PENGIRIMAN PESAN DALAM FILE GAMBAR DENGAN METODE *RC6* DAN *LSB* MENGGUNAKAN ANDROID

Sartono*, Riyan Apriyanto†, dan Fandy Kurniawan‡
Fakultas Teknologi Informasi
Universitas Budi Luhur
Jakarta, Indonesia
Email: *tonenton19@gmail.com, †riyan.apri99@gmail.com, ‡fandy@loyalto.id

Abstract—The development of digital media rapidly and its use covering various areas give rise to the demands of an increasingly large to create an information delivery system can be secured process of securing information can be done by hiding the information to other media or by a particular method, so people do not realize there is an information in the media. Technique known as Steganography, Steganography is a technique to hide or disguise the existence of secret messages in media containers. Changing common message (plaintext) into an encrypted message (ciphertext). with cryptographic methods. The combination of these two methods can be used for security messages into media images, so that the message can be converted into encrypted messages once can disembunyikan.Untuk open the message inserted in this image is used to unlock the secret key simultaneously translate pesan.Aplikasi will be built using android that implements the methods Steganography Simple subsitutions least significant bit (LSB) and cryptography Rivest Code 6 (RC6). The use of steganography and cryptography technology is expected to improve security in the process of delivering information, in order to get important information, will be masked its presence on a media image. It is also expected to assist in the protection of copyright works of electronic media.

Index Terms—android, RC6 cryptography, message insertion, LSB steganography.

Abstract—Perkembangan media digital yang pesat dan penggunaanya yang meliputi berbagai bidang menimbulkan tuntutan yang semakin besar untuk menciptakan suatu sistem penyampaian informasi dapat terjamin keamanannya Proses pengamanan informasi dapat dilakukan dengan menyembunyikan informasi tersebut pada media lain atau dengan metode tertentu, sehingga orang lain tidak menyadari ada suatu informasi didalam media tersebut. Dikenal dengan teknik Steganografi, Steganografi adalah teknik menyembunyikan atau menyamarkan keberadaan pesan rahasia dalam media penampungnya. Pengubahan pesan biasa(plaintext) menjadi pesan terenkripsi (chipertext). dengan metode kriptografi. Kombinasi kedua metode ini dapat digunakan untuk pengamanan pesan ke dalam media gambar, agar pesan yang ingin disampaikan dapat diubah menjadi pesan enkripsi sekaligus bisa disembunyikan.Untuk membuka pesan yang disisipkan dalam gambar ini digunakan kunci rahasia untuk membuka sekaligus menerjemahkan pesan.Aplikasi yang akan di bangun menggunakan android yang mengimplementasikan metode Steganography Simple least Significant Bit Subsitutions (LSB) dan kriptografi Rivest Code 6 (RC6). Penggunaan teknologi Steganografi dan kriptografi ini diharapkan dapat meningkatkan keamanan dalam proses penyampaian informasi, agar informasi informasi yang penting, akan tersamarkan keberadaannya pada sebuah media gambar. Hal ini juga diharapkan dapat membantu proses perlindungan hak cipta hasil karya media elektronik.

Index Terms—android, kriptografi RC6, penyisipan pesan, steganografi LSB.

1 INTRODUCTION

1.1 Latar Belakang

BEBERAPA tahun terakhir ini terjadi beberapa kasus penyadapan dalam bidang komunikasi di negara ini. Tidak hanya telepon tetapi juga penyadapan dalam bentuk (Short Message Service) SMS, sehingga meresahkan banyak masyarakat yang tidak ingin diketahui atau disadap pesannya. Kriptografi dalam penelitian ini digunakan untuk mengubah informasi yang asli (plainteks) menjadi informasi acak (cipherteks). Namun teknik kriptografi memiliki kelemahan, yaitu pesan acak yang dikirim justru dapat menimbulkan kecurigaan oleh pihak luar, sehingga pesan tersebut dapat dirusak dengan tujuan agar pihak penerima yang asli tidak berhasil mendapatkan pesan tersebut secara utuh. Steganografi merupakan salah satu bagian dari kriptografi, yaitu ilmu dan seni dalam menyembunyikan pesan rahasia sehingga manusia tidak dapat menyadari keberadaan pesan yang disembunyikan tersebut. Pada masa kini, steganografi lebih banyak dilakukan pada data digital, dengan menggunakan bentuk media digitalseperti teks, gambar, audio, atau video (Munir, 2006)[1]. Terdapat dua tujuan utama dalam penelitian ini: Tujuan pertama adalah untuk mendesain dan mengembangkan algoritma untuk mengamankan data. Tujuan kedua adalah menerapkan algoritma RC6 untuk enkripsi dan metode LSB untuk menyembunyikan data pada media gambar.

2 LANDASAN TEORI

2.1 Konsep Kriptografi

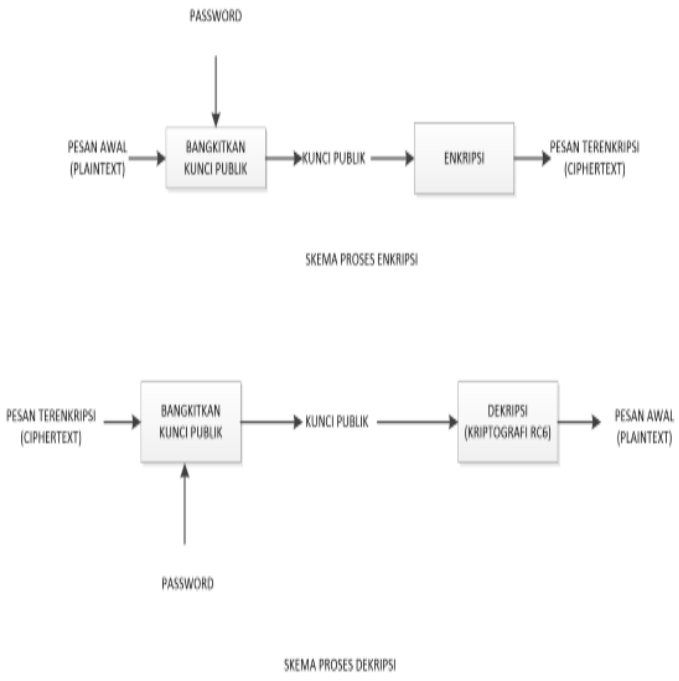
Kriptografi adalah ilmu untuk mengacak pesan sedemikian rupa sehingga tidak bisa dibaca oleh pihak ketiga atau yang tidak diberi otorisasi. Pada dasarnya, kriptografi terdiri dari beberapa aspek keamanan yaitu:

1) Autentikasi: Proses untuk menjamin keaslian suatu pesan, sehingga pihak yang menerima pesan dapat memastikan keaslian pesan tersebut datang dari orang yang dimintai informasi.
2) Integritas: Proses untuk menjaga agar sebuah pesan tidak diubah-ubah sewaktu dikirim atau disimpan.
3) Penghindaran Penolakan: Proses untuk menjaga bukti bukti bahwa suatu pesan berasal dari seseorang sehingga pihak yang mengirim tidak bisa menyangkal bahwa pesan tersebut berasal dari pihak tersebut.
4) Kerahasiaan: Kerahasiaan adalah penyembunyian pesan dari orang-orang yang tidak punya otoritas sehingga pesan penting hanya akan dibaca oleh orang yang dituju.

2.2 Algoritma Kriptografi RC6

Salah satu metode enkripsi yang umum digunakan yaitu menggunakan algoritma dan kunci yang dapat diubah-ubah sesuai kesepakatan untuk meningkatkan keamanan. Teknik ini disebut sebagai algoritma kunci semetri, yaitu suatu enkripsi dengan menggunakan kunci yang sama untuk melakukan proses enkripsi dan dekripsi. Contoh algoritma kunci simetri yaitu Rivest Code 6 (RC6) yang dirancang oleh Ronald L Rivest, M.J.B. Robshaw, R. Sidney dan Y.L. Yin. RC6 merupakan algoritma kriptografi pengembangan dari sistem sebelumnya yaitu RC5 yang dirancang khusus untuk memenuhi kebutuhan akan sebuah Advanced Encryption Standard(AES)[2]. Sama seperti RC5, RC6 membuat penggunaan sifat dasar pada data tergantung pada rotasi. Aplikasi tambahan pada RC6 yaitu tersedianya 4 register kerja sebagai pengganti 2 register kerja, inklusi dari perkalian integer sebagai operasi dasar tambahan. Penggunaan multiplikasi yang besar meningkatkan difusi setiap round(pe -ngulangan). Algoritma RC6 dilengkapi dengan beberapa parameter, sehingga dituliskan sebagai RC6-w/r/b. Parameter w merupakan ukuran kata dalam satuan bit, parameter merupakan bilangan bukan negatif yang menunjukan banyaknya iterasi selama proses enkripsi dan parameter b menunjukan ukuran kunci enkripsi dalam byte. Setelah algoritma ini masuk dalam kandidat AES, maka ditetapkan bahwa nilai w = 32, r=20 dan b bervariasi antara 16, 24 dan 32 byte. II-14 RC6-w/r/b memecah blok 128 bit menajdi 4 buah blok 32-bit, dan mengikuti aturan enam operasi dasar sebagai berikut :

1) a + b operasi penjumlahan bilangan integer
2) a - b operasi pengurangan bilangan integer
3) a Ł b operasi exclusive-OR (XOR)
4) a x b operasi perkalian bilangan integer
5) a¡¡¡b a dirotasikan ke kiri sebanyak variabel kedua (b)
6) a¿¿¿b a dirotasikan ke kanan sebanyak variabel kedua (b)



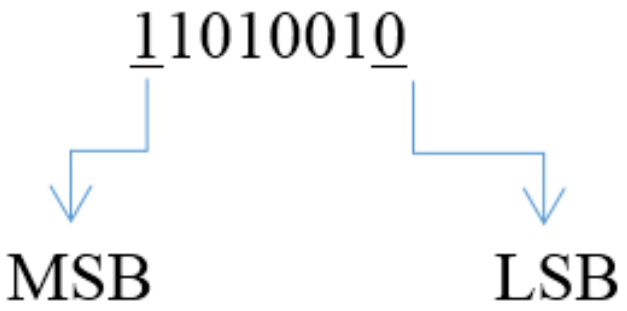
Gambar. 1. Diagram Blok Kriptografi RC6

Langkah-langkah algoritma RC6 dalam pelaksanaan penelitian ini akan dikelompokkan kedalam beberapa bagian, yaitu :

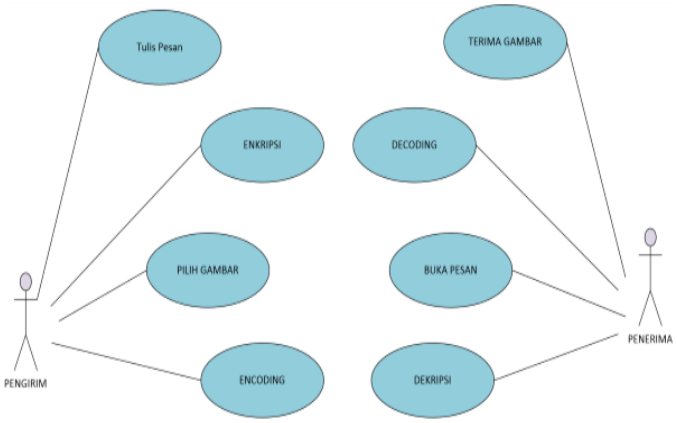
1) Pembangkit Subkunci Kunci dari pengguna ini akan dimasukkan oleh pengguna pada saat akan melakukan proses enkriosi dan dekripsi. Kunci ini memiliki tipe string dan memiliki panjang 16 byte (16 karakter).
2) Baca masukkan untuk proses enkripsi Yang dilakukan pada tahapan ini adalah membaca teks yang menjadi masukan pada proses enkripsi, yaitu field dari aplikasi enkripsi SMS. Pada proses enkripsi pesan, field-nya adalah isi pesan.
3) Enkripsi meliputi whitening awal, iterasi, dan whitening akhir. Whitening awal, dengan menjumlahkan B dengan subkunci S(0), dan D dengan subkunci S(1), Penjumlahan dilakukan dalam modulo 232 Iterasi dilakukan sebanyak 20 kali.[3] Setiap iterasi mengikuti aturan sebagai berikut:
tROTL((X[1]*(2*X[1]+1)),5) 1. Baca masukkan untuk Proses Dekripsi Yang dilakukan pada tahapan ini adalah membaca teks yang menjadi masukan pada proses dekripsi, yaitu record dari hasil pesan yang telah dienkripsi pada pengirim dan menjadi field pesan pada penerima 2. Deskripsi merupakan kebalikan dari proses enkripsi.

2.3 Steganografi Metode Least Significant Bit (LSB)

Steganografi adalah ilmu dan seni menulis atau menyembunyikan pesan ke dalam sebuah media sedemikian rupa sehingga keberadaan pesan tidak diketahui atau tidak disadari oleh orang selain pengirim dan penerima pesan tersebut. Metode LSB merupakan metode steganografi



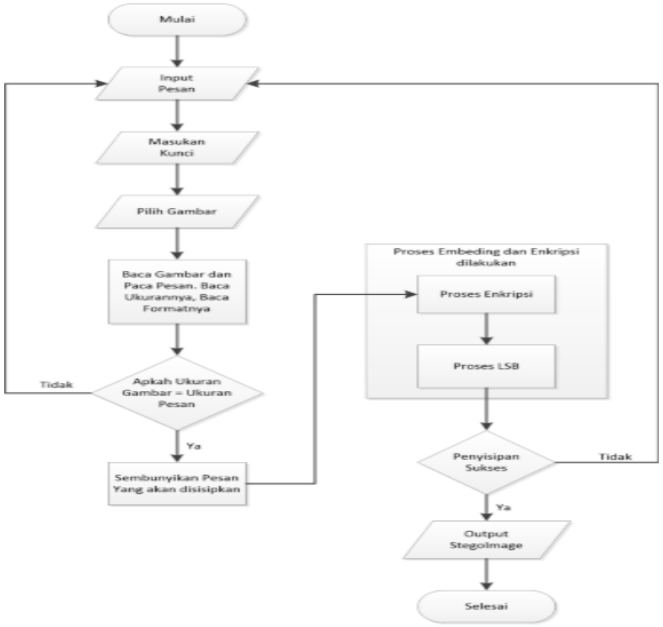
Gambar. 2. MSB dan LSB



Gambar. 3. Metode Kerja Sistem

yang paling sederhana dan mudah diimplementasikan.[4] 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 11010010, angka bit 1 (pertama, digaris-bawahi) adalah bit MSB, dan 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

MSB :Most Significant Bit LSB :Least Significant Bit Pada gambar 2, menandakan bahwa bit 1 dari depan menyatakan bit MSB dan bit 0 dari bilangan biner terakhir adalah bit LSB. Teknik LSB dilakukan dengan memodifikasi bit-bit yang tergolong bit-bit LSB pada tiap byte dalam sebuah file yang digunakan sebagai carrier file atau dengan kalimat yang lain dengan cara mengganti bit-bit LSB dengan bit-bit informasi yang ingin dilekatkan. Proses penggantian bit ini disebut dengan proses encoding/embedding



Gambar. 4. Flowchart Embedding dan Enkripsi Pesan

2.4 Android

Android merupakan sebuah sistem sistem operasi untuk perangkat mobile berbasis linux yang meliputi sistem operasi, middleware, dan aplikasi yang dirilis oleh Google. Sedangkan Android SDK (Software Development kit) menyediakan Tools dan API (Application Programming Interface) yang diperlukan untuk mengembangkan aplikasi pada platform Android dengan menggunakan bahasa pemrograman Java (Mulyadi, 2010). Android dikembangkan oleh Google bersama OHA (Open Handset Alliance) yaitu aliansi perangkat selular terbuka yang terdiri dari 47 perusahaan Hardware, Software dan perusahaan telekomunikasi. Android merupakan Open Development Platform dimana Android menawarkan kepada pengembang untuk membangun aplikasi dimana pengembang bebas untuk mengakses perangakat keras, akses informasi resources dan lainnya.

3 METODE PENELITIAN

3.1 Obyek Penelitian

Obyek penelitian yang dilakukan adalah penyembunyikan data pada media gambar yang diusulkan terdiri dari dua tahap: (1) data dienkripsi menggunakan algoritma RC6 sebelum data disembunyikan pada media gambar. (2) Chipertext dari hasil enkripsi menggunakan algoritma RC6 disembunyikan ke dalam media gambar menggunakan metode LSB. Proses penyembunyian ini disebut dengan proses embedding, dimana dua bit LSB pada masing-masing channel RGB pada pixel gambar akan digantikan dengan dua bit pada chipertext. Hasil gambar yang sudah disisipi oleh data disebut dengan stego image.

3.2 Metode Kerja Sistem Aplikasi

3.3 Proses Embedding

Embedding merupakan proses penyisipan pesan ke dalam suatu gambar.[5]

Gambar. 5. Flowchart Retrieving dan Dekripsi Pesan

Berdasarkan flowchart proses penyisipan yang ditunjukkan pada gambar 4. diatas dapat dijelaskan bahwa:

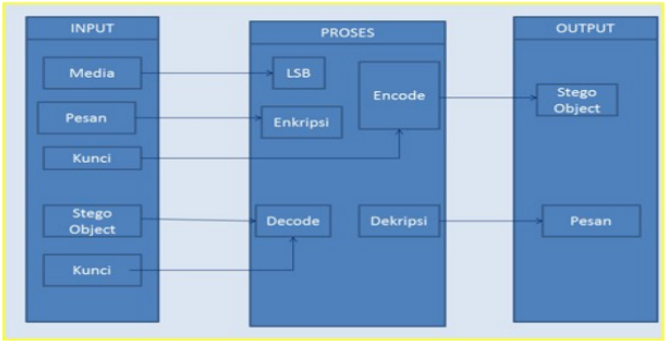
1) Penyisipan pesan rahasia dimulai dengan menginputkan requirement data ke dalam sistem, yang terdiri dari nomor kunci rahasia untuk mengacak dan mengembalikan pesan, pesan rahasia yang akan disembunyikan, dan media gambar yang berupa JPEG.
2) Selanjutnya, aplikasi akan membaca pesan rahasia dan ukurannya, kemudian membaca media penyisipan yang berupa gambar. Dilakukan validasi terhadap ukuran media penyisipan dan pesan yang akan disembunyikan. Jika ukuran media penyisipan lebih besar atau sama dengan ukuran pesan rahasia, maka proses akan berlanjut. Namun, jika ukuran media penyisipan lebih kecil dari ukuran pesan rahasia atau pesan lebih besar dari medianya, maka proses akan kembali ke langkah pertama.
3) Sembunyikan informasi penanda pesan yang akan disisipkan pada media. Tipe pesan yang disisipkan adalah teks, maka yang dijadikan penanda adanya pesan di dalam sebuah media adalah hanya berupa ukuran dari pesan yang akan disisipkan. Bagian ini menjadi bagian yang sangat penting ketika penerima ingin mengambil (retrieving) pesan.
4) Diperoleh output berupa stegoimage (file baru yang telah membawa pesan).
5) Selesai.

3.4 Proses Extracting (Retrieving)

Extracting merupakan proses mengembalikan pesan dari stego image.[6] Secara detil, proses ini ditunjukan pada gambar 5 dibawah ini

Berdasarkan alur proses retrieving yang ditunjukkan pada gambar 5. dapat dijelaskan bahwa:

1) Retrieving terjadi apabila requirement data berupa stegoimage dan kunci telah diinput kan pada sistem.



Gambar. 6. Skema Perancangan Sistem

2) Sistem akan membaca informasi penanda dari stegoimage yang diinputkan.
3) Membaca barisan bit-bit stegoimage untuk menemukan informasi ukuran pesan yang tersimpan. Jika ukuran pesan berubah dengan nilai aslinya, maka ditemukan informasi ukuran pesan yang tersimpan pada stegoimage.
4) Output yang dihasilkan adalah pesan rahasia.
5) Selesai.

3.5 Skema Perancangan Sistem

Berdasarkan gambar 6. dapat diketahui bahwa rancang bangun aplikasi steganografi ini memiliki proses, kebutuhan inputan data, dan output yang sama seperti aplikasi steganografi pada umumnya, yaitu :

1) Input, merupakan kebutuhan inputan data yang dibutuhkan oleh sistem yang terdiri dari empat jenis data yang dibedakan berdasarkan proses proses utama (main process) steganografi, yaitu pesan rahasia (message) yang akan disisipkan, media penampung (carrier file) yang menyatakan tempat dimana pesan rahasia akan disisipkan untuk proses embedding, dan kunci yang digunakan untuk menampilkan pesan tersembunyi, serta data yang telah membawa pesan(stego-object)untuk proses pengambilan pesan (retrieving).
2) Proses, menyatakan proses-proses utama yang terdapat pada rancang bangun aplikasi steganografi, yaitu proses penyembunyian atau penyisipan (embedding) dan proses pengambilan kembali pesan (retrieving). Pada proses inilah penerapan metode LSB Dilakukan untuk penyisipan bit-bit pesan ke bit-bit LSB medianya.
3) Output, merupakan hasil dari main process yang terjadi pada sistem. Output dari embedding disebut dengan stegoimage, sementara output dari retrieving adalah pesan rahasia yang tersembunyi di dalam stegoimage.

4 HASIL DAN PEMBAHASAN

4.1 Gambar Aplikasi

Algoritma ini telah diimplemetasikan kedalam versi aplikasi mobile yaitu Android Jelly Bean 4.2.1. Spesifikasi hardware pembuatan aplikasiIntel Core i3-3217U CPU @

Gambar. 7. Tampilan Utama Aplikasi

Gambar. 8. Tampilan Proses Encode Aplikasi

Gambar. 9. Tampilan Proses Decode Aplikasi

Gambar. 10. Tampilan Proses Decode Aplikasi

1.80 GHz, 4 GB RAM, 500 GB HD, Window 7 64-bit dan aplikasi yang digunakan adalah android studio 2.2.

5 SIMPUL DAN SARAN

5.1 Kesimpulan

Berdasarkan uji coba sistem aplikasi yang telah dibangun maka dapat ditarik beberapa kesimpulan sebagi berikut:

1) Dengan adanya sistem ini, maka dapat melakukan pertukaran informasi dengan lebih aman, dimana informasi disisipkan ke dalam media gambar.
2) Informasi akan menjadi lebih sulit untuk dipecahkan, dikarenakan sebelum proses penyisipan informasi, dilakukan proses enkripsi terlebih dahulu terhadap informasi tersebut sehingg secara visual tidak ada perbedaan untuk mengenali gambar mana yang telah disisipkan kode rahasia.

5.2 Saran

Pengujian masih dilakukan pada file gambar, perlu dikembangkan untuk penyisipan pesan dalam bentuk audio, file teks, file video(mp4) dan lain-lain karena itu masih perlu dilakukan pengujian lebih lanjut.

6 DAFTAR PUSTAKA

DAFTAR PUSTAKA

[1] David, Murtado A. dan Kasma Utin.Steganography Gambar Dengan MetodeLeast Significant Bit Untuk ProteksiKomunikasi Pada Media Online. Program Studi Teknik Informatika, Sekolah Tinggi Manajemen Informatika dan KomputerPontianak. 2012.
[2] Menezes, A, VanOorschot, P, Vanstone, S. 1997.Handbook of Applied Cryptography. CRC Press, Inc.
[3] Michael Siregar, Ivan, Membongkar Source Code berbagai Aplikasi Android, Halaman 227, Gava Media, Yogyakarta.
[4] Munir, Rinaldi, Steganografi dan Kriptografi, Halaman 301, Informatika, Bandung, 2006
[5] Singh, Gurpreet. dan Supriya. 2013. A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security.IJCA. 67(19): 0975-8887.
[6] Westfeld Andreas. Steganalysis in the Presence of Weak Cryptography and Encoding. Technische Universitat Dres den Institute for System Architecture, Germany.2006.

Sartono lahir di Trenggalek, Jawa Timur Indonesia in 1987. lulus S1 Tahun 2014 Jurusan Teknik Informatika di Institut Sains Teknologi Al Kamal.

Riyan Apriyanto Lahir di Bandung, Jawa Barat Indonesia Tahun 1992. Lulus S1 Tahun 2014 Jurusan Teknik Informatikan di STMIK Bani Saleh.

Fandy Kurniawan Lahir di kota Ambon Maluku Utara Indonesia Tahun 1992. Lulus S1 Tahun 2014 Jurusan Sistem Informasi di STMIK Bani Saleh