Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

15th June 2023. Vol. 2. No. 3; e-ISSN : 2808-4519

Hybrid Cryptosystem Algorithm Vigenere Cipher and Base64 for Text Message Security Utilizing Least Significant Bit (LSB) Steganography as Insert into Image

Raja Imanda Hakim Nasution[1*], Achmad Fauzi[2], Husnul Khair[3]

[1,2,3] Informatics Engineering, STMIK KAPUTAMA
Jl. Veteran No. 4A-9A, Binjai, North Sumatra, Indonesia
rajaimandahakim@gmail.com[1] , fauzyrivai88@gmail.com[2] , husnul.khair@gmail.com[3]

Abstract

Security message text is aspect important in modern communications for guard privacy and confidentiality information. Without exists guarantee security, of course just can raises risk when sensitive and valuable information are accessed by unauthorized persons responsible answer. Cryptography and steganography is two field used in a manner wide For reach objective this. Algorithm Vigenere Cipher and Base64 are method used for encryption message text and Least Significant Bit (LSB) steganography was used as method for insert message encrypted to in image. LSB makes use of the last bits from pixels image for keep information addition without bother image visual display in a manner significant. With utilise method here, order encrypted can hidden in a manner confidential in image that looks normal. This hybrid cryptosystem combine excess from third algorithm such, ie speed and effectiveness encryption use algorithm Vigenere Cipher as well ability Base64 characteristics, and levels security message more increase.

Keywords: *Vigenere cipher, Base64, LSB, Security, Message, Imagery*

1. Introduction

Fast development technology information give significant impact for life human. Everyone can exchange data, information, or message without limitation distance or time blessing technology information. Without exists guarantee security, of course just can raises risk when sensitive and valuable information are accessed by unauthorized persons responsible answer, so can be misused for detrimental purpose. Face threat security, required security techniques for guard secrecy message use Algorithm Cryptography. People who don't know key used for encrypt and decrypt message No can unlock encrypted data. Merge two method cryptography for get more security on the message you want to secure. Use algorithm Vigenere Cipher, Base64 is one method that can done. Algorithm the Vigenere Cipher uses different keys for every character in text, the Base64 algorithm has level enough trouble high, because must go through the changing process plaintext to binary number and break it down become a number of part so that add character in message confidential the. For hide message into the image used technique steganography Least Significant Bit (LSB). Method this work with replace one last bit value from every bit in image so that change the no detected by the eye human.

2. Research Methods

Use method science and resources reliable, methodology study look for information in a manner methodical. In cycle inspection This give useful results for user.

2.1. Cryptography

Knowledge or art make message confidential is what we mean when we talk about cryptography. Encryption process change plaintext from message original become encoded message, or ciphertext, and the decryption process change ciphertext back be plaintext. As method for evaluate security information, a lot algorithm cryptography has used in a manner broad. will difficulty crack ciphertext without key Because algorithm This own level complex difficulties. In cryptography two type key: symmetry and asymmetry [1] .

2.2. Hybrid Cryptosystem

Cryptosystems are tool for change plaintext to ciphertext and vice versa. That consists from algorithm that counts all possibility text plain, text password, and key. Algorithm hybrid is algorithms that take advantage of two level key that is key symmetric which is also called session key for data encryption and key secrets and keys public For protect key symmetrical. Hybrid cryptosystem is A technique that uses a number of different method For take advantage of each the advantages [2] .

2.3. Algorithm Vigenere Cipher

The Vigenère cipher is one algorithm cryptography classic. This is one method alphabetical substitution used for encode message text with use row key a word or summative sentences follow long from plaintext.
Formula encryption and decryption on this Vigenère cipher algorithm is like following:

Formula Encryption Vigenere **Ci = (Pi + Ki) mod 26**

Formula Decryption Vigenere **Pi = (Ci - Ki) mod 26**

Information:
Ci = value decimal from character *ciphertext*
Pi = value decimal from character *plaintext*
Ki = value decimal from character key
Where is the value decimal characters: A = 0, B = 1... Z = 25.

If the encryption process results Pi+Ki more of 26 then the use of mod 26 is used If No so direct just insert mark from results from Pi+Ki. And if on the description process results of Pi-Ki is mark negative, mod 26 does not happens, but results mark negative direct summed up with 26 [3] .

2.4. Base64 Algorithm

One algorithm used for encoding and decoding data to in ASCII format is Base64 transformation, which is based on numbers base 64. In this Base64 transformation, character consists from letter A..Z , a..z , and 0..9, plus two character The last symbol is + and /. Besides it, there is One character The same with (=) is used for change and complete binary data, or term For pad filler. Character generated symbol will depending on how algorithm operating [4].

Base64 encoding can grouped and distinguished in accordance with a number of criteria, as indicated in table following.

Table 1: Index Base64

Indexes (6 bits)	Char Base64	Indexes (6 bits)	Char Base64	Indexes (6 bits)	Char Base64	Indexes (6 bits)	Char Base64
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	Q	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/
						pad	=

If any remainder divider during the encoding process, add it character = as fulfillment remainder the.

2.5. Steganography

Steganography is arts and sciences hide message secret inside another message so no detected. Steganography function as complementary cryptography; in in practice, order confidential encrypted especially first, then the ciphertext hidden inside another message so party third No can see it. With the same way, order confidential hidden can extracted. Steganography more good than cryptography Because message

Algorithm cryptography can broken down become two category: algorithm cryptography contemporary and traditional based character and use key symmetrical is characteristics from algorithm cryptography classic. More from cryptography traditional, algorithm modern cryptography is improvement. Algorithm This use processing based binary symbols ASCII code (American Standard Code for Information

Interchange) because follow operation digital computer. For get the hang of it, somebody must own understanding about math. Cryptanalyst sent no interesting attention so that against no feel suspicious. This different with deep cryptography matter this message shaped ciphertext can raises suspicion for observer as secret message [5] .

2.6. LSB *(Last Significant Bit)* Algorithm

LSB is technique the most popular and easy steganography used. this LSB use digital image for insert text or message. The most significant bit (MSB) and the least bit (least significant bit, or LSB) is found in inner bit array a byte, which consists of 8 bits [6] . As example MSB and LSB positions are shown in the figure following

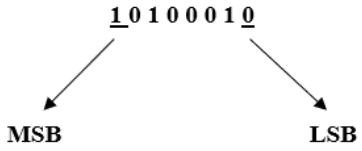

Figure 1: Position of MSB and LSB in 8 bit binary

As example, follows is part of image pixels before the message bits entered:

01010100	01001001	01000001	01010010
01000001	01001010	01001100	01010100

For example message secret “01010010” is represented by the character “R” every bit of message confidential will replaced by the last bit of image pixels to be:

0101010 0	0100100 1	0100000 0	0101001 1
0100000 0	0100101 0	0100110 1	0101010 0

Message bits in picture must can found back. The method is reads the bytes in the image, takes the LSB, and then string it together return into message bits.

2.7. Definition of Image

Something picture, picture, or appearance two describing dimensions something object called image. Create can made digitally or printed. Digital image consists from gathering composed numbers from two dimensions. The digital image is saved in array form or array digital numbers, which are results from count level the brightness of each pixel that makes up image. Elements so -called small pixels consists from stored digital image in array two dimensions. each pixel connected to the surface zone earth in a manner spatial. This array structure consists of rows (lines) and columns (samples). Every raster image pixels own digital numbers indicating level brightness the pixels. In digital image, array pixels in structure array called raster data. Digital image can processed in a manner mathematical in various method Because is array digital numbers [7] .

3. Results and Discussion

3.1. Calculation Encryption Message Algorithm Vigenere Cipher and Base64

On this process done with method combine two algorithm cryptography that is, the algorithm vigenere cipher and base64. As for messages secured text are:

Plaintext : JADILAH ORANG BAIK
Key : NASUTION

J	A	D	I	L	A	H	O	R	A	N	G	B	A	I	K
N	A	S	U	T	I	O	N	N	A	S	U	T	I	O	N

C1 : (9 + 13) mod 26
: 22 mod 26
: 22 = W
C2 : (0 + 0) mod 26
: 0 mod 26
: 0 = A
C3 : (3 + 18) mod 26
: 21 mod 26
: 21 = V
C4 : (8 + 20) mod 26
: 28 mod 26
: 2 = C
C5 : (11 + 19) mod 26
: 30 mod 26
: 4 = E
C6 : (0 + 8) mod 26
: 8 mod 26
: 8 = I

C7 : (7 + 14) mod 26
: 21 mod 26
: 21 = V
C8 : (14 + 13) mod 26
: 27 mod 26
: 1 = B
C9 : (17 + 13) mod 26
: 30 mod 26
: 4 = E
C10 : (0 + 0) mod 26
: 0 mod 26
: 0 = A
C11 : (13 + 18) mod 26
: 31 mod 26
: 5 = F
C12 : (6 + 20) mod 26
: 26 mod 26
: 0 = A
C13 : (1 + 19) mod 26
: 20 mod 26
: 20 = U
C14 : (0 + 8) mod 26
: 8 mod 26
: 8 = I
C15 : (8 + 14) mod 26
: 22 mod 26
: 22 = W
C16 : (10 + 13) mod 26
: 23 mod 26
: 23 = X

Ciphertext: WAVCEIV BEAFA UIWX

Obtained ciphertext here it is then encrypted return use Base64 algorithm.

1. Step One : Decide message to be entered “WAVCEIV BEAFA UIWX”

Text Content	W	A	V	C
ASCII	87	65	86	67

2. Second step : ASCII code is changed become binary code :

Text Content	W	A	V	C
ASCII	87	65	86	67
Bit Patterns	01010111	01000001	01010110	01000011

3. Step three : Share binary code into 6 bits/ block :

Text content	W								A								V							
ASCII	87								65								86							
Bit Pattern	0	1	0	1	0	1	1	1	0	1	0	0	0	0	0	1	0	1	0	1	0	1	1	0
Index	21				52				5				22											

4. Fourth step : Blocks the changed return become number decimal table index:

Text content	W								A								V							
ASCII	87								65								86							
Bit Pattern	0	1	0	1	0	1	1	1	0	1	0	0	0	0	0	1	0	1	0	1	0	1	1	0
Index	21				52				5				22											
Base64 Encoded	V				0				F				W											

5. Fifth step: Then you get the Base64 encode of "WAVC = V0FW"

   Then results from base64 encode compiled with follow pattern that has determined i.e. 6bit block and 4 row index, so got arrangement as following:

"V0FWQ0VJViBCRUFGQSBVSVdY"
Obtained ciphertext This then changed into the binary form for furthermore pasted into the image.

3.2. Insertion Encoding Process LSB Image Message

This process is supported with using image data from jpg images.

Figure 2: Image and Pixel Sample 8x8 Pixel Image

On this process aim for hide cipher text. For size image used is 720 x 720 pixels. Insertion process message on the image will be taken sample on the image with size 8 x 8 pixels, starts from point pixel (0,0) to with (7,7).

Table 2: Image Pixel Value 8 x 8 Pixel

(x,y)	0	1	2	3	4	5	6	7
0	R: 185 G: 182 B: 173	R: 202 G: 199 B: 190	R: 234 G: 231 B: 224	R: 238 G: 235 B: 228	R: 223 G: 225 B: 214	R: 228 G: 230 B: 219	R: 197 G: 200 B: 189	R: 163 G: 166 B: 155
1	R: 226 G: 223 B: 214	R: 231 G: 228 B: 219	R: 239 G: 236 B: 229	R: 232 G: 229 B: 222	R: 217 G: 219 B: 208	R: 216 G: 218 B: 207	R: 219 G: 222 B: 211	R: 194 G: 197 B: 186
2	R: 249 G: 248 B: 246	R: 254 G: 253 B: 251	R: 244 G: 243 B: 241	R: 229 G: 228 B: 226	R: 219 G: 221 B: 216	R: 210 G: 212 B: 207	R: 224 G: 231 B: 224	R: 208 G: 215 B: 208
3	R: 254 G: 253 B: 251	R: 250 G: 249 B: 247	R: 234 G: 233 B: 231	R: 226 G: 225 B: 223	R: 232 G: 234 B: 229	R: 231 G: 233 B: 228	R: 213 G: 220 B: 213	R: 186 G: 193 B: 186
4	R: 247 G: 248 B: 250	R: 236 G: 237 B: 239	R: 222 G: 228 B: 226	R: 228 G: 234 B: 232	R: 235 G: 246 B: 242	R: 238 G: 249 B: 245	R: 196 G: 208 B: 204	R: 160 G: 172 B: 168
5	R: 235 G: 236 B: 238	R: 224 G: 225 B: 227	R: 222 G: 228 B: 226	R: 235 G: 241 B: 239	R: 238 G: 249 B: 245	R: 236 G: 247 B: 243	R: 211 G: 223 B: 219	R: 183 G: 195 B: 191
6	R: 232 G: 233 B: 228	R: 228 G: 229 B: 224	R: 224 G: 229 B: 223	R: 236 G: 246 B: 238	R: 245 G: 255 B: 248	R: 244 G: 255 B: 247	R: 229 G: 242 B: 232	R: 199 G: 212 B: 202
7	R: 225 G: 226 B: 221	R: 227 G: 228 B: 223	R: 217 G: 222 B: 216	R: 223 G: 233 B: 225	R: 230 G: 241 B: 233	R: 225 G: 236 B: 228	R: 229 G: 242 B: 232	R: 205 G: 218 B: 208

Following is a calculation process use Steganography LSB:

Pixels (0,0)

Red = 185 = 10111001 insert 0 = 10111000 = 184

Green = 182 = 10110110 insert 1 = 10110111 = 183

Blue = 173 = 10101101 insert 0 = 10101100 = 172

Pixels (0.1)

Red = 202 = 11001010 insert 1 = 11001011 = 203

Green = 199 = 11000111 insert 0 = 11000110 = 198

Blue = 190 = 10111110 insert 1 = 10111111 = 191

Pixels (0.2)

Red = 234 = 11101010 insert 1 = 11101011 = 235

Green = 231 = 11100111 insert 0 = 11100110 = 232

Blue = 224 = 11100000 insert 0 = 11100000 = 224

Pixels (0.3)

Red = 238 = 11101110 insert 0 = 11101110 = 238

Green = 235 = 11101011 insert 1 = 11101011 = 235

Blue = 228 = 11100100 insert 1 = 11100101 = 229

Pixels (0.4)

Red = 223 = 11011111 insert 0 = 11011110 = 222

Green = 225 = 11100001 insert 0 = 11100000 = 224

Blue = 214 = 11010110 insert 0 = 11010110 = 214

Pixels (0.5)

Red = 228 = 11100100 insert 0 = 11100100 = 228

Green = 230 = 11100110 insert 0 = 11100110 = 230

Blue = 219 = 11011011 insert 1 = 11011011 = 219

Pixels (0.6)

Red = 197 = 11000101 insert0 = 11000100 = 196

Green = 200 = 11001000 insert 0 = 11001000 = 200

Blue = 189 = 10111101 insert 0 = 10111100 = 188

Pixels (0.7)

Red = 163 = 10100011 insert 1 = 10100011 = 163

Green = 166 = 10100110 insert 1 = 10100111 = 167

Blue = 155 = 10011011 insert 0 = 10011010 = 154

Then proceed until to pixel (7,7) so that in the know inserted bit value

Inserted bits:
0101011000110000010001100101011101010001001100000101011001001010010101100110100101000010010000110101001001010101100011000100011101010001010100110100001001010110010100110101011001100100011011001

3.3. Extraction Process Message on LSB Image

In the extraction process This aim displays message original. Following calculation use steganography LSB:

Pixels (0,0)

Red = 184 = 10111000 taken 0 = 0

Green = 183 = 10110111 taken 1 = 1

Blue = 172 = 10101100 taken 0 = 0

Pixels (0.1)

Red = 203 = 11001011 taken 1 = 1

Green = 198 = 11000110 takes 0 = 0

Blue = 191 = 10111111 taken 1 = 1

Pixels (0.2)

Red = 235 = 11101011 taken 1 = 1

Geen = 232 = 11100110 taken 0 = 0

Blue = 224 = 11100000 taken 0 = 0

Pixels (0.3)

Red = 238 = 11101110 taken 0 = 0

Green = 235 = 11101011 taken 1 = 1

Blue = 229 = 11100101 taken 1 = 1

Pixels (0.4)

Red = 222 = 11011110 taken 0 = 0

Green = 224 = 11100000 taken 0 = 0

Blue = 214 = 11010110 taken 0 = 0

Pixels (0.5)

Red = 228 = 11100100 taken 0 = 0

Green = 230 = 11100110 taken 0 = 0

Blue = 219 = 11011011 taken 1 = 1

Pixels (0.6)

Red = 196 = 11000100 taken 0 = 0

Green = 200 = 11001000 taken 0 = 0

Blue = 188 = 10111100 taken 0 = 0

Pixels (0.7)

Red = 163 = 10100011 taken 1 = 1

Green = 167 = 10100111 taken 1 = 1

Blue = 154 = 10011010 taken 0 = 0

Then continue until to pixels (7,7) so return inserted bit value

Result:
0101011000110000010001100101011101010001001100000101011001001010010101100110100101000010010000110101001001010101000110001000111010100010101001101000010010101100101001101010110011001000101100101

Extraction results then grouped with each group consists from 8 bits and after it 's converted using ASCII tables.

3.4. Calculation Decryption Message Base64 Algorithm and Vigenere Cipher

On this process extracted messages then in the description use Base64 Algorithm. As for the sequence of the encoding process for message the are:

1. First step : The result of encryption changed be indexes:

Base64 Encoded	V	0	F	W
Index	21	52	5	22

2. Step two: Change index code to be binary code (*bit pattern*):

Base64 Encoded	V	0	F	W
Index	21	52	5	22
Bit Patterns	010101	110100	000101	010110

3. Step three: create a bit each block containing 8 bits of data instead of 6 bits return:

Base64 Encoded	V						0						F						W					
Index	21						52						5						22					
Bit Pattern (6 bit)	0	1	0	1	0	1	1	1	0	1	0	0	0	0	0	1	0	1	0	1	0	1	1	0
Bit Pattern (8 bit)	0	1	0	1	0	1	1	1	0	1	0	0	0	0	0	1	0	1	0	1	0	1	1	0

4. Step four: Change binary code becomes ASCII then Strings:

Base64 Encoded	V						0						F						W					
Index	21						52						5						22					
Bit Pattern (6 bit)	0	1	0	1	0	1	1	1	0	1	0	0	0	0	0	1	0	1	0	1	0	1	1	0
Bit Pattern (8 bit)	0	1	0	1	0	1	1	1	0	1	0	0	0	0	0	1	0	1	0	1	0	1	1	0
ASCII	87						65						86											
Text content	W						A						V											

Then get it results decryption: "WAVC" with results decryption whole follow pattern the same calculation, then obtained results as following

results Base64 decryption: “WAVCEIV BEAFA UIWX”

Next in the description return use algorithm Vigenere Cipher with the same key in the encryption process.

Ciphertext : WAVCEIV BEAFA UIWX
Key : NASUTION

W	A	V	C	E	I	V	B	E	A	F	A	U	I	W	X
N	A	S	U	T	I	O	N	N	A	S	U	T	I	O	N

P1 : (22 – 13) mod 26
: 9 mod 26
: 9 = J
P2 : (0 – 0) mod 26
: 0 mod 26
: 0 = A
P3 : (21 – 18) mod 26
: 3 mod 26
: 3 = D
P4 : (2 – 20) mod 26
: -18 mod 26
: 8 = I
P5 : (4 – 19) mod 26
: -15 mod 26
: 11 = L
P6 : (8 – 8) mod 26
: 0 mod 26
: 0 = A
P7 : (21 – 14) mod 26
: 7 mod 26
: 7 = H
P8 : (1 – 13) mod 26
: -12 mod 26
: 14 = O
P9 : (4 – 13) mod 26
: -9 mod 26
: 17 = R

P10 : (0 – 0) mod 26
: 0 mod 26
: 0 = A
P11 : (5 – 18) mod 26
: -13 mod 26
: 13 = N
P12 : (0 – 20) mod 26
: -20 mod 26
: 6 = G
P13 : (20 – 19) mod 26
: 1 mod 26
: 1 = B
P14 : (8 – 8) mod 26
: 0 mod 26
: 0 = A
P15 : (22 – 14) mod 26
: 8 mod 26
: 8 = I
P16 : (23 – 13) mod 26
: 10 mod 26
: 10 = K
Plaintext back: JADILAH ORANG BAIK

3.5. Discussion

On research This built system using Visual Basic.Net 2010, and images under this give discussion about medium application developed moment this.

3.5.1. View Form Main

Appearance basic menu page will appear especially first, and some menus will be appears on the display main.

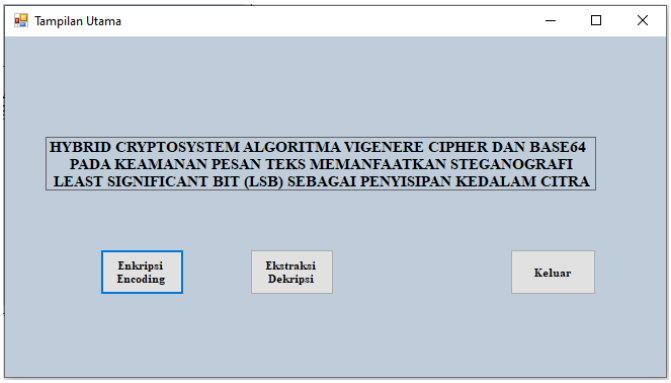

Figure 3: Main Menu Form

3.5.2. Encoding Encryption Menu Form

In this encoding encryption form can seen for search for text files use the *Browse* button (search) and order original will come on stage along filename, length message and, file size. Enter keywords For algorithm vigenere cipher then press knob encryption and will start the encryption process with two method, then For look for image used as the insertion medium use the *Browse* button furthermore will come on stage image, name image and size image. Press encoding button for start insertion and then press save button for keep image.

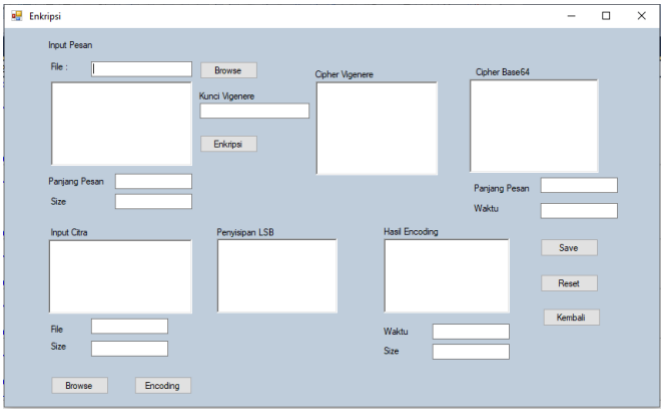

Figure 4: Encryption Menu Form

3.5.3. Extract menu form decryption

On the extraction form decryption can looking for image files via the Browse button for look for the image file to be decrypted, then image will appears and press knob extraction. Furthermore input key the same vigenere cipher with the encryption process and press knob decryption For return to message beginning Then save.

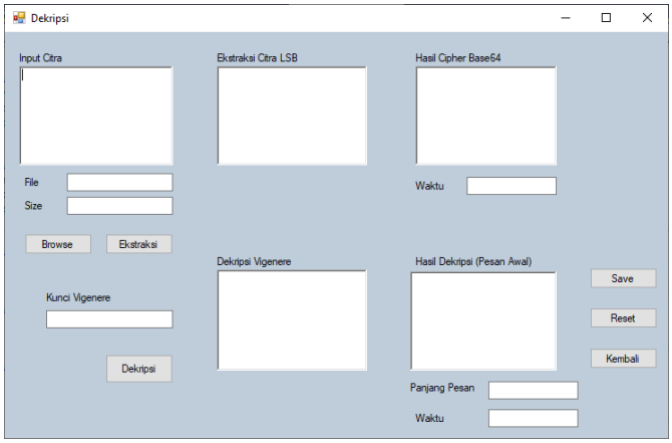

Figure 5: Decryption Menu Form

4. Conclusion

Results of planning and making cryptographic programs use algorithm vigenere cipher, base64 and least significant bit (LSB) steganography can seen as following:

1. Test results system show that messages that have through the process of encryption encoding and extraction decryption with algorithm vigenere cipher, base64, and least significant bit (LSB) steganography has same information with message first. The more Lots message, the longer the encoding and decryption process.
2. Research results show that proposed system succeed encrypt message text use algorithm Vigenere Cipher and Base64 inserts message to in image use LSB steganography. Security level message increase Because message encrypted text difficult solved without right key, whereas embedded message to in image difficult detected by the method ordinary visual analysis.
3. Least Significant Bit (LSB) steganography was used For insert message text that has encrypted to in pixels image, where information message pasted in bits at least significant from every pixel. Method This utilise resilience eye man to small changes in pixels image, so embedded message difficult detected by the eye human.

References

[1] Yusfrizal, "DESIGN OF CRYPTOGRAPHIC APPLICATIONS ON TEXT USING THE REVERSE CHIPER METHOD," vol. 3, no. 2, pp. 29–37, 2019.
[2] J. Jamaludin and R. Romindo, "Design of Text Security Using a Combination of Vigenere Cipher and RSA in Hybrid Cryptosystem," vol. 2, pp. 105–116, 2020.
[3] H. Triansyah, "Combination of Vigenere Cipher Cryptography Algorithm and AES Algorithm for Security of Text Messages," *TECHSI - J. Tek. inform.* , vol. 11, no. 3, p. 408, 2019, doi: 10.29103/techsi.v11i3.1874.
[4] WM br Purba, "IMPLEMENTATION OF KNAPSACK AND BASE64 ALGORITHMS ON TEXT FILE SECURITY," vol. 7, no. April, pp. 552–563, 2019.
[5] R. Munir, *Cryptography* . Bandung: Informatics Bandung, 2019.
[6] EV Haryanto, "Steganographic Design for Image Security with Android-Based RSA and LSB Algorithms," pp. 179–190, 2019.
[7] DA Prabowo, D. Abdullah, and A. Manik, "BASED ON COLOR USING," vol. V, no. september, pp. 85–91, 2018.