PENERAPAN *CHAFFING AND WINNOWING* PADA SISTEM *RADIO FREQUENCY IDENTIFICATION*

Austin Dini Gusli – NIM : 13506101

Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if16101@students.if.itb.ac.id

Abstraksi

Kebutuhan manusia terhadap informasi semakin meningkat. Pertukaran informasi menjadi salah satu kunci untuk meningkatkan kualitas hidup, baik untuk dirinya sendiri maupun untuk khalayak ramai. Pertukaran informasi tentu memerlukan metode untuk meningkatkan keamanannya. Dengan demikian, orang akan menjadi lebih nyaman dalam mempertukarkan informasi.

Salah satu alat untuk bertukar informasi adalah RFID, yaitu sebuah perangkat yang dapat digunakan untuk mengidentifikasi sebuah objek. Informasi yang disimpan pada RFID mudah diserang sehingga keamanan informasi dan privasi pemilik informasi tersebut terancam. Salah satu metode untuk meningkatkan keamanan pertukaran informasi adalah dengan menerapkan steganografi pada informasi tersebut.

Teknik steganografi yang akan menjadi fokus adalah *chaffing and winnowing*. Teknik ini tidak melakukan enkripsi dan masih menampilkan informasi apa adanya. Namun, informasi tersebut disertakan dengan informasi palsu sehingga dapat mengacaukan pesan sebenarnya.

Penerapan *multitag* pada RFID merupakan salah satu langkah pengembangan RFID. Sejumlah penelitian memaparkan bahwa *multitag* menawarkan cukup banyak keuntungan. Teknik *chaffing and winnowing* diharapkan dapat diimplementasikan pada tag tambahan tersebut.

Kata Kunci : steganografi, *chaffing and winnowing*, RFID, *multitag*

1. Pendahuluan

Pertukaran data saat ini sangatlah padat. Media yang digunakan untuk mempertukarkan data pun sangat bervariasi. Data yang ditukarkan tidak hanya merupakan data tak bermakna tetapi juga data penting dan rahasia. Umumnya, pihak yang mempertukarkan data penting dan rahasia akan menggunakan kriptografi. Algoritma kriptografi bermula dari persamaan-persamaan matematika, baik yang sederhana maupun yang kompleks. Sebagian besar algoritma kriptografi telah tersebar luas dan mudah diperoleh. Berbeda dengan steganografi, kriptografi menghasilkan pesan yang dapat diketahui dengan mudah sebagai pesan yang terenkripsi, meskipun pesan tersebut masih belum diketahui maknanya.

Steganografi, ilmu dan seni dalam menyembunyikan pesan sehingga tidak dicurigai, merupakan salah satu metode meningkatkan keamanan melalui penyamaran. Steganografi telah digunakan sejak 440SM oleh Herodotus. Kini, steganografi pun masih digunakan, seperti penggunaan tinta rahasia, pembagian pesan ke dalam bit-bit terkecil dari *noisy image*, dan metode *chaffing and winnowing*.

Bentuk-bentuk steganografi tersebut juga dapat diimplementasikan pada *Radio Frequency Identification* (RFID). Semakin hari, RFID semakin marak digunakan. Informasi pada RFID harus dapat disembunyikan maknanya untuk dapat menjaga privasi data tersebut. Contoh pengimplementasian steganografi pada RFID adalah penambahan sejumlah tag yang menyamarkan informasi asli yang disimpan pada RFID. Pemberian tag tambahan merupakan salah satu cara metode *chaffing and winnowing* yang akan menjadi fokus pembahasan makalah ini.

Makalah ini disusun dengan sistematika berikut. Bagian 2 merupakan penjelasan mengenai steganografi. Bagian 3 berisi penjelasan mengenai teknik *chaffing and winnowing*. Gambaran umum dan contoh penggunaan *Radio Frequency Identification* terdapat pada bagian 4. Bagian 5 menjelaskan tingkat keamanan RFID saat ini. Bagian 6 merupakan contoh penggunaan teknik *chaffing and winnowing* pada RFID sebagai salah sastu langkah untuk meningkatkan keamanan RFID. Selanjutnya bagian 7 merupakan kesimpulan yang dapat diperoleh dari makalah ini.

2. Steganografi

Steganografi adalah ilmu dan seni untuk menyembunyikan pesan dengan cara yang sedemikian rupa sehingga orang-orang selain pengirim dan penerima tidak mencurigai pesan tersebut. Kata "steganografi" berasal dari bahasa Yunani dan memiliki makna "tulisan tersembunyi".

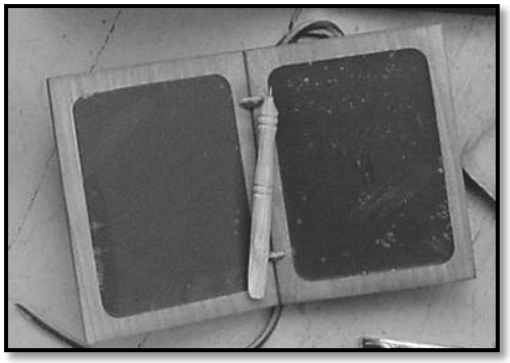
Pesan yang telah melalui proses steganografi kemungkinan besar tidak dicurigai sebagai pesan dengan makna tersembunyi. Pesan asli hanya disamarkan keberadaannya. Penggunaan fungsi enkripsi mengubah pesan asli menjadi pesan yang hampir pasti dicurigai. Hal ini merupakan kelebihan steganografi dibandingkan kriptografi.

Berdasarkan media yang digunakan, steganografi dapat dibedakan menjadi steganografi fisik, steganografi digital, dan steganografi cetak.

2.1. Steganografi fisik

Dari dulu hingga kini, steganografi jenis digunakan dengan berbagai cara. Sebagai contoh:

a. penggunaan lilin untuk menutupi ukiran pada kayu (*wax tablet*),
b. penyembunyian pesan pada tubuh manusia (seperti tato pada bagian kepala yang ditutupi rambut),
c. penggunaan tinta rahasia sehingga tinta tersebut hanya dapat ditampilkan dengan cara tertentu,
d. dan lain sebagainya.

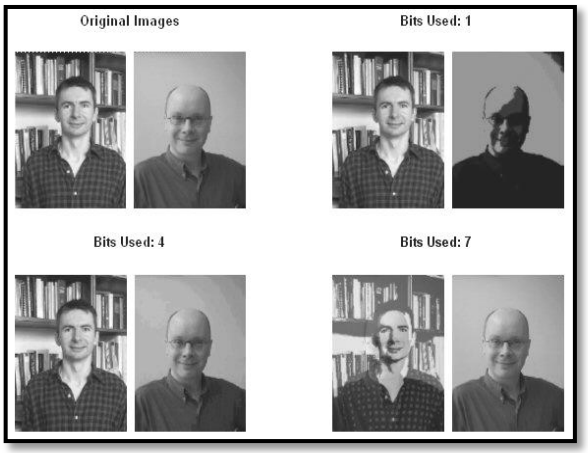


Gambar 1 Wax tablet (kayu yang disamarkan dengan lilin)

2.2. Steganografi digital

Seiring berjalannya waktu, teknologi digital semakin banyak. Data yang dipertukarkan melalui media digital pun semakin banyak. Oleh karena itu, telah banyak penggunaan steganografi pada digital juga. Steganografi digital telah dikembangkan sejak tahun 1985 dan hingga kini telah diolah menjadi lebih dari 700 aplikasi. Sejumlah teknik steganografi digital yaitu:

a. penyembunyian pesan ke dalam bit-bit terkecil dari berkas gambar atau suara,
b. penggunaan *mimic function*, menyamarkan properti objek,
c. *chaffing and winnowing* yang akan dijelaskan dengan lebih lanjut pada bagian 3,
d. dan lain-lain.



Gambar 2 Contoh perbedaan gambar biasa dan gambar yang telah diaplikasikan steganografi

2.3. Steganografi cetak

Hasil steganografi digital dapat saja dicetak. Pesan asli tersebut disembunyikan oleh *covertext* dan menjadi *stegotext*. Sebagai contoh, pesan dapat disembunyikan dengan mengubah ukuran tulisan, spasi, indentasi, dan karakteristik tulisan lainnya. Steganografi cetak ini diperdalam oleh Francis Bacon dan akhirnya mengembangkan *Bacon's cipher*.

3. *Chaffing and Winnowing*

Sebelumnya telah disebutkan bahwa *chaffing and winnowing* merupakan salah satu metode steganografi. *Chaffing and winnowing* diperkenalkan oleh Ron Rivest. Istilah ini berasal dari perlakuan terhadap *wheat* (gandum) yang perlu melakukan *winnow* terhadap *chaff*. Secara harafiah, *chaffing* berarti penambahan hal-hal yang tidak berguna, sedangkan *winnowing* berarti pengurangan hal-hal yang tidak berguna. Oleh karena itu, *chaffing and winnowing* merupakan teknik yang tetap menjaga data dalam wujud aslinya. Dengan kata lain, teknik ini menggunakan banyak *noise*.

Metode ini mengirimkan pesan dalam wujud aslinya. Tidak memecah pesan sedikit pun. Namun, metode ini membungkus pesan tersebut dengan beragam bit tidak bermakna. Oleh karena itu, penerima dituntut dapat melakukan *winnow* terhadap *chaff* yang telah diberikan pengirim.

Tingkat keamanan teknik *chaffing and winnowing* pun beragam. Tingkatan tersebut bergantung pada algoritma yang digunakan untuk melakukan *checksum*, teknik dalam menambahkan paket *chaff*, dan ukuran dari tiap paket.

3.1. Prosedur *chaffing and winnowing*

Langkah-langkah utama dalam melakukan teknik *chaffing and winnowing* sebagai berikut.

a. Pengirim memecah pesan ke dalam sejumlah paket.
b. Sistem melakukan *checksum* pada tiap paket. *Checksum* tersebut dibangkitkan berdasarkan kunci autentikasi. Kunci, sering disebut sebagai MAC (*Message Authentication Code*), ini merupakan kunci yang perlu diketahui oleh pengirim dan penerima.
c. Menambahkan sejumlah *chaff* atau data acak. Sistem tidak melakukan *checksum* menggunakan MAC pada *chaff*. *Checksum* akan berperan membantu penerima untuk menentukan paket yang benar dan paket yang salah.
d. Penerima pesan melakukan proses *winnowing* pada *stegotext*. Penerima menggunakan MAC untuk melakukan *checksum* pada tiap paket data yang diterimanya. Jika *checksum* tidak sesuai dengan *checksum* pada akhir paket, paket dihiraukan. Paket yang tersisa akhirnya disusun sedemikian rupa sehingga mampu menyampaikan makna sebenarnya.

3.2. Algoritma *chaffing and winnowing*

Berdasarkan langkah-langkah yang telah disebutkan sebelumnya, algoritma *chaffing and winnowing* dapat diberikan sebagai berikut.
Bangkitkan MAC : $\{0,1\}^k \times \{0,1\}^* \rightarrow \{0,1\}^l$. Paket merupakan pasangan (dt, tg) dengan dt sebagai data dan tg sebagai *tag* dengan panjang l buah bit (sesuai panjang MAC). Paket hanya valid jika $MAC_K(dt) = tg$ dengan $K \in \{0,1\}^k$. Penerima memvalidasi paket dengan cara $Pkt = (dt, MAC(K, dt))$.

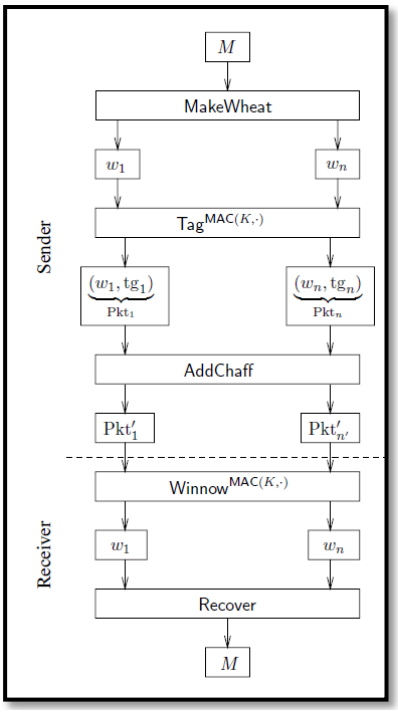
Algoritma pemberian *tag*:

```
Algorithm Tag^MAC(K,.)
   for i = 1,..,n do
      tg_i ← MAC(K, dt_i)
      return (dt_i, tg_i)
   endfor
```

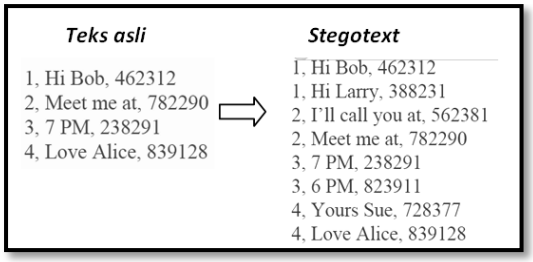
Algoritma proses *winnow*:

```
Algorithm Winnow^MAC(K,.)(Pkt_1, ..., n)
   for i = 1,..,n do
      parse Pkt_i as (dt, tg)
      if (MAC(K, dt)) = tg then
        return dt
   endfor
```

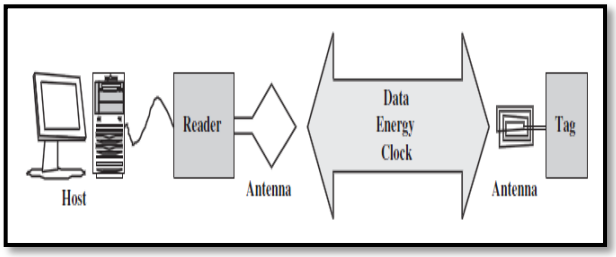
Jadi, secara garis besar, algoritma untuk teknik *chaffing and winnowing* dapat digambarkan seperti berikut.



Gambar 3 Proses *chaffing and winnowing*



Gambar 4 Contoh hasil penggunaan teknik *chaffing and winnowing*



Gambar 6 Komponen RFID

4. *Radio Frequency Identification* (RFID)

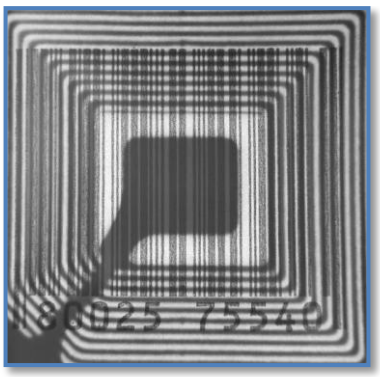
RFID merupakan teknologi yang digunakan untuk mengotomisasi proses identifikasi sebuah objek, bisa merupakan benda, hewan, atau manusia. Objek tersebut dilengkapi dengan sebuah RFID *tag*. Data disimpan pada tag tersebut dan dibaca oleh sebuah perangkat khusus.

RFID memiliki karakteristik c*ontactless* sehingga RFID masih dapat dipergunakan tanpa harus berinteraksi langsung dengan fisik RFID tersebut. Selain itu, RFID juga mengkonsumsi tenaga yang minim untuk mengirimkan sinyal. Meskipun demikian, RFID memiliki kekurangan yaitu biaya produksinya membutuhkan biaya yang lebih dibandingkan dengan *barcode* dan sejumlah alat identifikasi lainnya.

4.1. Komponen RFID

RFID memiliki tiga komponen utama, yaitu sebagai berikut.

a. *Transponder* atau RFID *tag*, ditempatkan pada objek dan mengandung data dari sistem.
b. *Transceiver* atau pembaca RFID, umumnya mampu membaca dan menuliskan data pada transponder.
c. Subsistem yang memproses data dari RFID yang juga sering disebut sebagai *host*.



Gambar 5 RFID *tag* dilengkapi sebuah *barcode*

4.2. Contoh Penggunaan RFID

Seperti yang telah disebutkan sebelumnya, RFID semakin marak digunakan. Contoh penggunaannya antara lain sebagai berikut.

a. Pembayaran tiket masuk tol
Pembayaran biaya jalan tol dapat dipermudah dengan pemberdayaan RFID. Loket pembayaran dilengkapi dengan *transceiver* sehingga kendaraan tidak perlu berhenti dan mengambil kartu atau membayar lagi. Selain mengambil data unik tiap kendaraan, *transceiver* juga dapat menuliskan biaya tol dalam RFID *tag.* Penerapan RFID ini telah diimplementasikan oleh Pakistan, Turki, Malaysia, dan sejumlah negara lainnya.

Gambar 7 RFID pada pembayaran tiket masuk tol

b. Pelacakan objek
Untuk dapat melacak objek, RFID ditanamkan ke dalam produk. Selanjutnya, RFID juga dapat digunakan untuk mengawasi hasil distribusi produk secara grosir. Pemanfaatan RFID seperti ini digunakan oleh Kolombia untuk mengawasi distribusi kopi, digunakan oleh Emirates airlines untuk mendeteksi bagasi, dan banyak negara/perusahaan lainnya.

c. Identifikasi hewan
RFID telah digunakan untuk mengidentifikasi hewan di peternakan

sejak bertahun-tahun yang lalu. Ini merupakan salah satu contoh pertama pengaplikasian RFID. Dengan demikian, identifikasi hewan dan penjaminan kualitas serta kesehatan hewan menjadi lebih mudah.

d. Penggunaan di perpustakaan.
Selain untuk mengidentifikasi buku, RFID juga dapat digunakan untuk mencegah terjadinya pencurian buku. Teknologi ini pertama diterapkan oleh perpustakaan di Singapura.

Gambar 8 RFID pada telinga hewan

5. Keamanan RFID

RFID merupakan sebuah perangkat yang sangat mudah diserang sebab RFID *contactless* dan bekerja tidak hanya di bawah pengawasan. Oleh karena itu, penyerang dapat menyerang dari kejauhan dan serangan pasif tidak dapat dideteksi.

Telah dilakukan sejumlah riset untuk meningkatkan keamanan RFID. Juels, Rivest, dan Szydlo mengemukakan penggunaan "blocker tag" untuk mencegah pelacakan konsumen sehingga sebuah *tag* merepresentasikan sejumlah ID. Selain itu, Weis juga memberikan sebuah cara lain, yaitu fungsi *hash* dan acak sehingga. Weis dan sejumlah rekannya pun memberikan usul lainnya, yaitu penghapusan ID dari produk yang telah dibeli.

Umumnya, data yang lebih rahasia, seperti data autentikasi bank, dienkripsi dengan kunci nirsimetri kriptografi. Namun, aloritma kriptografi yang baik memiliki biaya komputasi yang besar.

6. Peningkatan Keamanan RFID

RFID saat ini telah mengalami banyak perkembangan. Meningkatnya pemakaian RFID pun menuntun ke sejumlah penelitian terhadap RFID. Salah satu teknik yang dapat digunakan untuk meningkatkan kinerja RFID adalah dengan menggunakan *multitag*.

6.1. *Multitag* pada RFID

Umumnya, objek yang digunakan pada RFID hanya memiliki sebuah tag. Untuk ke depannya, RFID mungkin dapat mempertimbangkan penggunaan beberapa tag pada tiap objeknya. Penambahan tag dapat memberikan sejumlah keuntungan, antara lain:

a. meningkatnya induksi tegangan pada tag,
b. meluasnya jangkauan reader terhadap tag,
c. memori tag meningkat,
d. dan meningkatnya ketersediaan, keandalan, serta ketahanan sistem.

Multitag dapat diberdakan menjadi tiga, yaitu sebagai berikut.

a. Tag berulang, dua atau lebih tag yang memiliki informasi identik dan menjalankan fungsi identik.
b. *Dual-tags*, dua buah tag yang terhubung dan memiliki satu atau dua antena.
c. *N-tags*, *n* buah tag yang saling terhubung satu dan lainnya serta memiliki satu atau lebih antena.

6.2. Peran *multitag* pada keamanan RFID

Seperti yang telah disebutkan pada bagian 5, RFID sangat rawan penyerangan. Data yang disimpan pada RFID pun semakin bervariasi dan mengancam kemanan dan privasi. Untuk itu, RFID pun terkadang menggunakan enkripsi data. Enkripsi tentu telah menjadi hal yang umum. Namun, c*iphered text* memancing kecurigaan orang lain sehingga lebih berniat untuk memecahkannya. Oleh karena itu, RFID juga diharapkan dapat memanfaatkan steganografi di kemudian hari.

Penerapan *multitag* dan *chaffing and winnowing* dapat menjadi salah satu alternatif dalam meningkatkan keamanan RFID. Prosedur yang digunakan sama saja dengan prosedur *chaffing and winnowing* pada umumnya, seperti yang terdapat pada bagian 3.1. Dengan menggunakan *multitag*, tag tambahan dapat digunakan sebagai bibit pembangkit *chaff*. Pengiriman *chaff* atau penentuan jumlah *chaff* dapat meningkatkan tingkat keamanannya sebab menyembunyikan jumlah *tag* sebenarnya.

Namun, penggunaan *multitag* dan *chaffing and winnowing* tentu membutuhkan biaya yang cukup besar. Meskipun dapat digunakan untuk menjaga privasi, metode ini kurang baik diterapkan sebab biaya yang cukup besar tersebut. Akan tetapi,

penggunaan keduanya secara bersamaan dapat memberikan manfaat yang sesuai untuk informasi penting.

7. Kesimpulan

Multitag merupakan salah satu hasil pengembangan RFID. *Multitag* mampu menyimpan lebih banyak data dan mentransmisikan sinyal dengan lebih baik sehingga dapat menawarkan sejumlah nilai tambah.

Salah satu nilai tambah penggunaan *multitag* adalah mampu meningkatkan keamanan pada RFID. *Multitag* dapat digunakan untuk meningkatkan kompleksitas enkripsi atau dengan memfasilitasi *chaffing and winnowing*. Teknik *chaffing and winnowing* pada multitag RFID tidak memerlukan modifikasi yang banyak. Penggunaannya pada multitag RFID akan membutuhkan biaya yang cukup besar sehingga teknik ini hanya disarankan untuk menyembunyikan informasi rahasia.

DAFTAR PUSTAKA

[1] _____. (2009). *Steganography: Facts, Discussion Forum, and Encyclopedia Article*. http://www.absoluteastronomy.com/topics/Steganography. Tanggal akses 3 Maret 2010 pukul 23:39.

[2] Bellare, M., Boldyreva, A. (2000). *The Security of Chaffing and Winnowing*. Springer-Verlag Berlin Heidelberg.

[3] Feldhofer, M., Dominikus, S., Wolkerstrofer, J. (2004). *Strong Authentication for RFID Systems Using the AES Algorithm*. International Association for Cryptologic Research.

[4] Munir, Rinaldi. (2004). *Bahan Kuliah IF5054 Kriptografi*. Departemen Teknik Informatika, Institut Teknologi Bandung.

[5] Reavis, J. (1999). *Chaffing and Winnowing.* http://www.networkworld.com/newsletters/sec/1206sec1.html. Tanggal akses 3 Maret 2010 pukul 23:31.

[6] Ronald L. Rivest. (1998). *Chaffing and Winnowing: Confidentiality without Encryption*. CryptoBytes (RSA Laboratories), 4(1):12–17.

[7] Weis, A.S. (2003). *Security and Privacy in Radio-Frequency Identification Devices*. Massachusetts Institute of Technology.