Kajian Implementasi Perangkat Keras Metode Steganografi LSB Berbasis FPGA

Swelandiah E.P[1] dan Deny Rochman Arifatno[2]

[1]Jurusan Teknik Komputer, Universitas Gunadarma
[2]Jurusan Teknik Elektro, STTC
swelandiah@staff.gunadarma.ac.id, abu.n4b1l@gmail.com

Abstrak

Kebutuhan data dalam penggunaan informasi diharuskan adanya kebutuhan juga untuk melindungi data dari ancaman gangguan yang dapat merusak data atau ancaman kebocoran data sehingga dapat digunakan oleh pihak yang tidak berkepentingan. Permasalahan keamanan data di era ini sudah banyak diaplikasikan oleh beberapa perusahaan atau komunitas di berbagai bidang, seperti dalam penggunaan media internet, e-commerce dan lain-lain. Kemanan data yang dimaksud adalah menjaga integritas atau keutuhan data dari pihak yang tidak berkepentingan dengan menggunakan algoritma kemanan data seperti metode kriptografi, watermark atau steganografi. Steganografi adalah salah satu teknik yang sangat kuat dalam menyisipkan data pada sebuah turunan mutimedia seperti gambar, suara, video , teks, dan protokol. Terdapat 2 kategori umum pada steganografi gambar yaitu Domain Spasial dan Frekuensi. Domain spasial berbasis pesan tertanam (embedding message) terdapat teknik LSB (least significant bit) pada pixel gambar Saat ini teknik steganografi dapat dibangun pada perangkat keras FPGA. FPGA pada dasarnya merupakan perangkat untuk sistem tertanam (Embedded System) dengan konsep menggunakan bahasa pemrograman untuk perangkat keras dalam mendesain atau merancang desain elektronika berbasis digital atau gerbang-gerbang logika. Penulisan ini menjabarkan konsep awal implementasi FPGA pada teknik steganografi image dengan menggunakan metode LSB (Least Significant Bit).

Kata Kunci : Steganografi, LSB, FPGA

Pendahuluan

Data merupakan bentuk olah yang belum mempunyai arti bagi penerimanya dan masih memerlukan adanya suatu pengolahan. Data dapat berupa suatu keadaan, gambar, suara, huruf, angka, matematika, bahasa ataupun simbol-simbol lainnya yang bisa kita gunakan sebagai bahan untuk melihat lingkungan, obyek, kejadian ataupun suatu konsep yang akan menjadi sebuah informasi atau hak akses.

Kebutuhan data dalam penggunaan informasi diharuskan adanya kebutuhan juga untuk melindungi data dari ancaman gangguan yang dapat merusak data atau ancaman kebocoran data sehingga dapat digunakan oleh pihak yang tidak berkepentingan. Permasalahan keamanan data di era ini sudah banyak diaplikasikan oleh beberapa perusahaan atau komunitas di berbagai bidang, seperti dalam penggunaan media internet, e-commerce dan lain-lain. Menurut Rama I [7] kemanan data yang dimaksud adalah menjaga integritas atau keutuhan data dari pihak yang tidak berkepentingan dengan menggunakan algoritma kemanan data seperti metode kriptografi, watermark atau steganografi .

Salah satu konsep untuk kemanan data adalah dengan menggunakan algoritma yang dapat menjaga keutuhan data, dalam arti keutuhan isi data maupun ukuran data tidak mengalami perubahan saat proses transmisi data. Salah satu algoritma keamanan data yang sedang berkembang saat ini adalah algortima steganografi.

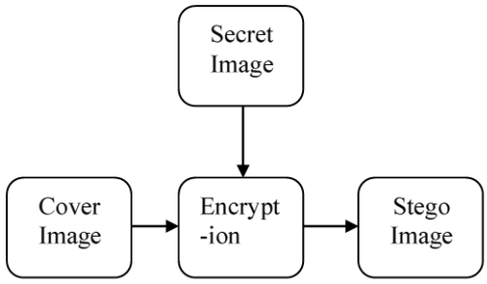
Menurut Kalpana Shanjay Shete,dkk [4], steganografi adalah salah satu teknik yang sangat kuat dalam menyisipkan data pada sebuah turunan mutimedia seperti gambar, suara, video , teks, dan protokol[4]. Steganografi berasal dari kata “steganos” yang berarti “tersem-

bunyi" dan "graphic" yang berarti tulisan, jadi steganografi berarti tulisan yang tersembunyi. Terdapat 2 kategori umum pada steganografi gambar yaitu Domain Spasial dan Frekuensi. Domain spasial berbasis pesan tertanam (embedding message) terdapat teknik LSB (least significant bit) pada pixel gambar . Saat ini teknik steganografi dapat dibangun pada perangkat keras FPGA. FPGA pada dasarnya merupakan perangkat untuk sistem tertanam (Embedded System) dengan konsep menggunakan bahasa pemrograman untuk perangkat keras dalam mendesain atau merancang desain elektronika berbasis digital atau gerbang-gerbang logika,

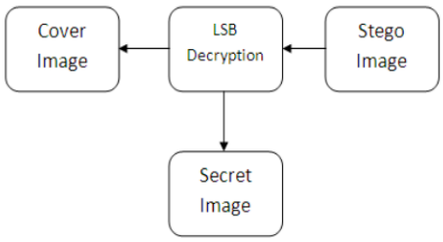
Artikel ini menjabarkan bebapa sumber pustaka yang menghasilkan arsitektur implementasi perangkat keras menggunakan metode steganografi LSB (Least Significant Bit) berbasis FPGA baik pada data gambar maupun teks. Penulisan ini juga mengusulkan topik penelitian baru dalam pengembangan arsitektur perangkat keras yang difokuskan pada desain arsitektur single chip pada perangkat keras terutama pada proses kompresi data image yang dapat mengefisiensikan penggunaan bandwidth jaringan pada proses pengiriman data. Atau desain arsitektur single chip pada lapisan keamanan data. Dengan menggunakan perangkat keras FPGA SPARTAN 6 dengan metode yang sama.

Steganografi Image

Apurva S.M,dkk menyatakan bahwa steganografi image terdapat 2 jenis gambar yaitu "Cover Image" dan "secret image". "Cover Image" adalah gambar yang digunakan untuk menyembunyikan gambar rahasia yang akan dikirim[1]. Diagram blok dari proses enkripsi disajikan pada gambar 1, untuk proses dekripsinya dapat dilihat pada gambar 2.

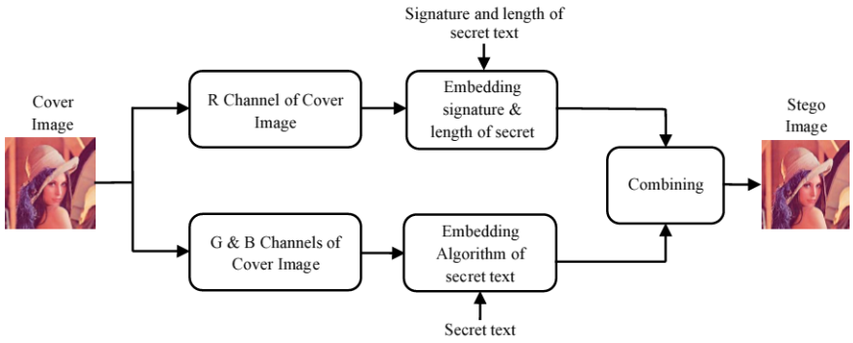


Gambar 1: Diagram blok proses enkripsi dari gambar

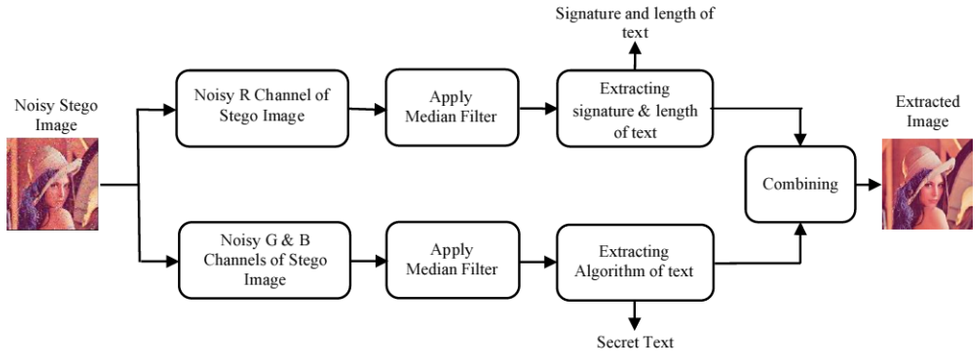


Gambar 2: Diagram blok proses Dekripsi dari Gambar

Berdasarkan penelitian yang dilakukan oleh E.A. Elshazly, Safey A, dkk mengatakan bahwa algoritma steganografi image berbasis LSB mempunyai 2 fase yaitu fase penanaman (embedding) dan fase ekstrasi [2]. Gambar 3 dan 4 adalah alur dari algoritma steganografi berbasis LSB pada masing-masing fase berdasarkan warna gambar.

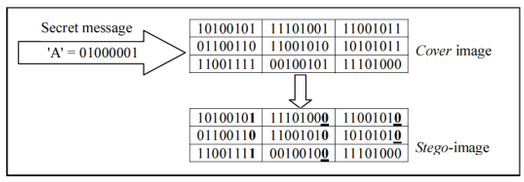


Gambar 3: Fase embedding

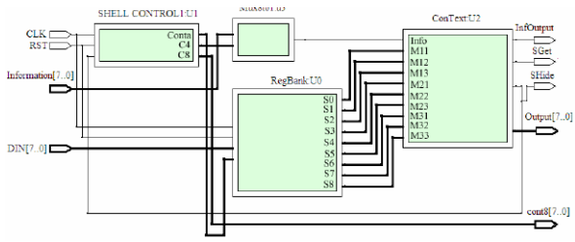


Gambar 4: Fase ekstrak

Dari gambar 3 dan 4 terlihat bahwa pada fase embedding "cover Image" terdiri dari saluran (channel) Merah, Hijau dan Biru, maka tanda dan panjang dari data rahasia tersimpan pada saluran merah, sementara bit pixel pada "secret text" tersimpan pada saluran hijau dan biru sebagai bentuk keamanan pesan dari luar. Setelah fase embedding maka dilakukan fase ekstak. Setelah alur pada kedua fase, gambar 5 ini adalah contoh dari teknik LS pada steganografi



Gambar 5: Proses Penyembunyian data pada LSB 24 bit



Gambar 6: Implementasi Teknik ConText

Implementasi metode LSB Pada Perangkat keras FPGA

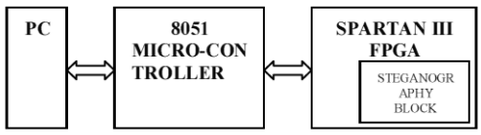
Saat ini teknik steganografi dapat dibangun pada perangkat keras FPGA. FPGA pada dasarnya merupakan perangkat untuk sistem tertanam (Embedded System) dengan konsep menggunakan bahasa pemrograman untuk perangkat keras dalam mendesain atau merancang desain elektronika berbasis digital atau gerbang-gerbang logika. Beberapa contoh implementasi steganografi menggunakan metode LSB pada FPGA yang berkembang berdasakan penelitian yang telah dilakukan. Berikut uraiannya

Arsitektur FPGA pada Teknik Steganografi ConText

Penelitian ini dilakukan oleh Edgar Gomez H, dkk, menghasilkan sebuah arsitektur perangkat keras yang menggunakan teknik ConText [3]. Gambar 6 adalah arsitektur yang dihasilkan sebagai implementasi dari teknik Steganografi ConText. Arsitektur perangkat keras ini dibangun menggunakan VHDL (Vhsic Hardware Description Language). Sementara pengujian outputnya menggunakan ModelSim pada Xilinx. Untuk proses sintesis, penempatan dan jalur menggunakan Quartus II dari Altera. Dan terakhir pengujian operasi untuk prototipe menggunakan Cyclone II EP2C35F672C6 dari Altera. Dengan simulink Matlab 7 dan DSP Builder versi 6.1.

Implementasi Steganografi pada FPGA

Penelitian ini dilakukan oleh Ankita Ganorkar,dkk, (2014) menggunakan metode LSB dengan mengilustrasikan komponen perangkat keras adalah sebagai berikut : PC, Mikrokontroler 8051 dan FPGA Spartan III. Dengan diagram blok pada chip disajikan pada gambar 7.

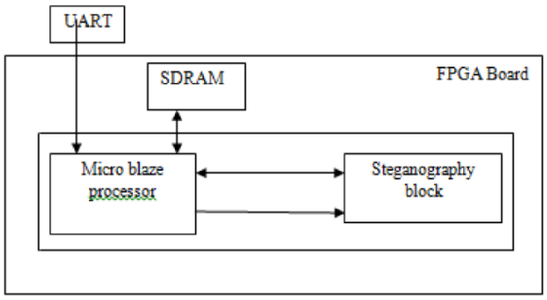


Gambar 7: Blok diagram implementasi pada FPGA

Blok diagram pada gambar 7 adalah implementasi dari Steganografi menggunakan metode 2/3 LSB. Dimana Mikrokontroler 8051 merupakan interface penghubung antara PC dan FPGA, serta memindahkan data dari/ke FPGA dan PC. Data disini adalah Cover Image dan Stego Image.

Implementasi FPGA menggunakan Metode Steganografi LSB.

Penelitian ini dilakukan oleh Pangavhane S.M, dkk [6] menghasilkan sistem arsitektur yang berbeda dengan peneltian sebelumnya oleh Ankita Ganorkar dkk [9], yaitu tidak menggunakan mikrokontroler melainkan menggunakan prosesor Micro blaze 32 bit RISC. Sistem arsitektur terlihat pada gambar 8.

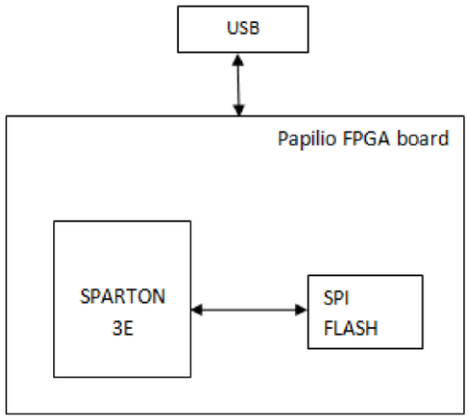


Gambar 8: Sistem Arsitektur

Desain implementasi ini menggunakan perangkat lunak XPS EDK 10.1 dan Matlab 7.5. Mengkonversi dari warna gambar yang asli ke dalam warna gambar abu-abu dan mengubah ukuran menjadi format 128*128 dengan menggunakan Matlab 7.5. Sedangkan desain coding menggunakan LSB encoding, Forward IWT, LSB Decoding dan Reverse IWT. Dan menggunakan IP core micro blaze yaitu prosesor RISC 32 bit.

Implementasi

Steganografi LSB pada Perangkat kerang menggunakan Matlab dan FPGA Penelitian ini dilakukan oleh Apurva S, dkk, menggunakan teknik steganografi image 2/3 LSB yang diimplementasikan pada perangkat keras FPGA dengan menggunakan Matlab, dengan menggunakan FPGA papan *Papilio* [1]. Dimana arsitektur dari FPGA Papilio dapat dilihat pada gambar 9.



Gambar 9: Arsitektur FPGA Papilio

Pada FPGA Papilio terdapat SPARTAN 3E dan SPI flash memory untuk implementasinya. Program dan gambar dari steganografi 2/3 LSB disimpan pada SPI flash memory dan di bangun menggunakan MATLAB.

Penelitian Lanjutan

Steganografi adalah salah satu teknik yang dapat digunakan dalam konsep keamanan data. Dimana keamanan data yang dimaksud adalah bagaimana menjaga integritas data. Integritas data yang dimaksud adalah menjaga keutuhan data, dalam arti keutuhan isi data maupun ukuran data tidak mengalami perubahan saat proses transmisi data. Algoritma Steganografi adalah salah satu contoh algoritma yang digunakan untuk menjaga keamanan data pada proses pengiriman. Pada saat ini algoritma Steganografi dapat diimplementasikan ke dalam bentuk perangkat keras yaitu FPGA metode yang digunakan adalah metode LSB (Least Significant Bit), karena metode ini sangat memungkinkan untuk digunakan dalam desain arsitektur keamanan pada perangkat keras. Dari beberapa hasil penelitian yang telah dijabarkan sebelumnya, maka penelitian selanjutnya dapat difokuskan pada desain arsitektur single chip pada perangkat keras terutama pada proses kompresi data image yang dapat mengefisiensikan penggunaan

bandwidth jaringan pada proses pengiriman data. Atau desain arsitektur single chip pada lapisan keamanan data. Dengan menggunakan perangkat keras FPGA SPARTAN 6.

Daftar Pustaka

[1] Apurva S.M and Prof.Sheetal G.K , "Hardware Implementation of LSB Steganography Using MATLAB and FPGA", in International Journal of Computer Science Trend and Technology, vol.3 Issue 4, July-August 2015.

[2] E.A.Elshazly, Safey A, R.M.Fikry S.M and O.Zahran M.El-Kordy, "FPGA Implementation of Robust Image Steganography Technique based on Least Significant Bit (LSB) in Spatial Domain", in International Journal of Computer Application (0975-8887), Vol 146, 2016

[3] [Edgar Gomez H, Claudia Feregrino U and Rene Cumplido, "FPGA Hardware Architecture of the Steganography ConText Technique", in 18th International Conference on Electronics, Communications and Computer, IEEE,2008

[4] [Kalpana Shanjay Shete, Manggal Patil and J.S.Chitode, "Least Significant Bit and Discrete Wavelet Transform Alghoritm for Image Steganography Employing FPGA", in International Journal Image, Graphi and Signal Processing, vol 6, 2016

[5] Linto Thomas, R. Jagadish and M. Pradeep, "FPGA Implementation of OFDM with Steganography", in International Journal of Computer Science and Mobile Computing, ISSN 2320-088X, vol 4, 2015

[6] [Pangavhane S.M and Punde S.S, " FPGA Implementation of LSB Steganography method", in IOSR Journal of Electronics and Communication Engeneering, e-ISSN : 2278-2834, p-ISSN:2278-8735, 2014.

[7] Rama I, "Wireless Secured Data Transmission Using Cryptographic Technique trough FPGA", in IJET, vol.8 No.1, Feb-Mar 2016

[8] Suraj Baddab, Ketan Khomane, Pratik D and Prof. Patharwalkal S, "Hardware Implementation of LSB Steganogrhapy for Data Security", in International Journal of Innovative Research Advanced Engineering, ISSN: 2349-2163, Vol. 2, 2015.

[9] Ankita Ganokar and Sujata Agrawal, " Implementastion of Steganogaphy on FPGA", International Journal of Recent Advances in Engineering & Technology, eISSN : 2347-2812, Vol :2, 2014.