PENGEMBANGAN METODE PENGAMANAN BERKAS MEMAFAATKAN PEWARNAAN GRAF

Yogi Kurniawan[1)] dan Tohari Ahmad[2)]
[1, 2)] Teknik Informatika, Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Sukolilo, Surabaya 60111, Indonesia
Telp: +6231 – 5939214 / Fax: +6231 – 5913804
e-mail: yogi.kur@ub.ac.id[1)], tohari@if.its.ac.id[2)]

ABSTRAK

Penyembunyian data pada citra digital adalah teknologi penyembunyian pesan yang populer, dimana pesan rahasia disembunyikan pada citra digital yang disebut citra cover. Kehadiran pesan rahasia tersebut tidak dapat dilihat. Dengan demikian, penyerang ilegal tidak dapat mendeteksi pesan rahasia, namun penerima yang sah dapat memperoleh pesan rahasia dengan menggunakan algoritma ekstraksi. Salah satu metode yang kerap kali digunakan untuk steganography adalah Difference Expansion (DE). Kelebihan dari metode DE adalah metode ini mampu menyediakan penyisipan yang besar dengan kompleksitas yang rendah. Metode DE membutuhkan sebuah location map untuk menandai pixel yang dapat dilakukan penyisipan. Untuk memperbesar kapasitas penyimpanan pada sebuah media maka location map dapat disimpan pada berkas yang berbeda. Akan tetapi hal tersebut membuat sebuah celah keamanan yang dapat dimanfaatkan oleh penyerang. Pada penelitian ini metode untuk mengamankan location map dalam penyembunyian data dilakukan dengan transformasi. Yaitu dilakukan dengan memanfaatkan proses pewarnaan pada graf sehingga transformasi dilakukan dengan menyusuri setiap sisi dari graf. Transformasi yang diusulkan mampu mengubah berkas flocation sebesar 94KB selama 2,83 detik mengungguli protocol yang diusulkan oleh metode sebelumnya.

***Kata Kunci**: Data Hiding, graf, location map.*

ABSTRACT

Data hiding in digital imagery is a popular message concealment technology, in which secret messages hidden in digital images called cover image. The presence of the secret message can not be seen. Thus, illegal attacker can not detect the secret message, but the recipient who can legitimately obtain secret message using extraction algorithm. One method that is often used for steganography is the Difference Expansion (DE). The advantages of this method is the method of DE is able to provide a large insertion with low complexity. DE method requires a location map to mark pixel do insertion. To increase storage capacity, the location map may be stored in a separate file. But it does create a security hole that could be exploited by attackers. This research will secure a location map in the transformation of data hiding. The transformation is done by utilizing the coloring process on the graph so that the transformation is done with down each side of the graph. The proposed transformation flocation capable of changing file of 94KB for 2.83 seconds better than the protocol proposed by the previous method.

***Keywords**: Data Hiding, Graph, Location Map*

I. PENDAHULUAN

PENYEMBUNYIAN data adalah salah satu cara untuk mengamankan data untuk ditransmisikan ataupun sebagai media authentikasi terhadap kebenaran suatu media. Berbeda dengan *cryptography* [1] penyembunyian data dilakukan dengan menyisipkan pesan pada sebuah media seperti pada sebuah citra. Banyak metode digunakan untuk menyembunyikan data, baik pada citra berwarna maupun citra *grayscale*. Kebanyakan teknik tersebut berdasarkan pada penggantian *least significant bit* (LSB) dan perbedaan nilai dari piksel pada domain spasial. Penggantian LSB adalah metode *steganography* populer di mana bit pesan rahasia yang tertanam ke dalam LSB dari citra sampul. Penggantian LSB dengan cara meningkatkan (atau menurunkan) nilai piksel atau membuat nilai piksel tersebut tidak dimodifikasi, setelah itu bit terendah dari citra stego mewakili pesan rahasia [2], [3], [4].

Metode yang populer berikutnya adalah dengan menyisipkan pesan rahasia pada perbedaan nilai piksel dengan meningkatkan atau menurunkan nilai perbedaan piksel dan membentuk nilai piksel yang baru.Salah satu metode penyembunyian data pada perbedaan nilai piksel adalah *Difference Expansion* (DE). DE menggunakan perbedaan yang dikembangkan dari pasangan piksel untuk menyisipkan data. Perbedaan dari piksel-piksel yang bertetangga tersebut dihitung dan dilipatgandakan. Pesan rahasia akan disisipkan pada LSB dari perbedaan yang dikembangkan. Hasil dari penyisipan kemudian digunakan untuk menghiting nilai baru dari piksel yang bertetangga [5].

Pada penelitian [6] diusulkan penyembunyian data dengan menurunkan perubahan selisih dari metode DE menggunakan fungsi modulus. Pesan rahasia tidak langsung dibebankan pada selisih antara sepasang piksel yang bersebelahan. Akan tetapi dibandingkan dengan hasil dari modulus dari selisih antara sepasang piksel yang bersebelahan. Pada penelitian [6] *location map* yang digunakan untuk menandai tiap pasang piksel pada sebuah blok

piksel, sehingga jika salah satu pasang piksel tidak dapat dilakukan penyisipan maka pasangan yang lain masih bisa dilakukan penyisipan. Hal ini berbeda dengan penelitian sebelumnya dimana ketika satu pasang piksel dalam satu blok tidak dapat dilakukan penyisipan maka kesuluruhan blok tidak dilakukan penyisipan seperti pada penelitian [5], [7], dan [8]. Akan tetapi location map yang dibutuhkan menjadi sangat besar sehingga pada penelitian [6] dilakukan pemecahan location map menjadi 2 bagian bagian pertama disisipkan kepada titik referensi dalam blok dan location map bagian kedua dituliskan pada sebuah berkas.

Penggunaan berkas untuk menyimpan location map tersebut menimbulkan permasalahan baru pada sisi keamanan dalam penyisipan data pada media. Pihak yang tidak bertanggung jawab dapat dengan mudah menebak baik isi dari pesan maupun lokasi dari penyisipan pesan rahasia tersebut. Penelitian yang dilakukan [9] melakukan pengamanan terhadap berkas transformasi sidik jari. Pada penelitian tersebut memanfaatkan graf yang telah diwarnai sisinya [10]. Sisi dari graf tersebut diwarnai dengan sebuah *initialization vector* (IV) yang berupa karakter dalam berkas yang akan diamankan. Kemudian dilakukan penyusuran terhadap graf yang sudah diwarnai tersebut sesuai dengan karakter pada berkas sidik jari. Pada penelitian selalu dilakukan dua kali transformasi dan dua kali detransformasi, yaitu transformasi IVclient yang akan dikirimkan ke penerima dan kemudian dilanjutkan transformasi berkas dengan IVclient sehingga waktu yang dibutuhkan untuk mentransformasi berkas dengan ukuran besar akan membutuhkan waktu yang lama ketika dilakukan transformasi maupun detransformasi pada berkas location map yang diusulkan pada penelitian [6].

Pada penelitian ini akan mempercepat proses transformasi dan detransformasi pada penelitian [9] dengan melakukan sekali transformasi hanya pada berkas yang akan ditransformasi. Sedangkan untuk menjamin keamanan dari hasil transformasi yang dilakukan akan dilakukan dua kali pengacakan terhadap IV pada sisi pengirim maupun pada sisi penerima sehingga IV yang dimiliki oleh kedua belah pihak tersebut sama dan berhasil melakukan transformasi dan detransformasi dengan waktu proses yang lebih cepat.

II. PENELITIAN TERKAIT

A. Difference Expansion dengan Fungsi Modulo

Dalam metode yang diajukan [6], penggunaan DE yang diintegrasikan dengan penggunaan fungsi modulus dapat mengurangi lonjakan selisih yang cukup besar tersebut. Hal ini dikarenakan tidak langsung membebankan data rahasia yang harus disimpan pada selisih antara sepasang piksel yang bersebelahan.

1. Pada informasi rahasia yang akan disimpan pada piksel citra *cover*, informasi rahasia dirubah menjadi bilangan basis tiga ($m_{(3)}$).
2. Mengacak posisi titik referensi (U_m) pada blok piksel dan menuliskan posisi U_m pada berkas *location map*.
3. Mencari nilai perbedaan piksel ($V_1, V_2, ..., V_n$) dari nilai piksel dalam sebuah blok ($U_1, U_2, ..., U_n$) dengan titik referensi (U_m) seperti pada Persamaan 1, 2, dan 3.

$$V_1 = U_1 - U_m \quad (1)$$
$$V_2 = U_2 - U_m \quad (2)$$
$$V_n = U_n - U_m \quad (3)$$

4. Nilai informasi rahasia yang sudah berupa bilangan 3 dibandingkan dengan selisih kedua piksel (Vn) yang telah dimodulus 3 dengan data rahasia dalam bentuk bilangan basis 3 ($m_{(3)}$). Kemudian dilakukan ekspansi nilai selisih sesuai dengan Persamaan 4 sehingga didapatkan nilai perbedaan yang baru ($\widetilde{Vn}$)

$$\widetilde{Vn}\begin{cases} Vn\,, jika\ Vn\ mod 3 = m_{(3)} \\ Vn + 1, jika\ Vn\ mod 3 = m_{(3)} + 1 \\ Vn - 1, jika\ Vn\ mod 3 = m_{(3)} + 2\ \ dan\ d > 0 \\ Vn + 2, jika\ Vn\ mod 3 = m_{(3)} + 2\ \ dan\ d = 0 \end{cases} \quad (4)$$

5. Langkah terakhir dalam penyisipan data adalah proses penyusunan kembali nilai *pixel* cover media ($\widetilde{Un}$), dengan menambahkan nilai titik referensi (Um) dengan nilai perbedaan yang baru ($\widetilde{Vn}$), seperti pada Persamaan 5.

$$\widetilde{Un} = Um + \widetilde{Vn} \quad (5)$$

TABEL I

BENTUK LOCATION MAP

REGION	Bagian 1	Bagian 2
Region positif	1	0
Region negatif	0	1
Region tak dirubah	0	0
Region d=0	1	1

Posisi *Um*, *lm1*, penambahan *lm2* (n), operasi;

Gambar 1. Bentuk penulisan berkas *location map* pada berkas

6. Untuk menanggulangi *overflow* dan *underflow* terhadap nilai *pixel* baru yang dibentuk maka perlu dilakukan pembatas nilai *pixel* yang dilakukan penyisipan, sehingga *pixel* yang digunakan sesuai dengan Persamaan 6. Nilai piksel yang tidak digunakan adalah piksel dengan nilai 0, 1, 254, dan 255. Hal ini dikarenakan perubahan masksimal yang dilakukan adalah ±2 sehingga piksel tersebut dapat mengakibatkan *overflow* dan *underflow.*

$$1<Un<254 \quad (6)$$

Location map dibutuhkan untuk menyimpan informasi bentuk penyisipan yang dilakukan sebagai informasi untuk melakukan pengembalian pada citra *cover medi*a. Pada metode yang diusulkan *location map* akan memiliki bentuk yaitu, region positif, region negatif dan region tak dirubah, seperti pada Tabel I.

Pada *location map* bagian 1 akan dimasukkan dalam sebuah file, sebelumnya nilai dari *location map* dirubah terlebih dahulu ke bilangan desimal. Kemudian pada *location map* bagian kedua dilakukan penyisipan kembali ke cover media yang telah dilakukan penyisipan.

Bentuk *location map* yang disimpan pada berkas memiliki bentuk seperti pada Gambar 1. Semisal 1,7,2,1;2,6,1,0#1,2,1,1, *lm1* berisi angka bulat dari 0 sampai 7, penambahan *lm2* berisi angka bulat yang digunakan sebagai penambah atau pengurang pada titik referensi, sedangkan operasi merupakan operasi penambahan atau pengurangan dari penambahan *lm2*. Tiap blok akan dipisahkan dengan tanda koma dan tiap warna akan dipisahkan oleh tanda pagar.

B. Pertukaran Kunci Diffie-Helman

Diffie-Hellman membentuk kunci rahasia bersama antara dua pihak yang dapat digunakan untuk komunikasi data rahasia melalui jaringan publik. Protokol ini memiliki dua parameter sistem *p* dan *g*. Keduanya bersifat publik dan dapat digunakan oleh semua pengguna dalam suatu sistem. Parameter *p* adalah bilangan prima dan parameter *g* (biasanya disebut generator) adalah bilangan bulat kurang dari *p* dan merupakan primitive root modul dari *p*. [11]

- Misalkan pengguna A dan pengguna B akan saling mengirimkan pesan, maka mereka akan menentukan p=23 dan g=5
- Pengguna A memilih sebuah bilangan acak a=6 yang akan dikirim ke B dalam bentuk $A=g^a \bmod p = 5^6 \bmod 23 = 8$.
- Pengguna B memilih sebuah bilangan acak b=15 yang akan dikirim ke A dalam bentuk $B=g^b \bmod p = 5^{15} \bmod 23 = 19$.
- Pengguna A menerima B dari pengguna B untuk menghitung kunci rahasia bersama $s=B^a \bmod p = 19^6 \bmod 23 = 2$.
- Pengguna B menerima A dari pengguna A untuk menghitung kunci rahasia bersama $s=A^b \bmod p = 8^{15} \bmod 23 = 2$.
- Pengguna A dan pengguna B memilki sebuah kunci bersama s=2.

C. Pengiriman Data Transformasi Sidik Jari Menggunakan Pewarnaan Graf

Metode yang diusulkan [9] melakukan pengamanan berkas transformasi Sidik Jari dengan melakukan transformasi terhadap berkas yang dihasilkan. Metode [9] diawali dengan pertukaran kunci dengan pertukaran kunci Diffie-Helman [11], kemudian langkah langkah pengamanan berkas sebagai berikut

1. Pengacakan *initialization vector* (IV) dengan kunci yang dihasilkan pada proses pertukaran kunci dan dihasilkan IV'.
2. IV' digunakan untuk mewarnai sisi graf.
3. Kemudian dilakukan pengacakan IV menjadi IVclient secara random
4. Transformasi dengan graf yang telah dibuat dengan menyusuri setiap node graf.
5. Mengirimkan hasil transformasi IVclient tersebut dikirimkan ke penerima.

6. Langkah selanjutnya adalah melakukan transformasi berkas dengan graf yang telah dilakukan pewarnaan dengan IVclient yang belum dilakukan transformasi.
7. Langkah terakhir adalah mengirimkan hasil transformasi ke sisi penerima.

III. PERLINDUNGAN BERKAS LOCATION MAP DENGAN PEWARNAAN GRAPH

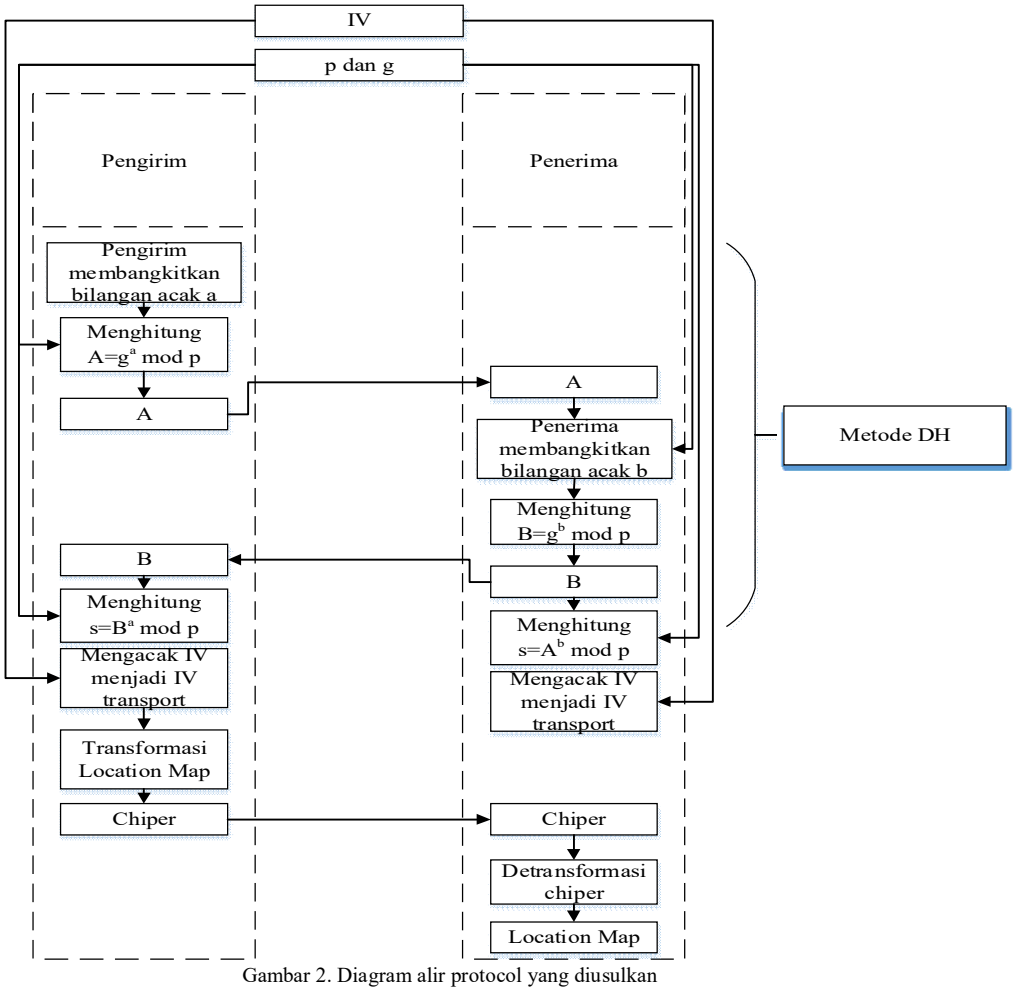
Pengamanan berkas *location map* dengan menggunakan metode pewarnaan *graph* yang diusulkan oleh Pambudi dan Ahmad, 2015 [9]. Akan tetapi tidak dilakukan pengiriman IVclient sehingga tidak ada lagi transformasi dan detransformasi untuk mengamankan IVclient sehingga proses yang dibutuhkan untuk melakukan transformasi dan detransformasi akan lebih cepat.

Pada metode yang diusulkan dilakukan inisialisasi vector (IV) dimana IV ini merupakan kumpulan huruf dan angka sehingga mempunyai panjang karakter 36. Langkah berikutnya adalah menggunakan metode DH dengan melakukan negosiasi bilangan prima yang digunakan (p) dan *primitive root modulo* dari bilangan prima tersebut (g). Kemudian pengirim dan penerima saling membangkitkan bilangan desimal yang digunakan untuk dikirim ke satu sama lain. Langkah-langkah dalam mengamankan pengiriman *location map* dapat dilihat pada Gambar 2.

A. Proses Transformasi

Seperti terlihat pada gambar 1. Pada proses transformasi dilakukan proses pertukaran kunci Diffie-Helman antara penerima dan pengirim. Kemudian transformasi dimulai dengan pengacakan 2 kali terhadap IV menjadi IV' dan IV transport. Langkah langkah pada proses transformasi adalah sebagai berikut:

- Pemilihan bilangan *primitive prime modulo* pada penerima dan pengirim.
- Pencarian bilangan kunci dengan metode Diffie-Helman.
- Pengacakan IV menjadi IV' dengan bilangan *B* dari metode Diffie-Helman.
- Pengacakan IV' menjadi IV transport dengan bilangan *s* dari metode Diffie-Helman.
- Pembentukan *graph* dengan node 0 sampai 9 dan karakter ',;#'.
- Pewarnaan *graph* dengan IV transport.
- Transformasi *Location Map* dengan menyusuri *graph*.



Gambar 2. Diagram alir protocol yang diusulkan

1) Initilization Vector (IV)

Initilization Vector (IV) merupakan himpunan karakter yang digunakan untuk mewarnai atau menandai sisi-sisi pada graf yang akan dibuat. IV yang digunakan pada penelitian ini adalah berupa kumpulan karakter huruf dan angka (a-z dan 0-9). Pada penelitian ini diguanakan 3 buah IV sebagai berikut :

- IV adalah IV awal sebelum dilakukan pengacakan dan telah diset sebelumnya pada sisi penerima dan pengirim. IV ini digunakan untuk menghasilkan IV'.
- IV' dibentuk dengan mengacak IV dengan bilangan B atau bilangan yang dikirim oleh penerima ke pengirim ketika proses pertukaran kunci DH.
- IV transport merupakan IV' yang telah diacak dengan bilangan kunci s.

Pengacakan 2 kali ini digunakan untuk memangkas waktu yang digunakan dalam transformasi location dari media penyembunyian data yang dibentuk. Dengan demikian penerima tidak perlu lagi melakukan detransformasi terhadap kunci yang digunakan untuk mengirim *location map*. Penerima hanya perlu melakukan pengacakan IV menjadi IV' dan IV transport sesuai dengan yang dilakukan oleh pengirim.Metode pengacakan yang diusulkan dapat dilihat pada Gambar 3. Misalkan IV{1,2,3,4} dan s=2, pada iterasi ke 1, IV' = {2}, pada iterasi 2, IV' = {2, 3}, pada iterasi 3, IV' = {2,3,4} , dan iterasi 4, IV' = {2,3,4,1}.

2) Pembuatan dan Pewarnaan graf

Setelah didapat IV transport kemudian dibuat sebuh graph yang berisi angka 0 sampai dengan 9 dan tanda baca koma, titik koma, dan tanda pagar. Seluruh simpul saling terhubung dan memiliki arah, simpul angka mempunyai loop agar memungkinkan perulangan pada angka seperti 11, 22, 33, .. , dst. Pada simpul koma, titik koma, dan pagar tidak keterhubungan setiap tanda baca lainya hanya memiliki hubungan dengan simpul angka. Contoh graf dengan dua simpul angka seperti pada Gambar 4.

Pewarnaan sisi graf dilakukan dengan memberikan jarak sesuai dengan bilangkan kunci s. Hal ini dilakukan sesuai dengan metode pewarnaan sisi pada graf dimana sisi yang bertetangga tidak boleh diberikan warna yang sama. Pewarnaan dilakukan sampai seluruh sisi telah diberi warna. Jika IV transport belum digunakan semua dan muncul warna yang berulang maka IV berikutnya yang belum digunakan yang digunakan. Ketika IV sudah digunakan semua dan masih terdapat sisi yang belum diwarnai maka set seluruh IV transport menjadi tidak digunakan dan kemudian diulangi pengambilan IV transport sampai seluruh sisi terwarnai.

Transformasi pada *location map* dimulai dengan hasil bilangan kunci di modulo oleh jumlah simpul angka dan digunakan sebagai simpul awal. Kemudian ambil 1 karakter dari *location map* sebagai simpul tujuan dan mulai bergerak ke simpul sesuai dengan karakter pada *location map*, catat warna sisi graf sebagai hasil transformasi. Ganti simpul awal dengan hasil simpul tujuan pada proses sebelumnya, kemudian ulangi proses ini sampai seluruh *location map* tertransformasi.

Contoh transformasi pada pengirim IV transport{1,x,r,2,4}, data yang ditransformasi {2,1,1} dan bilangan kunci s=2 . Graf telah dibuat sesuai dengan Gambar 4.

- Kunci bilangan s=2, simpul awal= 2 mod (10), simpul awal 2, Transformasi dimulai dengan Gambar 5a
- Bergerak ke simpul sesuai data yang ditransformasi, data pertama adalah 2 sesuai dengan Gambar 5b, sehingga hasil transformasi sementara adalah 1
- Kemudian 2 dijadikan simpul awal dan bergerak ke data berikutnya yaitu koma seperti pada Gambar 5c sehingga hasil transformasi sementara=14
- Kemudian dari koma menuju 1 sesuai dengan Gambar 5d sehingga data transformasi sementara menjadi 14x
- Simpul 1 dijadikan simpul awal dan menuju simpul tujuan koma seperti pada Gambar 5e dan membuat hasil transformasi sementara 14xx
- Data terakhir dari simpul awal koma bergerak ke simpul tujuan 1 seperti pada Gambar 5f dan membuat hasil transformasi 14xxx

```
        IV=26 huruf+10 angka
I=s mod length(IV)
count=1
a=0
while count <=length(IV)
        if IV[i] telah ada pada IV'
                i=(i+1) mod length(IV)
        IV'[count]=IV[i]
        i=(i+a+s) mod length(IV)
        a++
        count++
```

Gambar 3. Pseudocode pengacakan IV

B. Proses Detransformasi

Proses detransformasi diawali seperti pada proses transformasi yaitu pengacakan IV menjadi IV' oleh bilangan B dan pengacakan IV' menjadi IV transport dengan bilangan *s* pada metode Diffie-Helman. Kemudian dilakukan pewarnaan graf seperti pada proses transformasi. Kemudian tidak seperti pada proses transformasi dimana mencari simpul sesuai karakter pada *location map* pada proses detransformasi dilakukan pencarian pada nilai sisi yang sesuai dengan data yang akan didetransformasi. Langkah langkah detransformasi sebagai berikut:

1. Pemilihan bilangan *primitive prime modulo* pada penerima dan pengirim
2. Pencarian bilangan kunci dengan metode Diffie-Helman.
3. Pengacakan IV menjadi IV' dengan bilangan B dari metode Diffie-Helman.
4. Pengacakan IV' menjadi IV transport dengan bilangan s dari metode Diffie-Helman.
5. Pemebentukan graf dengan node 0 sampai 9 dan karakter ',;#'.
6. Pewarnaan graf dengan IV transport.
7. Detransformasi *location map* dari pengirim dengan menyusuri graf.

Langkah pertama yang dilakukan adalah seperti pada proses transformasi yaitu menentukan simpul awal melalui hasil modulo bilangan kunci oleh jumlah simpul angka. Kemudian bergerak dari simpul angka sesuai dengan data yang didetransformasi dan warna pada sisi graf. Kemudian simpul tujuan dari proses sebelumnya dijadikan simpul awal, dan proses sebelumnya diulangi sampai seluruh data didetransformasi. Contoh proses detransformasi sesuai dengan data transformasi sebelumnya s=2, data yang didetransformasi {14xxx}.

- Langkah pertama menentukan simpul awal dengan 2 *mod* 10, sehingga simpul awal 2
- Berikutnya dicocokkan data pertama dengan sisi graf, karena data 1 maka bergerak ke simpul 2 dan data hasil detransformasi sementara adalah 2
- Berikutnya data yang dicocokkan adalah 4 sehingga bergerak kepada simpul koma dan data hasil detransformasi sementara adalah 2
- Kemudian data yang dicocokkan adalah x sehingga bergerak ke simpul 1 dan data hasil detransformasi menjadi 2,1
- Dari simpul 1 data bergerak sesuai warna sisi dan data transformasi yaitu x sehingga bergerak ke simpul, dan merubah data hasil detransformasi sementara menjadi 2,1
- Terakhir data memiliki nilai x sesuai dengan warna pada simpul koma, simpul tujuannya adalah simpul 1 dan data hasil detransformasi akhirnya adalah 2,1,1

IV. HASIL DAN PEMBAHASAN

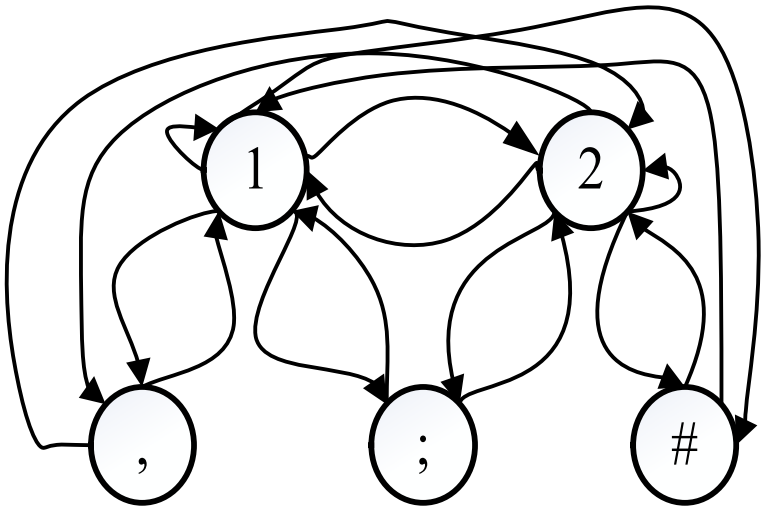
Evaluasi terhadap metode yang diusulkan dengan cara melakukan transformasi dan detransformasi pada hasil transformasi tersebut. *Location map* yang digunakan berukuran 94 KB sampai dengan 931 KB hasil dari penyisipan pada metode DE dengan fungsi modulo. Lingkungan pengujian dilakukan pada Matlab versi 2009a dengan spesifikasi komputer Prosesor AMD A8 4500 dan RAM 4 GB. Kemudian dilakukan perhitungan waktu proses dari metode yang diusulkan dan metode yang diusulkan oleh [9]. Uji coba dilakukan dengan melakukan 100 kali transformasi dan detransformasi untuk tiap ukuran *location map* dan diambil rata-ratanya. Tabel II merupakan hasil rata-rata pengukuran waktu proses.

Dari hasil uji coba pada Tabel II dapat dilihat bahwa metode yang diusulkan mampu melakukan proses transformasi dan detransformasi lebih cepat dibandingkan dengan metode yang diusulkan oleh Pambudi dan Ahmad [9]. Pada Tabel II juga dapat dilihat bahwa proses detransformasi pada metode yang diusulkan Pambudi dan Ahmad [9] membutuhkan waktu 2 kali lipat dari waktu detransformasi pada metode yang diusulkan. Hal ini dikarenakan terdapat dua proses detransformasi yang dilakukan oleh metode Pambudi dan Ahmad [9] sedangkan pada metode yang diusulkan hanya melakukan satu kali detransformasi pada *location map*. Peluang pemecahan dari metode yang diusulkan tidak berubah dari metode yang diusulkan Pambudi dan Ahmad [9] dikarenakan penggunaan panjang karakter dan karakter yang sama pada IV. IV sama-sama memiliki karakter huruf dan angka (a-z dan 0-9) dengan panjang 36 karakter sehingga peluang maksimal IV terpecahkan adalah IV! atau $36!= 3.7199x10^{41}$.

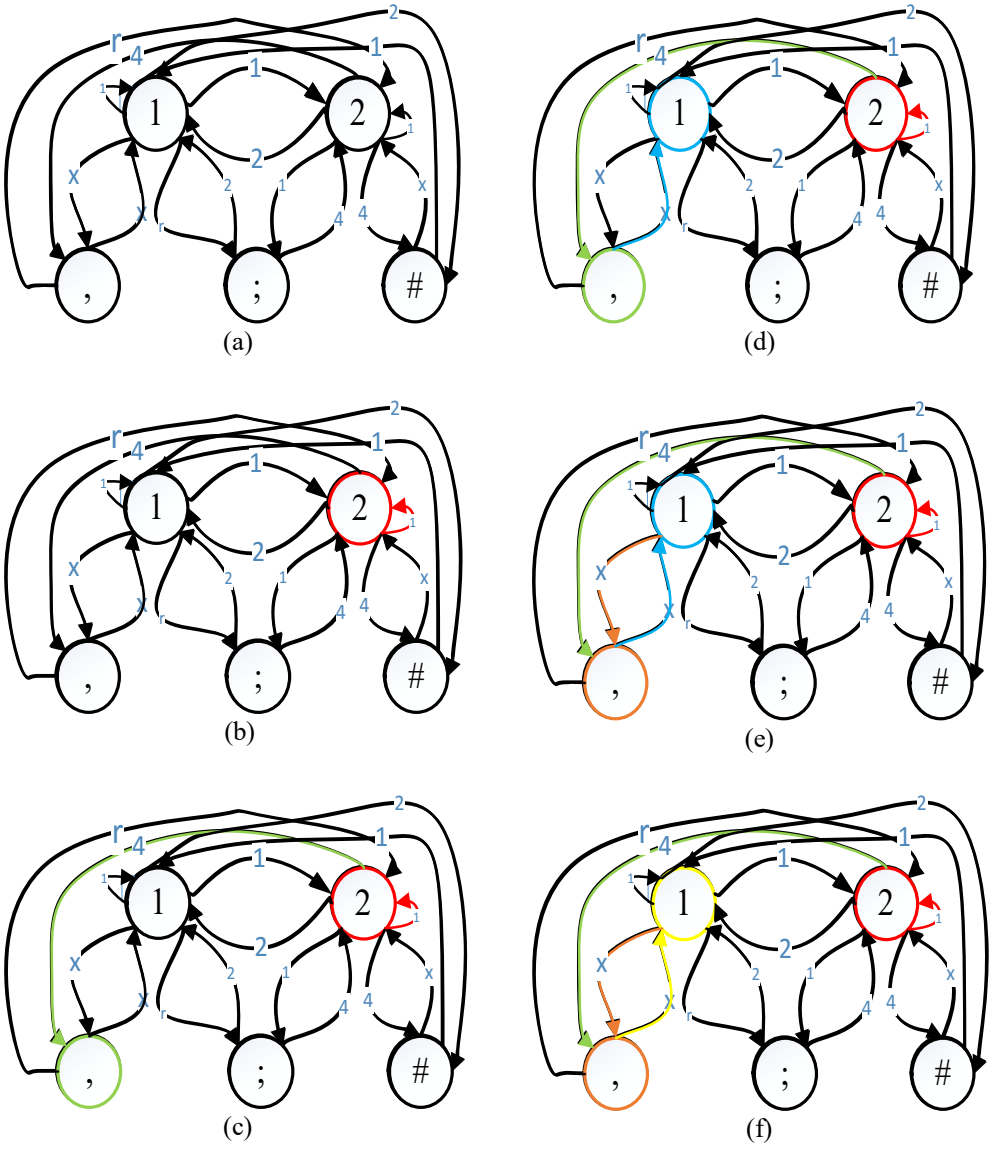
V. KESIMPULAN

Penyembunyian data dengan metode DE yang memiliki *location map* untuk menandai posisi penyisipan sebuah pesan. Penggunaan *location map* pada berkas yang berbeda dari media penyisipan dapat meningkatkan kapasitas penyimpanan dari metode penyembunyian DE akan tetapi memiliki permasalahan keamanan yang baru. Dengan metode transformasi yang digunakan dapat mentransformasi *location map* yang dihasilkan dari metode penyembunyian data DE dan memiliki waktu kerja lebih cepat dibandingkan dengan metode sebelumnya. Waktu proses pada sebuah berkas *location map* sebesar 94 KB selama 2,833 detik sedangkan pada berkas *location map*

terbesar 931 KB selama 33,2576 detik atau 3 kali lebih cepat dibandingkan metode yang diusulkan sebelumnya.



Gambar 4. Contoh graf dengan dua node angka dan 3 node tanda baca



Gambar 5. Contoh transformasi dengan menyusuri node pada graf

TABEL II
HASIL PENGUKURAN WAKTU PROSES

Ukuran Location Map (KB)	Metode Usulan		Metode [9]	
	waktu transform (s)	waktu detransfom (s)	waktu transform (s)	waktu detransfom (s)
94	2.833985	10.12621	5.668204	17.844602
187	5.799871	20.14825	13.793512	39.322293
280	9.373663	33.86073	16.194483	66.469033
373	11.42241	37.72728	20.764454	74.643498
466	15.91612	45.80442	27.357705	94.499885
599	17.83595	52.63642	32.438215	103.04897
652	22.68009	69.00072	34.927308	130.13927
745	25.96645	77.74190	39.572191	142.61011
838	26.30373	88.66931	50.856001	173.03248
931	33.25726	106.9157	57.267333	187.42134

DAFTAR PUSTAKA

[1] T. Ahmad, J. Hu and S. Han, "An efficient mobile voting system security scheme based on elliptic curve cryptography," in *In Network and System Security, 2009. NSS'09. Third International Conference on*, Gold Coast, QLD, 2009.

[2] D.-C. Lou and C.-H. Hu, "LSB steganographic method based on reversible histogram transformation function for resisting statistical steganalysis," *Information Sciences,* vol. 188, p. 346–358, June 2012.

[3] W. Luo, F. Huang and J. Huang, "Edge Adaptive Image Steganography Based on LSB Matching Revisited," in *Information Forensics and Security, IEEE Transactions on*, 2010.

[4] C.-H. Yang, "Inverted pattern approach to improve image quality of information hiding by LSB substitution," *Pattern Recognition,* vol. 41, no. 8, pp. 2674-2683, 2008.

[5] J. Tian, "Reversible Data Embedding Using a Difference Expansion," *IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 13, NO. 8,* 2003.

[6] Y. Kurniawan and T. Ahmad, "Enhancing Difference Expansion Reversible Data Hiding Method by using Modulo Function," *[unpublished]*.

[7] A. M. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform," *Image Processing, IEEE Transactions on,* vol. 13, no. 8, pp. 1147-1156, Agustus 2004.

[8] M. Holil and T. Ahmad, "Peningkatan Performa Metode Steganografi Berbasis Difference Expansion Menggunakan Reduksi Selisih," *JUTI: Jurnal Ilmiah Teknologi Informasi,* vol. 12, no. 2, pp. 9-17, September 2014.

[9] D. S. Pambudi and T. Ahmad, "Desain dan Analisis Protokol Pengiriman Data Transformasi Sidik Jari Pewarnaan Graf," *JUTI: Jurnal Ilmiah Teknologi Informasi,* pp. 124-132, 2015.

[10] M. Kubale, Graph Colorings, Rhode Island: American Mathematical Society, 2004, p. 95.

[11] W. Diffie and M. Hellman, "New direction in cryptograph," *IEEE Transactions on Information Theory,* pp. 644-654, 1976.