Jurnal Ilmiah Sinus (JIS) Vol : 20, No. 2, Juli 2022
ISSN (Print) : 1693-1173 , ISSN (Online): 2548-4028

The Application of the Blowfish Algorithm and the Least Significant Bit Method for Securing Student Transcripts

Wahyudi [1)]; Wawan Laksito YS[2)]; Iwan Ady Prabowo[3*)]
[1,2,3)] Program Studi S1-Informatika, STMIK Sinar Nusantara
[1)] wahyudi@gmail.com, [2)] wawanlaksito@sinus.ac.id, [3)] iwanadyp@sinus.ac.id

ABSTRACT

Academic transcripts are a summary of student's high-value achievement score and it must be guaranteed in their authenticity, as well as the source from which they are issued. Some universities, for example a university in Yogyakarta, were using technology to falsify academic transcripts. Several diplomas from Makassar have done this counterfeit so that a civil servant can pass his exam, whereas an equipment for creating fake diplomas as evidence from Banda Aceh had been found. This study aims to prevent transcripts from being modified or falsified by locking data into student photos using blowfish and least significant bit algorithms. Moreover, this study aims to keep transcripts from being easily modified or falsified. The methods of this study are data collection (student code data, GPA value, and photo), encryption with blowfish, conversion of encryption results into binary form, insertion of binary values into least significant bit method into photos, capture of encryption values from least significant bit photos, and returning messages encrypted with blowfish. In this study, the results showed that this system was able to secure data and enter information into student photos with an accuracy of 100% after testing on 60 transcript value data. We can conclude that the application of blowfish and least significant bit algorithms to secure data and enter data into student photos is extremely effective in transcript value.
***Keywords**: Securing Student Transcripts Academic, Blowfish, Least Significant Bit*

I. PENDAHULUAN

Transkrip nilai merupakan riwayat kuliah mahasiswa sehingga menjadi salah satu hal yang penting dalam dunia kerja. Transkrip nilai merupakan dokumen yang bernilai tinggi dan harus dijamin keaslian isinya, maupun sumber yang mengeluarkannya dan tempat penyimpanannya. Pencatatan data dan informasi database transkrip nilai diperlukan agar tempat penyimpanan informasi (basis data) transkrip nilai dapat lebih baik, terstruktur dan teratur(Prabowo, 2022). Oleh sebab itu, Semakin pesatnya kecanggihan teknologi pada saat ini yang dapat dengan mudahnya siapapun memanipulasi data dan dokumen dari yang semestinya menjadi tidak valid sebagai cara untuk memperoleh keuntungan pihak tertentu(Hamzah et al., 2013).

Seiring perkembangan teknologi, transkrip dapat dimodifikasi dengan mudah karena tidak adanya pengamanan terhadap data transkrip nilai mahasiswa. Beberapa temuan kasus ditemukan pemalsuan transkrip nilai di beberapa Perguruan Tinggi. Transkrip nilai telah dipalsukan untuk mendaftarkan diri di beberapa Perguruan Tinggi Swasta (PTS) di DIY (Keswara, 2014).Terdapat pemalsuan sejumlah ijazah yang mengatasnamakan terbitan Perguruan Tinggi Swasta (PTS) di Makassar, ijazah digunakan untuk meluluskan diri sebagai PNS(Sofyan et al., 2014). Polisi Banda Aceh telah mengamankan barang bukti pembuatan ijazah berupa dua unit komputer, masing-masing satu unit flashdisk, alat pemindai, kertas HVS, printer, ulano, alat sablon, serta 118 arsip ijazah bodong(Mardira, 2015). Dengan maraknya pemalsuan transkrip, manipulasi data nilai akademik, dan lain sebagainya yang terkait dengan bukti akademik yang bisa mengakibatkan kerugian terhadap pihak tertentu. Tindakan pencegahan ini dilakukan dengan dibuatnya sebuah sistem yang mampu mengamankan transkrip nilai. Beberapa penerapan pengamanan transkrip nilai seperti yang dilakukan di Politeknik Negeri Lhokseumawe dengan menggunakan algoritma

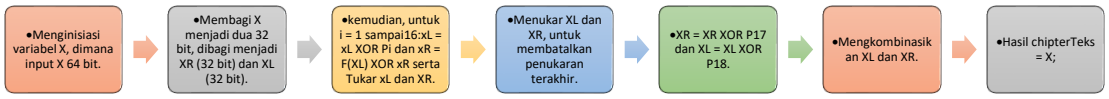
RSA dan QR Code(Hendrawaty et al., 2016). Implementasi keamanan data menggunakan algoritma *blowfish* pada sistem informasi (Althaf, 2017). Implementasi keamanan data menggunakan algoritma *blowfish* dan *lsb* pada citra (Siregar & Ariwibowo, 2014).

Tujuan penelitian ini untuk menjaga agar transkrip tidak mudah dimodifikasi atau dipalsukan dengan mengimplementasikan algoritma *blowfish* dan metode *least significant bit (LSB)* untuk pengamanan transkip nilai mahasiswa. Algoritma *blowfish* dipilih pada penelitian sebagai algoritma pengamanan data karena mempunyai kriteria cepat, ringan (*compact*), sederhana, dan memiliki tingkat keamanan yang bervariasi (Sitinjak et al., 2015).

II. TINJAUAN PUSTAKA

2.1.Algoritma Blowfish

Blowfish diciptakan oleh seorang *cryptanalyst* bernama Bruce Schneier, Presiden perusahaan Counterpane Internet Security, Inc (Perusahaan konsultan tentang kriptografi dan keamanan komputer) dan dipublikasikan tahun 1994. *Blowfish* merupakan algoritma yang tidak dipatenkan dan *license free*, dan tersedia secara gratis untuk berbagai macam kegunaan. Algoritma *blowfish* terdiri atas dua bagian, yaitu ekspansi kunci dan enkripsi-dekripsi data (Ariyus, 2008). Beberapa penelitian yang menggunakan algoritma *blowfish* seperti penelitian yang dilakukan oleh Saddam dan Ibrahim (Saddam et al., 2020) *state of the art* tentang *lightweight image encryption and Blowfish decryption for the secure internet of things. As an innovative technology of the future, the Internet of Things (IoT) is expected to connect billions of users.* Penelitian yang dilakukan oleh Retno, S dan Hasdyna N (Retno & Hasdyna, 2018) *state of the art* tentang analisis kinerja *algoritma honey encryption* dan algoritma *blowfish* pada proses enkripsi dan dekripsi. Penelitian yang dilakukan oleh Simanullang, H G dan Silalahi, A P (Simanullang & Silalahi, 2018) *state of the art* tentang algoritma *blowfish* untuk meningkatkan keamanan database *Mysql*. Penelitian yang dilakukan oleh Zulfikar, M I, Abdillah, G dan Komarudin, A (Zulfikar et al., 2019) *state of the art* tentang kriptografi untuk keamanan pengiriman email menggunakan *blowfish* dan rivest shamir adleman (RSA). Penelitian yang dilakukan oleh Althaf, S (Althaf, 2017), *state of the art* tentang implementasi keamanan data menggunakan algoritma *blowfish* pada sistem informasi. Penelitian yang dilakukan oleh Siregar & Ariwibowo (Siregar & Ariwibowo, 2014) *state of the art* tentang implementasi keamanan data menggunakan algoritma *blowfish* dan *lsb* pada citra. Penelitian yang dilakukan oleh Syed Zeeshan Abbas, Haroon Ibrahim & Majid Khan (Abbas et al., 2021) *state of the art* tentang *A hybrid chaotic Blowfish encryption for high-resolution satellite imagery*. Penelitian yang dilakukan oleh Shivam Ilasariya, Parth Patel, Vatsal Patel, dan Swapnil Gharat (Ilasariya et al., 2022) *state of the art* tentang *image steganography using blowfish algorithm and transmission via apache kafka*. Implementasi tahapan Algoritma Blowfis pada pemrograman dapat dilihat pada gambar 1 sebagai berikut.

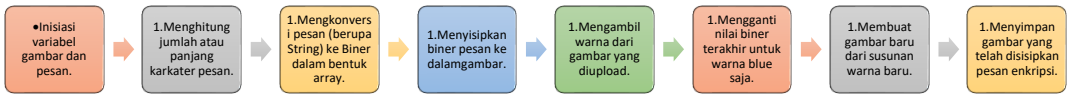


Gambar 1. Tahapan Algoritma Blowfis

2.2.Metode *Least Significant Bit* (LSB)

Least significant bit (LSB) merupakan teknik yang digunakan dalam enkripsi dan dekripsi informasi rahasia. Cara kerja metode *least significant bit (LSB)* yaitu mengubah bit *redundan cover image* yang tidak berpengaruh signifikan dengan bit dari pesan(Cheddad et al., 2010). Metode ini bekerja dengan cara mengganti bit terakhir dari masing-masing piksel

dengan pesan yang akan disisipkan. *Least significant bit (LSB)* merupakan algoritma terapan dari metode substitusi, dimana data normal digantikan dengan data rahasia(Krisnawati, 2015)(Pandapotan, 2016). Beberapa penelitian menggunakan metode *least significant bit (LSB)* antara lain penelitian yang dilakukan oleh Ashwak ALabaichi, Maisa'a Abid Ali K. Al-Dabbas, Adnan Salih (Alabaichi et al., 2020) *state of the art* tentang *Image steganography using least significant bit and secret map techniques.* Penelitian yang dilakukan oleh Raihan Islamadina, Baihaqi Baihaqi, Mauzar sulistriadi (Islamadina et al., 2019) *state of the art* tentang analisa steganografi untuk citra bewarna (RGB) menggunakan metode *less significant bit (LSB).* Penelitian yang dilakukan oleh Syed Farah Deeba,She Kun,Fayaz Ali Dharejo &Hira Memon (Deeba et al., 2020) *state of the art* tentang *Digital image watermarking based on ANN and least significant bit.* Penelitian yang dilakukan oleh Adit Pabbi, Rakshit Malhotra, K Manikandan (Pabbi et al., 2021) *state of the art* tentang *Implementation of Least Significant Bit Image Steganography with Advanced Encryption Standard.* Implementasi tahapan *least significant bit (LSB)* dapat dilihat pada gambar 2 sebagai berikut.



Gambar 2. Tahapan Least Significant Bit (LSB)

2.3.Transkrip Nilai

Transkrip nilai adalah laporan resmi yang wajib diterimakan kepada yang berwenang setelah menyelesaikan pendidikan di sebuah sekolah / dinyatakan lulus, transkrip nilai dapat dicetak oleh sekolah dan akan diberikan bersamaan dengan buku raport, ijasah, SKHUN, sertifikat, dan lain-lain. Fungsi transkrip nilai dapat menjelaskan prestasi akademik, menyampaikan pencapaian akademik, menunjukan perkembangan akademik mahasiswa sedangkan manfaat dan kegunaan transkrip nilai sebagai bukti prestasi akademik, bukti sudah menyelesaikan studi, bukti merupakan alumni suatu perguruan tinggi, memenuhi syarat melanjutkan studi, memenuhi syarat melamar pekerjaan(Azis, 2021).

III. METODE PENELITIAN

Sumber data penelitian ini menggunakan data transkrip nilai dan foto mahasiswa PTS di Surakarta. Pengambilan data melalui wawancara dan observasi. Wawancara dilakukan terhadap bagian akademik administrasi dan kemahasiswaan. Observasi dilakukan terhadap sistem yang selama ini berjalan. Adapun tahapan dalam metode penelitian seperti pada gambar 3 yaitu pengumpulan data (data kode mahasiswa, nilai ipk, foto), enkripsi dengan *blowfish*, konversi hasil enkripsi ke bentuk biner, penyisipan nilai biner ke metode *least significant bit (LSB)* ke dalam foto, mengambil nilai enkripsi dari foto hasil *least significant bit (LSB)*, dan mengembalikan pesan yang di enkripsi dengan *blowfish*.

Gambar 3. Tahapan Metode Penelitian Pengamanan Transkrip Nilai

IV. HASIL DAN PEMBAHASAN

4.1.Hasil Pengumpulan Data

Berdasarkan hasil penelitian yang dilakukan dengan mengambil data transkrip nilai dan foto mahasiswa dari hasil wawancara dan sampel data mahasiswa dari wakil ketua dan kepala badan administrasi akademik dan kemahasiswaan. Dari hasil wawancara didapatkan rata – rata jumlah data yang mendapatkan transkrip nilai lebih dari 100 orang dan biasanya segera dibutuhkan untuk mendaftarkan atau melanjutkan sekolah lagi atau mencari pekerjaan. Peneliti memutuskan untuk memilih data mahasiswa yang digunakan secara acak dengan jumlah sampel 10 dari masing – masing program studi. Data yang dikumpulkan berupa data nomor induk mahasiswa dan nilai IPK masing – masing mahasiswa. Beserta foto masing – masing mahasiswa yang biasanya digunakan pada transkrip nilai mahasiswa. Foto yang digunakan berukuran 210 piksel x 280 piksel seperti pada gambar 4. Data yang dienkripsi akan disisipkan pada foto tersebut. Pengambilan data latih sebanyak 30 data transkrip dan data mahasiswa yang diambil secara acak dari masing – masing prodi yang ada.

Gambar 4. Foto masing – masing mahasiswa

4.2.Enkripsi *Blowfish* dan *Least significant bit (LSB)*

Proses penelitian dari tahapan pengamanan data transkrip nilai dan data mahasiswa ini digambarkan pada gambar 3. Pada tahap pelatihan dilakukan beberapa proses yaitu:

1. Pengambilan data latih sebanyak 30 data transkrip dan data mahasiswa yang diambil secara acak dari masing – masing prodi yang ada. Data yang diambil berupa nomor induk mahasiswa (NIM), nilai IPK dan foto mahasiswa gambar 4.
2. Data NIM dan IPK dienkripsikan menggunakan algoritma *blowfish*. Hasil dari enkripsi ditunjukkan 10 data hasil enkripsi *Blowfish* dari 30 data latih ditunjukkan pada tabel 1.

Tabel 1. Hasil enkripsi data menggunakan *blowfish*

No	Nim	IPK	Hasil Enkripsi *Blowfish*
1	******001	3.53	j�z�7�r�]�T��
2	******002	3.08	U�����π�-%�7Cu�
…	…	…	…
30	******012	3.25	��Y>�Z�s����6

3. Konversi hasil data yang telah dienkripsi pada tabel 1 ke dalam bentuk biner sebelum disisipkan ke dalam foto mahasiswa. Hasil konversi dapat dilihat pada Tabel 2. Hasil enkripsi *Blowfish* diubah terlebih dahulu ke kode ASCII yang berupa data bertipe angka, kemudian diubah menjadi kode biner.

Tabel 2. Konversi hasil enkripsi ke ASCII

No	Hasil Enkripsi *Blowfish*	Jumlah Karakter	Hasil Konversi ASCII
1	j�z�7�r�]�T��	16	106 193 122 170 55 205 151 227 21 114 145 93 234 84 162 252
2	U�����π�-%�7Cu�	16	85 215 215 219 197 218 207 128 224 45 37 186 55 67 117 196
…	…	…	…
30	��Y>�Z�s����6	16	164 243 89 62 247 90 167 115 11 225 19 22 160 254 190 54

 DOI : https://doi.org/10.30646/sinus.v20i2.622

Tabel 3 menunjukan bahwa hasil enkripsi dari metode *Blowfish* pada proses enkripsi data latih ini menghasilkan 16 karakter dan dikonversikan menjadi ASCII dengan jumlah 16 bilangan bulat.

4. Setelah dikonversikan ke bentuk bilangan bulat, kemudian bilangan bulat yang didapatkan diubah ke bilangan biner. Bilangan yang terdiri hanya angka 0 dan 1. Pada penelitian ini konversi ke biner juga menggunakan fungsi PHP yang dibuat. Sehingga angka atau bilangan bulat dikonversikan ke bentuk biner.

Tabel 3. Proses Konversi ke Bilangan Biner

Bilangan Ke -	Bilangan Bulat	Konversi Biner
1	150	10010110
2	195	11000011
3	51	00110011
…	…	…
16	52	00110100

5. Langkah yang sama, diterapkan ke dalam 30 data latih yang lain sehingga hasilnya dapat dilihat pada Tabel 4.

Tabel 4. Hasil Konversi Data Latih ke Bilangan Biner

No	Bilangan Bulat (ASCII)	Bilangan Biner
1	106 193 122 170 55 205 151 227 21 114 145 93 234 84 162 252	01101010 11000001 01111010 10101010 00110111 11001101 10010111 11100011 00010101 01110010 10010001 01011101 11101010 01010100 10100010 11111100
2	85 215 215 219 197 218 207 128 224 45 37 186 55 67 117 196	01010101 11010111 11010111 11011011 11000101 11011010 11001111 10000000 11100000 00101101 00100101 10111010 00110111 01000011 01110101 11000100
…	…	…
30	164 243 89 62 247 90 167 115 11 225 19 22 160 254 190 54	10100100 11110011 01011001 00111110 11110111 01011010 10100111 01110011 00001011 11100001 00010011 00010110 10100000 11111110 10111110 00110110

6. Penyisipan bilangan biner ke citra menggunakan *least significant bit (lsb)*

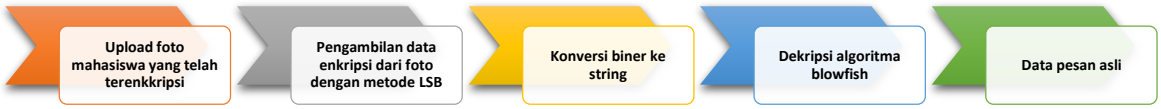
Proses penyisipan akan berjalan dengan menyisipkan tiap biner hasil enkripsi ke dalam digit terakhir nilai biner dari masing – masing piksel. Setelah enkripsi dilakukan terdapat perubahan ukuran file foto yang di enkrispi sebagaimana ditunjukan pada tabel 5 Pengukuran file ini menggunakan fungsi *php filesize().* Proses pengamanan transkrip nilai telah selesai.

Tabel 5. Perbandingan Ukuran Hasil Enkripsi Foto

No	Foto Hasil *least significant bit (LSB)*	Ukuran Sebelum Enkripsi (Kb)	Ukuran Sesudah Enkripsi (Kb)
1		17625	70419
2		16788	66105
…	…	…	…
30		17550	71867

4.3. Dekripsi *Blowfish* dan *Least Significant Bit (LSB)*

Pada tahapan dekripsi atau mengembalikan pesan ke bentuk asli ada beberapa tahapan yang diperlukan sebagaimana ditunjukkan pada Gambar 2. Proses – proses yang dilalui untuk mengembalikkan pesan asli



Gambar 5. Alur dekripsi *blowfish* dan *least significant bit (lsb)*

Hasil dari dekripsi data latih ditunjukkan pada tabel 6. Pada hasil dekripsi ini juga gambar yang digunakan diblur sebagai bentuk keamanan.

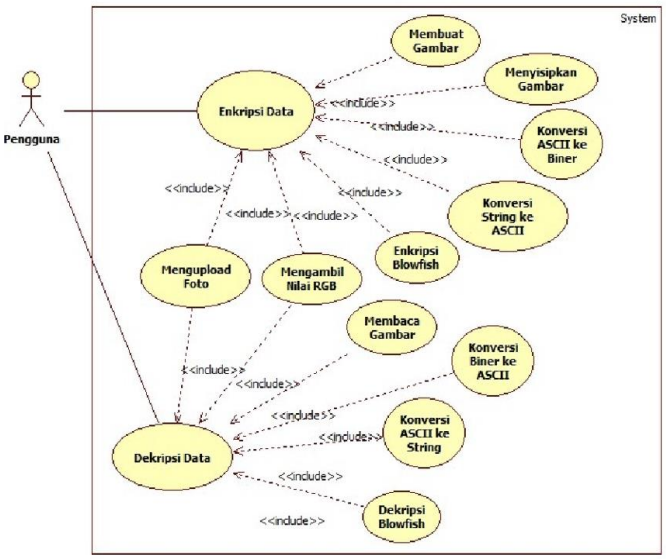
Tabel 6. Hasil Dekripsi Pesan dari Foto Mahasiswa

No	Foto Hasil *LSB*	Pesan Hasil Dekripsi	Status Pesan Hasil Dekripsi	Status Proses Enkripsi dan Dekripsi
1		******001;3.53	Terbaca	Berhasil
2		******002;3.08	Terbaca	Berhasil
…	…	…	…	…
30		******012;3.25	Terbaca	Berhasil

Dari hasil dekripsi yang ditunjukan Tabel 6 didapatkan hasil 30 data uji berhasil teridentifikasi dan terbaca pesan hasil enkrispi *blowfish* dan penyisipan *least significant bit (LSB)*.

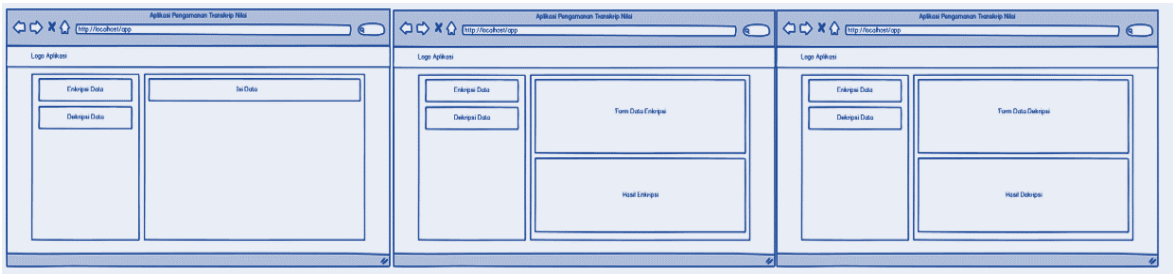
4.4. Perancangan Sistem, Antarmuka, dan Implementasi Aplikasi,

Pada tahap perancangan sistem, menggunakan diagram *use case* yang ditunjukan pada gambar 6, pada diagram *use case* terdapat *actor* pengguna dan terdapat 2 *use case* utama enkripsi data, dan deskripsi data. Perancangan antar muka ditunjukkan pada gambar 7 rancangan tampilan halaman beranda, tampilan halaman enkripsi, dekripsi. implementasi aplikasi ditunjukkan pada gambar 8 tampilan beranda, tampilan enkripsi, dan tampilan dekripsi.



Gambar 6. *Use case* diagram

 DOI : https://doi.org/10.30646/sinus.v20i2.622



Gambar 7. Rancangan tampilan halaman beranda, tampilan halaman enkripsi, dekripsi

Gambar 8. Tampilan aplikasi halaman beranda, halaman enkripsi dan halaman dekripsi

4.5. Pengujian Sistem

Pada tahap pengujian sistem dilakukan dengan pengujian fungsionalitas sistem dan pengujian tingkat akurasi data. Pengujian fungsional sistem dilakukan dengan metode *blackbox testing*. Hasil pengujian *blackbox* ditunjukan pada tabel 7. Rekapitulasi hasil uji untuk masing – masing menu didapatkan hasil sesuai atau berjalan sesuai fungsinya. Jadi, sistem untuk pengamanan trnaskrip nilai menggunakan metode *blowfish* dan algoritma *least significant bit (LSB)* ini sudah berjalan sesuai dengan yang diharapkan. Dari pengujian pada tabel 8 hasil uji enkripsi dan dekripsi data uji dari 60 data mahasiswa yang telah dienkripsi dan didekripsikan kembali untuk mengambil pesan asli berhasil terenkripsi 60 data mahasiswa. Sedangkan hasil pengujian tigkat akurasi data pada 60 data mahasiswa yang telah dienkripsi dan didekripsikan kembali untuk mengambil pesan dari pengujian tersebut didapatkan hasil 100% dari 60 data yang diuji sehingga sistem yang didapatkan mampu mengenkripsi pesan dan mengembalikan pesan enkripsi ke pesan asli yang disisipkan ke gambar.

Tabel 7. Hasil rekapitulasi uji fungsionalitas

Nama Fungsi	Hasil Uji
Menu Beranda	Sesuai
Menu Enkripsi Data	Sesuai
Menu Dekripsi Data	Sesuai

Tabel 8. Hasil uji enkripsi dan dekripsi data uji

No	Foto Mahasiswa	Nama Data	Hasil Enkripsi Data	Hasil *LSB*	Hasil Dekripsi	Hasil Uji
1		Data 1	Data Terenkripsi		Terbaca Pesan Asli	Berhasil
2		Data 2	Data Terenkripsi		Terbaca Pesan Asli	Berhasil
…	…	…	…	…	…	…
30		Data 30	Data Terenkripsi		Terbaca Pesan Asli	Berhasil
…	…	…	…	…	…	…
60		Data 60	Data Terenkripsi		Terbaca Pesan Asli	Berhasil

V. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil penelitian dengan mengambil sampel sebanyak dari 60 data uji yang digunakan proses pengamanan pesan dapat dilakukan dengan algoritma enkripsi *blowfish* dan pesan dapat dikembalikan lagi dengan algoritma dekripsi *blowfish*. Hasil enkripsi dapat disisipkan ke dalam foto mahasiswa dengan metode *least significant bit (LSB)* dan pesan dapat diambil kembali dari file foto dengan lengkap. Sistem mampu dengan prosentase 100% mengenkripsi pesan dan mendekripsikan pesan yang diambil dari foto hasil *least significant bit (LSB)*.

5.2 Saran

Peneliti memberikan saran agar semakin sempurna dalam proses pengamanan transkrip nilai di perguruan tinggi dapat mengoptimasi atau mengkombinasikan beberapa metode atau algoritma enkripsi yang lainnya, atau dengan menambahkan beberapa variabel selain yang ada di penelitian ini.

DAFTAR PUSTAKA

Abbas, S. Z., Ibrahim, H., & Khan, M. (2021). A hybrid chaotic blowfish encryption for high-resolution satellite imagery. *Multimedia Tools and Applications*, *80*(17), 26069–26091. https://doi.org/10.1007/s11042-021-10898-w

Alabaichi, A., Al-Dabbas, M. A. A. K., & Salih, A. (2020). Image steganography using least significant bit and secret map techniques. *International Journal of Electrical and Computer Engineering (IJECE)*, *10*(1), 935. https://doi.org/10.11591/ijece.v10i1.pp935-946

Althaf, S. (2017). Implementasi Keamanan Data Menggunakan Algoritma Blowfish Pada Sistem Informasi Koperasi Rias. *Simetris: Jurnal Teknik Mesin, Elektro Dan Ilmu …*. http://jurnal.umk.ac.id/index.php/simet/article/view/952

Ariyus, D. (2008). *Pengantar ilmu kriptografi: teori analisis & implementasi*. books.google.com. https://books.google.com/books?hl=en&lr=&id=3SSTJONEmX0C&oi=fnd&pg=PA49&dq=pengantar+ilmu+kriptografi+teori+analisis+dan+implementasi&ots=ujGEwhiGry&sig=4pWJmW8XUUt1C7qVSM8C5jIfuMg

Azis, Y. A. (2021, December 13). *Transkrip Nilai Kuliah: Pengertian, Fungsi dan Contoh*. Penerbitbukudeepublish.Com. https://penerbitbukudeepublish.com/transkrip-nilai/

Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. *Signal Processing*, *90*(3), 727–752. https://doi.org/https://doi.org/10.1016/j.sigpro.2009.08.010

Deeba, F., Kun, S., Dharejo, F. A., & Memon, H. (2020). Digital image watermarking based on ANN and least significant bit. *Information Security Journal: A Global Perspective*, *29*(1), 30–39. https://doi.org/10.1080/19393555.2020.1717684

Hamzah, A., GA, I. B., & Raharjo, S. (2013). Penerapan Digital Signature Pada Transkrip Nilai Sebagai Otentikasi Data. *Jurnal Jarkom*, *1*(1), 29–36.

Hendrawaty, H., Azhar, A., & Atthariq, A. (2016). Implementasi Algoritma RSA dan QR Code Untuk Keamanan Transkrip Nilai di Politeknik Negeri Lhokseumawe. *Jurnal Infomedia: Teknik …*. http://e-jurnal.pnl.ac.id/infomedia/article/view/331

Ilasariya, S., Patel, P., Patel, V., & Gharat, S. (2022). Image Steganography Using Blowfish Algorithm and Transmission via Apache Kafka. *2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT)*, 1320–1325. https://doi.org/10.1109/ICSSIT53264.2022.9716292

Islamadina, R., Baihaqi, B., & Sulistriadi, M. (2019). Analisa Steganografi untuk Citra Bewarna (RGB) Menggunakan Metode Less Significant Bit (LSB). *Jurnal Nasional Komputasi Dan Teknologi Informasi (JNKTI)*, *2*(1), 55. https://doi.org/10.32672/jnkti.v2i1.1058

Keswara, R. (2014, January 10). *Marak pemalsuan transkip nilai PTS*. Www.Sindonews.Com. https://daerah.sindonews.com/berita/825247/22/marak-pemalsuan-transkip-nilai-pts

Krisnawati, K. (2015). Metode Least Significant Bit (Lsb) Dan End of File (Eof) Untuk Menyisipkan Teks Ke Dalam Citra Grayscale. *Seminar Nasional Informatika (SEMNASIF)*. http://103.23.20.161/index.php/semnasif/article/view/698

Mardira, S. (2015). *Polisi Bongkar Sindikat Pemalsu Ratusan Ijazah Unsyiah*. Www.News.Okezone.Com. https://news.okezone.com/read/2015/06/11/340/1163572/polisi-bongkar-sindikat-pemalsu-ratusan-ijazah-unsyiah

Pabbi, A., Malhotra, R., & Manikandan, K. (2021). Implementation of Least Significant Bit Image Steganography with Advanced Encryption Standard. *2021 International Conference on Emerging Smart Computing and Informatics (ESCI)*, 363–366. https://doi.org/10.1109/ESCI50559.2021.9396884

Pandapotan, T. S. (2016). Analisa Perbandingan Least Significant Bit (LSB) Dan End Of File (EOF) Untuk Steganografi Citra Digital Menggunakan Matlab. In *Jurnal INFOTEK* (Vol. 1, Issue 3). www.stmik-budidarma.ac.id

Prabowo, I. A. (2022). BAB 2 Pencatatan dan Penyimpanan Informasi Database. *Pengantar Teknologi Informasi*. https://books.google.com/books?hl=en&lr=&id=PspuEAAAQBAJ&oi=fnd&pg=PA18&dq=iwan+ady+prabowo&ots=WZ3-TNhq2I&sig=cAD299BDK-jfAtx0fwhiWBvc7PM

Retno, S., & Hasdyna, N. (2018). Analisis Kinerja Algoritma Honey Encryption dan Algoritma Blowfish Pada Proses Enkripsi Dan Dekripsi. *TECHSI-Jurnal Teknik Informatika*. https://ojs.unimal.ac.id/techsi/article/view/858

Saddam, M. J., Ibrahim, A. A., & ... (2020). A lightweight image encryption and blowfish decryption for the secure internet of things. *2020 4th International …*. https://ieeexplore.ieee.org/abstract/document/9254366/

Simanullang, H. G., & Silalahi, A. P. (2018). Algoritma Blowfish Untuk Meningkatkan Keamanan database Mysql. *METHODIKA: Jurnal Teknik …*. https://ejurnal.methodist.ac.id/index.php/methodika/article/download/58/47

Siregar, K. P., & Ariwibowo, E. (2014). Implementasi Keamanan Data Menggunakan Algoritma Blowfish dan LSB Pada Citra. *Jurnal Sarjana Teknik …*. https://garuda.kemdikbud.go.id/documents/detail/1872221

Sitinjak, S., Fauziah, Y., & Juwairiah, J. (2015). Aplikasi Kriptografi File Menggunakan Algoritma Blowfish. *Seminar Nasional Informatika …*. http://103.23.20.161/index.php/semnasif/article/view/1174

Sofyan, D. ; K., Elfany ; Elisa, Fanny ; Sinaga, Fathan Ghifari ; Girsang, Ken ; Mesya, & M. ; Amjad, M. (2014, December 12). *UNM Usut Pembuat Ijazah Palsu*. Https://Www.Jpnn.Com. https://www.jpnn.com/news/unm-usut-pembuat-ijazah-palsu

Zulfikar, M. I., Abdillah, G., & Komarudin, A. (2019). Kriptografi untuk Keamanan Pengiriman Email Menggunakan Blowfish dan Rivest Shamir Adleman (RSA). *Seminar Nasional Aplikasi Teknologi Informasi …*.