Journal of Information Sistem Research (JOSH)
Volume 2, No. 1, October 2020
ISSN 2686-228X (media online)
Hal: 14-25

Implementasi Algoritma Camellia Pada Penyandian Citra USG

Fara Dibba Mutiara Maharani

Program Studi Teknik Informatika, Universitas Budi Darma, Medan, Indonesia
Email: faradibbamutiaramaharani@gmail.com

Abstrak−Citra digital sangat rentan terhadap penyandapan maupun pencurian data oleh pihak- pihak yang tidak bertanggung jawab.. Demi menjaga keamanan citra USG dapat dilakukan dengan pemanfaatan teknik kriptografi.Teknik kriptografi dapat menyandikan citra USG dengan mengenkripsikannya ke dalam bentuk sandi-sandi yang tidak dipahami. Algoritma Camellia adalah salah satu algoritma yang dapat diandalkan dalam mewujudkan teknik kriptografi. Algoritma simetri ini akan menghasilkan tingkat keamanan yang lebih tinggi terhadap citra USG karena dapat menyandikannya kebentuk sandi dengan proses yang cukup rumit sehingga akan mempersulit kriptanalis untuk mengakses citra tersebut. Penelitian ini akan menggunakan Algoritma Camellia 128 bit untuk proses enkripsi dan dekripsinya, sehingga dalam prosesnya perlu melalui beberapa tahap yang panjang agar dapat menghasilkan cipher akhirnya. Algoritma ini memerlukan 18 ronde dimana setiap enam ronde harus memasuki Fungsi F dan Fungsi FL-1dan juga memerlukan sebanyak 26 subkunci yaitu kw, k dan kl. Penelitian ini menguraikan proses pengamanan citra USG dengan menyandikannya berdasarkan algoritma Camellia, dalam bentuk sandi yang sulit dipahami dan dimengerti oleh orang lain. Hal ini dilakukan sebagai upaya untuk meminimalisir tindakan-tindakan penyalahgunaan citra USG.

Kata Kunci: Kriptografi, Citra USG, Camellia

Abstract−Digital images are very vulnerable to data capture or theft by irresponsible parties. For the sake of maintaining the security of USG images can be done by using cryptographic techniques. Cryptographic techniques can encode ultrasound images by encrypting them in the form of codes that are not understood. Camellia Algorithm is one algorithm that can be relied upon to realize cryptographic techniques. This symmetry algorithm will produce a higher level of security to the USG image because it can encode it into a cipher with a process that is complex enough so that it will be difficult for cryptanalysts to access the image. This research will use the 128-bit Camellia Algorithm for the encryption and decryption process, so the process needs to go through several long stages in order to produce the final cipher. This algorithm requires 18 rounds where every six rounds must enter Function F and FL-1 Functions and also requires as many as 26 subkeys namely kw, k and kl. This study describes the process of securing the USG image by encoding it based on the Camellia algorithm, in the form of a password that is difficult for others to understand and understand. This is done as an effort to minimize acts of misuse of the USG image.

Keywords: Cryptography, Ultrasound Images, Camellia

1. PENDAHULUAN

Keamanan data hal yang sangat penting dalam menjaga kerahasiaan informasi, teruama yang berisi informasi penting yang hanya diketahui isinya oleh pihak tertentu, sehingga perlu dilakukan penyandian data. Salah satu metode dalam keamanan data adalah kriptografi. Mengamankan data dengan teknik kriptografi merupakan sebuah aktivitas menyembunyikan data dengan mengubah data asli kedalam bentuk lain, dalam arti makna pesan tersebut diubah dari data yang bermakna ke data yang tidak bermakna. Pada saat ini kriptografi terus berkembang sehingga algoritma-algoritma kriptografi yang ada semakin bertambah jumlahnya.

Masalah yang sering terjadi selama ini yaitu kurangnya kemanan data pada hasil USG. Dimana hasil USG itu sangat penting untuk diamankan dan dirahasiakan oleh pihak agar tidak terjadinya perubahan data dari hasil USG yang baik dan benar diubah dalam data atau bentuk yang tidak baik atau tidak benar. Diagnostik ultrasonik berkembang dengan pesatnya, sehingga saat ini masih banyak ibu hamil tidak mengamankan hasil USG tersebut. Pengamanan data pada dunia maya atau didunia nyata sangatlah penting supaya data yang sangat penting tidak tersebar ke publik atau orang lain yang nanti berakibat dapat disalah gunakan oleh orang lain.

Didalam kriptografi banyak metode yang dapat digunakan, salah satu metode kriptografi yang dapat digunakan untuk mengamankan data adalah algoritma Camellia, dimana algoritma camellia banyak kemampuan dalam menjaga dan merahasiakan suatu data dengan cara mengacak isi data. Adapun data yang dapat diamankan dengan metode kriptografi yaitu seperti data teks, video, gambar, suara dan lain sebagainya. Algortima ini dapat menyelesaikan proses enkrip dan dekripsi dengan cepat, yang mana juga merupakan salah satu algoritma memiliki banyak variasi kunci yaitu 128 bit, 192 bit dan 256 bit. Algoritma Camellia merupakan salah satu blok *cipher* yang memiliki ukuran 128 bit. Algoritma Camellia merupakan modifikasi Feistel *Cipher* yang memiliki putaran sebanyak 18 *round* jikalau menggunakan kunci berukuran 128 bit atau sebanyak 24 *round* jikalau menggunakan kunci berukuran 192 bit atau 256 bit.

Citra USG diproses dengan algoritma camellia sehingga menghasilkan multirasolusi dari citra aslinya. Algoritma ini mampu mengekripsikan data dengan mengubah data kedalam bentuk simbol-simbol yang tidak dapat dimengerti oleh pembaca. Setelah data disandikan, maka data dapat dikirim ataupun disimpan dengan aman. Data yang terenkripsi dapat dikembalikan ke bentuk semula dengan melakukan proses dekripsi dengan menggunakan variasi kunci yang sama sehingga data yang disandikan kembali ke dalam bentuk semula. Ultrasonografi (USG) merupakan salah satu imaging diagnostic (pencitraan diagnostik) untuk pemeriksaan alat-alat dalam tubuh manusia, dimana kita dapat mempelajari bentuk. Ukuran anatomis, gerakan serta hubungan dengan jaringan sekitarnya.

Berdasarkan penelitian yang dilakukan oleh Herman Zuhri dalam Implementasi metode camellia dalam keamanan data file berekstensi TXT dan DOC bahwa, algoritma camellia dikenal dengan metode memiliki waktu ekripsi dan dekripsi yang cepat. Metode camellia ini memiliki keistimewaan dibandingkan dengan metode kriptografi yang lainnya

Submitted: **09/07/2020**; Accepted: **09/10/2020**; Published: **26/10/2020**

Journal of Information Sistem Research (JOSH)
Volume 2, No. 1, October 2020
ISSN 2686-228X (media online)
Hal: 14-25

maka dapat menghasilkan pengiriman data-data rahasia berbentuk Txt dan Doc dapat diterima oleh orang yang berhak menggunakannya dan tersimpan dengan aman. Kemudian menurut penelitian Wahyuni Khabzli perkembangan teknologi sekarang ini sangat penting dalam pengiriman suatu informasi, sehingga menyebabkan tingginya tingkat resiko dalam pembajakan data. Camellia merupakan block chipper yang dirancang oleh ahli-ahli dalam riset dan pengembangan teknik kriprografi.

2. METODOLOGI PENELITIAN

2.1 Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa yunani, yaitu dari kata *cypto* dan *graphia* yang berarti penulisan rahasia. Kriptografi adalah ilmu ataupun seni yang mempelajari bagaimana membuat suatu pesan yang dikirim oleh pengirim dapat disampaikan kepada penerima dengan aman. Kriptografi juga merupakan studi terhadap teknik matematis yang terkait dengan aspek keamanan suatu sistem informasi seperti kerahasiaan, integritas data, autentikasi dan ketiadaan penyangkalan [2].

2.2 Algoritma Camellia

Algoritma Camellia dikembangkan secara ber-sama oleh NTT dan Mitsubishi Electric Corporation pada tahun 2000. Algoritma ini mengadopsi algorit-ma kriptografi E2 (dikembangkan oleh NTT) dan algoritma kriptografi MISTY (dikembangkan oleh Mitsubishi).

Pada algoritma Camellia, sebuah blok memiliki ukuran 128 bit. Panjang kunci bervariasi antara 128 bit, 192 bit atau 256 bit. Algoritma Camellia me-rupakan modifikasi Feistel Cipher sebanyak 18 putaran (ketika panjang kunci 128 bit) atau 24 putaran (ketika panjang kunci 192 atau 256 bit).

Algoritma Camellia merupakan algoritma yang dipatenkan namun memiliki *royalty free licences* yang menjadikan pengguna algoritma Camellia tidak membayar dalam penggunaan algoritma ini. *Royalty free licences* ini berlaku jika tidak merubah algoritma yang telah ditetapkan.

1. Prosedur Enkripsi 128 bit
   Enkripsi menggunakan kunci 128 bit meng-gunakan struktur Feistel Cipher yang terdiri atas 18 putaran dengan 2 lapisan fungsi FL/FL-1 setelah tahap keenam dan tahap keduabelas. Pertama-tama blok pertama plainteks dipecah menjadi dua, kemudian masing-masing dixor-kan dengan kw1 dan kw2. Hasilnya ialah L0 dan R0. Pada putaran pertama, L0 dimasukkan ke fungsi F beserta k1. Hasilnya kemudian dixor-kan dengan R0. Pada putaran kedua, L0 akan menjadi R1, sedangkan hasil xor tadi menjadi L1. L1 ini kemudian dimasukan ke fungsi F lagi beserta k2. Demikian seterusnya hingga putaran keenam. Sebelum putaran ketujuh, L6 akan memasuki fungsi FL bersama kl1, dan R6 akan memasuki fungsi FL-1 bersama kl2. Hasil masing-masing akan kembali dienkripsi dengan cara seperti tadi sebanyak 6 putaran lagi, dan sebelum putaran ketigabelas akan menggunakan fungsi FL/FL-1 lagi. Kemudian dienkripsi dengan fungsi F lagi sebanyak 6 putaran. Sehingga total putaran adalah 18. Terakhir L18 akan dixor-kan dengan kw4 dan R18 akan dixor-kan dengan kw3. Hasilnya kemudian digabung, itulah cipherteks dari blok pertama plainteks.
2. Proses Dekripsi
   Pada proses dekripsi dengan kunci 128 bit, pertama-tama blok cipherteks akan dibagi menjadi dua kemudian masing-masing dixor-kan dengan kw3 dan kw4. Setelah itu subblok kiri maupun kanan akan didekripsi dengan cara yang sama seperti pada proses enkripsi, namun perbedaannya ialah peng-gunaan subkuncinya digunakan dari subkunci terakhir. Kemudian sebelum putaran berikutnya akan memasuki fungsi FL dan FL-1 menggunakan sub-kunci kl4 dan kl3. Setelah itu kembali akan memasuki Feistel Cipher sebanyak 6 putaran, masing-masing dengan menggunakan subkunci k12 hingga k7. Kemudian masuk ke fungsi FL dan FL-1 menggunakan subkunci kl2 dan kl1. Setelah itu didekripsi lagi dengan Feistel Cipher 6 putaran, masing-masing dengan menggunakan subkunci k6 hingga k1. Pada tahap terakhir, subblok kiri dixor-kan dengan kw1 dan subblok kanan akan dixor-kan dengan kw2. Hasil penggabungan dua subblok ini merupakan plainteks blok pertama dari cipherteks [7].

2.3 Citra Digital

Salah satu bentuk citra adalah citra yang mengandung abstrak dari citra matematis yang berisi fungsi kontinu dan fungis diskrit atau citra digital. Citra yang memiliki fungsi diskrit inilah yang dapat diolah oleh komputer. Setiap citra digital memiliki beberapa karakterstik, antara lain ukuran citra, resolusi dan format nilainya. Untuk itu citra digital harus mempunyai format tertentu yang sesuai sehingga dapat merepresentasikan obyek pencitraan dalam bentuk kombinasi data biner [8].

3. HASIL DAN PEMBAHASAN

Citra digital sangat rentan terhadap penyandapan maupun pencurian data oleh pihak-pihak yang tidak bertanggung jawab untuk keuntungan pribadi maupun kelompok. Citra digital sangat mudah didistribusikan secara bebas melalui jaringan internet.

Submitted: **09/07/2020**; Accepted: **09/10/2020**; Published: **26/10/2020**

Journal of Information Sistem Research (JOSH)
Volume 2, No. 1, October 2020
ISSN 2686-228X (media online)
Hal: 14-25

Citra hasil USG yang merupakan suatu informasi rahasia yang dapat digunakan dalam beberapa bentuk bidang. maka dari itu citra hasil usg perlu diamankan agar tidak di salah gunakan oleh pihak-pihak yang tidak ertanggung jawab. Apabila citra hasil USG tersebar luaskan tanpa adanya pengamanan dapat menimbulkan kerugian pada pihak tertentu. Keamanan pada citra hasil USG dapat dilakukan dengan menggunakan salah satu metode pada teknik kriptografi.

3.1 Penerapan Algoritma Camellia

Berdasarkan *plainimage* diatas, maka akan diambil 16 pixel sebagai contoh perhitungan manual. Enam belas piksel tersebut akan diambil nilai desimal pada setiap warnanya. Nilai warna dari 16 piksel *plainimage* contoh diatas adalah: =(154 118 78 63 150 116 78 61 149 118 81 63 149 122 86 65).

1. Kunci masukkan dibagi menjadi dua bagian variabel, yaitu K_L dan K_R. Masing-masing variabel berukuran 128 bit. Khusus kunci berukuran 128 bit, K_R=0.
2. Variabel K_L dan K_R di-XOR kan, kemudian dienkripsikan dengan nilai konstanta $\sum_1$ dan $\sum_2$.
3. Hasil enkripsi sebelumnya di-XOR kan dengan K_L dan kemudian diekripsikan dengan nilai konstanta $\sum_3$ dan $\sum_4$. Hasil dari enkripsi ini adalah K_A.
4. Kemudian K_A di-XOR dengan K_R dan kemudian diekripsikan dengan nilai konstanta $\sum_5$ dan $\sum_6$.Hasil dari enkripsi ini adalah K_B.

Tabel 1. Nilai Konstanta

$\sum_1$	0xA09E6673FBCC908B
$\sum_2$	0xB67AE8584CAA73B2
$\sum_3$	0xC6EF372FE94F82BE
$\sum_4$	0x54FF53A5F1D36F1C
$\sum_5$	0x10E527FADE682D1D
$\sum_6$	0xB05688C2B3E6C1FD

Ciphertext : 154 118 78 63 150 116 78 61 149 118 81 63 149 122 86 65
Key = FARADIBBA-221997
= 4641 5241 4449 4242 412D 3232 3139 3937

1. Penjadwalan Kunci
   KL = 4641 5241 4449 4242 412D 3232 3139 3937
   KL_L = 4641 5241 4449 4242
   KL_R = 412D 3232 3139 3937

   a. Misalkan $P(S(KL_L \oplus \sum_1))$= A

   $A \oplus KL_R$ = A'
   $P(S(A' \oplus \sum_2))$ = B
   $B \oplus KL_L$ = B'
   $P(S(B \oplus \sum_3))$ = C
   $C \oplus A$ = C'
   $P(S(C' \oplus \sum_4))$ = D
   $D \oplus B$ = D'
   $D' \| C'$ = K_A

   A = $KL_L \oplus \sum_1$
   = 4641 5241 4449 4242$\oplus$ A09E6673FBCC908B
   = E6DF 3432 BF85 D2C9

   $P(S(A_{8(8)}))$ = E6 = $S_1(230)$ =172
   $P(S(A_{7(8)}))$ = DF = $S_4(223)$ = 46
   $P(S(A_{6(8)}))$ = 34 = $S_3(52)$ =234
   $P(S(A_{5(8)}))$ = 32 = $S_2(50)$ = 95
   $P(S(A_{4(8)}))$ = BF = $S_4(47)$ = 4
   $P(S(A_{3(8)}))$ = 85 = $S_3(133)$ =196
   $P(S(A_{2(8)}))$ = D2 = $S_2(210)$ =239
   $P(S(A_{1(8)}))$ =C9 = $S_1(201)$ =245

   A = AC2E EA5F 04C4 EFF5
   A' = A $\oplus$ KL_R
   = AC2E EA5F 04C4 EFF5$\oplus$ 412D 3232 3139 3937
   = ED03 D86D 35FD D6C2
   B = A'$\oplus \sum_2$
   = ED03 D86D 35FD D6C2$\oplus$ B67AE8584CAA73B2
   = 5B79 3035 7957 A570

   $P(S(B_{8(8)}))$ = 5B = $S_1(91)$ = 49
   $P(S(B_{7(8)}))$ = 79 = $S_4(121)$ = 211
   $P(S(B_{6(8)}))$ = 30 = $S_3(48)$ = 83

Submitted: **09/07/2020**; Accepted: **09/10/2020**; Published: **26/10/2020**

Journal of Information Sistem Research (JOSH)
Volume 2, No. 1, October 2020
ISSN 2686-228X (media online)
Hal: 14-25

$P(S(B_{5(8)}))$ = 35 $=S_2(53)$ = 142
$P(S(B_{4(8)}))$ = 79 $=S_4(121)$ = 211
$P(S(B_{3(8)}))$ = 57 $=S_3(87)$ = 130
$P(S(B_{2(8)}))$ = A5 $=S_2(165)$ =148
$P(S(B_{1(8)}))$ = 70 $=S_1(112)$ = 254

B = 31D3 538E D382 94FE
B' = B $\oplus$ KL_L
= 31D3538ED38294FE $\oplus$ 4641 5241 4449 4242
= 7792 01CF 97CB D6BC

B' $\oplus$ KL_L = B
A' $\oplus$ KL_R = A
C = $P(S(B \oplus \sum_3))$
= 7792 01CF 97CB D6BC $\oplus$ C6EF372FE94F82BE
= B17D 36E0 7E84 5402

$P(S(C_{8(8)}))$ = B1 $=S_1(177)$ =155
$P(S(C_{7(8)}))$ = 7D $=S_4(125)$ = 173
$P(S(C_{6(8)}))$ = 36 $=S_3(54)$ = 174
$P(S(C_{5(8)}))$ = E0 $=S_2(224)$ =114
$P(S(C_{4(8)}))$ = 7E $=S_4(126)$ = 119
$P(S(C_{3(8)}))$ = 84 $=S_3(132)$ = 208
$P(S(C_{2(8)}))$ = 54 $=S_2(84)$ =52
$P(S(C_{1(8)}))$ = 02 $=S_1(02)$ =44

C = 9BAD AE72 77D0 342C
C' = C $\oplus$ A
= 9BAD AE72 77D0 342C $\oplus$ AC2E EA5F 04C4 EFF5
= 3783 442D 7314 DBD9

D = $P(S(C' \oplus \sum_4))$
= 3783 442D 7314 DBD9 $\oplus$ 54FF53A5F1D36F1C
= 637C 1788 82C7 B4C5

$P(S(D_{8(8)}))$ = 63 $=S_1(99)$ = 97
$P(S(D_{7(8)}))$ = 7C $=S_4(124)$ = 21
$P(S(D_{6(8)}))$ = 17 $=S_3(23)$ = 144
$P(S(D_{5(8)}))$ = 88 $=S_2(136)$ = 47
$P(S(D_{4(8)}))$ = 82 $=S_4(130)$ = 39
$P(S(D_{3(8)}))$ = C7 $=S_3(199)$ = 71
$P(S(D_{2(8)}))$ = B4 $=S_2(180)$ = 145
$P(S(D_{1(8)}))$ = C5 $=S_1(197)$ = 110

D = 6115 902F 2747 916E
D' = D $\oplus$ B
= 6115 902F 2747 916E $\oplus$ 31D3 538E D382 94FE
= 50C6 C3A1 F4C5 0590

K_A = C' || D'
K_A = 3783 442D 7314 DBD9 50C6 C3A1 F4C5 0590

Tabel 2. Subkunci algoritma Camellia

	Subkunci	Nilai
Prewhitening	$Kw_{1(64)}$	$(KL<<<0)_{L(64)}$
	$Kw_{2(64)}$	$(KL<<<0)_{R(64)}$
F (Tahap 1)	$k_{1(64)}$	$(KA<<<0)_{L(64)}$
F (Tahap 2)	$k_{2(64)}$	$(KA<<<0)_{R(64)}$
F (Tahap 3)	$k_{3(64)}$	$(KL<<<15)_{L(64)}$
F (Tahap 4)	$k_{4(64)}$	$(KL<<<15)_{R(64)}$
F (Tahap 5)	$k_{5(64)}$	$(KA<<<15)_{L(64)}$
F (Tahap 6)	$k_{6(64)}$	$(KA<<<15)_{R(64)}$
FL	$kl_{1(64)}$	$(KA<<<30)_{L(64)}$
FL^{-1}	$kl_{2(64)}$	$(KA<<<30)_{R(64)}$
F (Tahap 7)	$k_{7(64)}$	$(KL<<<45)_{L(64)}$
F (Tahap 8)	$k_{8(64)}$	$(KL<<<45)_{R(64)}$
F (Tahap 9)	$K_{9(64)}$	$(KA<<<45)_{L(64)}$
F (Tahap 10)	$k_{10(64)}$	$(KL<<<60)_{R(64)}$
F (Tahap 11)	$k_{1164)}$	$(KA<<<60)_{L(64)}$

Submitted: **09/07/2020**; Accepted: **09/10/2020**; Published: **26/10/2020**

Journal of Information Sistem Research (JOSH)
Volume 2, No. 1, October 2020
ISSN 2686-228X (media online)
Hal: 14-25

	Subkunci	Nilai
F (Tahap 12)	$k_{12(64)}$	$(KA<<<60)_{R(64)}$
FL	$kl_{3(64)}$	$(KL<<<77)_{L(64)}$
FL^{-1}	$kl_{4(64)}$	$(KL<<<77)_{R(64)}$
F (Tahap 13)	$k_{13(64)}$	$(KL<<<94)_{L(64)}$
F (Tahap 14)	$k_{14(64)}$	$(KL<<<94)_{R(64)}$
F (Tahap 15)	$k_{15(64)}$	$(KA<<<94)_{L(64)}$
F (Tahap 16)	$k_{16(64)}$	$(KA<<<94)_{R(64)}$
F (Tahap 17)	$k_{17(64)}$	$(KL<<<111)_{L(64)}$
F (Tahap 18)	$k_{18(64)}$	$(KL<<<111)_{R(64)}$
Postwhitening	$Kw_{3(64)}$	$(KA<<<111)_{L(64)}$
	$Kw_{4(64)}$	$(KA<<<111)_{R(64)}$

K_A = 3783 442D 7314 DBD9 50C6 C3A1 F4C5 0590
KL = 4641 5241 4449 4242 412D 3232 3139 3937

a. $Kw_{1(64)} = (KL <<< 0)_{L(64)}$ = 4641 5241 4449 4242
$Kw_{2(64)} = (KL <<< 0)_{R(64)}$ = 412D 3232 3139 3937
$k_{1(64)} = (KA <<< 0)_{L(64)}$ = 3783 442D 7314 DBD9
$k_{2(64)} = (KA <<< 0)_{R(64)}$ = 50C6 C3A1 F4C5 0590
$k_{3(64)} = (KL <<< 15)_{L(64)}$ = A920 A224 A121 2096
$k_{4(64)} = (KL <<< 15)_{R(64)}$ = 9919 189C 9C9B A320
$k_{5(64)} = (KA <<< 15)_{L(64)}$ = A216 B98A 6DEC A863
$k_{6(64)} = (KA <<< 15)_{R(64)}$ = 61D0 FA62 82C8 1BC1
$kl_{1(64)} = (KA <<< 30)_{L(64)}$ = 5CC5 36F6 5431 B0E8
$kl_{2(64)} = (KA <<< 30)_{R(64)}$ = 7D31 4164 0DE0 D10B
$k_{7(64)} = (KL <<< 45)_{L(64)}$ = 2848 4825 A646 4627
$k_{8(64)} = (KL <<< 45)_{R(64)}$ = 2726 E8C8 2A48 2889
$k_{9(64)} = (KA <<< 45)_{L(64)}$ = 9B7B 2A18 D874 3E98
$k_{10(64)} = (KL <<< 60)_{R(64)}$ = 7464 1524 1444 9424
$k_{11(64)} = (KA <<< 60)_{L(64)}$ = 950C 6C3A 1F4C 5059
$k_{12(64)} = (KA <<< 60)_{R(64)}$ = 378 3442 D731 4DBD
$kl_{3(64)} = (KL <<< 77)_{L(64)}$ = A646 4627 2726 E8C8
$kl_{4(64)} = (KL <<< 77)_{R(64)}$ = 2A48 2889 2848 4825
$k_{13(64)} = (KL <<< 94)_{L(64)}$ = 8C4E 4E4D D190 5490
$k_{14(64)} = (KL <<< 94)_{R(64)}$ = 5112 5090 904B 4C8C
$k_{15(64)} = (KA <<< 94)_{L(64)}$ = D874 3E98 A0B2 06F0
$k_{16(64)} = (KA <<< 94)_{R(64)}$ = 6885 AE62 9B7B 2A18
$k_{17(64)} = (KL <<< 111)_{L(64)}$ = 9C9B A320 A920 A224
$k_{18(64)} = (KL <<< 111)_{R(64)}$ = A121 2096 9919 189C
$Kw_{3(64)} = (KA <<< 111)_{L(64)}$ = 7D31 4164 0DE0 D10B
$Kw_{4(64)} = (KA <<< 111)_{R(64)}$ = 5CC5 36F6 5431 B0E8

2. Proses Enkripsi
Hasil pixel : 154 118 78 63 150 116 78 61 149 118 81 63 149 122 86 65
$\mathbf{M_{(128)}}$ = 9A76 4E3F 9674 4E3D 9576 513F 957A 5641
$M_{L(64)}$ = 9A76 4E3F 9674 4E3D
$M_{R(64)}$ = 9576 513F 957A 5641
$L_0 = M_{L(64)} \oplus kw_1$
= 9A76 4E3F 9674 4E3D $\oplus$ 4641 5241 4449 4242
= DC37 1C7E D23D 0C7F
$R_0 = M_{R(64)} \oplus kw_2$
= 9576 513F 957A 5641$\oplus$ 412D 3232 3139 3937
= D45B 630D A443 6F76

Round →1
$L_1 = R_0 \oplus F(L_0, k_1)$
$R_1 = L_0$
$L_1 = R_0 \oplus F(L_0, k_1)$
= D45B 630D A443 6F76$\oplus$F (L_0, k_1)
R_1 = D45B 630D A443 6F76
k_1 = 3783 442D 7314 DBD9
$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = P(S(X_{(64)} \oplus k_{(64)}))$

Submitted: **09/07/2020**; Accepted: **09/10/2020**; Published: **26/10/2020**

$X_{(64)} \oplus k_{18(64)}$ = D45B 630D A443 6F76 $\oplus$ 3783 442D 7314 DBD9
= E3D8 2720 D757 B4AF

$P(S(X_{8(8)} \oplus k_{2(8)})$ =E3 = $P(S_1(14))$ = Y(174)
$P(S(X_{7(8)} \oplus k_{2(8)}))$ =D8 = $P(S_4(216))$ = Y(155)
$P(S(X_{6(8)} \oplus k_{2(8)}))$ =27 = $P(S_3(39))$ = Y(103)
$P(S(X_{5(8)} \oplus k_{2(8)}))$ =20 = $P(S_2(32))$ = Y(13)
$P(S(X_{4(8)} \oplus k_{2(8)}))$ =D7 = $P(S_4(215))$ = Y(226)
$P(S(X_{3(8)} \oplus k_{2(8)}))$ =57 = $P(S_3(87))$ = Y(130)
$P(S(X_{2(8)} \oplus k_{2(8)}))$ =B4 = $P(S_2(180))$ = Y(145)
$P(S(X_{1(8)} \oplus k_{2(8)}))$ =A4 = $P(S_1(164))$ = Y(2)

z'_1= z1$\oplus$z3$\oplus$z4$\oplus$z6$\oplus$ z7$\oplus$ z8 =2$\oplus$130$\oplus$226$\oplus$103$\oplus$155$\oplus$174 = 48
z'_2 = z1$\oplus$z2$\oplus$z4$\oplus$z5$\oplus$ z7$\oplus$ z8 =2$\oplus$145$\oplus$226$\oplus$13$\oplus$155$\oplus$174 = 73
z'_3 = z1$\oplus$z2$\oplus$z3$\oplus$z5$\oplus$ z6$\oplus$ z8 =2$\oplus$145$\oplus$130$\oplus$13$\oplus$103$\oplus$174 = 213
z'_4 = z2$\oplus$z3$\oplus$z4$\oplus$z5$\oplus$ z6$\oplus$ z7 =145$\oplus$130$\oplus$226$\oplus$13$\oplus$103$\oplus$155 = 0
z'_5 = z1$\oplus$z2$\oplus$z6$\oplus$ z7$\oplus$ z8 =2$\oplus$145$\oplus$103$\oplus$155$\oplus$174 = 193
z'_6 = z2$\oplus$z3$\oplus$z5$\oplus$ z7$\oplus$ z8 =145$\oplus$130$\oplus$13$\oplus$155$\oplus$174 = 43
z'_7 = z3$\oplus$z4$\oplus$z5$\oplus$ z6$\oplus$ z8 =130$\oplus$226$\oplus$13$\oplus$103$\oplus$174 = 164
z'_8 = z1$\oplus$z4$\oplus$z5$\oplus$ z6$\oplus$ z7 =2$\oplus$226$\oplus$13$\oplus$1035$\oplus$155 = 17
$z'_{(64)}$ = 3049 D50 C12B A411
L_1 = R_0 $\oplus$F(L_0, k_1)
= D45B 630D A443 6F76 $\oplus$3049 D50 C12B A411
= D75F FE5D 6568 CB67
R_1 = CE0B 4273 96B3 B2EC

Round →2
L_2 = R_1 $\oplus$ F(L_1, k_2)
R_2 = L_1
L_2 = R_1 $\oplus$ F(L_1, k_2)
= CE0B 4273 96B3 B2EC $\oplus$ F (L_1, k_2)
R_2 = D75F FE5D 6568 CB67
k_2 = 50C6 C3A1 F4C5 0590
$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = P(S(X_{(64)} \oplus k_{(64)}))$
$X_{(64)} \oplus k_{2(64)}$ = D75F FE5D 6568 CB67 $\oplus$ 50C6 C3A1 F4C5 0590 = 8799 3DFC 91AD CEF7
$P(S(X_{8(8)} \oplus k_{2(8)})$ =87 = $P(S_1(135))$ = Y(151)
$P(S(X_{7(8)} \oplus k_{2(8)}))$ =99 = $P(S_4(153))$ = Y(71)
$P(S(X_{6(8)} \oplus k_{2(8)}))$ =3D = $P(S_3(61))$ = Y(43)
$P(S(X_{5(8)} \oplus k_{2(8)}))$ =FC = $P(S_2(252))$ = Y(119)
$P(S(X_{4(8)} \oplus k_{2(8)}))$ =91 = $P(S_4(145))$ = Y(235)
$P(S(X_{3(8)} \oplus k_{2(8)}))$ =AD = $P(S_3(173))$ = Y(191)
$P(S(X_{2(8)} \oplus k_{2(8)}))$ =CE = $P(S_2(206))$ = Y(180)
$P(S(X_{1(8)} \oplus k_{2(8)}))$ =F7 = $P(S_1(247))$ = Y(193)
z'_1 = z1$\oplus$z3$\oplus$z4$\oplus$z6$\oplus$ z7$\oplus$ z8 =193$\oplus$191$\oplus$235$\oplus$43$\oplus$71$\oplus$151 = 110
z'_2 = z1$\oplus$z2$\oplus$z4$\oplus$z5$\oplus$ z7$\oplus$ z8 =193$\oplus$180$\oplus$235$\oplus$119$\oplus$71$\oplus$151 = 57
z'_3 = z1$\oplus$z2$\oplus$z3$\oplus$z5$\oplus$ z6$\oplus$ z8 =193$\oplus$180$\oplus$191$\oplus$119$\oplus$43$\oplus$151 = 1
z'_4 = z2$\oplus$z3$\oplus$z4$\oplus$z5$\oplus$ z6$\oplus$ z7 =180$\oplus$191$\oplus$235$\oplus$119$\oplus$43$\oplus$71 = 251
z'_5 = z1$\oplus$z2$\oplus$z6$\oplus$ z7$\oplus$ z8 =193$\oplus$180$\oplus$43$\oplus$71$\oplus$151 = 142
z'_6 = z2$\oplus$z3$\oplus$z5$\oplus$ z7$\oplus$ z8 =180$\oplus$191$\oplus$119$\oplus$71$\oplus$151 = 172
z'_7 = z3$\oplus$z4$\oplus$z5$\oplus$ z6$\oplus$ z8 =191$\oplus$235$\oplus$119$\oplus$43$\oplus$151 = 159
z'_8 = z1$\oplus$z4$\oplus$z5$\oplus$ z6$\oplus$ z7 =193$\oplus$235$\oplus$119$\oplus$43$\oplus$71 = 49
$z'_{(64)}$ = 6E39 1FB 8EAC 9F31
L_2 = R_1 $\oplus$ F(L_1, k_2)
= CE0B 4273 96B3 B2EC $\oplus$ 6E39 1FB 8EAC 9F31
= C8E8 D388 181F 2DDD
R_2 = D75F FE5D 6568 CB67

Round→3
L_3 = R_2 $\oplus$ F(L_2, k_3)
R_3 = L_2
L_3 = R_2 $\oplus$ F(L_2, k_3)
= D75F FE5D 6568 CB67 $\oplus$ F (L_2, k_3)
R_3 = C8E8 D388 181F 2DDD

Submitted: **09/07/2020**; Accepted: **09/10/2020**; Published: **26/10/2020**

Journal of Information Sistem Research (JOSH)
Volume 2, No. 1, October 2020
ISSN 2686-228X (media online)
Hal: 14-25

k_3 = A920 A224 A121 2096
$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = P(S(X_{(64)} \oplus k_{(64)}))$
$X_{(64)} \oplus k_{3(64)}$ = C8E8 D388 181F 2DDD ⊕ A920 A224 A121 2096
= 61C8 71AC B93E 0D4B

$P(S(X_{8(8)} \oplus k_{2(8)})$	= 61	= $P(S_1(97))$	= Y(88)
$P(S(X_{7(8)} \oplus k_{2(8)}))$	= C8	= $P(S_4(200))$	= Y(196)
$P(S(X_{6(8)} \oplus k_{2(8)}))$	= 71	= $P(S_3(113))$	= Y(34)
$P(S(X_{5(8)} \oplus k_{2(8)}))$	= AC	= $P(S_2(172))$	= Y(59)
$P(S(X_{4(8)} \oplus k_{2(8)}))$	= B9	= $P(S_4(185))$	= Y(178)
$P(S(X_{3(8)} \oplus k_{2(8)}))$	= 3E	= $P(S_3(62))$	= Y(54)
$P(S(X_{2(8)} \oplus k_{2(8)}))$	= 0D	= $P(S_2(13))$	= Y(24)
$P(S(X_{1(8)} \oplus k_{2(8)}))$	= 4B	= $P(S_1(75))$	= Y(32)

z'_1 = z1⊕z3⊕z4⊕z6⊕ z7⊕ z8	=32⊕54⊕178⊕34⊕196⊕88	= 26
z'_2 = z1⊕z2⊕z4⊕z5⊕ z7⊕ z8	=32⊕24⊕178⊕59⊕196⊕88	= 45
z'_3 = z1⊕z2⊕z3⊕z5⊕ z6⊕ z8	=32⊕24⊕54⊕59⊕34⊕88	= 79
z'_4 = z2⊕z3⊕z4⊕z5⊕ z6⊕ z7	=24⊕54⊕178⊕59⊕34⊕196	= 65
z'_5 = z1⊕z2⊕z6⊕ z7⊕ z8	=32⊕24⊕34⊕196⊕88	= 134
z'_6 = z2⊕z3⊕z5⊕ z7⊕ z8	=24⊕54⊕59⊕196⊕88	= 137
z'_7 = z3⊕z4⊕z5⊕ z6⊕ z8	=54⊕178⊕59⊕34⊕88	= 197
z'_8 = z1⊕z4⊕z5⊕ z6⊕ z7	=32⊕178⊕59⊕34⊕196	= 79

$z'_{(64)}$ = 1A2D 4F41 8689 C54F
L_3 = $R_2 \oplus F(L_2, k_3)$
= D75F FE5D 6568 CB67⊕ 1A2D 4F41 8689 C54F
= CD72 B11C E3E1 0E28
R_3 = D2D0 27A2 CE05 3C24

3. Dekripsi Camellia

Plainteks = 221 4 2 184 159 160 195 19 78 204 30 88 92 218 57 190
$C_{(128)}$ = DD04 02B8 9FA0 C313 4ECC 1E58 5CDA 39BE
$C_{(128)} \oplus (kw_{3(64)} \| kw_{4(64)}) = R_{18(64)} \| L_{18(64)}$
DD04 02B8 9FA0 C313 4ECC 1E58 5CDA 39BE ⊕ (7D31 4164 0DE0 D10B ||5CC5 36F6 5431 B0E8)= A035 43DC 9240 1218||1209 28AE 08EB 8956
$R_{18(64)}$ = A035 43DC 9240 1218
$L_{18(64)}$ = 1209 28AE 08EB 8956

Round →1
R_{r-1} = $L_r \oplus F(R_r, k_r)$
L_{r-1} = R_r
$R_{17} = L_{18} \oplus F(R_{18}, k_{18})$
$L_{17} = R_{18}$
$R_{17} = L_{18} \oplus F(R_{18}, k_{18})$
= 1209 28AE 08EB 8956⊕ F (R_{18}, k_{18})
L_{17}= A035 43DC 9240 1218
k_{18} = A121 2096 9919 189C
$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = P(S(X_{(64)} \oplus k_{(64)}))$
$X_{(64)} \oplus k_{18(64)}$ = A035 43DC 9240 1218⊕ A121 2096 9919 189C
= 114 634A 0B59 0A84

$P(S(X_{8(8)} \oplus k_{2(8)})$	= 1	= $P(S_1(1))$	= Y(130)
$P(S(X_{7(8)} \oplus k_{2(8)}))$	= 14	= $P(S_4(20))$	= Y(62)
$P(S(X_{6(8)} \oplus k_{2(8)}))$	= 63	= $P(S_3(99))$	= Y(176)
$P(S(X_{5(8)} \oplus k_{2(8)}))$	= 4A	= $P(S_2(74))$	= Y(86)
$P(S(X_{4(8)} \oplus k_{2(8)}))$	= 0B	= $P(S_4(11))$	= Y(165)
$P(S(X_{3(8)} \oplus k_{2(8)}))$	= 59	= $P(S_3(89))$	= Y(219)
$P(S(X_{2(8)} \oplus k_{2(8)}))$	= 0A	= $P(S_2(10))$	= Y(174)
$P(S(X_{1(8)} \oplus k_{2(8)}))$	= 84	= $P(S_1(132))$	= Y(161)

z'_1 = z1⊕z3⊕z4⊕z6⊕ z7⊕ z8	=161⊕219⊕165⊕176⊕62⊕130	= 211
z'_2 = z1⊕z2⊕z4⊕z5⊕ z7⊕ z8	=161⊕174⊕165⊕86⊕62⊕130	= 64
z'_3 = z1⊕z2⊕z3⊕z5⊕ z6⊕ z8	=161⊕174⊕219⊕86⊕176⊕130	= 176
z'_4 = z2⊕z3⊕z4⊕z5⊕ z6⊕ z7	=174⊕219⊕165⊕86⊕176⊕62	= 8
z'_5 = z1⊕z2⊕z6⊕ z7⊕ z8	=161⊕174⊕176⊕62⊕130	= 3
z'_6 = z2⊕z3⊕z5⊕ z7⊕ z8	=174⊕219⊕86⊕62⊕130	= 159
z'_7 = z3⊕z4⊕z5⊕ z6⊕ z8	=219⊕165⊕86⊕176⊕130	= 26
z'_8 = z1⊕z4⊕z5⊕ z6⊕ z7	=161⊕165⊕86⊕176⊕62	= 220

Submitted: **09/07/2020**; Accepted: **09/10/2020**; Published: **26/10/2020**

$z'_{(64)}$ = D340 B08 39F 1ADC
R_{17} = $L_{18} \oplus F(R_{18}, k_{18})$
= 1209 28AE 08EB 8956 $\oplus$ D340 B08 39F 1ADC
= 12D4 681E 8B74 938A
L_{17}= A035 43DC 9240 1218

Round →2
R_{16} = $L_{17} \oplus F(R_{17}, k_{17})$
L_{16} = R_{17}
R_{16} = $L_{17} \oplus F(L_{16}, k_{17})$
= A035 43DC 9240 1218 $\oplus$ F (L_{16}, k_{17})
L_{16} = 12D4 681E 8B74 938A
k_{17} = 9C9B A320 A920 A224
$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = P(S(X_{(64)} \oplus k_{(64)}))$
$X_{(64)} \oplus k_{17(64)}$ = 12D4 681E 8B74 938A $\oplus$ 9C9B A320 A920 A224
= 8E4F CB3E 2254 31AE

$P(S(X_{8(8)} \oplus k_{2(8)})$	= 8E	= $P(S_1(142))$	= Y(100)
$P(S(X_{7(8)} \oplus k_{2(8)}))$	= 4F	= $P(S_4(79))$	= Y(221)
$P(S(X_{6(8)} \oplus k_{2(8)}))$	= CB	= $P(S_3(203))$	= Y(91)
$P(S(X_{5(8)} \oplus k_{2(8)}))$	= 3E	= $P(S_2(62))$	= Y(216)
$P(S(X_{4(8)} \oplus k_{2(8)}))$	= 22	= $P(S_4(34))$	= Y(251)
$P(S(X_{3(8)} \oplus k_{2(8)}))$	= 54	= $P(S_3(84))$	= Y(26)
$P(S(X_{2(8)} \oplus k_{2(8)}))$	= 31	= $P(S_2(49))$	= Y(19)
$P(S(X_{1(8)} \oplus k_{2(8)}))$	= AE	= $P(S_1(174))$	= Y(191)

z'_1 = $z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8$	=191⊕26⊕251⊕91⊕221⊕100	= 188
z'_2 = $z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8$	=191⊕19⊕251⊕216⊕221⊕100	= 54
z'_3 = $z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8$	=191⊕19⊕26⊕216⊕91⊕100	= 81
z'_4 = $z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7$	=19⊕26⊕251⊕216⊕91⊕221	= 172
z'_5 = $z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8$	=191⊕19⊕91⊕221⊕100	= 78
z'_6 = $z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8$	=19⊕26⊕216⊕221⊕100	= 104
z'_7 = $z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8$	=26⊕251⊕216⊕91⊕100	= 6
z'_8 = $z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7$	=191⊕251⊕216⊕91⊕221	= 26

$z'_{(64)}$ = BC36 51AC 4E68 61A
R_{16} = $L_{17} \oplus F(R_{17}, k_{17})$
= A035 43DC 9240 1218 $\oplus$ BC36 51AC 4E68 61A
= ABF6 26C6 56A6 9402
R_{17} = 12D4 681E 8B74 938A

Round →3
R_{15} = $L_{16} \oplus F(R_{16}, k_{16})$
L_{15} = R_{16}
R_{15} = $L_{16} \oplus F(R_{16}, k_{16})$
= ABF6 26C6 56A6 9402 $\oplus$ F (L_{14}, k_{15})
R_{15} = DC3C 8D4E 0858 2502
k_{15} = D874 3E98 A0B2 06F0
$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = P(S(X_{(64)} \oplus k_{(64)}))$
$X_{(64)} \oplus k_{15(64)}$ = DC3C 8D4E 0858 2502 $\oplus$ D874 3E98 A0B2 06F0
= 448 B3D6 A8EA 23F2

$P(S(X_{8(8)} \oplus k_{2(8)})$	= 4	= $P(S_1(4))$	= Y(179)
$P(S(X_{7(8)} \oplus k_{2(8)}))$	= 48	= $P(S_4(72))$	= Y(16)
$P(S(X_{6(8)} \oplus k_{2(8)}))$	= B3	= $P(S_3(179))$	= Y(19)
$P(S(X_{5(8)} \oplus k_{2(8)}))$	= D6	= $P(S_2(214))$	= Y(226)
$P(S(X_{4(8)} \oplus k_{2(8)}))$	= A8	= $P(S_4(168))$	= Y(76)
$P(S(X_{3(8)} \oplus k_{2(8)}))$	= EA	= $P(S_3(234))$	= Y(21)
$P(S(X_{2(8)} \oplus k_{2(8)}))$	= 23	= $P(S_2(35))$	= Y(31)
$P(S(X_{1(8)} \oplus k_{2(8)}))$	= F2	= $P(S_1(242))$	= Y(211)

z'_1 = $z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8$	=211⊕21⊕76⊕226 ⊕16⊕179	= 203
z'_2 = $z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8$	=211⊕31⊕76⊕226⊕16⊕179	= 97
z'_3 = $z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8$	=211⊕31⊕21⊕226⊕19⊕179	= 155
z'_4 = $z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7$	=31⊕21⊕76⊕226⊕19⊕16	= 167
z'_5 = $z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8$	=211⊕31⊕19⊕16⊕179	= 124
z'_6 = $z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8$	=31⊕21⊕226⊕16⊕179	= 75

Submitted: **09/07/2020**; Accepted: **09/10/2020**; Published: **26/10/2020**

Journal of Information Sistem Research (JOSH)
Volume 2, No. 1, October 2020
ISSN 2686-228X (media online)
Hal: 14-25

$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 \quad = 21 \oplus 76 \oplus 226 \oplus 19 \oplus 179 \quad = 27$
$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 \quad = 211 \oplus 76 \oplus 226 \oplus 19 \oplus 16 \quad = 126$
$z'_{(64)} = CB61\ 9BA7\ 7C4B\ 1B7E$
$R_{15} = L_{16} \oplus F(R_{16}, k_{16})$
$= 12D4\ 681E\ 8B74\ 938A \oplus CB61\ 9BA7\ 7C4B\ 1B7E$
$= D9B5\ F3B9\ F73F\ 88F4$
$L_{15} = ABF6\ 26C6\ 56A6\ 9402$

3.2 Implementasi

Tampilan input pada pembahasan ini terdiri dari tampilan menu utama, tampilan form enkripsi, tampilan form dekripsi dan tampilan form profil. Kesimpulan yang diambil adalah apakah tampilan program sesuai dengan rancangan sebelumnya. Adapun tampilan keseluruhan menu program sebagai berikut :

Menu utama adalah tampilan yang akan pertama kali muncul ketika program aplikasi dibuka oleh user. Adapun tampilan menu utama aplikasi adalah sebagai berikut :

Gambar 1. Tampilan Menu Utama

Tampilan form enkripsi adalah menu yang digunakan untuk proses enkripsi citra digital. Adapun tampilan menu enkripsi dapat dilihat pada gambar di bawah.

Gambar 2. Tampilan Form Enkripsi

Tampilan form dekripsi adalah form untuk mendekripsikan citra, yang mana form ini tampil jika dipilih menu dekripsi pada menu utama. Adapun tampilan menu dekripsi dapat dilihat pada gambar di bawah ini :

Gambar 3. Tampilan Form Dekripsi

Tampilan output ini didapat dari proses pengujian sistem. Pengujian sistem aplikasi bertujuan untuk mengetahui apakah aplikasi berjalan dengan sesuai fungsinya, yaitu mengenkripsi dan dekripsi citra USG. Pengujian memiliki 2 tahap yaitu proses enkripsi citra digital awal dan proses dekripsi citra hasil enkripsi.

1. Proses Enkripsi Citra
   Proses enkripsi citra memiliki beberapa tahap yaitu, proses pemilihan citra digital awal (plainimage), proses pemasukan kunci dan proses enkripsi.
   a. Pemilihan Plainimage
   Adapun proses pemilihan citra awal (plainimage) dilakukan dengan memilih buton pilih gambar seperti pada gambar di bawah ini :

Submitted: **09/07/2020**; Accepted: **09/10/2020**; Published: **26/10/2020**

Journal of Information Sistem Research (JOSH)
Volume 2, No. 1, October 2020
ISSN 2686-228X (media online)
Hal: 14-25

Gambar 4. Tampilan Pemilihan Citra Plainimage

Gambar 5. Tampilan Citra Plainimage

Setelah proses pemilihan citra plainimage proses selanjutnya adalah memasukan kunci enkripsi. Adapun kunci enkripsi dapat dilihat pada gambar di bawah ini :

Gambar 6. Tampilan proses memasukan kunci

Berdasarkan pada gambar di atas kunci yang digunakan untuk proses enkripsi untuk algoritma Camellia adalah FARADIBBA-221997

b. Enkripsi Plainimage

Adapun proses enkripsi tersebut dapat dilihat pada gambar di bawah ini :

Gambar 7. Tampilan Proses Enkripsi

Berdasarkan pada gambar di atas, proses enkripsi berhasil menyandikan citra USG plainimage ke cipherimage. Cipherimage tersebut dapat disimpan kembali kedalam direktori komputer dengan memilih button save seperti gambar di bawah ini:

Submitted: **09/07/2020**; Accepted: **09/10/2020**; Published: **26/10/2020**

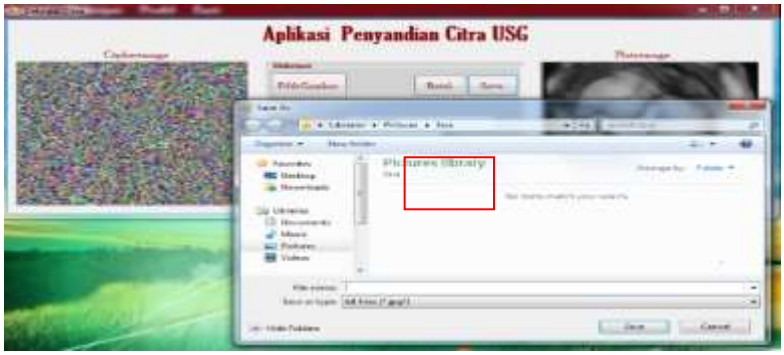
Journal of Information Sistem Research (JOSH)
Volume 2, No. 1, October 2020
ISSN 2686-228X (media online)
Hal: 14-25

Gambar 8. Tampilan Proses simpan hasil Enkripsi

Form dekripsi pada aplikasi akan tampil jika menu form dekripsi pada menu utama dipilih. ada pengiriman pesan masuk di menu utama sistem aplikasi. Adapun tampilan form dekripsi dapat dilihat pada gambar di bawah.

Gambar 9. Tampilan Form Dekripsi

Form dekripsi di atas telah mencakup seluruh proses sebelumnya seperti pilih gambar, memasukan kunci dan proses dekripsi. Plainimage dari hasil dekripsi ini kemudian disimpan kembali ke direktori komputer. Adapun tampilan untuk simpan plainimage dapat dilihat pada gambar di bawah.



Gambar 10. Tampilan Proses simpan plainimage hasil dekripsi

4. KESIMPULAN

Berdasarkan hasil penerapan algoritma Camellia pada penyandian Citra USG yang telah dilakukan, penulis dapat menarik kesimpulan sebagai berikut:

1. Penyandian Citra USG berdasarkan algoritma Camellia mampu mempersulit pihak-pihak lain untuk mengerti dan memahami Citra USG.
2. Tingkat keamanan yang dihasilkan sangat tinggi karena algoritma Camellia termasuk salah satu cipher blok dengan ukuran blok yang besar dan juga memiliki variasi kunci yang banyak. Variasi kunci terdiri dari 128 bit, 192 bit dan 256 bit yang dapat membangkitkan 24 subkunci untuk kunci 128 bit dan 26 subkunci untuk 192 dan 256 bit.
3. Menyandikan citra USG diawali dengan gambar hasil USG dan memilih gambar hasil USG yang akan disandikan.

REFERENCES

[1] Lanny Sutanto, Gregorius Setia Budhi, Leo Willyanto Santoso, "PERBANDINGAN METODE CAMELLIA 128 BIT KEY DAN 256 BIT KEY, "Vol. 12,No.2, pp. 109-115, Noveermber 2014.
[2] Herman Zuhri, Mesran, Henry Kristian Siburian, "IMPLEMENTASI METODE CAMELLIA DALAM KEAMANAN DATA FILE BEREKSTENSI TXT DAN DOC, "Volume 16, Nomor 4, Oktober 2017.
[3] & dkk Sutoyo.T., Teori Pengolahan Citra Digital, I. Yogyakarta, 2009.

Submitted: **09/07/2020**; Accepted: **09/10/2020**; Published: **26/10/2020**

[4] E. Setyaningsih, Kriptografi & Implementasinya Menggunakan MATLAB, I. Yogyakarta:ANDI, 2015.
[5] B.S.W Poetra and R. Wardoyo, "Perbandingan Efesiensi, Efektifitas dan Kualitas Algoritma Rijndael dengan Algoritma Camellia pada Citra Digital, "Journal off Math. Nat.Set., vol. 24, no. 3, pp. 281-291, 2014.
[6] K. Aoki et al, " Camellia : A 128-Bit Block Cipher Suitable for Multiple Platforms – Design and Analysis Structure of Camellia, "Springer-Verlag Berlin Heidelb, pp. 39-56, 2001.
[7] Kasiman Peranginangin, Pengenalan MATLAB, Yogyakarta, 2006.