Seminar Nasional Sains & Teknologi Informasi (SENSASI)
SENSASI 2019

ISBN: 978-602-52720-2-8
Juli 2019
Hal: 505 – 509

Aplikasi Steganografi Pengamanan Data Nasabah di Standard Chartered Bank Menggunakan Metode Least Significant Bit dan RC4

Muhammad Syahril[1*], Hendra Jaya[2]

[1]Program Studi Sistem Informasi, STMIK Triguna Dharma, Medan, Indonesia
[2]Program Studi Teknik Komputer, STMIK Triguna Dharma, Medan, Indonesia
Email: [1*]m_syahril@trigunadharma.ac.id, [2]hendra_jaya@trigunadharma.ac.id

Abstrak

Standard Chartered Bank adalah salah satu bank dari beberapa bank yang ada di kota Medan. Dalam Pengamanan data nasabah ini belum memiliki suatu sistem pengamanan. Apabila tidak adanya pengamanan data maka hal sperti ini akan rawan terjadi penyadapan data yang nantinya akan berakibat fatal karena data nasabah bisa saja diubah bahkan dihapus oleh orang yang tidak bertanggung jawab. Oleh karena itu, Standard Chartered Bank membutuhkan suatu sistem Kriptografi dan Steganografi pengamanan data nasabah dengan menggunakan metode LSB dan RC4 untuk menghindari penyadapan data.Hasil dari penelitian ini diharapkan dapat membantu pihak Standard Chartered Bank dalam melakukan pengamanan data nasabah sehingga data nasabah dapat terjaga dengan baik sampai ke tangan nasabah yang berhak melihatnya.

Kata Kunci: Kriptografi, Steganografi, Data Nasabah, Least Significant Bit, RC4, Keamanan Data Nasabah

1. PENDAHULUAN

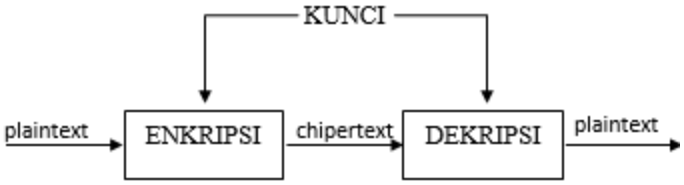
Pesatnya perkembangan teknologi sekarang ini membuat proses penyimpanan data menjadi lebih mudah. Akan tetapi, banyak orang yang kini telah meragukan keamanan apabila data disimpan di perangkat komputer. Hal ini tidak terlepas dari terjadinya berbagai tindakan penyadapan dan pemantauan oleh pihak-pihak yang tidak berkepentingan atau tidak bertanggung jawab sehingga kerahasiaannya kurang terjaga dalam mengamankan suatu data. Banyak cara untuk mengamankan data salah satunya dengan metode Kriptografi dan Steganografi.

Kriptografi secara umum adalah ilmu dan seni untuk menjaga kerahasian pesan. Sedangkan Steganografi adalah seni untuk menyembunyikan pesan dalam media digital sedemikian rupa sehingga orang lain tidak menyadari ada sesuatu pesan di dalam media tersebut. Dalam Kriptografi dan Steganografi maka data yang dianggap rahasia akan disamarkan dengan sedemikian rupa sehingga jika data itu bisa didapatkan maka tidak akan bisa dimengerti oleh pihak yang tidak berhak. Adapun salah satu metode yang dapat digunakan pada teknik kriptografi adalah Least Significant Bit (LSB) dan RC4 [1] [3].

2. METODOLOGI PENELITIAN

Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyinkan pesan. Namun pada pengertian modern kriptografi adalah ilmu yang berdasarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas. Jadi pengertian kriptografi modern adalah tidak saja berurusan hanya dengan penyembunyian pesan namun lebih pada sekumpulan teknik yang menyediakan keamanan informasi [7] [8] [10]

Pesan atau informasi yang dapat dibaca disebut dengan plaintext atau cleartext. Proses yang digunakan untuk menyamarkan atau menyembunyikan plaintext disebut enkripsi. Teks yang sudah disamarkan atau disembunyikan pada proses enkripsi berisi inforamasi yang tidak dapat atau tidak mudah dibaca dan dimengerti dengan jelas. Teks hasil enkripsi ini disebut dengan chipertext. Proses kebalikan enkripsi, yaitu mengubah chipertext menjadi plaintext disebut dengan proses dekripsi [6] [12] [14]



Gambar 1. Skema Enkripsi Simetris

Kelompok algoritma simetris adalah OTP, DES, RC2, RC4, RC5, RC6, IDEA, Twofish, Magenta, FEAL, SAFER, LOKI, CAST, Rijndael (AES), Blowfish, GOST, A5 Kasumi, dan lain-lain [6] [9] [16]

Steganografi merupakan suatu cabang ilmu yang mempelajari tentang bagaimana menyembunyikan atau informasi rahasia didalam informasi lainnya. Steganografi mempunyai sejarah yang hampir sama dengan kriptografi, keduanya banyak digunakan ketika zaman perang. Perbedaan steganografi dengan kriptografi terletak pada bagaimana proses penyembunyian data dan hasil akhir dari proses terebut. Kriptografi melakukan proses pengacakan data aslinya sehingga menghasilkan data terenkripsi yang benar-benar acak dan berbeda dengan aslinya, sedangkan steganografi menyembunyikan data dalam data lain yang akan ditumpangi sebelum dan setelah proses penyembunyian hampir sama [3] [5] [11] [15].

ISBN: 978-602-52720-2-8
Juli 2019
Hal: 505 – 509

Metode LSB merupakan metode steganografi yang sederhana dan mudah diimplementasikan. Metode ini menggunakan citra digital sebagai covertext. Pada susunan bit didalam sebuah byte (1 byte = 8 bit), ada bit yang paling berarti (MSB) dan bit yang paling kurang berarti (LSB). Sebagai contoh byte 11010010, angka bit 1 (pertama, digaris-bawahi) adalah bit MSB, dan angaka bit 0 (terahir, digaris-bawahi) adalah bit LSB. Bit yang cocok untuk diganti adalah bit LSB, sebab perubahan tersebut hanya mengubah nilai byte satu atau lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan byte tersebut menyatakan warna merah, maka perubahan satu bit LSB tidak mengubah warna merah tersebut secara berarti. Mata manusia tidak dapat membedakan perubahan kecil tersebut [2]
Sistem sandi RC4 dikembangkan oleh Ronald Rivest pada tahun 1984 merupakan sistem sandi stream yang paling banyak digunakan misalnya pada protokol SSL/TLS, (Stalling, 2006). RC4 merupakan sistem sandi stream berorientasi byte. Masukkan algoritma enkripsi RC4 merupakan sebuah byte, kemudian dilakukan operasi XOR dengan sebuah byte kunci, dan menghasilkan sebuah byte sandi [4]

3. ANALISA DAN PEMBAHASAN

3.1 Analisa Permasalahan

Penggunaan teknik kriptografi dengan algoritma RC4 dan steganografi dengan metode LSB diharapkan mampu melindungi dan mengamankan pesan rahasia pada saat pesan tersebut disampaikan melalui media internet dari pihak yang tidak berkepentingan, hal ini untuk menghindari terjadinya kejahatan seperti pengambilan atau penyadapan terhadap pesan rahasia yang disampaikan tersebut.

Metode LSB ini cukup rentan terhadap kehadiran steganalisis yang mencurigai adanya informasi rahasia didalamnya. Jika steganalisis berhasil mendeteksi keberadaan tersebut, maka pesan akan segera diketahui. Namun lain halnya apabila pesan tersebut dienkripsi terlebih dahulu menggunakan algoritma RC4 sebelum dilakukan proses penyisipan. Apabila steganalisis berhasil mengungkapkan pesan didalam citra stega, pesan tersebut masih tidak mudah diketahui karena masih dalam keadaan terenkripsi.

Peningkatan keamanan dengan mengkombinasikan teknik kriptografi dengan algoritma RC4 dan steganografi dengan metode LSB secara bersamaan akan menghasilkan tingkat keamanan pesan rahasia menjadi lebih baik. Proses keamanan pesan rahasia yang dilakukan adalah dengan menyisipkan pesan tersebut kedalam sebuah penampung (cover) yaitu berupa citra digital dengan menggunakan teknik steganografi, dimana pesan tersebut sebelum disisipkan sudah dienkripsi terlebih dahulu menggunakan teknik kriptografi.

1. Proses Enkripsi:
   a. Inisialisasi *S-Box* pertama, S[0], S[1], ..., S[255} dengan bilanagn 0 sampai 255. Pertama isi secara berurutan S[0] = 0, S[1] = 2, S[3] = 3, ..., S[255] = 255.
      Proses inisialisasi *S-Box* (*Array* S):
      For i = 0 to 255
      S[i] i = i
   b. Kemudian inisialisasi array lain (*S-Box lain*), misal *array* K dengan panjang 256. Isi *array* K dengan kunci diulangi samapai seluruh *array* K[0], K[1], ..., K[255] terisi seluruhnya.
      Proses inisialisasi *S-Box* (*array* K):
      Array kunci // array dengan panjang kunci ”*length*”.
      for i = 0 to 255
      K[1] = Kunci [i mod length]
   c. Kemudian lakukan langkah pengacakan *S-Box.*
      Proses pengacakan *S-Box*:
      I = 0 ; j = 0
      for i = 0 to 255
      {
      j = (j + S[i] + K[i] mod 255
      Swap S[i] dan S[i]
      }
   d. Setelah itu buat pseudo random byte, dengan langkah sebagai berikut:
      Pseudo *Random byte*:
      i = (i + 1) mod 255
      j = (j + S[i] mod 255
      Swap S[i] dan S[j]
      T = (S[i] + S[j] mod 255
      K = S[t]

ISBN: 978-602-52720-2-8
Juli 2019
Hal: 505 – 509

Byte K di-Xor-kan dengan plainteks untuk menghasilkan chiperteks, atau di-Xor-kan dengan chiperteks untuk menghasilkan plainteks

2. Proses Dekripsi:
   a. Ubah chiperteks kedalam bentuk biner.
   b. Byte K di-Xor-kan dengan pseudo random byte dengan chiperteks.

Berikut adalah contoh kasus untuk penerapan algoritma RC4 dengan menggunakan mode 5 byte, dengan menyajikan data sebagai berikut:

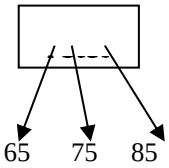
Plainteks: " S T A N D A R T "

Kunci : " B U K A [spasi] k u n c i "

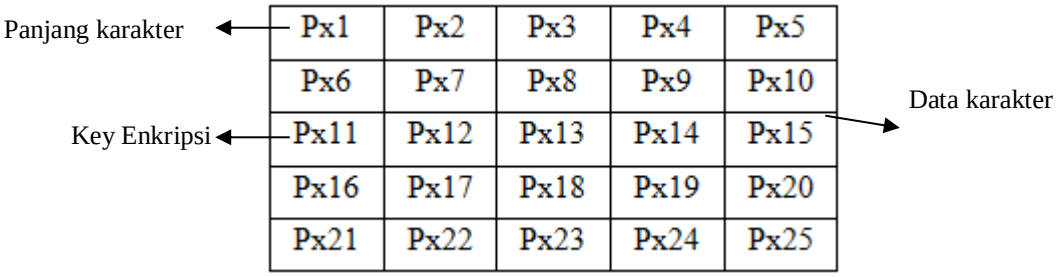
Chiperteks] . ˜ ă ŕ k u

Kunci S T A N D A R

Teknik dalam penyisipan sebuah data dalam gambar ini menggunakan metode LSB(Least Significant Bit), dimana data tersebut akan disisipkan pada bit-bit rendah (4 bit bawah) tetapi pada bit-bit ganjil dari nilai RGB sebuah pixel (satuah data terkecil yang membentuk gambar). 2 bit ke dalam nilai R dan 2 bit lagi ke dalam nilai B, sehingga satu karakter akan membutuhkan 2 buah pixel penampung. Misalkan langkah-langkahnya untuk penyisipan karakter "AKU", dengan asumsi sudah dilakukan pengacakan data dengan metode RC4, maka akan dilakukan tahapan-tahapan sebagai berikut:

1. 

   Dari tiap-tiap karakter akan diambil nilai dari Kode ASCII-nya.
2. Setalah itu akan diubah menjadi nilai biner sehingga dihasilkan perhitungan sebagai berikut:
   a. 65 = 01000001, b. 75 = 01001011, c. 85 = 01010101
3. Kemudian mengambil nilai dari tiap-tiap *pixel* gambar yang akan disisipi. Seperti pada gambar 1.

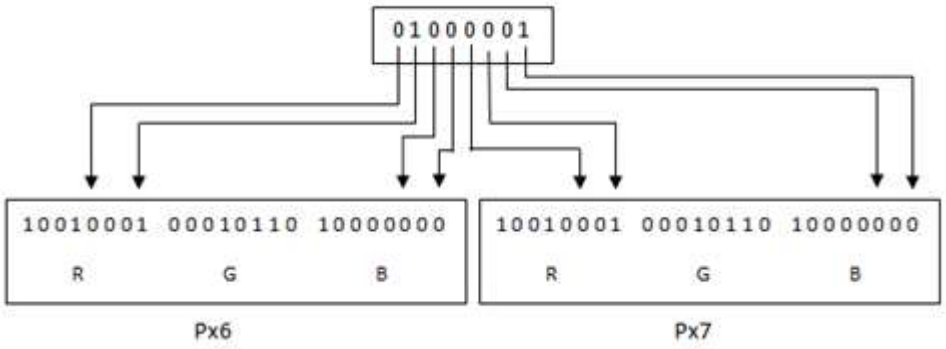


Gambar 2. Ilustrasi *pixel* sebuah image

Dari *pixel-pixel* diatas maka px1 (*pixel* 1) – px5 (*pixel* 5) digunakan untuk menampung panjang karakter, yang berfungsi sebagai batas pengambilan data-data yang telah tersisipi oleh karakter-karakter lain. Kemudian px6 (*pixel* 6) – px20 (*pixel* 20) sesuai kebutuhan penampungan data digunakan untuk menampung data-data karakter, dan selanjutnya px21 (*pixel* 21) sampai seterusnya digunakan untuk menyimpan elemen-elemen matrik enkripsi. Misalkan data-data tiap *pixel* adalah sebagai berikut:

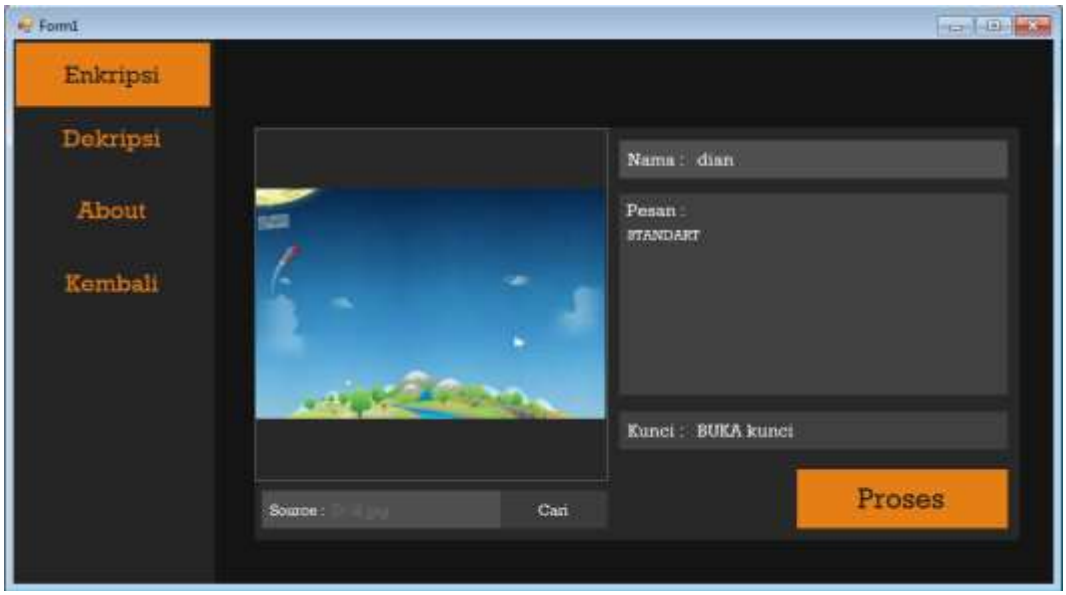
a. Px6 -> R = 145, G = 22, B = 128
b. Px7 -> R = 150, G = 22, B = 129
c. Px8 -> R = 155, G = 21, B = 130
d. Px9 -> R = 220, G = 19, B = 131
e. Px10 -> R = 215, G = 30, B = 125
f. Px7 -> R = 214, G = 16, B = 150

ISBN: 978-602-52720-2-8
Juli 2019
Hal: 505 – 509

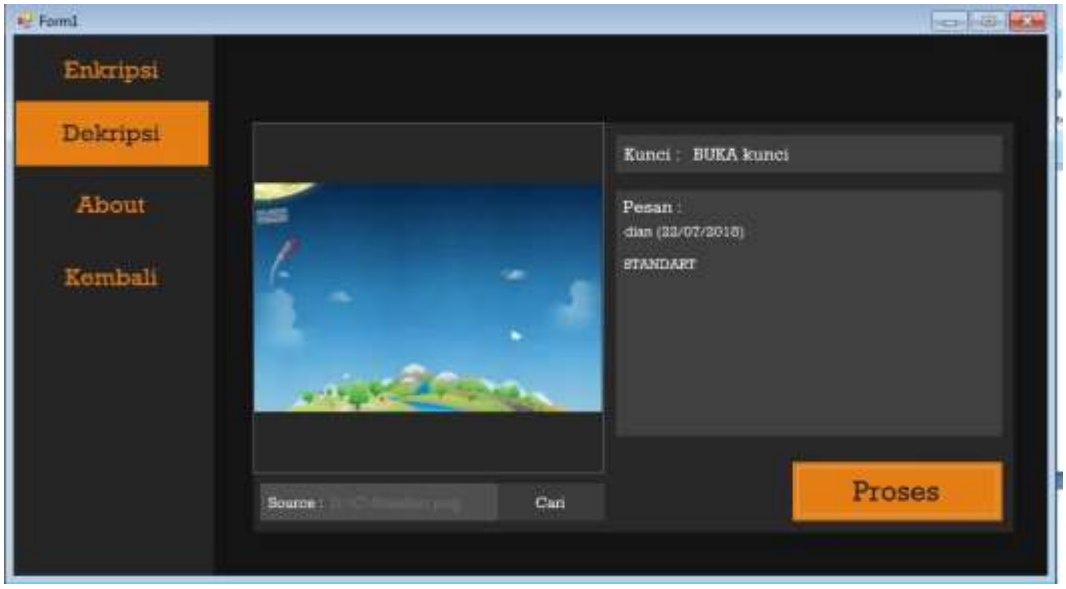


Gambar 3. Ilustrasi Penyisipan

Gambar berikut merupakan hasil saat program di jalankan.



Gambar 4. Form Enkripsi



Gambar 5. Form Deskripsi

ISBN: 978-602-52720-2-8
Juli 2019
Hal: 505 – 509

4. KESIMPULAN

Dari hasil perancangan aplikasi steganografi pengamanan data nasabah di *Standard Chartered Bank* maka diperoleh suatu kesimpulan sebagai berikut:

1. Dengan menggunakan metode LSB dan RC4 ternyata dapat mengamankan data nasabah pada *Standard Chartered Bank.*
2. Dengan dibangunnya aplikasi steganografi ternyata dapat membantu *Standard Chartered Bank* dalam mengamankan data nasabah.
3. Dengan menguji sistem yang telah dirancang untuk melihat sejauh mana kinerjanya dalam pemecahan permasalahan mengenai pengamanan data nasabah.
4. Dengan dibangunnya sistem yang telah dirancang aplikasi dapat menjadikan solusi dalam pengamanan data nasabah

REFERENCES

[1] Champakamala, B. S., Padmini, K., Professors, R. D. K. A., & Bosco, D. (2014). Least Significant Bit algorithm for image steganography Overview of Steganography. International Journal of Advanced Computer Technology.
[2] Gupta, N., & Sharma, N. (2014). Dwt and LSB based Audio Steganography. ICROIT 2014 - Proceedings of the 2014 International Conference on Reliability, Optimization and Information Technology. https://doi.org/10.1109/ICROIT.2014.6798368
[3] Roy, S., Parida, J., Singh, A. K., & Sairam, A. S. (2012). Audio steganography using LSB encoding technique with increased capacity and bit error rate optimization. https://doi.org/10.1145/2393216.2393279
[4] Dumitrescu, S., & Wu, X. (2005). A new framework of LSB steganalysis of digital media. IEEE Transactions on Signal Processing. https://doi.org/10.1109/TSP.2005.855078
[5] Masud Karim, S. M., Rahman, M. S., & Hossain, M. I. (2011). A new approach for LSB based image steganography using secret key. 14th International Conference on Computer and Information Technology, ICCIT 2011. https://doi.org/10.1109/ICCITechn.2011.6164800
[6] Haji, W. H., & Mulyono, S. (2012). Implementasi Rc4 Stream Cipher Untuk Keamanan Basis Data. Implementasi Rc4 Stream Cipher Untuk Keamanan Basis Data.
[7] Hakim, E. L., Khairil, & Utami, F. H. (2014). Aplikasi Enkripsi Dan Deskripsi Data Menggunakan Algoritma Rc4 Dengan Menggunakan Bahasa Pemrograman Php. Jurnal Media Infotama.
[8] Ruri Hartika Zain, S. Kom, M. K. (2012). Perancangan Dan Implementasi Cryptography Dengan Metode Algoritma Rc4 Pada Type File Document Menggunakan Bahasa Pemrograman Visual Basic 6 . 0. Jurnal Momentum ISSN : 1693-752X.
[9] Nugroho, at al. (2016). Aplikasi Keamanan Email Menggunakan Algoritma Rc4. Jurnal SAINTIKOM.
[10] Basuki Rakhmat; Muhammad Fairuzabadi. (2010). Steganografi Menggunakan Metode Least Significant Bit Dengan Kombinasi Algoritma Kriptografi Vigenère Dan Rc4. Zhurnal Eksperimental'noi i Teoreticheskoi Fiziki.
[11] Harsa, A. K. (2014). KEAMANAN DATA DENGAN MENGGUNAKAN ALGORITMA RIVEST CODE 4 (RC4) DAN STEGANOGRAFI PADA CITRA DIGITAL. INFORMATIKA Mulawarman Februari.
[12] Siswanto, Feriadi, Gunawan Pria Utama, Aditya Firdaus Achmad. (2016). Pengamanan Data Dengan Menggunakan Algoritma Kriptografi Aes , Rc4 Dan Kompresi Lz77. Seminar Nasional Telekomunikasi Dan Informatika (SELESIK 2016).
[13] Busran, & Mandani, P. (2012). Analisa Komputasi Enkripsi Dan Dekripsi Dara Gambar, Teks Dan Audio Dengan Menggunakan Algoritma RC4, Berbasis Visual Basic 6.0. Jurnal Teknologi Informasi & Pendidikan.
[14] Pria Utama, G., Firdaus Achmad, A., Siswanto, & Feriadi. (2016). Pengamanan Data Dengan Menggunakan Algoritma Kriptografi Aes, Rc4 Dan Kompresi Lz77 Berbasis Java Pada Badan Karantina Pertanian. Seminar Nasional Telekomunikasi Dan Informatika Aditya Firdaus A. Seminar Nasional Telekomunikasi Dan Informatika.
[15] Mesran, M. (2012). APLIKASI PENGAMANAN DATA TEKS PADA CITRA BITMAP DENGAN MENERAPKAN METODE LEAST SIGNIFICANT BIT (LSB). *Pelita Informatika: Informasi Dan Informatika*, *2*(1).