KRIPTOGRAFI VIDEO MENGGUNAKAN TRANSPOSISI DAN *RANDOM MATRIX AFFINE CIPHER*

SKRIPSI

Diajukan untuk memenuhi sebagian syarat untuk memperoleh gelar
Sarjana Matematika

Oleh:
Haryo Dhafa Putra Hima
1905648

PROGRAM STUDI MATEMATIKA
DEPARTEMEN PENDIDIKAN MATEMATIKA
FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS PENDIDIKAN INDONESIA

2023

LEMBAR HAK CIPTA

KRIPTOGRAFI VIDEO MENGGUNAKAN TRANSPOSISI DAN *RANDOM MATRIX AFFINE CIPHER*

Oleh:
Haryo Dhafa Putra Hima
1905648

Diajukan untuk memenuhi sebagian syarat untuk memperoleh gelar Sarjana Matematika pada Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam

Universitas Pendidikan Indonesia
Januari 2023

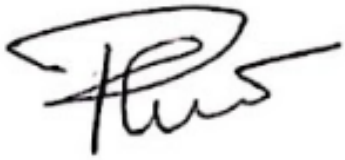
LEMBAR PENGESAHAN

HARYO DHAFA PUTRA HIMA

KRIPTOGRAFI VIDEO MENGGUNAKAN TRANSPOSISI DAN *RANDOM MATRIX AFFINE CIPHER*

Disetujui dan disahkan oleh pembimbing:

Pembimbing I



Dra. Hj. Rini Marwati, M.S.

NIP. 196606251990012001

Pembimbing II

Dr. Kartika Yulianti, M.Si.

NIP. 198207282005012001

Mengetahui,

Ketua Departemen Pendidikan Matematika

Dr. H. Dadang Juandi, M.Si.

NIP. 196401171992021001

LEMBAR PERNYATAAN

Dengan ini saya menyatakan bahwa skripsi dengan judul "Kriptografi Video Menggunakan Transposisi dan *Random Matrix Affine Cipher*" ini beserta seluruh isinya adalah benar-benar karya saya sendiri. Saya tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika ilmu yang berlaku dalam masyarakat keilmuan. Atas pernyataan ini, saya siap menanggung risiko/sanksi apabila dikemudian hari ditemukan adanya pelanggaran etika keilmuan atau ada klaim dari pihak lain terhadap keaslian karya saya ini.

Bandung, Januari 2023

Yang membuat pernyataan,

Haryo Dhafa Putra Hima

NIM. 1905648

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Puji serta syukur penulis panjatkan kehadirat *Allah Subhanahu Wa Ta'ala* yang telah memberikan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul "Kriptografi Video Menggunakan Transposisi dan *Random Matrix Affine Cipher*". Skripsi ini diajukan untuk memenuhi sebagian syarat untuk memperoleh gelar sarjana matematika.

Pada kesempatan ini, penulis mengucapkan terima kasih kepada semua pihak yang telah memberikan semangat dan motivasi dalam menyelesaikan skripsi ini. Skripsi ini harapannya dapat memberikan ilmu pengetahuan mengenai penelitian yang dilakukan oleh penulis.

Penulis menyadari masih ada kekurangan pada skripsi ini yang disebabkan oleh keterbatasan kemampuan penulis. Oleh karena itu, penulis sangat mengharapkan saran dan kritik yang membangun untuk menyempurnakan skripsi ini. Demikian skripsi ini penulis susun, semoga menjadi manfaat dan mohon maaf bila ada kekurangan.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Bandung, Januari 2023

Penulis

UCAPAN TERIMA KASIH

Dengan memanjatkan puji serta syukur kehadirat *Allah Subhanahu Wa Ta'ala* dan shalawat serta salam kepada Nabi Muhammad *Shalallaahu Alaihi Wassalam*, penulis dapat menyelesaikan skripsi dengan tepat waktu. Penulisan skripsi ini tidak terlepas dari dukungan, bantuan dan do'a dari berbagai pihak. Oleh karena itu penulis mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Ibu Dra. Hj. Rini Marwati, M.S., selaku Dosen Pembimbing I yang telah meluangkan waktunya untuk memberikan arahan, masukan dan motivasi yang banyak membantu penulis dari awal hingga akhir penyusunan skripsi ini.
2. Ibu Dr. Kartika Yulianti, M.Si., selaku Dosen Pembimbing II yang telah meluangkan waktunya untuk memberikan arahan, masukan dan motivasi yang banyak membantu penulis dari awal hingga akhir penyusunan skripsi ini.
3. Ibu Fitriani Agustina, S.Si., M.Si., selaku Dosen Pembimbing akademik yang telah meluangkan waktunya untuk membantu dalam pendampingan akademik perkuliahan, memberikan arahan dan motivasi yang banyak membantu penulis dari awal perkuliahan.
4. Bapak Drs. Cece Kustiawan, M.Si., selaku Ketua Program Studi Matematika, Universitas Pendidikan Indonesia.
5. Bapak Dr. H. Dadang Juandi, M.Si., selaku Ketua Departemen Pendidikan Matematika, Universitas Pendidikan Indonesia.
6. Seluruh dosen dan civitas akademika di lingkungan Departemen Pendidikan Matematika, Universitas Pendidikan Indonesia.
7. Kedua orang tua tercinta, Ibu dan Bapak, yang telah memberikan dukungan moral, dukungan materil, kasih sayang, semangat, serta do'a yang terus dipanjatkan kepada penulis sehingga penyusunan skripsi bisa berjalan dengan lancar.
8. Kepada Syifa Hanifa sebagai *partner* yang selalu setia membersamai di dalam suka dan duka, memberikan banyak dukungan, bantuan, do'a dan

semangat kepada penulis serta sahabat yang selalu memberikan semangat dan dukungan, Gusti, Denata, Azifah dan Yasinta.

9. Keluarga besar Putra Putri Bumi Siliwangi Universitas Pendidikan Indonesia yang telah mengajarkan banyak ilmu berharga, memberikan sebuah keluarga yang hangat di akhir masa perkuliahan serta banyak dukungan dan do'a dari Putra Putri Bumi Siliwangi angkatan 2022.
10. Rekan-rekan yang ada di *COSINE* Depdikmat 2019 dan seluruh mahasiswa Departemen Pendidikan Matematika, Universitas Pendidikan Indonesia.
11. Rekan-rekan yang telah membersamai penulis selama berorganisasi di kampus baik di tingkat himpunan, fakultas dan universitas.
12. Pihak-pihak yang tidak dapat penulis cantumkan namanya, yang telah secara langsung dan/atau tidak langsung memberikan saran dan dukungan, memberi rasa senang, sedih, aman, selama proses penulisan skripsi ini sehingga memotivasi penulis untuk menyelesaikannya.

Semoga dukungan, do'a, bantuan dan kebaikan yang telah diberikan mendapatkan balasan berkali-kali lipat dari *Allah Subhanahu Wa Ta'ala*.

ABSTRAK

Dunia digital memiliki peran penting dalam kehidupan sehari-hari khususnya dalam pertukaran informasi seperti file video, namun pertukaran informasi di jaringan internet memiliki keamanan yang berisiko. Kriptografi merupakan salah satu solusi untuk mengamankan file video sehingga informasi file tersebut tersamarkan. Penelitian ini akan mengimplementasikan dan mengkonstruksi program aplikasi kriptografi video menggunakan transposisi dan *Random Matrix Affine Cipher* untuk mengamankan file video serta menganalisis peningkatan keamanan dari algoritma *Affine Cipher* asli menjadi algoritma *Random Matrix Affine Cipher*. Kriptografi video merupakan penggabungan dari kriptografi pada gambar dan kriptografi pada audio. Pada file video, dilakukan proses pemisahan kumpulan *frame* (gambar) dan data audio. Kemudian, urutan *frame* ditransposisikan menggunakan algoritma *Affine Cipher* dan nilai *pixel* pada setiap *frame* dienkripsi menggunakan algoritma *Random Matrix Affine Cipher* yang dapat memberikan *noise* yang lebih baik pada tampilan video dibandingkan algoritma *Affine Cipher* asli. Pada data audio, urutan dan nilai data audio dienkripsi menggunakan algoritma *Affine Cipher*. Kumpulan cipher *frame* dan cipher audio kemudian digabungkan kembali sehingga menghasilkan cipher video (video yang tersamarkan). File cipher video kemudian dapat didekripsi sehingga kembali menjadi file video asli.

Kata Kunci: Kriptografi, Kriptografi Video, File Video, Transposisi, *Affine Cipher*, *Random Matrix Affine Cipher*.

ABSTRACT

"Video Cryptography Using Transposition and Random Matrix Affine Cipher"

The digital world has an important role in everyday life, especially in exchanging information such as video files, but exchanging information on the internet has risky security. Cryptography is a solution for securing video files so that the file information is disguised. This research will implement and construct a video cryptography application program using transposition and Random Matrix Affine Cipher to secure video files and analyze security enhancements from the original Affine Cipher algorithm to the Random Matrix Affine Cipher algorithm. Video cryptography is a combination of cryptography on images and cryptography on audio. In video files, the process of separating a collection of frames (images) and audio data is carried out. Then, the sequence of frames is transposed using the Affine Cipher algorithm and the pixel values in each frame are encrypted using the Random Matrix Affine Cipher algorithm which can provide better noise on the video display than the original Affine Cipher algorithm. In audio data, the audio data sequence and values are encrypted using the Affine Cipher algorithm. The collection of cipher frames and audio ciphers is then combined again to produce a video cipher (obscure video). The video cipher file can then be decrypted so that it returns to the original video file.

***Keywords**: Cryptography, Video Cryptography, Video Files, Transposition, Affine Cipher, Random Matrix Affine Cipher.*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR PUSTAKA

Agrawal, P., Sahu, S., & Choudhary, A. (2018). *A New Method of MPEG Video Encryption Using Frame Shuffling*. *6*(2), 16–17.

Chawla, R. (2015). *A Review on Audio Cryptography*. *7*, 14–16.

Hussain, S. S., Ibrahim, M. S., Mir, S. Z., Yasin, S., Majeed, M. K., & Ghani, A. (2019). Efficient Video Encryption using Lightweight Cryptography Algorithm. *2018 3rd International Conference on Emerging Trends in Engineering, Sciences and Technology, ICEEST 2018, January 2020*, 1–6. https://doi.org/10.1109/ICEEST.2018.8643317

Jawahir, A., & Haviluddin. (2015). An audio encryption using transposition method. *International Journal of Advances in Intelligent Informatics*, *1*(2), 98–106. https://doi.org/10.26555/ijain.v1i2.24

Lone, P. N., Singh, D., & Mir, U. H. (2021). A novel image encryption using random matrix affine cipher and the chaotic maps. *Journal of Modern Optics*, *68*(10), 507–521. https://doi.org/10.1080/09500340.2021.1924885

Mezaal, Y. S., & Abdulkareem, S. F. (2017). Affine cipher cryptanalysis using genetic algorithms. *JP Journal of Algebra, Number Theory and Applications*, *39*(5), 785–802. https://doi.org/10.17654/NT039050785

Mishra, D. C., Sharma, R. K., Dawar, M., & Hanmandlu, M. (2015). Two layers of security for color video by matrix affine cipher with two-dimensional discrete wavelet transform. *Fractals*, *23*(4), 1–22. https://doi.org/10.1142/S0218348X15500371

Munir, R. (2004). *Teori Bilangan (Number Theory)*. Departemen Teknik Informatika Institut Teknologi Bandung.

Munir, R. (2010). Matematika Disktrit. *Informatika Bandung*, 281–308.

Naufal, M. F. (2021). *Kriptografi Audio Menggunakan Transposisi dan Affine Cipher yang Dikembangkan Dengan Algoritma Blum Blum Shub. (Skripsi)*. Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam, Universitas

Pendidikan Indonesia. (Repositori UPI).

Qadir, A. M., & Varol, N. (2019). A review paper on cryptography. *7th International Symposium on Digital Forensics and Security, ISDFS 2019*, *June*, 1–6. https://doi.org/10.1109/ISDFS.2019.8757514

Rosen, K. H. (1987). Elementary Number Theory and Its Applications. In *Mathematics of Computation* (Vol. 48, Nomor 177). https://doi.org/10.2307/2007902

Siswanto, Shofian, A., & Anif, M. (2015). Aplikasi Kriptografi Video Menggunakan Algoritma Rivest Shamir Adleman (RSA). *Prosiding SENTIA*, *7*, 53–58.

Stinson, D. R. (2005). *Cryptography: Theory and Practice, Third Edition*. Taylor \& Francis.

Sweigart, A. (2019). *Automate the Boring Stuff with Python, 2nd Edition: Practical Programming for Total Beginners*. No Starch Press. https://books.google.co.id/books?id=RQ6xDwAAQBAJ

Thankachan, B., Thakkar, B., & Scholar, R. (2021). *A Multilevel Approach of Transposition Ciphers for Data Security over Cloud*. *May*, 1732–1738. https://www.researchgate.net/publication/351928830

Zahra, D. A., Marwati, R., & Sispiyati, R. (2021). Kriptografi Visual Pada Gambar Berwarna (RGB) Menggunakan Algoritma Elliptic Curve Cryptography. *Jurnal EurekaMatika*, 163–174. https://ejournal.upi.edu/index.php/JEM/article/view/40054

Zalukhu, M. (2018). Aplikasi Pengamanan File Video Menggunakan Teknik Kriptografi Algoritma Transposisi Zig-Zag. *Jurnal Mahajana Informasi*, *3*(2), 33–40.