Pengamanan *File* dengan Memanfaatkan Gambar

Risalah Widjayanti - 13509028
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13509028@std.stei.itb.ac.id

Privasi dan hak pribadi, dua kata itu menjadi alibi untuk kerahasiaan dari kepemilikan orang terhadap sesuatu. Setiap orang punya rahasia, sayangnya rahasia pribadi tidak pernah dijamin undang-undang dan tidak bisa diasuransikan sehingga terjaga tidaknya rahasia itu menjadi tanggung jawab masing-masing pemiliknya.

Manusia mencoba menggunakan banyak cara untuk* menyembunyikan *dan mengamankannya, mulai dari kunci hingga kata sandi. Akan tetapi, masih ada pengamanan* file *dengan cara lain. Penyamaran, misalnya. Didasari ide tentang bagaimana membagikan sesuatu yang terlalu berharga untuk dibagikan ketika ia sudah dalam wujud berbeda. Enkripsi dan dekripsi teks dan gambar menjadi sesuatu yang baru sudah lama ditemukan manusia. Memanipulasi* file *pribadi dalam bentuk apapun ke dalam bentuk gambar. Tidak hanya gambar, namun juga* file *suara, video, teks, jenis apapun. Hal inilah yang akan dibahas dalam makalah ini.

***Kata kunci:* file *pribadi, rahasia, enkripsi, penyamaran* file**

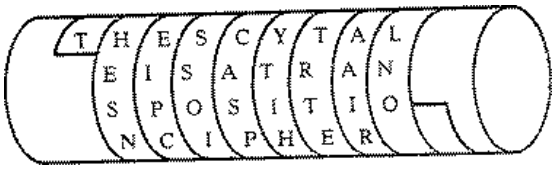
I. PENDAHULUAN

Dahulu pernah ada buku harian dilengkapi gembok untuk penulis-penulis kecil dengan rasa malu mereka menuliskan cerita dalam buku yang inginnya tidak ingin dibaca siapapun selain pemiliknya. Kemudian metode kunci brankas dengan sandi lewat berupa kombinasi angka. Hingga kode pengaman dan pin untuk akses telepon genggam dan mesin ATM. Manusia menginginkan kerahasiaan yang lebih rahasia lagi, muncullah pemindai lewat sidik jari dan retina mata, bahkan DNA .

Pengamanan dengan "kunci pintu", bukan satu-satunya jalan. Kriptografi disinyalir menjadi alternatif lain untuk pengamanan rahasia. Di mana kita tidak akan merasa rugi apabila orang lain menemukan apa yang kita sembunyikan karena ketidakmengertian mereka atas apa yang kita maksudkan.

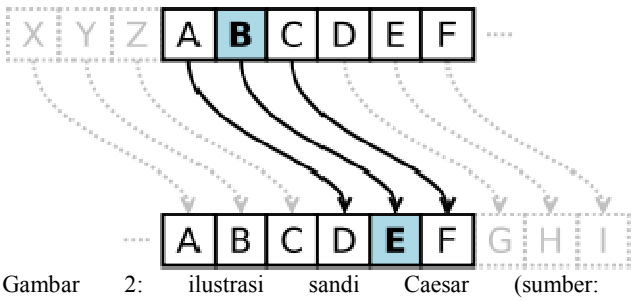
Aeni, dalam blognya (*ae89crypt5.wordpress.com*) menuturkan sejarah kriptografi dengan cukup jelas. Cikal bakal kriptografi diklaim telah ada sejak 4000 tahun yang lalu. Di suatu tempat yang sekarang bernama Mesir, berupa Hieroglyph. Aeni yang mengambil sumber dari buku karangan Davin Kahn yang berjudul *The Code Breakers*, merunut sejarah kriptografi. Berawal dari kriptografi klasik dengan metode enkripsi kuno menggunakan kertas dan pensil. Jauh dari teknik enkripsi masa kini di mana sudah melakukan enkripsi dengan komputerisasi.

Dalam diktat kuliah *Struktur Diskrit* pun, Rinaldi Munir menyebutkan bahwa sejarah mencatat, sekitar 400 tahun sebelum masehi, kriptografi digunakan sebagai alat penyampai pesan yang digunakan tentara Sparta di Yunani. Para tentara ini menggunakan lebih dari sekadar pensil dan kertas. Namanya *syctale*, sebuah tabung dengan pita dari daun papyrus yang bertuliskan huruf-huruf yang hanya bisa membentuk satu makna tertentu apabila dililitkan di tabung dengan diameter yang tepat. Dengan begini, jelas bahwa pengirim dan penerima harus memiliki tabung berdiameter sama dan itulah yang menjadi kunci enkripsi-dekripsi teknik kriptografi yang kemudian dinamakan *transposition cipher* ini. *Transposition cipher* juga dinobatkan sebagai teknik enkripsi tertua.



Gambar 1: ilustrasi *syctale* (sumber: www.cs.ubbcluj.ro)

Selain transposisi *cipher*, sebetulnya masih ada teknik enkripsi lain yang menurut penulis malah lebih sederhana. Idenya adalah menggeser huruf sedemikian rupa sehingga tidak membentuk kalimat yang utuh. Ditemukan oleh Julius Caesar, seorang kaisar Romawi yang termahsyur. Namanya diabadikan dalam nama sandi ini, sandi Caesar, atau disebut juga sandi geser karena enkripsi dan dekripsi sandi ini dengan menggeser huruf. Sandi ini telah banyak diketahui orang sehingga penggunaan sandi ini disinyalir tidak lagi aman. Apalagi cara dekripsinya juga cukup mudah dilakukan meskipun tanpa kunci, yakni hanya tinggal menggeser huruf-huruf sampai menemukan kata yang dirasa pas.



Gambar 2: ilustrasi sandi Caesar (sumber: www.wikipedia.org)

Konon, setiap harinya sandi baru bermunculan dengan dan setiap hari itu juga manusia mencari pemecahan

masalahnya. Ada sebuah forum menarik beralamatkan http://www.kaskus.us/forumdisplay.php?f=18 (*Can You Solve This Game*) yang memfasilitasi anggotanya untuk menjadi seorang kriptografer dan kriptanalis kecil-kecilan. Setiap harinya sebuah topik baru yang memberikan sebuah kalimat yang tidak bermakna bermunculan. Anggota lain dituntut untuk menebak apa arti dari kalimat tersebut berikut cara memecahkannya. Hal itu membuktikan betapa kayanya cara mengenkripsi berikun mendekripsikan sebuah sandi. Sekaligus juga membuktikan, pengamanan dengan menggunakan enkripsi dan dekripsi teks tidak lagi tinggi tingkat keamanannya.

Lantas, bagaimana cara pengamanan yang lebih baik?

II. SANDI LEWAT BERUPA GAMBAR

Untuk sebagian besar orang, kesalahan proteksi *file* mereka adalah pemakaian sandi lewat yang terlalu mudah ditebak. Bukan hanya proteksi *file* berharga dan rahasia, tetapi juga untuk akun surat elektronik, jejaring sosial, dan sebagainya. Kebanyakan orang menggunakan kumpulan karakter yang sederhana seperti tokoh idola, tanggal lahir, atau bahkan nama depan. Kelemahan tingkat keamanan sandi lewat ini sering menjadikan *file* pribadi menjadi mudah untuk bocor di tangan orang lain. Pembobol bisa masuk hanya dengan mencoba berbagai kemungkinan untuk menyusup, atau teknik ini biasa disebut dengan *brute force*.

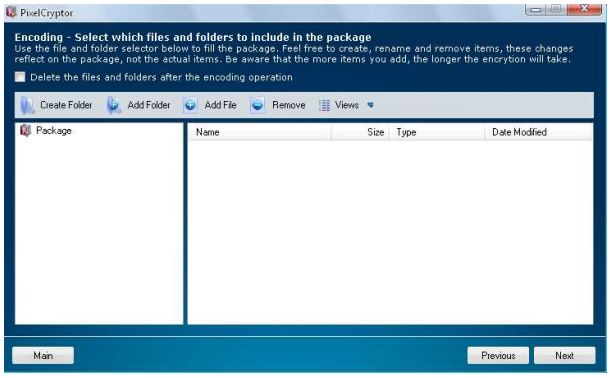
Sayangnya, meskipun tahu dengan jelas resiko dari penggunaan karakter yang kelewat sederhana untuk sandi lewat, orang-orang enggan mengganti sandi lewat mereka dengan sesuatu yang lebih rumit. Alasannya adalah kemudahan mengingat sandi lewat itu sendiri. Semakin sederhana suatu sandi lewat, mereka akan lebih mudah mengingatnya. Demikian juga orang-orang enggan menggunakan kombinasi karakter yang lebih rumit (dengan huruf kapital, angka, dan karakter khusus) untuk alasan yang sama. Padahal semakin rumit kombinasi sandi lewat, semakin susah sandi lewat tersebut bobol dengan *brute force* yang artinya akan lebih aman pemroteksian *file* tersebut.

Seperti musik yang lebih mudah diingat daripada lirik, gambar (terutama yang berwarna) pun lebih mudah diingat daripada kata-kata. Hal ini telah dibuktikan oleh Andy Bell untuk tips mengimprovisasi memorinya lewat pemvisualisasian, bukan dengan kata-kata.

Perangkat lunak dengan inovasi terbaru, dapat mewujudkan ide tentang enkripsi dan dekripsi dengan sandi lewat berupa gambar. Salah satunya adalah *PixelCryptor* dari *CodeGazer*. Perangkat lunak buatan Bernd de Graaf dan Yvo van Beek ini dapat membantu mengamankan data pribadi dengan memanfaatkan prinsip memori, enkripsi, dan tingkat keamanan sandi lewat. Perangkat lunak ini bersifat gratis dan dapat diunduh di situs *CodeGazer* di www.codegazer.com dengan ukuran *installer* sebesar 3,36 MB dan dapat dibawa kemana-mana alias *portable*, *PixelCryptor* menjadi lebih mudah digunakan. Antar muka pengguna juga mudah dimengeri dan jauh dari kesan enkripsi dan dekripsi yang rumit, penggunanya bahkan untuk penggunaan pertama kali.

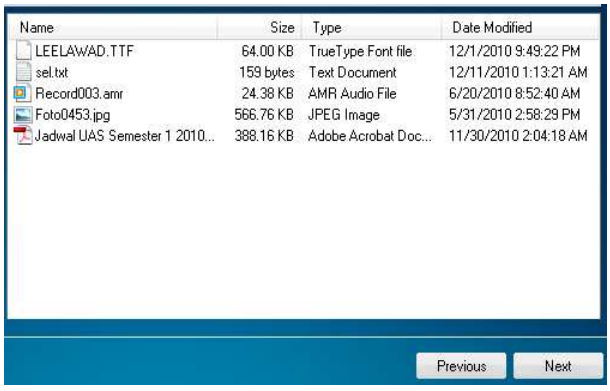
Gambar 3: tampilan awal *PixelCryptor*

Pengguna harus memilih ikon kedua dari kiri untuk mengenkripsi *file* atau *folder*. Setelah itu, pengguna akan dibawa ke dalam tampilan seperti di bawah ini:



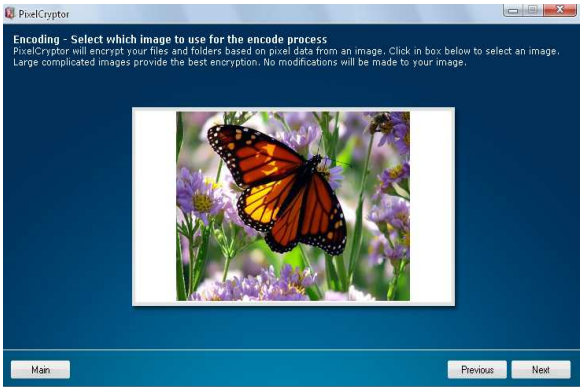
Gambar 4: modus enkripsi

Di sini pengguna bisa memilih *file* atau *folder* yang ingin dienkripsi. Pengguna juga dapat membuat folder baru kemudian menambahkan *file* dengan beragam ekstensi agar dapat dienkripsi. Di sini penulis mencontohkan dengan membuat *folder* baru yang diberi nama "contoh" kemudian mengisinya dengan lima buah *file* berbeda ekstensi seperti yang bisa dilihat pada gambar di bawah ini:



Gambar 5: daftar *file* yang akan dienkripsi

Kemudian pengguna menekan tombol "*Next*" yang berada di pojok kanan bawah layar untuk masuk ke menu selanjutnya.

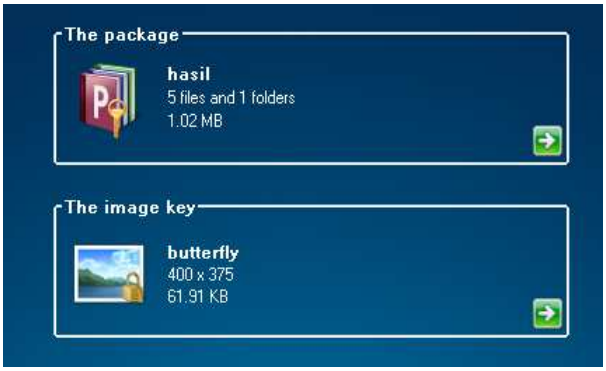


Gambar 6: menu pemilihan gambar untuk *encoding file/folder*

Seperti yang bisa dilihat di gambar, penulis menggunakan gambar kupu-kupu untuk encode. Gambar yang lebih kompleks menghasilkan enkripsi yang lebih baik. Meski begitu, tidak ada pengubahan sama sekali yang terjadi kepada gambar yang dipilih. Kemudian pengguna harus kembali menekan tombol "*Next*" untuk masuk ke menu berikutknya.

Gambar 7: bagian dari menu pemilihan *file* hasil enkripsi

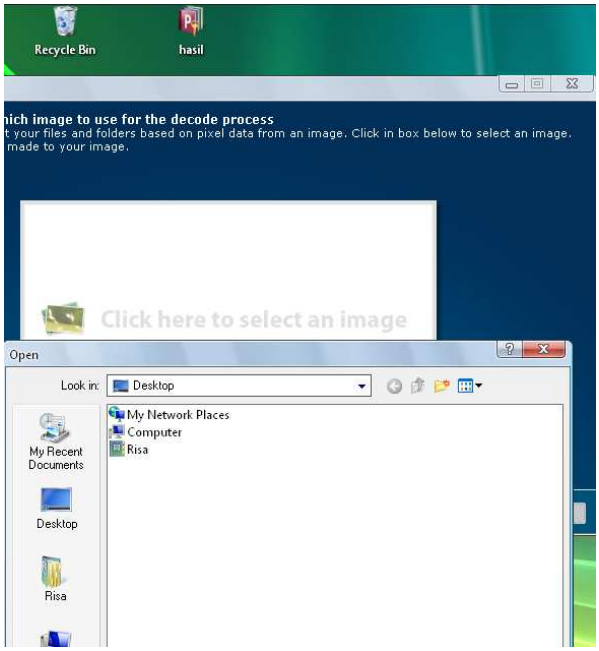
Penempatan *file* berekstensi *PixelCruptor files* (.cgp) ini bisa di mana saja. Nantinya *file* ini dapat diletakkan di sembarang tempat tanpa perlu khawatir dilihat orang karena akan sulit sekali mencari gambar yang tepat untuk dicocokkan sebagai sandi lewat. Penulis menyarankan untuk memberi nama *file* yang tidak mencolok dan tidak mencurigakan.



Gambar 8: tampilan setelah *file* berhasil dienkripsi

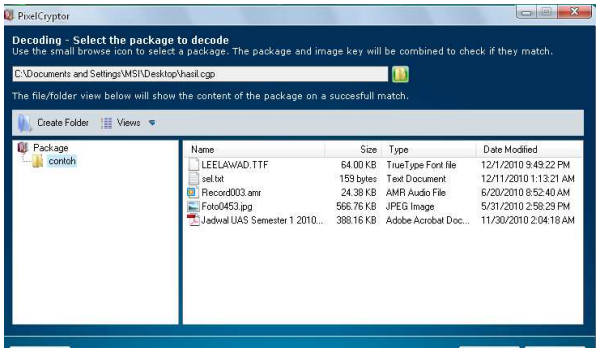
Gambar 9: *file* di *desktop* yang telah dienkripsi dengan bantuan *PixelCryptor*

Orang awam mungkin tidak akan mengetahui bahwa *file* yang terpampang tersebut adalah *file* pribadi yang disamarkan. Namun, meskipun diketahui kerahasian *file* tersebut, bukan berarti mudah untuk mengetahui isinya. Karena begitu *file* tersebut dipilih, akan menghasilkan tampilan seperti di bawah ini:



Gambar 10: tampilan apabila *file* dicoba dibuka

Pengguna harus memilih gambar yang tepat dari ratusan atau bahkan ribuan gambar yang terdapat dalam *harddisk*. Selain lewat cara menge-klik langsung *file hasil*, dekripsi *file* dapat juga dilakukan dengan memilih modus dekripsi yang berada di menu utama (ikon kedua dari kanan). Apabila menggunakan menu tersebut, pengguna harus memasukkan gambar kunci terlebih dahulu baru kemudian folder yang disamarkan. Apabila berhasil didekripsi kembali, maka tampilan yang muncul adalah seperti gambar di bawah ini:



Gambar 11: tampilan ketika *file* tersamar berhasil dibuka

Perangkat lunak ini dapat digunakan untuk melindungi *file* dengan tingkat pengamanan cukup tinggi. Meski begitu, pengamanan dengan gambar tidak selalu mesti menggunakan perangkat lunak khusus dengan cara yang sama. Masih ada cara lain yang bahkan tingkat kebocorannya lebih kecil dibandingkan menggunakan teknik enkripsi *file* dengan menggunakan kunci bentuk gambar. Teknik tersebut akan dibahas dalam bab berikutnya.

III. ENKRIPSI FILE KE DALAM SATU FILE GAMBAR

Ada cara yang lebih aman dibandingkan dengan alternatif sebelumnya. Jika alternatif sebelumnya dengan jelas membeberkan bahwa pengguna memiliki rahasia (dengan keberadaan *file* berformat *PixelCryptor file* itu sendiri), masih ada cara lain yang bisa digunakan. Cara ini terbilang lebih aman karena tidak meninggalkan jejak sama sekali. Selain itu, untuk komputer dengan sistem operasi *Windows*, tidak diperlukan perangkat lunak tambahan apapun. Penyamaran *file* ini dapat dilakukan hanya dengan menggunakan *Command Prompt*.

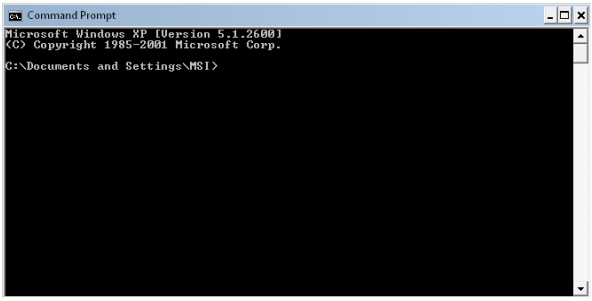
Pengamanan *file* dengan cara ini menjadikan seseorang tidak perlu lagi khawatir apabila komputernya diutak-atik sedemikian rupa. Bahkan fitur *search* untuk pencarian file pun tidak berhasil digunakan untuk melacak *file* tersembunyi yang disamarkan ke dalam *file* gambar seperti ini.

Sehingga dapat disimpulkan kelebihan menggunakan cara ini dibandingkan dengan alternatif sebelumnya adalah:

1) Keamanan yang lebih. *File* tersamar dengan lebih sempurna. Tidak ada hasil enkripsi yang berwujud mencurigakan. Karena sifatnya adalah penyatuan *file* yang hendak dirahasiakan dengan *file* gambar, fusi dari dua *file* tersebut ke dalam bentuk gambar biasa akan terlihat amat sangat normal jika dibuka dari perangkat lunak pengolah gambar. Misalnya *Microsoft Picture Viewer*, *Paint*, dan sebagainya. Selain itu, penulis sudah membuktikan dengan fitur *search* bahwa *file* yang sudah diamankan tidak dapat dilacak lagi keberadaannya.
2) Tidak diperlukannya perangkat lunak tambahan. Berbeda dengan cara sebelumnya di mana pengguna harus memiliki *software PixelCryptor* untuk menyamarkan *file*. Sehingga lebih praktis lagi dalam penggunaannya.

Akan tetapi, dibanding dengan metode sebelumnya, cara ini terbilang lebih rumit jika ditinjau dari keharusan penggunanya memiliki pengetahuan dasar tentang perintah dasar DOS. Tidak banyak memang perintah dasar DOS yang diperlukan untuk menerapkannya, hanya perintah untuk menyalin data (menulis ulang) dan perintah masuk keluar direktori yang dapat direduksi dengan menggunakan direktori standar dari *Command Prompt*. Meski begitu, tetap saja, bagi orang yang terbiasa menggunakan *software* dengan antar pengguna yang baik dan untuk pemula, menggunakan metode macam ini bisa jadi menyulitkan.

Untuk *file* yang hendak disamarkan, penulis menyarankan menggunakan *file* yang sudah dikompresi. Apalagi untuk *file* dalam jumlah banyak yang hendak digabungkan menjadi satu, sebaiknya dikompres dahulu ke dalam *archive* sehingga ekstensinya menjadi ekstensi *file* terkompres. Kembali penulis memberi saran untuk memberi ekstensi *file* yang populer. Misalnya ekstensi .zip atau .rar. Hal ini berhubungan dengan dekripsi *file* yang sudah disamarkan tersebut. Dengan demikian, pengguna sebaiknya memiliki perangkat lunak untuk mengekstrak *file* terkompresi tersebut, misalnya *WinRAR* atau *WinZIP*. Namun apabila tidak memiliki perangkat lunak tersebut, tidak mengapa. Hanya perlu sedikit penyesuaian pada saat dekripsi.



Gambar 13: tampilan awal *command prompt*

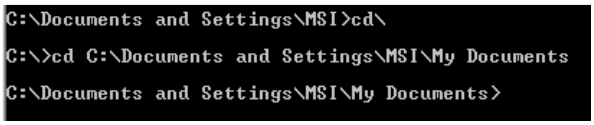
Arahkan *command prompt* untuk masuk ke direktori penyimpanan gambar sekaligus *file* yang ingin disamarkan. Menggunakan perintah DOS untuk mengarahkan direktori dapat dilakukan dengan petunjuk berikut:

```
cd\
```

Untuk keluar dari direktori kembali ke induk (C:\).

```
cd c:\(direktori)
```

Untuk masuk ke dalam direktori yang diinginkan.



Gambar 14: mengarahkan *command* ke direktori *file*

Setelah itu pengguna tinggal memasukkan kode untuk menyamarkan *file* tersebut. Adapun caranya adalah sebagai berikut:

```
copy /b (nama file gambar)+(nama file yang ingin disembunyikan) (namafilegambar)
```

Nama *file* diikuti dengan ekstensi. Misalkan gambar yang berformat .png dengan nama *latch* dituliskan dengan nama *latch.png*. Demikian juga untuk nama file yang ingin disembunyikan. Sebagai contoh, penulis menyamarkan *file* berekstensi .zip yang merupakan kompresi dari *folder Alstrukdat* ke dalam sebuah gambar *latch* yang berekstensi .png. Sehingga kode yang penulis buat adalah sebagai berikut:

```
copy /b latch.png+alstrukdat.zip latch.png
```

Jika berhasil, maka yang muncul adalah pesan sebagai berikut ini:

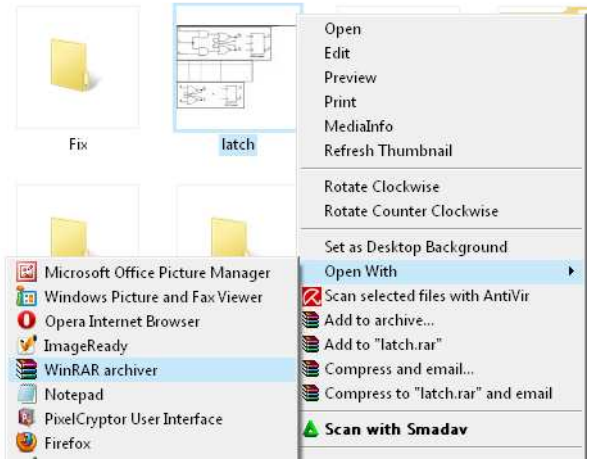
Gambar 15: Tulisan pada *command prompt* ketika *file* berhasil dienkripsi

Ketika tulisan tersebut muncul, berarti kedua *file* tersebut telah berhasil disalin dan dimasukkan ke dalam satu *file* saja, yakni *file* gambar *latch* tersebut. Ketika dilihat tampilannya, tidak ada sama sekali gambar yang berubah. Namun apabila dilihat ukuran dari gambar

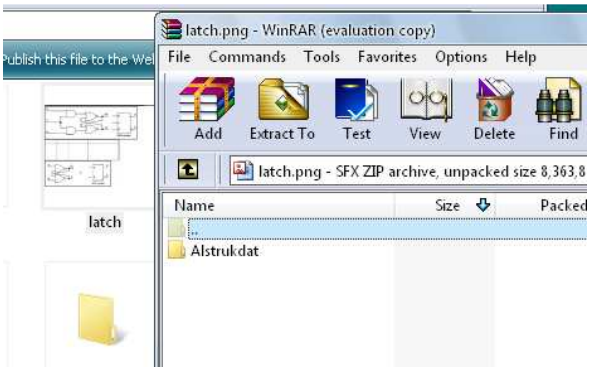
tersebut, pasti *file* gambar mengalami penambahan jumlah *Byte*.

Setelah berhasil disamarkan, gambar tersebut tidak akan bereaksi aneh seperti meminta sandi lewat atau kunci ketika diklik. Semuanya akan terlihat normal kecuali pengguna membuka gambar bukan dengan program pengolah gambar.

Lantas bagaimana cara mendekripsikannya? Di sini, pengguna membuka dengan program sesuai dengan tipe *file* yang disamarkan tersebut. Misalnya, jika pengguna menyamarkan teks dokumen, maka pengguna membuka gambar tersebut dengan *Microsoft Word* atau program pengolah kata yang lain. *File* video bisa dibuka dengan *media player* dan sebagainya. Penulis memberi contoh membuka *file* tadi dengan *WinRAR archiver* seperti pada gambar di bawah ini:



Gambar 16: membuka *file* gambar sesuai dengan ekstensi *file* yang disamarkan



Gambar 17: gambar ketika dibuka dengan *WinRAR*

Setelah ini, membuka *file* yang ada dalam folder *Alstrukdat* seperti membuka *file* dengan cara biasa karena penyamaran *file* dalam *folder* terkompresi tidak mempengaruhi *file* tersebut.

Cara pendekripsian *file* gambar dengan perangkat lunak selain pengolah gambar menimbulkan pertanyaan, bagaimana jika yang ingin disamarkan justru merupakan *file* gambar? Hal ini tidak bisa dilakukan secara langsung. Karena begitu gambar disalin dengan *command prompt*, dua gambar yang digabungkan tidak berfusi menjadi dua gambar dalam satu *file*. Justru, gambar yang hendak menjadi wujud penyamaran akan disalin ulang menjadi gambar yang sama dengan gambar yang ingin disamarkan. Untuk mengakalinya, gambar tersebut bisa dijadikan *archive* (dikompresi dulu) agar tipenya bukan lagi *file* gambar.

IV. Kelebihan Menggunakan Gambar Untuk Proteksi Data

- Gambar lebih mudah diingat memori
  Pada prinsipnya, orang lebih baik mengingat suatu informasi apabila membayangkan gambarnya. Inilah sebab mengapa film lebih mudah dicerna daripada buku.
  Selain itu, warna-warna secara psikologis juga membantu merangsang otak untuk mengingat. Apalagi warna yang berbeda. Itulah sebabnya orang menggunakan stabile untuk memberi latar belakang yang berbeda pada tulisan agar lebih mudah mengingatnya. Makin terang suatu warna, makin mudah untuk diingat.
  Penggunaan gambar sebagai sandi lewat seperti pada alternatif pertama lebih mudah diingat dibandingkan dengan menggunakan kata-kata. Terlebih lagi, sandi lewat baru dikatakan aman apabila memiliki panjang karakter tertentu dan kombinasi karakter tertentu.
- Kemungkinan dibobol lewat *brute force* lebih kecil
  Hal ini berkaitan dengan sulitnya menerka gambar apa yang digunakan oleh pengguna. Dengan asumsi bahwa pengguna dalam memori penyimpanan komputernya memiliki ribuan gambar (sebagai contoh, penulis memiliki sekitar 2400 gambar) yang sangat sulit diterka gambar mana yang merupakan kunci. Sementara berkaitan dengan poin#1 di atas, pengguna sendiri sudah lebih mengingat gambar mana yang digunakan.
  Kemudian untuk alternatif kedua (penyamaran *file*) menjadi lebih sulit lagi, karena meskipun pembobol sudah berhasil mendapatkan gambar yang telah dienkripsi, belum tentu pembobol itu mengetahui aplikasi mana yang dapat digunakan untuk mengenkripsi *file*. Kesalahan pemilihan aplikasi malah memunculkan pesan *error*.

V. Kesimpulan

Gambar dapat digunakan sebagai mendia untuk mengamankan data. Apalagi dengan kelebihan gambar itu sendiri sebagai media yang mempermudah pengguna untuk mengingatnya, gambar bisa dinilai lebih unggul dari segi kemudahan mengingat dan tingkat keamanan *file* itu sendiri. Untuk saat ini, belum banyak orang yang mengetahui keamanan menyimpan *file* dengan memanfaatkan gambar sehingga akan lebih aman untuk menggunakannya. Ada banyak perangkat lunak yang dapat digunakan misalnya *PixelCryptor* yang dapat

digunakan tanpa menutup kemungkinan masih banyak aplikasi sejenis yang beredar di luar sana.

REFERENCES

Munir, Rinaldi. *Diktat Kuliah IF 2091 Struktur Diskrit*. Program Studi Teknik Informatika, Sekolah Teknik Elektrodan Informatika, Institut Teknologi Bandung, 2008.

Aeni. *Sejarah Kriptografi.* (http://ae89crypt5.wordpress.com/2008/05/12/sejarah-kriptografi/ Tanggal akses 11 Desember 2010, pukul 19.00)

Artikel non persona. *Encrypt Files and Folders With Pictures and Not Passwords.* (http://www.raymond.cc/blog/archives/2008/01/22/encrypt-files-and-folders-with-pictures-and-not-passwords/ Tanggal akses 12 Desember 2010 pukul 20.00)

Attayaya. *Combining 2 Files by encrypted then decrypted.* (http://www.attayaya.net/2010/06/combining-2-files-by-encrypted-then.html Tanggal akses 12 desember 2010 pukul 23.00)

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 16 Desember 2010

ttd

Risalah Widjayanti - 13509028