SinarFe7
Seminar Nasional Fortei Regional 7

ISSN (Print) : 2621-3540
ISSN (Online) : 2621-5551

Rancang Bangun Sistem Pengaman Transmisi Video pada Pesawat Tanpa Awak

[1]Fery Setiawan, [2]Ronny Mardiyanto, [3]Astria Nur Irfansyah
Departemen Teknik Elektro, Fakultas Teknologi Elektro, Institut Teknologi Sepuluh Nopember
[1]ferykun@gmail.com,[2] ronny@elect-eng.its.ac.id, [3]irfansyah@ee.its.ac.id

***Abstrak*— Pentingnya pengamanan data transmisi video mendorong perkembangan algoritma enkripsi yang aman. Enkripsi tersebut dimaksudkan untuk mengubah video biasa menjadi gambar yang acak untuk mencegah orang lain mengakses video yang ditangkap oleh kamera *Unmanned Aerial Vehicle (UAV)*. Dalam tulisan ini, penulis mengusulkan proses yang sederhana dan aman untuk mengamankan gambar. Proses enkripsi gambar menggunakan *Pseudo Random Number Generator*. Gambar mula-mula dipotong menjadi beberapa bagian sesuai kebutuhan pengguna, kemudian potongan-potongan tadi dirangkai secara acak menggunakan algoritma *Linear Feedback Shift Register*. Karena enkripsi yang dihasilkan harus dapat dibaca kembali oleh pengguna maka dari itu perlu dilakukan dekripsi. Dekripsi bertujuan untuk menata kembali gambar yang dikirim secara acak menjadi sebuah gambar utuh yang benar. Berbagai tes dan analisis kemudian dilakukan untuk memeriksa kualitas gambar yang dienkripsi. Hasil pengujian membuktikan similaritas dari proses dekripsi yang dilakukan sebesar 98,24 persen.**

Kata kunci: Unmanned Aerial Vehicle, *enkripsi*, *dekripsi*, pseudo random, Linear Feedback Shift Register.

Abstract – The importance of securing video transmission data encourages the development of secure encryption algorithms. The encryption is intended to convert an ordinary video into a video with a random image to prevent intruders from accessing the video captured by the Unmanned Aerial Vehicle (UAV) camera. In this paper, the authors propose a simple and safe process for securing display of video. The image encryption process uses Pseudo Random Number Generator. The images were first cut into sections according to the user's needs, then the pieces were randomly assembled using the Linear Feedback Shift Register algorithm. Because the result of encryption must be readable by the user then it needs to be decrypted. Decryption aims to rearrange randomly sent images into a true intact image. A variety of tests and analyzes were performed to check the quality of the decrypted image. The test results prove the similarity between the original image with the result of decryption which is 98.24 percent.

Keywords: *Unmanned Aerial Vehicle*, encryption, decryption, *pseudo random*, *Linear Feedback Shift Register*

I. PENDAHULUAN

Perkembangan teknologi pesawat tak berawak belakangan ini sangatlah pesat. Penggunaan sistem seperti ini pada awalnya hanya digunakan pada militer yang bertujuan sebagai pengintai maupun sebagai peluru kendali. Namun seiring berjalannya waktu sistem ini dikembangkan untuk kebutuhan non-militer maupun komersial seperti pemadam api, pemeriksaan jalur pipa, fotografi maupun sebagai pengirim barang.

Salah satu keunggulan dari pesawat tak berawak adalah mampu mengirimkan data transmisi kepada pengguna dengan jarak tertentu. Salah satu data transmisi yang sangat sering dipakai adalah transmisi video. Sistem PAL(Phase Alternating Line) yang digunakan sebagai transmisi sangat mudah untuk diakses oleh orang lain, padahal untuk beberapa kasus, video transmisi bersifat rahasia dan hanya orang-orang tertentu yang boleh mengaksesnya. Untuk mengatasi hal ini, dibutuhkan sebuah sistem keamanan transmisi video yang hanya dapat diakses dengan benar oleh orang-orang tertentu.

Pada [9] penulis menyarankan dua teknik untuk mengenkripsi gambar dan kedua teknik menggunakan gambar sebagai kunci. Setiap piksel dari gambar asli XOR dengan setiap piksel dari gambar kunci untuk mendapatkan gambar yang dienkripsi. Penulis dalam [10] menyarankan penggunaan gambar cover untuk mengenkripsi gambar lain. Gambar cover akan digunakan untuk menyembunyikan gambar asli. Satu-satunya kelemahan dalam teknik yang diusulkan adalah bahwa gambar sampul dan gambar asli harus memiliki ukuran yang sama. Dalam tulisan ini, kami mengusulkan proses enkripsi gambar yang menggunakan substitusi serta transposisi yang pada gilirannya memberikan keamanan yang lebih baik daripada salah satu dari mereka yang digunakan.

ISSN (Print) : 2621-3540
ISSN (Online) : 2621-5551

II. METODE PENELITIAN

Langkah-langkah yang dikerjakan pada tugas akhir ini adalah sebagai berikut:

1. Studi literatur

Studi literatur berisi serangkaian kegiatan pengumpulan dan pengkajian dasar teori yang relevan dan terpercaya untuk menunjang penulisan tugas akhir ini. Literatur dapat bersumber dari paper, jurnal, artikel, buku, maupun *website*, yang bertaraf nasional dan internasional.

2. Observasi dan Analisa Masalah

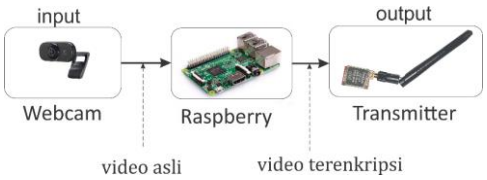
Pada tahap ini dilakukan pengkajian terhadap sistem-sistem trasmisi video yang sudah ada, meneliti bagaimana membuat enkripsi secara sederhana. Dan mengaplikasi-kannya dalam program di Raspberry.

3. Persiapan Alat dan Bahan

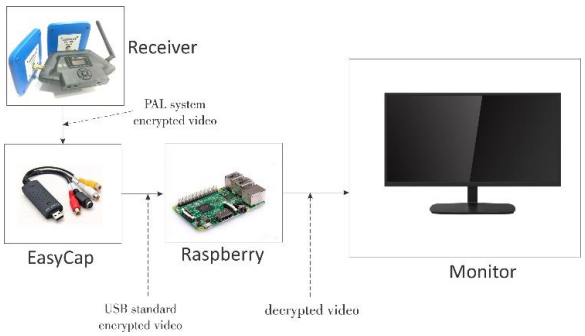
Persiapan dilakukan agar dalam perancangan alat menjadi lebih terstruktur. Tahap ini merupakan tahap pencarian informasi mengenai konsep-konsep yang dibutuhkan untuk merancang *Sistem pengaman video* ini, yang bisa didapatkan dari studi literatur disertai dengan bimbingan yang intensif dengan dosen. Kemudian dilakukan pengumpulan alat dan bahan yang dibutuhkan.

4. Perancangan Perangkat Keras *(Hardware)*

Perancangan bertujuan mendapatkan desain dan mekanisme yang optimal dengan memperhatikan data-data sebelumnya. Hardware yang digunakan meliputi Raspberry Pi3, dan sebuah EasyCap (Composite Video Capture).



Gambar 1. Rancangan Perangkat keras pada sisi Pemancar



Gambar 2. Rancangan Perangkat keras pada sisi Penerima

5. Perancangan Perangkat Lunak *(Software)*

Pada tahap ini dilakukan perancangan pengembangan pemrograman. Pemrograman meliputi enkripsi data video yang akan dipancarkan (ditransmisikan) pada raspberry. Dan program untuk mendekripsi data video yang dipancarkan pada raspberry yang lain.

6. Tahap Pengujian

Pengujian dilakukan bertahap. Pertama dilakukan pegujian pada pada system enkripsi. Sistem diharapkan mampu menampilkan video yang tidak dapat dikenali oleh mata. Kemudian data ditransmisikan ke raspberry yang lain dengan menggunakan Easycap

Tahap pengujian selanjutnya dilakukan dengan mendeskripsikan data yang diterima. Proses Dekripsi diawali dengan proses cropping, mapping dan kemudian swaping.

Pengujian berikutnya dilakukan dengan mengubah-ubah seed enkripsi (sebuah angka mirip password) dan menguji apakah seed yang berbeda akan menghasilkan hasil enkripsi maupun dekripsi yang berbeda.

7. Analisa dan Evaluasi

Analisa dilakukan terhadap hasil pengujian sehingga karakteristik *software* dan *hardware* dapat diketahui. Analisa dilakukan pada dua bagian utama, yaitu pada sisi Enkripsi dan sisi Dekripsi

8. Penyusunan Laporan

Tahap penyusunan laporan merupakan tahap terakhir dari proses pengerjaan tugas akhir ini. Laporan berisi seluruh hal yang berkaitan dengan tugas akhir yang telah dikerjakan yaitu meliputi pendahuluan, studi literatur, tinjauan pustaka, perancangan dan pembuatan sistem, pengujian dan analisa, serta penutup.

III. HASIL DAN PEMBAHASAN

Pengujian dilakukan untuk mengukur keberhasilan suatu system. Pada tulisan ini penulis menguji performa dari system dengan cara mengujinya pada computer dan pada perangkat Raspberry.

A. Pengujian Enkripsi dengan File Gambar pada Komputer

Pengujian dilakukan untuk menguji keberhasilan enkripsi dan pengaruh seed (benih) terhadap hasil enkripsi. Pengujian dilakukan pada file gambar terlebih dahulu agar lebih memudahkan dalam pemrograman berikutnya

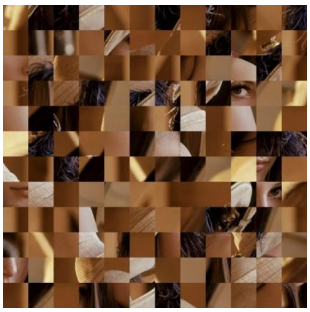
ISSN (Print) : 2621-3540
ISSN (Online) : 2621-5551

Hasil Pengujian

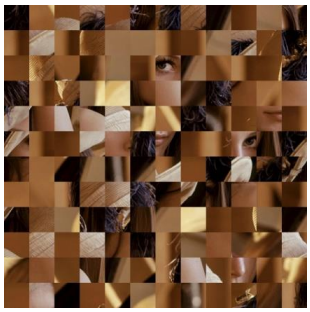
- Kasus 1

Gambar 3. Gambar Asli

Gambar 4. Enkripsi seed 44257



Gambar 5. Enkripsi seed 1234



Gambar 6. Enkripsi seed 1111

- Kasus 2

Gambar 7. Gambar Asli

Gambar 8. Enkripsi seed 44257

Gambar 9. Enkripsi seed 1234

Gambar 10. Enkripsi seed 1111

Tabel 1. Similaritas Gambar pada Kasus 1

Seed	Nilai Koeffisien Korelasi	Nilai Similaritas
44257	0.05261677	5.261676984
1234	0.007384094	0.738409394
1111	-0.039455548	3.94555479
	Rata-rata	3.315213722

Tabel 2. **Similaritas Gambar pada Kasus 2**

Seed	Nilai Koeffisien Korelasi	Nilai Similaritas
44257	0.042408179	4.240817872
1234	-0.105766526	10.5766526
1111	-0.04489818	4.489818024
	Rata-rata	6.435762833

B. Pengujian Enkripsi dengan Kamera pada Raspberry

Pengujian bertujuan untuk Mensimulasikan program ketika mendapatkan input dengan kamera dan mengenkripsikannya. Pengujian ini dilakukan secara realtime dengan pengirim atau transmitter yang dilengkapi kamera. Dan pada sisi receiver digunakan sebuah monitor yang digunakan untuk memvisual-isasikan gambar yang dipancarkan.

- **Hasil Pengujian**

Gambar 11. Gambar yang tertangkap kamera

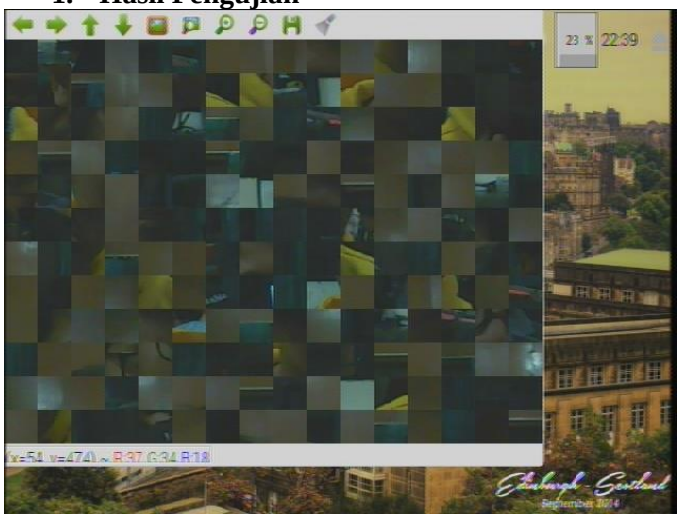
Gambar 12. Hasil Enkripsi Gambar dari kamera

C. Pengujian Software Dekripsi dengan Kamera

Bertujuan untuk menguji system dekripsi secara keseluruhan. Sinyal dari Transmitter yang diterima oleh receiver kemudian diubah menjadi standar USB oleh Easycap. Kemudian data gambar yang telah dienkripsikan. Perlu diuji apakah dapat didekripsikan dengan benar.

ISSN (Print) : 2621-3540
ISSN (Online) : 2621-5551

1. Hasil Pengujian



Gambar 13. Gambar output EasyCap

Gambar 14. Gambar hasil Crop

Gambar 15. Gambar hasil Dekripsi

Setelah melakukan pengujian selanjutnya dilakukan analisis derajat kemiripan gambar asli sebelum di transmisikan dengan gambar hasil dekripsi menggunakan Matlab. Tes ini digunakan untuk membandingkan hubungan antara dua piksel yang berdekatan pada gambar terenkripsi. Koefisien korelasi antara piksel dari citra terenkripsi harus mendekati satu**.** Pengujian dilakukan dengan menggunakan matlab, dan didapatkan nilai koefisien korelasi antara Gambar 11 dan Gambar 15 yaitu **0.9824341279799247**. Dapat dikatakan bahwa kemiripan gambar asli dengan reknstruksi/dekripsi sebesar 98,24%.

IV. KESIMPULAN

Berdasarkan percobaan yang telah dilakukan pada pelaksanaan tugas akhir ini didapat beberapa kesimpulan sebagai berikut:

1. Seed yang diberikan pada PseudoRandom akan mempengaruhi pola pengacakan enkripsi dengan similaritas rata-rata adalah 3.94 %
2. Seed yang diberikan pada enkripsi dan dekripsi harus sama agar gambar dapat di rekonstruksi dengan benar.
3. Kemiripan gambar asli dengan rekontruksi gambar pada dekripsi memiliki kemiripan 98,24 %. Sedangkan kemiripan gambar asli dengan gambar yang terenkripsi adalah sebesar 3,41%.

V. DAFTAR PUSTAKA

[1] Behrouz A. Forouzan, “Data Communications and Networking”, 4th Edition

[2] William Stallings, ”Cryptography and Network Security”, 5th Edition

[3] Ayushi, “A Symmetric Key Cryptographic Algorithm”, International Journal of Computer Applications (0975-8887) Volume 1- No. 15

[4] Arihant Kr. Banthia, Namita Tiwari, “Image Encryption using Pseudo Random Number Generators”, International Journal of Computer Applications (0975-8887) Volume 67-No.20, April 2013

[5] R Stinson, “Cryptography Theory and Practice”, 3rd Edition.

[6] Faheem Masoodi, Shadab Alam, M U Bokhari, “An Analysis of Linear Feedback Shift Registers in Stream Ciphers”, International Journal of Computer Applications (0975-8887) Volume 46-No.17, May 2012

[7] M.Sahithi, B.Murali Krishna, M.Jyoti, K.Purnima, A.Jhansi Rani,N.Naga Sidhu, “Implementation of Random Number Generator Using LFSR for High Secured Multipurpose Applications”, International Journal of Computer Science and Information Technologies, Vol. 3(1),3287-3290.

[8] Nishith Sinha, Anirban Bhowmick, Kishore B, “Encrypted Information Hiding using Audio Steganography and Audio Cryptography”, International Journal of Computer Applications(0975-8887) Volume 112-No. 5,February 2015.

[9] Shrija Somaraj, Mohammed Ali Hussain, “Securing Medical Images by Image Encryption using Key Image”,

ISSN (Print) : 2621-3540
ISSN (Online) : 2621-5551

International Journal of Computer Applications(0975-8887) Volume 104-No. 3, October 2014.

[10] Reshu Choudhary, Arjun JB, “Multimedia Content Security using Image Encryption”, International Journal of Computer Applications(0975-8887)

[11] Musheer Ahmad, M. Shamsher Alam, “A New Algorithm of Encryption and Decryption of Images Using Choatic Mapping”, International Journal on Computer Science andEngineering, Vol.2(1),2009,46-50.

[12] V. Kapur, S. T. Paladi and N. Dubbakula, "Two Level Image Encryption using Pseudo Random Number Generators," *International Journal of Computer Applications,* vol. 115, 2015.

[13] B. Eckel, Thinking in C++, Vol. 1: Introduction to Standard C++, 2nd Edition, Prentice Hall, 2000.

[14] The RAND Corporation, "A Million Random Digits," 30 March 2017. [Online]. Available: https://www.rand.org/pubs/monograph_reports/MR1418/index2.html. [Accessed 26 May 2018].

[15] P. Geremia, "Cyclic Redundancy Check Computation: An Implementation Using the TMS320C54x," Texas Instrument, Texas, 1999.

[16] "C++," Wikipedia, [Online]. Available: https://id.wikipedia.org/wiki/C%2B%2B#cite_ref-2. [Accessed 25 May 2018]