusus dalam ilmu komputer yang mempelajari karakteristik dan performa dari suatu metode dalam menyelesaikan masalah, terlepas dari implementasi metode tersebut. Dalam cabang disiplin metode dipelajari secara abstrak, terlepas dari sistem komputer atau bahasa pemrograman yang digunakan. Meode yang berbeda dapat diterapkan pada suatu masalah dengan kriteria yang sama.

Metode Mid Position Value digunakan untuk enkripsi dan deskripsi chiperteks pada file video. Enkripsi dan dekripsi dengan menggunakan metode Mid Position Value hanya menggunakan 26 karakter huruf. Dalam file Video

Mid-value = 3
 Key 1 = $p(i, j) \text{ mid value mod } 36$
 = $1^3 \text{ mod } 36$
 = $1 = 0000001$
 Key 2 = $\text{key } 1 \text{ mod } (4 \text{ bit.dec.pix (key)}) + 1$
 = $1 \text{ mod } (1) + 1$
 = $1 \text{ mod } 2$
 = 1
 Key 1 = 1 = odd
 Key 2 = 1 = odd
 P(i,1) = 0 = 01001001
 Bit Secret = 00 = complementary = 01
 P(i,1) = 0000001 = 1

Sebelum					
0					

Proses

Sesudah					
1					

Gambar 2. Hasil Iterasi 1

Lakukan sampai seluruh pesan di sisipkan sampai iterasi ke 24
 Iterasi 24.

$i = 4, j = 6, m = 118$

$p(i, j) = (i-1) * m + j$

$p(4,6) = (4-1) * 118 + 6$

$p(4,6) = (3) * 118 + 6$

$p(4,6) = 354$

Total digit = 4

Mid-position = $(\text{Total digit}/2) + 1$
 = $(4/2) + 1 = 3$

Mid-value = 3

Key 1 = $p(i, j) \text{ mid-value mod } 36$
 = $354^3 \text{ mod } 36$
 = $44361864 \text{ mod } 36$
 = $0 = 00000000$

Key 2 = $\text{key } 1 \text{ mod } (4 \text{ bit.dec.pix (key)}) + 1$
 = $0 \text{ mod } (0) + 1$
 = $0 \text{ mod } 0$

Key 1 = 0 = odd
 Key 2 = 0 = odd
 } Reverse tow bit complementary embedding/extraction

P(i,3) = 118 = 01110110

Bit Secret = 10 = complementary = 01

P(i,3) = 01110101 = 117

Sebelum					
0	0	0	32	102	116
105	155	1	109	105	115
0	0	0	8	102	114
131	121	131	85	88	188

Proses

Sesudah					
1	0	1	32	101	166
104	155	1	109	105	113
1	0	3	11	101	112
130	121	131	85	90	177

Gambar 2. Hasil Iterasi 24

Berdasarkan Proses penyisipan pertama kali dilakukan dengan mengubah nilai pesan menjadi biner sesuai ketentuan ASCII dan melakukan iterasi untuk mendapatkan bit secret yang akan ditempatkan pada posisi per sel 6 x 6 matrik video



dan dilakukan hingga selesai. Sehingga perhitungan dan proses penyisipan pesan yang dilakukan oleh penulis dengan menggunakan metode Mid Position Value cukup baik untuk digunakan dalam teknik penyisipan pesan.

4. KESIMPULAN

Dengan diselesaikannya penelitian skripsi ini yang mencakup penggunaan metode Mid Position Value dalam melakukan penyisipan pesan dapat diperoleh beberapa kesimpulan dimana poroses penyisipan pertama kali dilakukan dengan mengubah nilai pesan menjadi biner sesuai ketentuan ASCII dan melakukan iterasi untuk mendapatkan bit secret yang akan ditempatkan pada posisi per sel 6 x 6 matrik video dan dilakukan hingga selesai. Dengan perhitungan dan proses penyisipan pesan yang dilakukan oleh penulis dengan menggunakan metode Mid Position Value cukup baik untuk digunakan dalam teknik penyisipan pesan.

REFERENCES

- [1] Sembiring Sandro, Perancangan Aplikasi Steganografi Untuk Menyisipkan Pesan Teks. Medan: Pelita Informatika, 2013.
- [2] Nunung Nurmaesah, Tutik Lestari, and Arni Retno Mariana, "Aplikasi Steganografi Untuk Menyisipkan Pesan," Vol. Viii, Pp. 13-17, July 2017.
- [3] wikipedia. (2010, juni) <https://id.wikipedia.org>.
- [4] Ginanjar Wiro Sasmito2, Oman Somantri3 Siti Rohayah1, "APLIKASI STEGANOGRAFI UNTUK PENYISIPAN PESAN," Vol. 9, Pp. 975-980, January 2015.
- [5] pengertian ahli. (2013, November) <https://pengertianahli.id>.
- [6] Subhajit Roya , Goutam Sanyala Srilekha Mukherjeea, "Image Steganography Using Mid Position Value Technique," Image Steganography Using Mid Position Value Technique, pp. 461-468, 2018.
- [7] R.A.S M Shalahuddin, "Rekaya Perangkat Lunak," Rekaya Perangkat Lunak, 2014.