The Combination of Bit Matching-Based Steganography and DES Cryptography for Data Security

Budi Prasetiyo [1)]
Semarang State University, Semarang
email : prasemath@gmail.com

Rahmat Gernowo [2)] Beta Noranita [3)]
[2) 3)] Diponegoro University, Semarang

Abstract - This research discussed the combination of steganography and cryptography to secure data without changing the quality of cover medium. Steganographic method is used to match bit of the message with bit of the MSB image cover. Matching process is done by divide and conquer method. The result will be a bit indexposition, and then it will be encrypted using cryptographic DES (Data Encryption Standard). The input are text message, image, and key. The output is ciphertext bit index which can be used to secure the messages. To read the contents of the message, we require the same image cover and key.Outcomes of proposed method can be used to secure the data. The advantages of this method are the image quality will not change and the capacity of stored messages can be larger than the image. Acoording to the research, both grayscale and colorful images can be used as image cover, except the image contains 100% black and 100% white. Bit matching process on image which have much variety of color takes less time. The damage of messages due to the addition of "salt and pepper" noise starts from 0,0067 of MSE value and gaussian starts from MSE 0,00234.

Keywords:***steganography, bit matching, divide and conquer, bit index, MSB, encryption, decryption, DES.***

I. INTRODUCTION

These recent years, the human need for information is increasing. In the midst of rapid development of information technology, the internet is no longer providing secure information. The developmentof search-enginecoupled with the development of virus, bugs, spam and hackers who can steal confidential data (Kautzar, 2007). To solve this problem, various ways have been developed to improve data security, such as cryptography and steganography.

Steganography is the art and science of hiding data in other media as a cover(e.g. image)in order to makethe data looks sketchy (Provos and Honeyman, 2003). Cryptography is the art and science of maintaining the confidentiality of data (Schneier, 1996). In cryptography, the original data is converted into another form that can not be read. The combination of steganography and cryptography can simultaneously increase the security of the data (Krenn, 2004).

Method for combining steganography and cryptographyhas been developed. In general, the mostly used technique is message encrypting first (cryptography), then hiding it into media cover (steganography)(Raphael and Sundaram, 2011). However, the embedding process can affect the quality of the cover media.

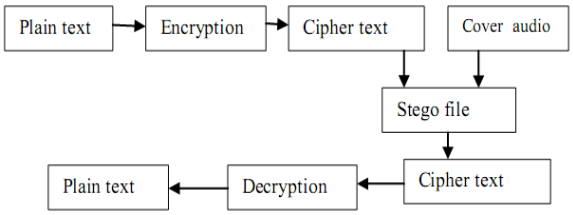
Efforts to minimize the quality changes of cover image can be done by embeddingthe data in the least significant bit. Changes in the quality of cover isinvisible (Chan and Cheng, 2004), but the embedding of cover into the least bit tends to make the cover prone to robust. Robust resistance can be done by embedding the data in the first bit (most significant bit), but it will change the quality of the cover and it will look suspicious.

Other studies conducted by (Challita and Farhat, 2011) developed a new way of merger steganography and cryptography without changing the media cover. The technique is performed by matching the message bits on the cover, and then continue the process of encryption (cryptographic). One well-known cryptographic algorithms since 1977 and became a worldwide standard is the Data Encryption Standard (DES) .

This research will combine steganography and cryptography without changing the media cover. The steganography method used is a method based on bit matching in the first bit (most significant bit) and the cryptographic method used is the DES algorithm.

II. REVIEW OF LITERATURE

Variousmethods have been developedfordata security. In general,thetechniques usedisencrypting themessagefirst(cryptographic process), and thenembedding it into themediacover(steganographyprocess) (Raphael andSundaram, 2011).



Fugure1.Combination ofsteganographyandcryptography(Raphael andSundaram, 2011)

Combinationtechniqueis not only limitedas shown in Figure1. Research (NarayanaandPrasad, 2010)examinestwoapproachestosecuresteganography mediacover(image). Securing steganography imageis doneby encrypting. The firstmethod, steganography image isdirectlyencryptedwithS-DES, the result is aciphertext. The secondmethod, the image is encrypted thenciphertextfrom encryptionwill beembeddedonanotherimage.

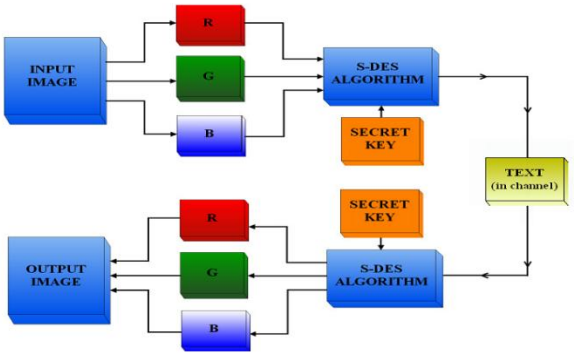


Figure2.Firstapproach (NarayanadanPrasad, 2010)

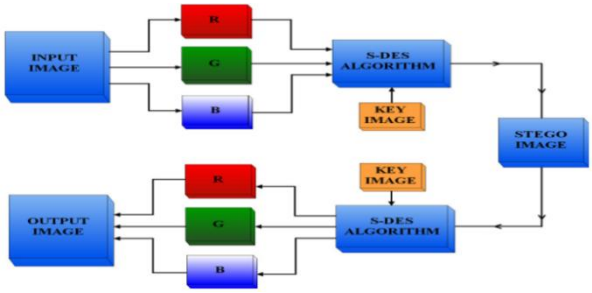


Figure3.Second approach (NarayanadanPrasad, 2010)

One of the easiest methods of steganography is LSB (Least Significant Bit). The procedure to perform this method is to embedthe least bit at each pixel with the message bits. Terminology LSB is reviewed by (Sharp, 2001). The LSB embedding will change the bit value, but it will be invisible, so that the third party does not know the existence of the secret message behind the media cover (Chan and Cheng, 2004).

The use of LSB on the combination of steganography and cryptography was done in aresearch conducted by(Sharp, 2001). The process consists of three stages, namely encryption, steganography and, decryption. Encryption and decryption is done with DES algorithm (Data Encryption Standard). The use of LSB can minimize the image quality changes, but the capacity of messages that can be accommodated is due to the size of the image. (Kekre, et al., 2012) conducted a LSB steganography study to increase the messages capacitywith PVD approach (Pixel value differencing). LSB insertion is based on comparison of the MSBbit value (Most Significant Bit). If the value of the first 4 MSB bits is "1", then embed it on the last 4 bits. If the first 3 bits MSB is " 1 ", then embed it on the last 3 bits. If the first 2MSB bit is " 1", then embedit on the last 2 bits. If the value is outside the criteria, then the embedding is done on the last bit (least).

Image quality is an important component in steganography. (Challita and Farhat, 2011) developed another way to combine both steganography and cryptography without changing the image quality. The technique is performed by matching the message bits on the cover, the results is in the form of bit position index. Index is then encrypted. The output is bit indexciphertext. Bit matching is done by divide and conquer (Cormen, 2009) that consist of three processes, namely divide, conquer, and combine. Arrangement of long bits is splitting it into two smaller parts (divide), then match each section (conquer). The results of each part of the solution then combined into a total solution (combine).

III. BASIC THEORY

3.1 Steganography

Steganographycomesfrom the Greek, meaningSteganosmeansto hideandGraptosmeanswriting, so thatsteganographyis defined as"hidden writing(covered writing)". Steganographyis the scienceandart of hidinga secretmessage(hiding message)so thatthe existence ofthe messageis notdetectedbyhuman senses. The data hidingprocess into media iscalled embedding, whereasthe reverse processis calledextraction. In general,the processis shownin Figure4.

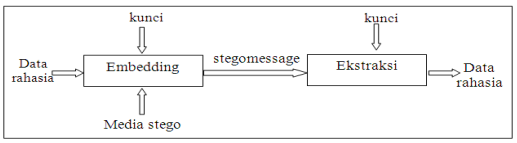


Figure4.Embeddingandextractionprocessinsteganography

3.2 Cryptography

Cryptographycomes fromtwo Greek words,Crypto whichmeansthesecretandGraphowhichmeans writing. Cryptographyis the study ofmathematicaltechniquesrelated toaspects ofinformation security, such asdata confidentiality, data authenticity, data integrity, andauthenticationof data(Menezeset al., 1996).

Cryptographybasicallyconsistsoftwoprocesses, namelythe encryptionanddecryptionprocess. In general, the encryptionanddecryptionprocessescan be seenin Figure5.

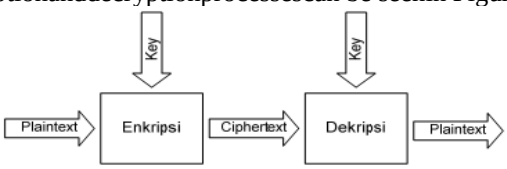


Figure5.Proses enkripsidandekripsi

*3.3 DataEncryption Standard(*DES*) Algorithm*

DESis ablockcipheralgorithmthat operateson64-bit inputblockandkeysize of128bits(Munir, 2006). DESalgoritnageneralschemeis shownin Figure6(Munir, 2006).

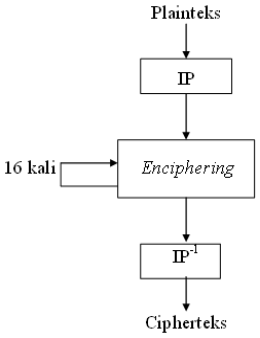


Figure6. DES Algorithm (Munir, 2006)

Input of encryption process is plaintext and key. Working principle of the DES algorithm for encryption are

as follows:
a. Broke the 64-bit plaintext into L (32bit) R (32bit)
b. Perform initial permutation (IP),
c. Encrypt in 16 rounds (enchipering). Internal locks on each different lap.
d. Invert the initial permutation (IP-1).

3.4 Combination ofSteganographyandCryptography

Combination ofsteganographyandcryptographyin general isperformedwiththe cryptographic processfirst and thensteganography, whichencrypts themessagefirst and thenembedthe encryptedciphertextto a cover media(Raphael andSundaram, 2011). The mergingconceptsof cryptographyandsteganographyis shownin Figure8.

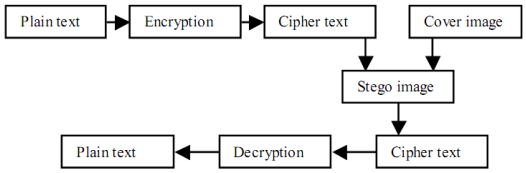


Figure7. Combination of Steganography and Cryptography (Raphael danSundaram, 2011)

3.5 BitMatchinginDivideand Conquer

Message bit matchingin thebitimageis donebythedivideand conquermethodwhichconsistsofthreerocesses: divide, conquerandcombine. It means tobreak the probleminto smaller parts(divide), and thenrecursivelyresolveanyminor issues(conquer). Thenthe solutionsofevery minor problem aremerged into onemainsolution(combine) (Cormenet al., 2009).

The use ofdivideand conquermethodinsteganographyis done byChallitaandFarhat(2011) in his researchto matchthe location ofmessagebitsandbits ofthe image. SupposegivenasequenceS1andS2, anddenotedin LCS(S1, S2),isan algorithmforlong substringsearch(longest commonsubsequence) ofS1that appearsonS2. Next it willyieldtrue value if theentireS1occurs inS2. algorithmIllustration(LCS) is givenin Figure9.

```
SPS(secretMessage, coverImage);
  if LCS(secretMessage, coverImage) is true,
       then
       store the positions of the indexes
       of the start and end bits of Secret
       that occur within Image the output
       file Output,
       else
       SPS(LeftPart-secretMessage,coverImage)
       SPS(RightPart-secretMessage,coverImage)
return Output,
```

Figure8.Imagematching algorithmon themessage

3.6 Methodology

The method usedinthis study isthe integration ofsteganographyandcryptography.Cryptographic algorithmsusedare theDES. There aretwoprocesses involved insteganography, theembeddingandextraction. In this studyconstructedastego-crypto softwarewiththe waterfall model. Waterfall methodis shownin Figure10.

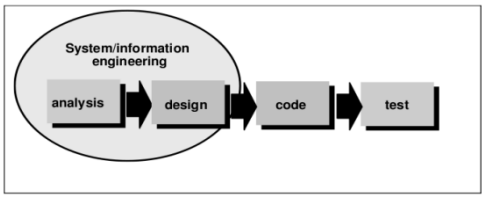


Figure9.WaterfallMethod (Pressman, 2001)

Waterfall methoddividesthe researchintofourphaseswhichare interrelatedandinfluence. Thefourstages aretheneeds analysis(analysis), design, codeandtest(Pressman, 2001).

The combinationof cryptographyandsteganography inthis studyrequired 4processes,they are bitmatching, encryption, decryptionandreconstruction. The details are as follow.

3.1. Matching Bit

In this study the method of matching is done with divide and conquer(Cormen, 2009). Input to this process is the message and image.

The steps are performed in the bit matching are :

a) Convert the message and image in binary form
b) Taking the value of MSB image
c) Perform the matching messages on MSB image. If the bit message is contained in the MSB image, then proceed to save the position of the bit index. Index saving consists of index position of the first(start) and the position index of the last bit(end). If the matching process does not occur, continue the process d) as follows.
d) Divide the message into two parts of equal length of the left (L [i]) and right (R [i])
e) Repeat the same steps as in number b), with L [i] and R [i] as input. If all the bit message are contained in the image, the matching process is completed and continue to f). If not, repeat step c)with L [i] and R [i] as an i step .
f) Keep all bit index from matching results
g) The output is a vector that contains the index structure of bit position.

For example, suppose bit message and bit image are known as follows:
Message (M) :10110111
Image (I) : 10010001101011010101010011
Since M is not contained in I then M was split into two parts left (L) and right (R), namely :

1. L[1]: 1011which is locatedat the positionindex"11 14", which is10010001101011010101010011.
2. R[1]: 0111, notpresent inthe image, thendivideR[1] into twoparts, namely:
3. a.L[2]: 01, located at index position"3 4"
   b. R[2]: 11, located at index position"8 9"
4. Because ofall thebit positionis found, then thematching processes are completedandproceedto step 4.
5. Combineallsolutions fromstep 1, step2a, and2b. Retrievedwholebitindexposition"11 14 3 4 8 9".

3.2. Encryption

Position vectorof bit isobtained at3.1sectionlaterinencryption. Encryption processis donewith theDESalgorithm.

3.3. Decryption

Inputto this processis theciphertextandthe key. Decryptionof theciphertextis the inverse ofthe encryptionprocess. DESusesthe same algorithmfor encryptionanddecryption. In theprocess ofdecryption, thekeysequenceusedisthe inverse one namelyK16, K15, ...,K1. For eachround of16, 15, ...,1, the outputateachround ofdecipheringis

$L_i = R_{i-1}$

$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$

3.4. Reconstruction

Reconstruction aims to restore the message to its original form. Input at this stage consists of bit and image index location. Process that is carried out is taking the composition of the image bit based on vector of index bit location. The prsesoutput is in the form of the bit message composition.

The steps are performed in the reconstruction process are:

a) Convert the image in binary form and take the bit of MSB image.
b) Read the contents of two index vectors. The first index is a bit's early position (start) and the second index is the bit's end position (end),
c) Taking the value of bit image based on step b),
d) Repeating the process b) and c) until the last index position.
e) The composition of the bits will create an output in the form of bit message.

For example, suppose the unknown vector and image as follows:

Vector : 11 14 3 4 8 9
Image : 1001000110101101010010011

Extractionstepis done by taking thevalue ofth bite image based onthe location ofvectors. Putting all thebit value from matchesresult of the vector. In that casea matchisobtained

•Vector11,14, producedin 1011.
•Vector34, generating01.
•Vector89, yielding 11.

Allthe aboveresultsare combined, resulting in outputs10,110,111.

3.5. Combination Steganography and Cryptography

3.5.1.Overview

Combination ofsteganographyandcryptographyin this studyconsistsoftwomainprocesses, namelythe process ofembeddingandextractionwhich is generallyshown in Figure11.

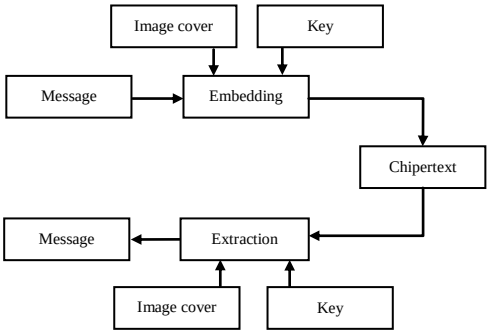


Figure10.General description ofthe combination ofsteganographyandcryptographyonthe study

Embeddingprocess(Figure 12) consistsofbit matchingandencryption, the result isciphertext. Extractionprocess(Figure 13) consistsofdecryptionandreconstruction;the results arein the form ofa message.

3.5.2.*EmbeddingProcess*

Embeddingprocess(Figure 12) aimstogeneratebit indexposition. The input ofembeddingprocessis in the form ofmessages, images, andkeys.

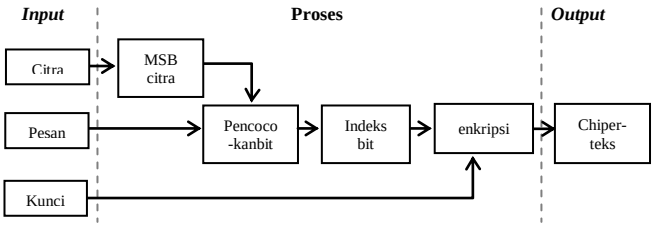


Figure11.Embedding Process

Embeddingstepsare asfollows:

a) Integrate the input in the form of images, messages, and key.
b) Convert the message and image in binary form.
c) Match the bit message with the bit of MSB image. The same bit positions are stored in the bit vector index.
d) Encrypt the bit vector index with DES algorithm.
e) The output is ciphertext. The ciphertext contains a bit vector that has been encrypted.
f) Finish.

3.5.3.Extraction process

Extractionprocessaimstorestorethe message toits originalformin order to maintain theoriginal contents. The inputs of extractionprocess are aciphertextvector, a key, andimagery.

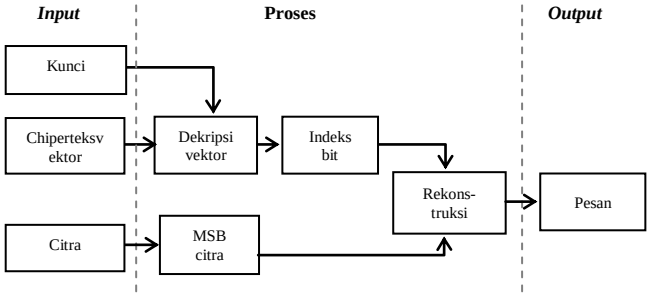


Figure12.Extractionprocess

Extractionprocess stepsare asfollows:

a) Inputkey, ciphertextvector, andimagery.
b) Decryptthe vectorwith the key, the decryptedplaintext isin the form ofbit index.
c) Do a message reconstructionby matching bit of MSB image based onbitindex vector.
d) The output isthe message.
e) Finish.

IV. RESULTS AND DISCUSSION

The resultof this research is in the form ofapplicationprogramswhich is developedusingthe programminglanguageMATLABR2009athen it was tested fordata security.

4.1. Testing the image color

1) Embedding Process

The stepstoperformthe embeddingprocessareasfollows:

a Selectingthemessagefilewhich willbe embedded. In this case, atransfer.txt file wasselected. The contents:

Money transfer, 50millions via ATM
Bank account: 0123456
Password PIN: 9x8d7g
Under the name of Budi Prasetiyo

b Choosingacoverimagefile, for exampleBaboon.bmp(Figure 14).

Figure13.Citra cover

c Typing the password as the encryption key for DES, for example key: 1234567.

d the output of embedding are after a bit index (Figure 15. A) and bit index of ciphertext (Figure 15. B).

42 45 1 3 213 219 1008 1014 47 53 210 216 312 318 1008 1014 565 570 1837 1843 65 71 81 87 15278 15283 331 337 4577 4583 1112 1118 22 27 59 65 42 45 13 15 235 241 7266 7272 1428 1434 6552 6558 62 68 21 26 59 65 2204 2210 7668 7674 51 56 22 28 12 18 15277 15283 44 49 313 319 1431 1437 1268 1281 672 678 21 27 210 216 84 89 6199 6205 475 481 1837 1843 45 50 59 65 1285 1291 40 46 1429 1434 2204 2210 42 45 43 45 311 317 3019 3025 7773 7786 6552 6558 13 18 1013 1026 6346 6358 1112 1118 313 319 473 479 89 94 50 56 314 320 41 47 631 637 50 56 1837 1843 4577 4583 475 480 1432 1438 7346 7352 564 570 1112 1117 11 17 273 279 26696 26708 212 218 374 380 5542 5555 275 281 235 241 95 101 22 27 474 480 2204 2210..	73EC5D33ED571677592BC89A5CD F7F5AD9B6AB528FEFA99B0C14DA 667E37447140680ADAAA9F11A1E2 5A8E32DA7588D4D2DA4F45FC5A5 76B199C70D34BA5494DD5EF40EE D3478B13C55F3FE12D0BDD123673 E8401B45FC49D26AC285240A32ED 3465144D83E42479A622C80B95772 20ABBD2E8CF305BCA9D5BF7FC9 C0E11028E79DCD37F1291F2E0AA 09CB20DDB286BF9BEF7D5856B2B 39D0B3B1321A128BFDFD52834514 EA8E2CF03CEA7E63CD280773CD9 8F24C5751766B0D780465473182D E7318DF9681C1E0BC19F00241845 D8AC0BCB5593728B66A428C6C20 967A546F1D0EC79F22B71EF1F0D7 1D51E7BDE2823A770435F31C1FE5 AB4F3B0640FD7196DC68A99CD0E 07A41104AFDFA42D6B4ECC4BBA3 0D488339CB8B21BE4E514109125C B80F20F26A01CE976590D1CAEB7(FBCACDB6E061F9F4375127..
(a)	(b)

Figure14.(a) bitindex, (b) encryptedbitsIndex

2) ExtractionProcess

In testing theextractionprocess, the authorwill returna messagefrom thevectorthathas beenencryptedbythe fileextraction.

The stepstoperformthe extractionprocessareasfollows:

a. Choosea vectorfile, vektor_Baboon.txt
b. Choosingacoverimagefile, i.eBaboon.bmp(Figure 14).
c. Keyinput. Keymust be the sameas the onewhen performingembedding, which is "1234567".
d. Performthe extraction.

Afterthe extraction processthe messagesuccessfullyreturnedto normal, with theoutput:

Money transfer, 50millions via ATM
Bank account: 0123456
Password PIN: 9x8d7g
Under the name of Budi Prasetiyo

Table 1.Execution time onthe black and white image

No	Citra	Embedding (detik)			Ekstraksi (detik)		
		Matching	Enkripsi	Total	Dekripsi	Rekonstruksi	Total
1.	Block.bmp	1,327	24,265	25,82	25,044	0,397	25,86
2.	Gradasi.bmp	0,374	31,53	32,06	33,386	0,321	34,37
	Rata-rata	0,850	27,897	28,940	29,215	0,359	30,115

Tabel 2.Execution time onthe colorful image

No	Citra	Embed (detik)			Ekstrak (detik)		
		Matching	Enkripsi	Total	Dekripsi	Rekonstruksi	Total
1.	Lenna.bmp	0,165	12,451	12,71	12,621	0,184	13
2.	Pepper.bmp	0,157	10,152	10,40	11,872	0,183	12,24
3.	Jet.bmp	0,138	11,828	12,06	12,131	0,154	12,46
4.	Baboon.bmp	0,162	10,121	10,37	10,143	0,138	10,45
5.	Foto.bmp	0,199	15,108	15,41	15,318	0,160	15,72
	Rata-rata	0,164	11,932	12,19	12,417	0,164	12,774

Thetestingshowedthataveragely theembedding process of black and whiteimagetook28.94sec,0.850 sec for bit matching,27.897sec.forencryption,30.115sec for extraction,29.215secfordecryptionandmessagereconstructi on took0.359sec. Whilethecolorful image, averagelythe embeddingprocesstook12.19sec, 0.164 forbit matching,and11.932forencryption. Theextractionprocesstook12.774sec, 12.417sec for decryption and0.1638sec for message reconstruction.

4.2. Test Results with Different Size Resolution

The application was also testedwith differentimagesizes,ranging from512px, 256px, 128px, to64px. The test result (Table 3) showsthat the larger theimageresolution, the longer the bit matching processwilltake.The shortestbit matching is bit matching of "Baboon" (0.590 sec), whilethe longestbitmatching is the bit matchingof "Block" (2.022 sec). Baboonhasthe mostcolorvariation, while the"Block" onlyhas2colorvariations(black andwhite).

Tabel 3.The test resultswith differentimagesizes

Citra	Resolusi (px)	Proses Embedding (dtk)			Proses Ekstraksi (dtk)		
		Matching	Enkripsi	Total	Dekripsi	Rekons-truksi	Total
"Block"	512 x 512	5,57	6,576	7,576	8,576	9,57	10,57
	256 x 256	1,70	30,165	32,13	29,58	0,40	30,70
	128 x 128	0,54	31,673	32,37	27,22	0,33	28,09
	64 x 64	0,25	24,033	24,41	23,87	0,32	24,59
	Rata-rata	2,02	23,112	24,12	22,31	2,66	23,49
"Gradation"	512 x 512	5,54	24,986	31,08	24,72	0,69	25,90
	256 x 256	1,72	31,963	33,96	29,81	0,41	30,96
	128 x 128	0,54	27,441	28,14	27,38	0,33	28,21
	64 x 64	0,25	24,033	24,41	23,87	0,32	24,59
	Rata-rata	2,01	27,106	29,40	26,45	0,44	27,42
"Lena"	512 x 512	1,86	9,681	11,86	11,78	0,17	12,19

	256 x 256	0,56	10,919	11,69	10,62	0,29	11,08
	128 x 128	0,19	11,026	11,34	10,30	0,21	10,71
	64 x 64	0,09	10,033	10,20	10,08	0,18	10,41
	Rata-rata	0,67	10,415	11,27	10,70	0,21	11,10
	512 x 512	1,86	9,637	11,98	9,460	0,56	10,17
	256 x 256	0,64	10,097	10,92	10,54	0,27	10,99
"Pepper"	128 x 128	0,23	10,214	10,58	10,26	0,23	10,99
	64 x 64	0,09	9,427	9,639	9,547	0,13	9,824
	Rata-rata	0,71	9,844	10,78	9,954	0,30	10,49
	512 x 512	2,03	12,186	14,71	10,56	0,18	10,90
	256 x 256	0,56	11,341	12,09	11,09	0,26	11,57
"Jet"	128 x 128	0,22	10,714	11,03	10,70	0,18	11,50
	64 x 64	0,08	10,734	10,90	10,57	0,17	10,94
	Rata-rata	0,72	11,244	12,18	10,73	0,20	11,23
	512 x 512	1,63	7,375	9,561	7,337	0,56	8,011
	256 x 256	0,46	7,067	7,715	7,057	0,24	7,421
"Baboon	128 x 128	0,16	7,453	7,669	7,223	0,16	7,526
"	64 x 64	0,09	8,645	8,625	8,358	0,16	8,641
	Rata-rata	0,59	7,635	8,393	7,494	0,28	7,900
	512 x 512	2,44	14,795	17,75	14,74	0,56	15,54
	256 x 256	0,68	15,591	16,49	14,90	0,27	15,44
"Foto"	128 x 128	0,27	15,497	15,87	15,16	0,22	15,62
	64 x 64	0,11	14,128	14,35	13,85	0,19	14,27
	Rata-rata	0,88	15,003	16,11	14,66	0,31	15,21

In general it canbe concludedthat the embeddingof black and whiteimageis 2times longerthan thecolorful image. The process ofbitmatchingofimagewithmanycolorvariations isshorterthan theimagethathasa littlecolorvariation. This is due tothecolorvariationsimageallowsmanyopportunities fora lot ofsimilaritiesbetween thearrangement ofbitmessageand bitimage, so ittakesless time.

4.3. Testing with Giving Noise

Noise'salt and pepper' (Figure 15) andgaussian(Figure 16) was given to the imagein the nextembeddingprocess. The imagewas givennoise'salt and pepper' with standarddeviation,d=0.001; 0.005, 0.01; 0.05. The imagewas given noise'gaussian' withzeromeanandstandarddeviation,d=0.001; 0.005, 0.01; 0.05. The imagehas beengiven anoisethentestedin the extraction processtorecover the messages.

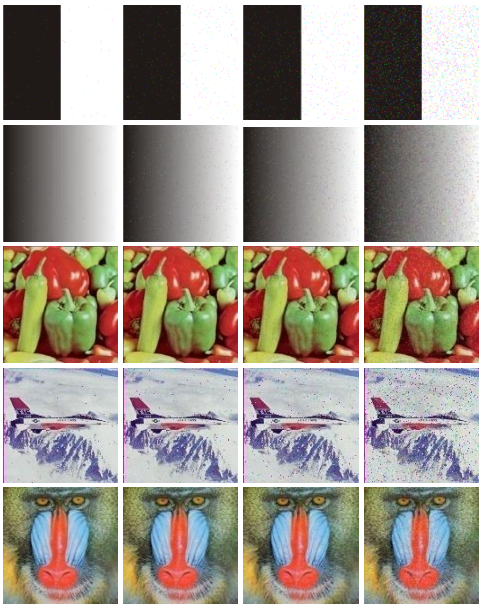


Figure15. Imagewithnoise'salt andpepper' (from leftto right, d=0.001; 0.005, 0.01; 0.05)

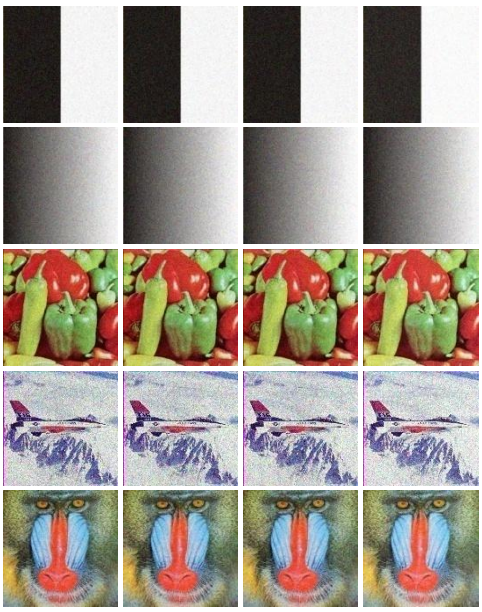


Figure16.Imagewithnoise'Gaussian' with zero mean (from leftto right, d=0.001; 0.005, 0.01; 0.05)

Tabel 4.The Test resultswithNoise

Citra	Salt & pepper (d)				Gaussian (mean=0)			
	∂	MSE	PSNR	Pesan	∂	MSE	PSNR	Pesan
	0,001	0,00030	34,987	baik	0,10%	0,00307	52,3101	Rusak
	0,005	0,00140	28,435	baik	0,50%	0,00304	52,3080	Rusak
"Lenna"	0,01	0,00310	25,014	terbacarusak	1%	0,00302	52,2815	Rusak
	0,05	0,01400	18,282	terbacarusak	5%	0,00345	51,4609	Rusak
	0,001	0,00010	67,295	baik	0,10%	0,00328	52,4225	Rusak
	0,005	0,00483	50,094	terbacarusak	0,50%	0,00329	52,4045	Rusak
"Pepper"	0,01	0,00094	57,320	terbacarusak	1%	0,00333	52,3485	Rusak
	0,05	0,00483	50,094	terbacarusak	5%	0,00404	51,3140	Rusak
	0,001	0,00013	67,773	baik	0,10%	0,00320	52,2707	Rusak
	0,005	0,00049	60,369	terbacarusak	0,50%	0,00318	52,2517	Rusak
"Baboon"	0,01	0,00091	57,660	terbacarusak	1%	0,00320	52,2316	Rusak
	0,05	0,00494	50,410	terbacarusak	5%	0,00380	51,3988	Rusak
	0,001	0,00014	61,398	baik	0,10%	0,00322	48,2885	Rusak
	0,005	0,00056	55,936	baik	0,50%	0,00319	48,3709	Rusak
"Jet"	0,01	0,00123	52,807	baik	1%	0,00321	48,2902	Rusak
	0,05	0,00515	46,077	terbacarusak	5%	0,00379	47,6589	Rusak
	0,001	0,00010	66,863	baik	0,10%	0,00296	53,0124	Rusak
	0,005	0,00067	59,135	terbacarusak	0,50%	0,00296	52,9414	Rusak
"Foto"	0,01	0,00116	56,401	terbacarusak	1%	0,00305	52,8322	Rusak
	0,05	0,00601	49,286	terbacarusak	5%	0,00386	51,5197	Rusak
	0,001	0,00009	67,871	baik	0,10%	0,00310	52,4209	Rusak
	0,005	0,00058	59,557	baik	0,50%	0,00309	52,4483	Rusak
"Grad"	0,01	0,00108	56,889	baik	1%	0,00311	52,4256	Rusak
	0,05	0,00538	50,026	rusak	5%	0,00371	51,6761	Rusak
	0,001	0,00012	65,675	baik	0,10%	0,00220	54,0692	terbacarusak
	0,005	0,00069	58,685	baik	0,50%	0,00221	54,0967	terbacarusak
"Block"	0,01	0,00163	55,358	baik	1%	0,00216	54,1347	Rusak
	0,05	0,00745	48,624	baik	5%	0,00234	53,6779	terbacarusak

Test resultsof message reconstruction ona black and whiteimagewiththe addition ofsalt&peppernoiseremains good. Messages canbe read, buttherewas one image which was damaged. While most of thecolorful imagesweredamage, exceptthe image of"Jet" and"Lenna" which only suffer from a little damage. Both “jet” and “lenna” images havethe highestMSEvalue0.014. Damage to colorful imageoccurred from0.0067MSEonimage"Photos" whichincidentally has afairlysimplecolorvariations. The addition ofGaussiannoisecauses most ofthe message contents corrupted. Damagebegan to occuron theMSE0.00234. This is due tothe addition ofnoiseaffects thevalue ofbitimage, whilematchingbitstaketheappropriatebitpositionindex.The resultof message reconstructionwillproduce the changedmessageas well.

V. CONCLUSION

The process of steganography in this study include the bit matching and reconstruction, while the cryptographic processes include encryption and decryption .

The combination of steganography and cryptography in this study can be used for data security. The input are message, image and key. The output is chipterteks. To be noticed, to see the message content we need the same key and image.

Either grayscale orcolorful images can be used as the cover media. The only exception is thecolorful image with 100 % black or 100 % white, because the image consists of a homogeneous bit structure. All bit values in the image with 100 % white is 0 (zero) and the image with100 % black is 1 (one). The bit composition of message varies from 0 to 1, so the bit matching will not find any results.

The addition of noise to the image causes some changes in the message content, the degree of changes vary. In the black and white image, the changes are not significant, while in the colorful imagethe message content changes a lot. Damage occurred on the addition of salt and pepernoise start from MSE 0.0067 and the damage to the gaussiannoise start from MSE 0.00234.

The bit matching process withcolor variation took shorter time than the image with less color variation. One advantages of this method is there was no change of theimage quality. In terms of security, even if the index vector of bit was not encrypted, the data was secure enough. This is due to the need of the right image to reconstruct the index into the originalmessage;otherwise the results will be unreadable.

Other researchers can perform encryption on the image first before matching the bit. They can performoperations on the image image with 100 % black or 100 % white, so that both black and white images can be used as covers. Besides, other researchers can modify the output ciphertext into stego image.

References

[1]. Challita, K., danFarhat, H., 2011, Combining Steganography and Cryptography: New Directions, *International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(1),* 199-208.

[2]. Chan, C. K., dan L.M. Cheng, 2004, Hiding Data in Images by Simple LSB Substitution, *Pattern Recognition Vol. 37(3),* 469–474.

[3]. Cormen, T.H., Leiserson C.E., Rivest R.L., dan Stein D., 2009, *Introduction to Algorithms*, Third Edition, The MIT Press, England.

[4]. Kautzar, M.G., 2007, *StudiKriptografiMengenai Triple DES dan AES*, ITB, Bandung.

[5]. Kekre, H.B., Archana A., danPallavi N.H., 2012, Comparison between the basic LSB Replacement Technique and Increased Capacity of Information Hiding in LSB's Method for Images, *International Journal of Computer Applications (0975 – 8887) Vol .45 (1),* 33-38.

[6]. Krenn, R., 2004, *Steganography and Steganalysis*, Whitepaper.

[7]. Menezes A.J., Oorschot, P.C., dan Vanstone, S.A., 1996, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, New York.

[8]. Munir, R., 2006, *PengantarKriptografi*, ITB, Bandung.

[9]. Narayana, S., dan Prasad, G., 2010, Two New Approaches for Secured Image Steganography Using Cryptographic Techniques and Type Conversions, *Signal & Image Processing: An International Journal (SIPIJ) Vol. 1(2),* 60-73.

[10]. Pressman, R.S., 2001, *Software Engineering*: *A Practitioner's Approach,6th Edition*, The McGraw-Hill Companies, Inc, Singapore.

[11]. Provos, N., danHoneyman, P., 2003, Hide and Seek: An Introduction to Steganography, *IEEE Security & Privacy Vol. 1(3),* 32-44.

[12]. Raphael danSundaram, A.J., danSundaram, V., 2011, Cryptography and Steganography – A Survey, *International Journal Comp. Tech. Applied Vol. 2 (3),* 626-630.

[13]. Schneier, B., 1996, *Applied Cryptography 2nd Edition*, Wiley & Sons. Inc., New York.

[14]. Seth, D., Ramanathan, L., danPandey, A., 2010, Security Enhancement: Combining Cryptography and Steganography, *International Journal of Computer Applications (0975 – 8887) Vol. 9 (11),* 3-6.

[15]. Sharp, T., 2001, An implementation of Key-based Digital Signal Steganography,*Proc. Information Hiding Workshop Vol. 2137, Springer LNCS*, 13–26.