Kriptografi Gambar dengan menggunakan Algoritma *Blowfish*

SKRIPSI

Diajukan untuk memenuhi sebagian syarat untuk memperoleh gelar

Sarjana Matematika

Oleh:

Muhammad Reyhan Zelvian

1904095

PROGRAM STUDI MATEMATIKA

DEPARTEMEN PENDIDIKAN MATEMATIKA

FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS PENDIDIKAN INDONESIA

2023

LEMBAR PENGESAHAN

MUHAMMAD REYHAN ZELVIAN

KRIPTOGRAFI GAMBAR DENGAN MENGGUNAKAN ALGORITMA *BLOWFISH*

Disetujui dan disahkan oleh pembimbing:

Pembimbing I

Dra. Hj. Rini Marwati, M.Si.

NIP. 196606251990012001

Pembimbing II

Hj. Dewi Rachmatin, S.Si., M.Si.

NIP. 196909291994122001

Mengetahui

Ketua Departemen Pendidikan Matematika

Dr. H. Dadang Juandi, M.Si.

NIP. 196401171992021001

SURAT PERNYATAAN

Dengan ini saya menyatakan bahwa skripsi dengan judul "Kriptografi Gambar dengan menggunakan Algoritma *Blowfish*" ini beserta seluruh isinya adalah benar-benar karya saya sendiri, kecuali kutipan-kutipan dari ringkasan yang semuanya telah saya jelaskan sumbernya. Apabila dikemudian hari ditemukan adanya pelanggaran, saya bersedia menanggung resiko atau sanksi yang dijatuhkan kepada saya.

Bandung, 10 April 2023

Yang membuat pernyataan,

Muhammad Reyhan Zelvian

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Allah SWT, karena berkat rahmat dan karunia-Nya penulis dapat menyelesaikan skripsi yang berjudul "Kriptografi Gambar dengan menggunakan Algoritma *Blowfish*" sebagai salah satu syarat memperoleh gelar Sarjana Matematika di Universitas Pendidikan Indonesia (UPI).

Pertukaran informasi pada saat ini dapat diretas oleh pihak yang tidak bertanggung jawab. Untuk mengamankan data gambar dapat menggunakan kriptografi gambar. Salah satu algoritma kriptografi adalah algoritma *Blowfish*. Penulis mengimplementasikan algoritma *Blowfish* terhadap kriptografi gambar dan juga mengonstruksi program aplikasi kriptografi gambar dengan menggunakan algoritma *Blowfish*.

Penulis menyadari bahwa penulisan skripsi ini tidak luput dari kekurangan. Oleh karena itu kritik dan saran yang membangun sangat diperlukan guna menyempurnakan dan mengembangkan skripsi ini. Penulis berharap skripsi ini dapat bermanfaat bagi pada pembaca, khususnya yang sedang mendalami kriptografi gambar dan kriptografi algoritma *Blowfish*.

Bandung, 10 April 2023

Penulis

UCAPAN TERIMA KASIH

Puji dan syukur penulis panjatkan kehadirat Allah SWT yang telah memberikan rahmat dan karunia nya sehingga penulis dapat menyelesaikan skripsi ini. Penulis menyadari bahwa selama penulisan skripsi terdapat pihak secara langsung maupun tidak langsung telah memberikan semangat, bantuan, dan doa. Oleh karena itu, penulis ingin menyampaikan terimakasih kepada:

1. Ibu Dra. Hj. Rini Marwati, M.S. selaku dosen Pembimbing I yang telah mengajarkan penulis dengan penuh kesabaran mengenai topik yang penulis bahas dalam skripsi ini.
2. Ibu Hj. Dewi Rachmatin, S.Si., M.Si. selaku dosen Pembimbing II yang telah memberikan arahan dan bimbingan dari awal hingga akhir penulisan skripsi ini.
3. Ibu Dr. Kartika Yulianti, M.Si., selaku Ketua KBK Terapan, Program Studi Matematika, Universitas Pendidikan Indonesia;
4. Bapak Imam Nugraha Albania, Ph.D. selaku dosen pembimbing akademik yang telah membina penulis selama menjalani perkuliahan di UPI.
5. Kedua Orang tua yang telah mendo'akan dan mendukung agar skripsi ini dapat diselesaikan tepat waktu.
6. Rekan-rekan mahasiswa Matematika UPI 2019 yang juga telah memberikan motivasi dan dukungannya, serta menemani penulis belajar selama masa perkuliahan.
7. Pihak lainnya yang tidak bisa disebutkan satu persatu yang telah membantu penulis dalam perkuliahan maupun penyelesaian skripsi ini.

Penulis

ABSTRAK

Kemajuan teknologi memudahkan orang untuk mengakses informasi. Namun seiring berkembangnya teknologi seringkali pesan yang dikirim diretas oleh pihak-pihak yang tidak berhak mengetahui informasi tersebut. Oleh karena itu diperlukan adanya suatu sistem yang dapat digunakan untnuk mengamankan informasi tersebut. Media informasi yang digunakan pada saat ini ada berbagai jenis, salah satunya adalah *file* gambar. Salah satu cara untuk mengamankan data dengan menggunakan kriptografi. Penelitian ini mengimplementasikan dan mengonstruksi program aplikasi kriptografi gambar dengan menggunakan algoritma *Blowfish*. Kriptografi gambar dilakukan dengan mengubah nilai *RGB* pada setiap *pixel* yang ada pada gambar. Nilai *RGB* dienkripsi menggunakan algoritma *Blowfish* untuk menghasilkan gambar yang terenkripsi. *Package opencv* digunakan untuk membaca *file* gambar dan mengambil nilai *RGB* untuk dilakukan proses enkripsi. Program aplikasi kriptografi gambar dengan menggunakan algoritma *Blowfish* akan dikonstruksi menggunakan bahasa pemrograman *Python*. Hasil enkripsi gambar dengan ukuran yang kecil menghasilkan gambar yang masih mirip dengan gambar sebelum dienkripsi. Sedangkan, hasil enkripsi gambar dengan ukuran sedang dan besar sudah menghasilkan gambar dengan *noise* yang cukup baik untuk menyamarkan gambar aslinya.

Kata Kunci: Kriptografi, Kriptografi Gambar, Algoritma *Blowfish*, *File* Gambar.

ABSTRACT

Advances in technology make it easier for people to access information. However, as technology develops, messages sent are often hacked by parties who are not entitled to know this information. Therefore it is necessary to have a system that can be used to secure this information. There are various types of media information used today, one of which is an image file. One way to secure data is by using cryptography. This study implements and constructs an image cryptographic application program using the Blowfish algorithm. Image cryptography is done by changing the RGB value of each pixel in the image. RGB values are encrypted using the Blowfish algorithm to generate encrypted images. The opencv package is used to read image files and retrieve RGB values for the encryption process. Image cryptographic application programs using the Blowfish algorithm will be constructed using the Python programming language. The results of encrypting images with a small size produce images that are still similar to the images before being encrypted. Meanwhile, the results of image encryption with medium and large sizes have produced images with good enough noise to disguise the original image.

***Keywords**: Cryptography, Image Cryptography, Blowfish Algorithm, Image File.*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR LAMPIRAN

DAFTAR PUSTAKA

Abdullah, D., & Saputro, D. N. (2016). Implementasi Algoritma *Blowfish* Dan Metode Least Significant Bit Insertion Pada Video Mp4. *Pseudocode*, 3(2), 137-145.

Alabaichi, A., Ahmad, F., & Mahmod, R. (2013). Security analysis of *Blowfish* algorithm. In 2013 Second International Conference on Informatics & Applications (ICIA) (pp. 12-18). *IEEE*.

Arrijal, I. M. A., Efendi, R., & Susilo, B. (2016). Penerapan Algoritma Kriptografi Kunci Simetris Dengan Modifikasi Vigenere *Cipher* Dalam Aplikasi Kriptografi Teks. *Pseudocode*, 3(1), 69-82.

Chandra, S., Paira, S., Alam, S. S., & Sanyal, G. (2014). A comparative survey of symmetric and asymmetric key cryptography. *2014 international conference on electronics, communication and computational engineering (ICECCE)* (hlm. 83-93). IEEE.

Fauzi, R. R., & Wellem, T. (2021). Perancangan Kriptografi Block *cipher* berbasis Pola Dribbling Practice. *AITI*, 18(2), 158-172.

Kessler, G. C. (2003). *An overview of cryptography*.

Khatri–Valmik, M. N., & Kshirsagar, V. K. (2014). *Blowfish* algorithm. *IOSR Journal of Computer Engineering (IOSR-JCE)*, 16(2), 80-83.

Lubis, U. R. S., Mesran, M., & Zebua, T. (2017). Implementasi Algoritma Chua Chaotic Noise Pada Enkripsi Citra *RGB. KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer)*, 1(1).

Marwati, R., & Sispiyati, R. Kriptografi Visual Pada Gambar Berwarna (*RGB*) Menggunakan Algoritma Elliptic Curve Cryptography. *Jurnal EurekaMatika*, 9(2), 163-174.

Munir, R. (2016). *Matematika diskrit*.

Rakhman, A. A., & Kurniawan, A. W. (2015). Implementasi Algoritma Kriptografi Rivest Shamir Adleman (Rsa) Dan Vigenere *Cipher* Pada Gambar Bitmap 8 Bit. *Techno. Com*, 14(2), 122-134.

Rosen, K. H. (1999). *Discrete mathematics & applications.* McGraw-Hill.

Sanner, M. F. (1999). Python: a programming language for software integration and development. *J Mol Graph Model*, 17(1), 57-61.

Schneier, B. (1996). *Applied cryptography protocols algorithms and source code in C*.

Schneier, B. (2005). Description of a new variable-length key, 64-bit block cipher (Blowfish*). Fast Software Encryption: Cambridge Security Workshop Cambridge, UK, December 9–11, 1993 Proceedings* (hlm. 191-204). Berlin, Heidelberg: Springer Berlin Heidelberg.

Stinson, D. R. (2005). *Cryptography: theory and practice.* Chapman and Hall/CRC.

Thakur, J., & Kumar, N. (2011). DES, AES and *Blowfish*: Symmetric key cryptography algorithms simulation based performance analysis. *International journal of emerging technology and advanced engineering*, 1(2), 6-12.

Weir, J. P. (2011). *Visual cryptography and its applications.* Bookboon.

Yuliana, C. T. E. (2014). Implementasi Algoritma Kriptografi *Blowfish* dan Metode Steganografi End Of File (EOF) untuk Keamanan Data. *Jurnal ePrint Udinus*.

Zuli, F., & Irawan, A. (2016). Implementasi Kriptografi Dengan Algoritma *Blowfish* dan Riverst Shamir Adleman (RSA) Untuk Proteksi File. *Jurnal Format*, 6(2), 27-38.