IMPLEMENTASI PENYISIPAN PESAN PADA CITRA DIGITAL MENGGUNAKAN METODE LEAST SIGNIFICANT BIT (LSB) DAN ENKRIPSI ONE TIME PAD

Risqo Maulana[1], Achmad Wahid Kurniawan, S.Si, M.Kom[2]
Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
Jl. Nakula I No. 5-11, Semarang, Jawa Tengah 50131 - (024) 3517261
E-mail : risqomaulana@gmail.com.com[1], wahid@dsn.dinus.ac.id[2]

Abstrak

Keamanan dan kerahasiaan informasi merupakan aspek penting yang dibutuhkan dalam proses pertukaran informasi terlebih bila sudah menyangkut karya cipta salah satu bentuknya yaitu citra (image) yang disajikan secara visual, sebuah karya cipta harus dilindungi supaya tidak ada penyalahgunaan atau pengakuan sebuah karya karena dapat merugikan pemiliknya. Sebab itu sebuah karya perlu adanya identitas pemilik. Metode Least Significant Bit (LSB) merupakan salah satu teknik penyisipan teks atau pesan kedalam data digital seperti data citra, maka data pesan bisa dijadikan sebagai identitas pemilik. LSB akan mengubah nilai bit dari setiap piksel pada cover sesuai dengan nilai biner pada pesan secara berurutan. Peneliti akan menggabungkan algoritma LSB dengan algoritma One Time-Pad (OTP) untuk mendapatkan bentuk pesan yang acak atau terenkripsi sehingga pesan tidak mudah untuk dimanipulasi. Namun, citra yang tersisipi pesan akan mengalami penurunan kualitas citra sehingga perlu dilakukan evaluasi kualitas citra dengan perhitungan nilai Mean Square Error (MSE) dan Peak Signal to Noise Ratio (PSNR). Hasil pengujian menunjukkan bahwa gambar dengan resolusi 512 x 512 piksel menghasilkan nilai MSE : 0,0000762939 dan PSNR(db): 79,3399, gambar dengan resolusi 256 x 256 piksel MSE : 0,0031 dan PSNR(db) : 73,3193, serta gambar dengan piksel 128 x128 piksel menghasilkan MSE : 0,012 dan PSNR(db) : 67,2987

Kata kunci : *Steganografi, Keamanan, Least Significant Bit, One Time-Pad*

Abstract

Security and confidentiality of information is an important aspect which needed in exchange of information especially when it comes to copyrighted works that form one image is presented visually, a copyright work must be protected so that there is no abuse or recognition of a work bcause it can be detrimental to the owner. Because of it is necessary for the owner's identity. Least Siginificant Bit (LSB) method is one of the text insertion techniques or message into digital data such as image data, then the message data can be used as the owner's identity. LSB will change the bit value of each pixel on the cover in accordance with the binary value of the message sequentially. Researchers will combine LSB and One Time-Pad (OTP) algorithm to get a random shape or encrypted message so that the message is not easy to manipulate. However, the insertion message image will be decreased so that the image quality necesssary to evaluate the image quality by calculating Mean Square Errir (MSE) and Peak Signal to Noise Ratio (PSNR) value. The test results indicate that the images with a resolution of 512 x 512 pixels produce MSE: 0.0000762939 and PSNR (db): 79.3399, images with a resolution of 256 x 256 pixels MSE: 0.0031 and PSNR (db): 73.3193, as well as 128 x128 pixel image with pixels produce MSE: 0.012 and PSNR (db): 67.2987

Keywords : *Steganograph, security, Least Significant Bit, One Time-Pad*

1. PENDAHULUAN

1.1 Latar Belakang

Keamanan dan kerahasiaan data pada jaringan komputer saat ini menjadi isu yang sangat penting dan terus berkembang sehingga kemajuan bidang jaringan komputer dengan konsep *open system* akan memberi peluang untuk mengakses kawasan – kawasan vital tersebut. Sebab itu data, informasi perlu dilakukan pengamanan [1]. Selain itu hal yang menjadi permasalahan adalah hak cipta, sebuah karya cipta harus dilindungi supaya tidak ada penyalahgunaan atau pengakuan sebuah karya karena dapat merugikan pemiliknya. [2]

Salah satu sarana untuk mengamankan sebuah karya cipta yakni pada data digital seperti foto yakni dengan menggunakan teknik *watermarking*, dengan *watermarking* identitas dalam sebuah data digital dapat disembunyikan sehingga dapat dijadikan tanda identifikasi yang tidak terdeteksi, seperti data penulis atau informasi hak cipta. Namun apabila identitas dari sebuah karya cipta mudah terdeteksi maka informasi dapat disalahgunakan, sehingga data yang berupa pesan informasi hak cipta perlu diamankan kembali. [3]

Kriptografi merupakan sarana untuk mengamankan sebuah pesan dengan cara mengacak isi pesan sehingga pesan sulit untuk dibaca, sehingga dapat digunakan untuk meningkatkan aspek keamanan suatu informasi. Algoritma kriptografi yang baik akan memerlukan waktu yang lama untuk memecahkan data yang telah disandikan [4]. Suatu data yang tidak disandikan disebut *plaintext* sedangkan data yang telah disandikan disebut *ciphertext*. Proses yang dilakukan untuk mengubah plaintext menjadi *ciphertext* disebut enkripsi *(encryption)* sedangkan proses yang dilakukan untuk mengubah ciphertext menjadi plaintext disebut dekripsi *(decryption)* [1].

Kriptografi saat ini telah menjadi salah satu syarat penting dalam keamanan teknologi informasi terutama dalam pengiriman pesan rahasia. Pengiriman pesan rahasia sangat rentan terhadap serangan dari luar seperti penyadapan, pemutusan komunikasi maupun pengubahan isi pesan [1]. Ada beberapa metode dalam teknik steganografi yakni metode vigenere cipher yang merupakan algoritma kriptografi klasik namun metode ini sudah dapat dipecahkan dengan analisa frekuensi [5]. *One time pad* (OTP) adalah salah satu teknik enkripsi pesan yakni satu pad hanya digunakan sekali *(one time)* saja untuk mengenkripsi pesan. Setelah kunci digunakan maka kunci dihancurkan sehingga teknik OTP menghasilkan keamanan yang sempurna. Pesan yang sudah terenkripsi meskipun bentuknya acak dan tidak dapat dibaca dengan jelas akan tetapi masih menimbulkan kecurigaan bahwa teks acak tersebut berisi sebuah informasi penting, maka diperlukan penggabungan dari teknik kriptografi [6] [7].

Ada beberapa teknik dalam steganografi yakni *Most Significant Bit* (MSB) yakni penyisipan bit pesan terhadap bit yang paling berarti, misalkan pada bit 11010010 angka yang bergaris bawah merupakan bit yang berarti, bit tersebut membunyai nilai yang besar sehingga adanya perubahan nilai bit MSB yang besar akan memberikan efek perubahan warna pada citra y ang dapat dibedakan secara kasat mata [8]. *Least Significant Bit* (LSB) merupakan metode dengan menyisipkan bit pesan pada bit terakhir yakni bit yang tidak berarti atau bit yang mempunyai nilai paling sedikit, itu berarti hanya akan memberikan perubahan nilai satu lebih tinggi maupun satu lebih rendah, perubahan yang sedikit ini tidak dapat dibedakan secara kasat mata dan dalam implementasi pada konsep steganografi sebab tidak mengubah tampilan citra

digital secara signifikan ketika citra sudah disisipi pesan. Teknik ini memberikan kinerja yang lebih baik dan merupakan teknik yang aman untuk pesan rahasia sehingga teknik LSB dapat digunakan untuk metode *watermarking* [3] [9] [8] .

Steganogafi memiliki dua proses, yaitu *encoding* dan *decoding*. *Encoding* merupakan proses penyisipan pesan kedalam media penampung *(covertext)* dalam hal ini adalah gambar/citra digital, sedangkan *decoding* adalah proses ekstraksi pesan dari gambar *stego (stegotext).* Kedua proses tersebut mungkin memerlukan kunci rahasia *(stegokey)* untuk proses penyisipan pesan dan ekstraksi pesan, hanya pihak yang berhak saja yang dapat melakukan penyisipan dan ekstraksi pesan. Penggabungan dua metode kriptografi dan steganografi dapat meningkatkan keamanan sebuah pesan, karena pesan yang akan disisipkan kedalam sebuah media gambar akan dilakukan proses enkripsi terlebih dahulu sehingga pesan yang sudah tersembunyi sudah berupa pesan acak [8].

Pada Penelitian ini peneliti menggunakan 90 dataset yakni 30 file citra dengan format *bmp, 30 file citra dengan format *jpg, dan 30 file citra dengan format *png. Dengan masing masing format citra mempunyai resolusi 512 x 512 piksel, 256 x256 piksel, dan 128 x 128 piksel. Semua data set akan dilakukan proses enkripsi dan dekripsi menggunakan metode *One-Time pad* dan proses *Embedded* dan *Extract* menggunakan teknik *Least Significant Bit (LSB).*

Namun citra yang tersisipi data akan pengalami penurunan kualitas citra akan menurun sehingga perlu adanya evaluasi kualitas citra yang telah disisipi secara obyektif yakni menghitung nilai *Mean Square Error* (MSE) dan *Peak Signal* to *Noise Ratio* (PSNR) [10]

1.2 Rumusan Masalah

1. Bagaimana mengenkripsi dan mendekripsi pesan menggunakan metode *Least Significant Bit* (LSB) dan metode *One – Time Pad*.
2. Menganalisa kualitas citra setelah tersisipi pesan menggunakan teknik MSE dan PSNR.

1.3 Batasan Masalah

1. Penyisipan teks hanya dilakukan pada file image dengan format .jpeg, .bmp, dan .png dengan masing masing mempunyai resolusi 512 x 512 piksel, 256 x 256 piksel, dan 128 x 128.
2. Pesan yang disisipkan hanya dalam bentuk teks karakter A-Z dan diketik secara manual.
3. Tidak membahas perubahan ukuran file citra setelah disisipkan pesan teks.

1.4 Tujuan Penelitian

1. Mengamankan pesan dengan metode *Least Significant Bit* (LSB) dan metode *One – Time Pad.*
2. Menganalisa kualitas citra hasil steganografi sehingga dapat menentukan jenis citra yang layak untuk dilakukan penyisipan.

2. METODE PENELITIAN

Penelitian ini merupakan penelitian eksperimental, yaitu penelitian dengan mencatat langsung hasil percobaan sebagai media pengumpulan data. Pengumpulan data juga dilakukan dengan perhitungan dan analisa visual untuk mengetahui perbandingan kualitas citra setelah disisipkan pesan.

2.1 Pengumpulan Data

Data yang digunakan untuk untuk implementasi steganografi dengan metode LSB adalah data citra digital. Citra digital yang digunakan yaitu citra standar dan pengumpulan data yang digunakan yaitu teknik langsung, dimana data diperoleh secara langsung dari internet.

Pengujian citra digital tersebut menggunakan citra digital dengan format *bmp,*jpeg, dan *png. Ukuran

(dimensi) citra yang digunakan adalah citra dengan resolusi 512 x 512 px, 256 x 256 px dan 128 x 128 px. Setiap format dan ukuran citra diambil beberapa sample yang selanjutnya akan digunakan pada proses implementasi steganografi dengan metode LSB.

2.2 Algoritma One Time Pad

Secara sederhana proses enkripsi dapatdituliskan sebagai berikut :

ci = (pi + ki) mod 26 ... . (2.1)

sedangkan proses dekripsi dituliskan sebagai berikut :

pi = (ci – ki) mod 26 ... . (2.2)

dengan:

c : chipertext (pesan acak) p : plaintext (pesan asli)

k : kunci rahasia yang digunakan

Berikut adalah proses enkripsi pesan : Misalkan pesan yang akan dikirim adalah 'RISQO' dengan kunci 'BUNUH' tetapkan indeks masing – masing karakter ke dalam nilai numerik seperti "0" ke A dan seterusnya.

Tabel 2.1 Indeks Karankter

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9

K	L	M	N	O	P	Q	R
10	11	12	13	14	15	16	17

S	T	U	V	W	X	Y	Z
18	19	20	21	22	23	24	25

Dengan menggunakan rumus enkripsi *one-time pad* pi = (ci – ki) mod 26 maka :

(R + B) mod 26 = (17 + 1) mod 26 = 18 (S)

(I + U) mod 26 = (8 + 20) mod 26 = 2 (C)

(S + N) mod 26 = (18 + 13) mod 26 = 5 (F)

(Q + U) mod 26 = (16 + 20) mod 26 = 10 (K)

(O + H) mod 26 = (14 + 7) mod 26 = 21 (V)

Sehingga diperoleh *ciphertext* **'S C F K V'**

Selanjutnya lakukan dekripsi dengan rumus pi = (ci – ki) mod 26 maka:

(S - B) mod 26 = (18 - 1) mod 26 = 17 (R)

(C - U) mod 26 = (2 - 20) mod 26 = 8 (I)

(F - N) mod 26 = (5 - 13) mod 26 = 18 (S)

(K - U) mod 26 = (10 - 20) mod 26 = 16 (Q)

(V - H) mod 26 = (21 - 7) mod 26 = 14 (O)

Sehingga diperoleh *plaintext* = '**R I S Q O**'

2.3 Least Significant Bit

Metode LSB merupakan metode steganografi yang paling sederhana dan mudah diimplementasikan. Metode ini menggunakan citra digital sebagai *covertext*. Pada susunan bit di dalam sebuah byte (1 *byte* = 8 bit), ada bit yang paling berarti (*most significant bit* atau MSB) dan bit yang paling kurang berarti (*least significant bit* atau LSB). Sebagai contoh byte 1 101001 0, angka bit 1 (pertama, digaris-bawahi) adalah bit MSB, da angka bit 0 (terakhir,digaris-bawahi) adalah bit LSB. Bit yang cocok untuk diganti adalah bit LSB, sebab perubahan tersebut hanya mengubah nilai *byte* satu 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 [8].

Misalkan segmen pixel - pixel citra/gambar sebelum penambahan bit - bit adalah:

00110011 10100010 11100010
10101011 00100110 10010110
11001001 11111001 10001000
10100011

Pesan rahasia (yang telah dikonversi ke sistem biner) misalkan '**1110010111**', maka setiap bit dari pesan tersebut menggantikan posisi LSB yang ada pada bit terakhir.

00110011 10100011 11100011

10101010 00100110 10010111
11001000 11111001 10001001
10100011

2.4 Pengujian

Kualitas media penampung setelah ditambahkan pesan rahasia tidak jauh berbeda dengan kualitas media penampung sebelum ditambahkan pesan. Setelah penambahan pesan rahasia, kualitas citra penampung tidak jauh berubah, masih terlihat dengan baik. Sehingga pengamat tidak mengetahui kalau di dalam citra tersebut terdapat pesan rahasia. Untuk mengukur kualitas citra steganografi diperlukan suatu pengujian secara obyektif. Pengujian secara objektif adalah dilakukan dengan menghitung nilai PSNR.

Peak Signal to Noise Ratio (PSNR) adalah perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal tersebut. PSNR diukur dalam satuan desibel. Pada penelitian ini, PSNR digunakan untuk mengetahui perbandingan kualitas citra *cover* sebelum dan sesudah disisipkan pesan. Untuk menentukan PSNR, terlebih dahulu harus ditentukan MSE *(Mean Square Error).* MSE adalah nilai *error* kuadrat rata-rata antara citra *cover* dengan citra tersteganografi, yakni untuk membandingkan kualitas rata rata citra sebelum dan sesudah tersisipi pesan. Secara matematis dapat dirumuskan sebagai
berikut [10]:

$$MSE = \frac{1}{M\,N}\sum_{y=1}^{M}\sum_{x=1}^{N}[\mathrm{I}(x,y) - \mathrm{I}'(x,y)]^2$$

Dimana :

MSE = Nilai *Mean Square Error* citra steganografi
M = Panjang citra stego
N = Lebar citra stego (dalam *pixel)*
I(x,y) = nilai piksel dari citra sebelum disisipi pesan
I'(x,y) = nilai piksel pada citra yang sudah disisipi pesan

Setelah diperoleh nilai MSE selanjutnya nilai PSNR dapat dihitung dari kuadrat nilai maksimum dibagi dengan MSE. Secara matematis, nilai PSNR dirumuskan sebagai berikut :

$$PSNR = 10\ log_{10}\left(\frac{MAXi^2}{MSE}\right)$$

$$= 20\ log_{10}\ \frac{MAX}{MSE^{1/2}}$$

$$= 20 * log\ \left(\frac{MAX}{\sqrt{MSE}}\right)$$

Dimana:

MAXi = nilai maksimum dari pixel citra yang digunakan

3. HASIL DAN PEMBAHASAN

Pada proses implementasi penyisipan pesan pada citra digital menggunakan dataset citra. Untuk file pengujian menggunakan 90 file citra dengan 3 jenis format file dan 3 jenis resolusi. Macam dari jenis file citra yang akan di uji adalah 30 file *bmp, bmp adalah bitmap terbentuk dr kumpulan garis/piksel. Kualitas gambar tergantung piksel. Jika gambar diperbesar akan pecah. File yang akan diuji terdiri dari 10 file *bmp dengan resolusi 512 x 512 piksel, 10 file dengan 256 x 256 piksel serta 10 file dengan resolusi 128 x 128 piksel. Semua file citra akan dilakukan proses steganografi yakni menggunakan metode LSB, namun sebelum proses penyisipan teks dilakukan, sebelumnya harus sudah dilakukan proses esnkripsi yakni pengacakan pesan sehingga pesan yang disisipkan bukan lagsi pesan asli melainkan pesan acak yang tidak ada maknanya sehingga tingkat keamanan aka lebih meningkat. Dalam penelitian ini data pesan terdiri dari 25 karakter yakni plaintext =”PERCOBAANKUAKANTERDETEKSI” untuk melakukan proses enkripsi membutuhkan key = “UNIVERSITASDIANNUSWANTOR

O”

Dalam hal ini jumlah karakter ada 25, 1 karakter terdiri dari 8 bit biner. Jika jumlah karakter ada 25 maka jumlah bit menjadi 200 bit biner. Proses selanjutnya adalah menyisipkan bit – bit kedalam nilai piksel citra, namun supaya dapat diimplementasikan nilai dari piksel gambar dikonversi terlebih dahulu kedalam bit biner. Dibawah ini adalah sampel piksel yang diambil pada citra B3512 yakni file dengan format *bmp yang mempunyai resolusi 512 x 512 piksel.

Berikut adalah sample perubahan nilai bit dari pikse (1,1) sampai (1,20)

Tabel 3.1 Konversi Nilai dan Embedded

Piksel	Nilai Asli	Bit Asli	Bit LSB	Nilai LSB
(1,1)	193	11000001	11000000	192
(2,1)	198	11000110	11000111	199
(3,1)	195	11000011	11000010	194
(4,1)	195	11000011	11000010	194
(5,1)	200	11001000	11001001	201
(6,1)	201	11001001	11001000	200
(7,1)	199	11000111	11000111	199
(8,1)	202	11001010	11001010	202
(9,1)	197	11000101	11000100	196
(10,1)	198	11000110	11000111	199
(11,1)	196	11000100	11000100	196
(12,1)	192	11000000	11000001	193
(13,1)	192	11000000	11000000	192
(14,1)	193	11000001	11000000	192
(15,1)	190	10111110	10111111	191
(16,1)	186	10111010	10111010	186
(17,1)	198	11000110	11000110	198
(18,1)	184	10111000	10111001	185
(19,1)	182	10110110	10110110	182
(20,1)	179	10110011	10110011	179

Dari analisa tabel diatas, menjelaskan bahwa perubahan nilai hanya terpaut naik satu nilai, turun satu nilai, bahkan tetap. Sehingga perubahan warna yang tidak terlalu signifikan menjadikan perubahan warna pada gambar tidak terlihat perbedaanya secara kasat mata.

Dari jumlah citra yang digunakan sebagai bahan uji yakni berjumlah 90 file dengan 30 file citra dengan format *bmp, 30 file citra dengan format *jpg, dan 30 file citra dengan format *png. Dengan masing masing format citra mempunyai resolusi 512 x 512 piksel, 256 x256 piksel, dan 128 x 128 piksel, menunjukan bahwa gambar dengan resolusi 512 x 512 menghasilkan nilai MSE : 0,0000762939 dan PSNR(db): 79,3399, gambar dengan resolusi 256 x 256 piksel MSE : 0,0031 dan PSNR(db) : 73,3193, serta gambar dengan piksel 128 x128 piksel manghasilkan MSE : 0,012 dan PSNR(db) : 67,2987

4. KESIMPULAN DAN SARAN

4.1 Kesimpulan

1. Pesan berhasil di enkripsi dan dekripsi dengan *metode one time-pad.*
2. Pesan berhasil tersisipi dan terekstraksi pada semua sample citra baik dengan format *bmp, *jpg, *png dan pada resolusi 512 x 512 piksel, 256 x 256 piksel, serta 128 x 128 piksel.
3. Nilai MSE dan PNSR tidak berpengaruh pada format file citra baik *bmp, *png, tidak berpengaruh juga pada ukuran file. Namun nilai MSE dan PNSR dipengaruhi oleh ukuran piksel darri sebuah citra. Semakin besar resolusi citra maka nilai PNSR akan semakin besar begitu sebaliknya, PNSR semakin kecil apabila nilai resolusi semakin kecil.

4.2 Saran

1. Masih terbatas dengan 26 karakter yakni A-Z sehingga kombinasi masih terbatas dibandingkan 256 karakter yang dapat dikombinasikan dengan simbol – simbol.
2. Perlu dilakukan analisa lamanya waktu saat proses penyisipan pada masing – masing dataset.

5. DAFTAR PUSTAKA

[1]. H. dan S. Primaini, "Kriptografi Password Menggunakan Modifikasi Metode Affine Ciphers," *Jurnal Sigmata,* vol. II, no. 1, pp. 40-50, 2014.

[2]. S. M. Mastur, "Perlindungan Hukum hak kekayaan intelektual Dibidang Paten," *Jurnal Ilmiah Ilmu Hukum QISTI,* vol. 6, no. 1, pp. 65-81, 2012.

[3]. D. Chopra, P. Gupta, G. S. B.C dan A. Gupta, "Lsb Based Digital Image Watermarking For Gray Scale Image," *Jornal of Computer Engineering (IOSRJCE),* vol. 6, no. 1, pp. 36-41, 2012.

[4]. A. N. Tarigan, "Pembuatan Aplikasi Penyisipan Pesan pada File Mp3 Menggunakan Metode Parity Coding dan Enkripsi Caesar Cipher," *Pelita Informatika Budi Darma,* vol. VII, no. 2, pp. 50-56, 2014.

[5]. M. Fairuzabadi, "Implementasi Kriptografi Klasik Menggunakan Borland Delphi," *Jurnal Dinamika Informatika,* vol. IV, no. 2, pp. 65-78, 2010.

[6]. R. Munir, "Algoritma Enkripsi Citra dengan Pseudo One-Time Pad yang menggunakan Sistem Chaos," *Konferensi Nasional Informatika,* pp. 12-16, 2011.

[7] B. S. Waluyo poetro, A. Sugiharto dan S. N. Endah, "Kriptografi Citra Digital dengan Algoritma Rijndael dan Transformasi Wavelet Diskrit," dalam *Seminar Nasional Ilmu Komputer Universitas Diponegoro*, Semarang, 2010.

[8]. B. Rakhmat dan M. Fairuzabadi, "Steganografi menggunakan Metodw Least Significant Bit dengan Kombinasi Algoritma Kriptografi Vigenere dan RC4," *Dinamika Informatika,* vol. V, no. 2, pp. 1-17, 2010.

[9]. K. Anand dan E. R. Sharma, "Comparison of LSB and MSB Based Image Steganography," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 4, no. 8, pp. 906-909, 2014.

[10]. G. M. Male, W. dan E. Setijadi, "Analisa KUalitas Citra pada Stegnografi untuk Aplikasi E-goverment," dalam *Seminar Nasional Manajemen Teknologi XV*, 2012, 2012.

[11]. T. Cahyadi, "Implementasi Steganografi LSB dengan Enkripsi Vigenere cipher pada CItra Jpeg," *Transient,* vol. I, no. 4, pp. 281-288, 2012.

[12]. M. A. Sharma, M. R. Chaturvedi, M. Hemrajani dan M. D. Goyal, "New Improved And Robust Watermarking Technique based on 3rd LSB Subtitution Method," *International Journal of Scientific Research Publications,* vol. 2, no. 3, pp. 1-4, 2012.

[13]. R. Munir, Kiptografi, Bandung: Informatika, 2006.

[14]. A. Zelvina, S. Efendi dan D. Arisandi, "Perancangan Aplikasi

Pembelajaran Kriptografi Kunci Publik E1Gamal untuk Mahasiswa," *Jurnal Teknologi Informasi,* vol. I, no. 1, pp. 56-62, 2012.

[15]. Y. Saleem, M. Rahman, F. Hayat, F. Izhar dan M. Saleem, "Soeech Encyption Impelementation Of 'One Time Pad Algorithm' in Matlab," *Pakistan Journal of Science,* vol. LXV, no. 1, pp. 114-118, 2013.

[16]. S. Munawaroh dan F. A. Sutanto, "PEngolah Citra Digital untuk Identifikasi Uang Kertas," *Jurnal Teknologi Informasi DINAMIK,* vol. XV, no. 1, pp. 34-40, 2010.

[17]. A. R. Lubis, M. S. Lidya dan M. A. Budiman, "Perancangan Perangkat Lunak Steganografi Audio Mp3 Menggunakan Metode Least Significant Bit (LSB) dengan Visual Basic 6.0," *Jurnal Teknologi Informasi* , vol. I, no. 1, pp. 63-68, 2012.