The 5th ICIBA 2016, International Conference on
Information Technology and Engineering Application
Palembang-Indonesia, 19-20 February 2016

Steganography Application Bitwise Method of Encrypted Message with Vigenere Cipher

Nazori Agani, Charles Victor B. Saragih, Chris Simon

Postgraduate Program, Budi Luhur University
Jl. Raya Ciledug, Jakarta Selatan, Indonesia
e-mail: nazori@budiluhur.ac.id, chs8582004@yahoo.com, chris_simon92@yahoo.com

Abstract

Computer security has become a very serious problem. It has been reported that according to the United States Department of Defense (DoD) in 1996 has been estimated there are 250 thousand per year attacks on computer systems and this had increased 100% each year. Boulanger [16]. Cryptography can be defined as an art and knowledge in preparing a secret message. Plaintext message to be encoded into a cipher text through a process of enciphering or encryption and the plaintext message will be returned from the cipher text through the process of deciphering or decryption. Research done is to calculate the Euclidean distance to the insertion of a message that has been encrypted using Vigenere Polyalphabetic to an image. The results obtained are encrypted message using Vigenere Polyalphabetic can be well done on the image. Has successfully decrypted the ciphertext back after being separated from the image so back to plaintext. The message can not be decrypted back when there is a change in the image stegano.

Keywords : *Vigenere cipher, Bitwise, Ciphertext, Eucledean.*

1 INTRODUCTION

With the development of internet access is needed good security such as banking transactions , the risk of transaction data is also growing. To protect data from unauthorized access or loss of data should the necessary encryption to the data at any time. Currently there are several encryption methods like AES and DES. However, the limitations of 56bits key length for DES increasingly make such methods less secure. On the other hand AES newly discovered and untested. This leads to many things in the AES should be retested such as DES. Kasiski method can be used to predict the length of a cipher key words and search for the period of polyalphabetic cipher [1],[2]. Merging Playfair and Vigenere method can produce a layer of security that baik [3]. Polyalphabetic cipher used in each letter on the Caesar cipher key to determine which one will be used . After all the letters on the keys are already in use then subsequently re-used letters in the beginning. Illustration of the use of the key KEY is as follows in Table 1 :

Table 1: Encryption

Kunci	Pesan	Chipertext
KEYKEYK	MESSAGE	WIRCEEO

The cipher form based methodology confusion to form the ciphertext. Repetition of key follow the message or plaintext diffusion is not done just a camouflage against Caesar shift. The longer the keyword the more difficult to break the encryption. If the key length is along the plaintext, the ciphertext have immunity from attack cipher. At the time this condition is met then also called a block cipher. By adding specific bit to the message before it is encrypted then it will increase the security methods polyalphabetical [4].

In general there are two types of an encryption: symmetric and asymmetric. Symmetric encryption uses the same key to encrypt and decrypt a message. Asymmetric encryption is often also referred to as public key or two-key encryption uses one key for encryption and another for decryption of the keys.Another method in polyalphabetical is a permutation/transposition different methods of substitution and called Playfair Cipher. Ciphertext will be formed by reading a column in the order by the key. Place the message to be encrypted into a matrix as in Table 2, then fill the matrix with an extra character. Keywords identify how many times the columns will be used and how the order when the column is used. The order of the columns used is determined by the order of the alphabet contained on keywords.

Table 2: Matrix Transpotion

S	A	M	P	A	I
B	E	R	T	E	M
U	K	E	M	B	A
L	I	E	S	O	K
H	A	R	I	D	I
S	I	N	I	Y	Y

For example if a keyword is SEPATU, then the alphabetical order of the word is 423 156 where A is the first, the second E, P the third and so on. The order placed on the top of the matrix as shown in Table 3.

Table 3: Matrix Based on Seuence Key

4	2	3	1	5	6
S	A	M	P	A	I
B	E	R	T	E	M
U	K	E	M	B	A
L	I	E	S	O	K
H	A	R	I	D	I
S	I	N	I	Y	Y

Readings are decreased in the order numbers to perform encryption. The first column will contain sequentially PTMSII and overall message will be PTMSII AEKIAI MREERN SBULHS AEBODX IMAKIY. This method can also be referred to as a column transposition in general . With the addition of the transposition cipher Vigenere method can be more complex to solved [5].Vigenere Encryption can also be done by applying the following formula Algebra as the encryption process :

$$Ci = EK(Pi) = (Pi + Ki) mod 26 \tag{1}$$

Decryption process can use the formula :

$$Pi = DK(Ci) = (Ci - Ki) mod 26 \tag{2}$$

P is the message or plaintext, C is encrypted or ciphertext , and K is the key. To increase the security Vigenere Algebra then be calculated by Alpha Qwerty by the formula :

$$Ci = EK(Pi) = (Pi + Ki) mod 92 \tag{3}$$

Decryption by the formula :

$$Pi = DK(Ci) = (Ci - Ki) mod 92 \tag{4}$$

The result is Vigenere with Alpha Qwerty safer [6]. Vigenere substitution calculations can also use modulo 64 taking into account the ASCII code [7]. The formula also known as shift cipher [8].There are some crypto systems such as the use of formulas such as the following to encipher :

$$f(x) = 3x \ mod \ 26 \tag{5}$$

The formula for performing decipher is :

$$f^{-1}(x) = a^{-1} \ x \ mod |R| = 9x \ mod \ 92 \tag{6}$$

By using the algebraic formula such as the security in cryptography can be done to prevent any unauthorized access to information [9]. The least significant bit (LSB) is a common method used for the insertion of the merger process messages with pictures. The ability to hide a message called steganography [10]. Bitwise method can provide an effective and efficient performance of the safety factor data [11]. Without the key description of the message is pasted with LSB can not understand the meaning [12]. Bitwise method can perform calculations of data in the form of bits, but for the simpler the better used in binary computation [13]. The best approach when making steganography using bitwise LSB is a method where the message can be hidden in an object [14]. Euclidean distance can be used to seek a common particular state or environmental similarity [15].

The research objective is to analyze the data encryption using the polyalphabetical Vigenere cipher using process developed by Rahmani.et.al.[6], the level of success in the overall process, including the process of LSB bitwise stegano. Measurements were performed by calculating the Euclidean distance between the inserted image and the original image.

2 RESEARCH METHODOLOGY

Encryption is the process by which a message (plaintext) is transformed into another form of message (ciphertext) using a mathematical function and a special password encryption key that is known by the term. Decryption is the reverse process of his which ciphertext is transformed back into plaintext with mathematical method and using a key. Subtitution cipher is a condition in which each letter of a plaintext is replaced by another symbol and is usually used in the replacement of these symbols are the letters of the alphabet series. The study design is shown in Figure 1.

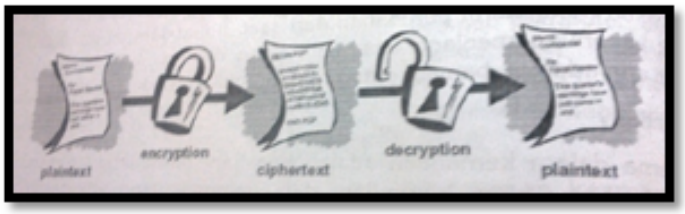

Figure 1: Design of the study

Message encryption using polyalphabetical without transposition process. Vigenere Cipher calculations can use Table 4 as a reference shift. Polyalphabetical algorithm used to perform the encryption is shown in Figure 2.

```
function ciphertext = encrypt(plaintext, key)
v = vigenere;

% Squeeze out everything except letters and the space character
exclude = regexp(plaintext, '[^a-zA-Z ]');
plaintext(exclude) = [];

% Make the key and the plaintext lower case, and convert to
% numeric values.
key = lower(key) - double('a') + 1;
key(key < 0) = 26;
plaintext = lower(plaintext) - double('a') + 1;
plaintext(plaintext < 0) = 26;

% Replicate the key so that it is as long as the plaintext.
keyIndex = mod(0:(numel(plaintext)-1), numel(key))+1;
k = key(keyIndex);

% Encrypt: C(m,n) = V(k(j), plaintext(j))
ciphertext = arrayfun(@(m,n) v(m,n), k, plaintext) - 1;
ciphertext(ciphertext == 25) = double(' ') - double('a');
ciphertext = upper(char(ciphertext + double('a')));
```

Figure 2: Encryption Polyalphabetical

After the encryption process with the shift cipher polyalphabet done then the next process is inserting a message into the picture. The flow of the process used is bitwise LSB which transpose into a message in binary form and then pasted into the picture with a particular

pixel location as shown in Figure 3. In a similar algorithm message is retrieved from the image.

```
for i = 1 : height
    for j = 1 : width
         LSB = mod(double(c(i,j)), 2);

        if (k>m || LSB == b(k))
            s(i,j) = c(i,j);
        else
            if(LSB == 1)
                s(i,j) = c(i,j) - 1;
            else
                s(i,j) = c(i,j) + 1;
            end

            k = k + 1;
        end
    end
end
```

Figure 3: Algorithm LSB Stegano.

With the algorithm shown in Figure 4. The message is retrieved from the image to be ready to be decrypted. Sampling was done by random that way provide an opportunity or an equal chance of each element in the population to be selected as a sample. Measurements in this study using accidental sampling, where sampling can be done by chance along the information or represents necessary [16].

In conducting the study used computer with i5 series processor with Windows 7 operating system and applications MatLab 2013a.

3 RESULTS AND DISCUSSION

To calculate the distance of Euclidean the characteristics used are Mean, Standard deviation, contrast, homogeneity, Entropy, Correlation and Energy. The complete results of the calculation of distance Euledian of the original image with the image polyalphabetical is shown in Table 5.

Results of this research is the conclusion of the testing that has been done. The test results based on specifications of the application indicates that this application be successful for each factor testing. Factors to be examined include the suitability factors, the suitability of data, and image quality stegano. In the conformance testing process, the application can perform encryption and decryption process text message properly.

Results obtained after several trials are as shown in Table 5 and Table 6. All plaintext encryption can be done well and can be inserted into the image well too. Euclidean distance

```
function plaintext = decrypt(ciphertext, key)
v = vigenere;

% Convert the key and the ciphertext to one-based numeric values;
% A=1, B=2, etc. SPACE=27
key = lower(key) - double('a') + 1;
key(key < 0) = 26;
ciphertext = lower(ciphertext) - double('a') + 1;
ciphertext(ciphertext < 0) = 26;

% Replicate the key so that it is as long as the ciphertext.
keyIndex = mod(0:(numel(ciphertext)-1), numel(key))+1;
k = key(keyIndex);

% Decrypt. Each letter of the key determines a row in the Vigenere
% square. In that row, find the column index of the corresponding
% ciphertext letter. Convert the index back to a letter to determine
% the decrypted character (1=A, 2=B, etc.).
plaintext = arrayfun(@(m,n) find(v(m,:) == n), k, ciphertext) - 1;
plaintext(plaintext == 25) = double(' ') - double('a');
plaintext = upper(char(plaintext + double('a')));
```

Figure 4: Algorithm decryption.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 5: Matrix Vigenere.

calculations used indicates that the resulting values vary according to the ciphertext inserted. EU1 value indicates also that there is a change in the value of LSB particular pixel in the image. This is evidenced by Euclidean distance greater than zero and no zeroes . As we know that if Euclidean value is zero then there is no change in the structure of the pixels of an image before and after the process stegano.

As shown in Table 6 by using the key word length of 10 and 20, the resulting time encryption and decryption are quite stable. A big change from small to large files has implications

Table 4: Research result

No	Plaintext	Key	Chipertext	Eu1
1	VIGENERE CIPHER	RAHMANI	MINQNR V JUPUMI	0.0277855
2	ALGEBRA CIPHER	Kabachinski	KLHEDYIMUSXRES	0.147195
3	Bitwise	Kasiski	LILEACM	0.210274
4	Eucledean	Klaus	OFCFWNPAH	0.0649331
5	STEGANOGRAFI	WILSON	OBPYOAKOCSTV	0.129141
6	good morning	Diposumarto	JWDRRGAREBBJ	0.0334618
7	tehnik komputasi	Liss	EM FTSRC UHMEIKA	0.0670482
8	polyalphabetical	Ahmed	PVXCDLWTEEEAUGDL	0.0234007
9	security ciphers	Mollin	ESNF VFMKNQCTSCD	0.368105
10	accidental random	Klima	KNKUDOYBMLICIDYX	0.390709

Table 6. Elapse time result.

	Test	Filename	File Size (bytes)	Encryption (millisec) Enc	Decryption (millisec) Dec
Keywords 10 lengths	1	tes1.txt	1,370	41,165	19,740
	2	tes2.txt	4,026	60,078	79,788
	3	tes3.txt	11,765	103,028	138,001
	4	tes4.txt	35,477	223,663	294,650
	5	tes5.txt	50,831	316,540	409,685
	6	tes6.txt	203,324	1,090,959	395,867
	7	tes7.txt	406,648	2,220,333	397,942
	8	tes8.txt	609,972	3,278,398	423,814
	9	tes9.txt	813,296	4,273,272	438,266
	10	tes10.txt	1,219,944	6,771,573	398,032

	Test	Filename	File Size (bytes)	Encryption (millisec) Enc	Decryption (millisec) Dec
Keywords 20 lengths	1	tes1.txt	1,370	27,235	38,099
	2	tes2.txt	4,026	60,353	58,879
	3	tes3.txt	11,765	105,285	133,705
	4	tes4.txt	35,477	224,609	308,607
	5	tes5.txt	50,831	315,420	394,019
	6	tes6.txt	203,324	1,108,263	377,548
	7	tes7.txt	406,648	2,169,558	402,453
	8	tes8.txt	609,972	3,227,332	397,868
	9	tes9.txt	813,296	4,342,471	367,058
	10	tes10.txt	1,219,944	6,495,980	360,670

linearly with time is used for encryption, but not with the decryption process. Decryption process looks fairly stable at an average of 280k millisecond . It can be clearly seen in Figure 5.

In testing the suitability of data, text messages are decrypted in accordance with the pasted text messages. Suitability in terms of the content of the text message. Image quality testing showed that the insertion of the bits of text messages into an image does not affect the picture quality. This is because changes in the first bit is very difficult to be detected by the human eye. And this is also shown by the images before and after the insertion is practically invisible difference. In testing the durability of data to image manipulation stega, all the

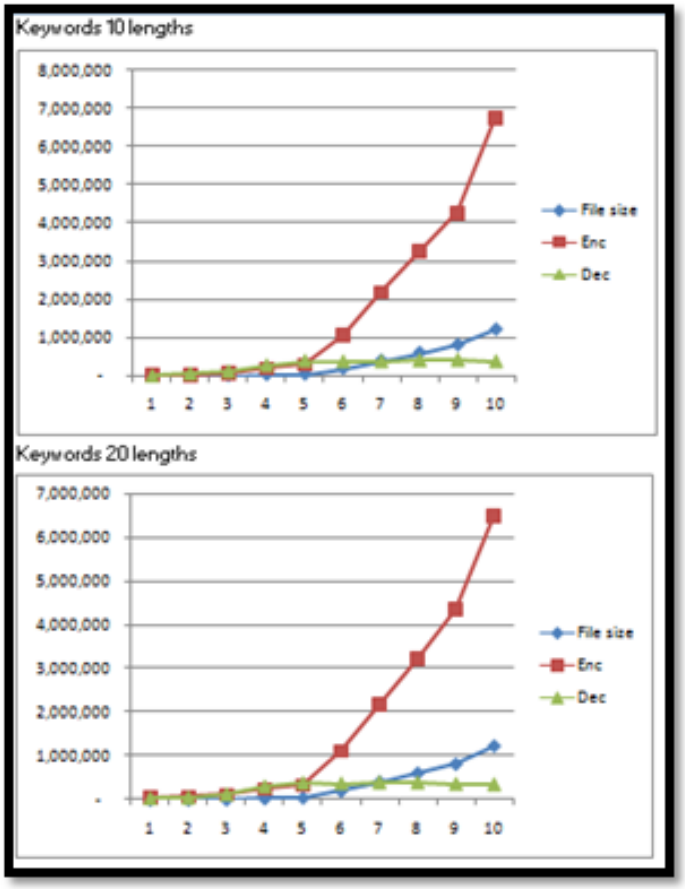

Figure 6: Cipher Result in millisecond.

test results indicate that a text message can not be decrypted. Stegano image manipulation process causes changes in the random bit image stegano. Where the random bit is a place to insert text messages. And based on the test results, it can be concluded that the image stega results vigenere cipher encryption and steganography bitwise operations cannot tolerate the manipulation of images. The results can be seen in Table 7.

4 CONCLUSIONS

From the test results based on the application specifications, with vigenere cipher encryption method and operation of LSB steganography, encryption and decryption can be done well. For the suitability of data, text messages and the decryption result is the same as the original message . Insertion of the message also does not affect the picture quality because it is difficult to detect by the human eye, but there is a change in the distance calculation Euclidean.

From the test results based on resistance data, it can be concluded that the image file stegano not resistant to factor image manipulation. The message can not be decrypted after stegano manipulated images . This is caused by the insertion of the ciphertext message on

Table 7. Durability test.

	Test	Filename	File Size (bytes)	Encryption (millisec) Enc	Decryption (millisec) Dec
Keywords 10 lengths	1	tes1.txt	1,370	41,165	19,740
	2	tes2.txt	4,026	60,078	79,788
	3	tes3.txt	11,765	103,028	138,001
	4	tes4.txt	35,477	223,663	294,650
	5	tes5.txt	50,831	316,540	409,685
	6	tes6.txt	203,324	1,090,959	395,867
	7	tes7.txt	406,648	2,220,333	397,942
	8	tes8.txt	609,972	3,278,398	423,814
	9	tes9.txt	813,296	4,273,272	438,266
	10	tes10.txt	1,219,944	6,771,573	398,032

	Test	Filename	File Size (bytes)	Encryption (millisec) Enc	Decryption (millisec) Dec
Keywords 20 lengths	1	tes1.txt	1,370	27,235	38,099
	2	tes2.txt	4,026	60,353	58,879
	3	tes3.txt	11,765	105,285	133,705
	4	tes4.txt	35,477	224,609	308,607
	5	tes5.txt	50,831	315,420	394,019
	6	tes6.txt	203,324	1,108,263	377,548
	7	tes7.txt	406,648	2,169,558	402,453
	8	tes8.txt	609,972	3,227,332	397,868
	9	tes9.txt	813,296	4,342,471	367,058
	10	tes10.txt	1,219,944	6,495,980	360,670

the image placed on the location of the image pixels are spread out so if there is the slightest change in the pixel image that is inserted then the message can not be restored to perfection.

Future studies could analyze the use of media other than the image to accommodate the encryption and stegano . Other media that can be considered is the MIDI file or an MP3 file.The application of this research is to use a .txt file that stores messages. Future studies could attempt to use other than the file .txt file.In this study tested the Euclidean distance between distegano pictures before and after. There are several methods such as Manhattan and/or Mahalanobis that can be applied to test whether the image has a distance analysis.

References

[1] Kasiski, Friedrich W., 1863, *Die Geheimschriften und die Dechiffrirkunst (Cryptography and the Art of Decryption)*, Mittler und Sohn, Berlin.

[2] Pommerening, Klaus, 2006, *Kasiskis Test: Couldnt the Repetitions be by Accident?*, University of Mainz.

[3] Ahmed , Muhra, Quang Hieu Vu, Rasool Asal, Hassan Al Muhairi, Chan Yeob Yeun, 2014, Lightweight secure storage model with fault-tolerance in cloud environment, *Springer Science and Business Media*, New York.

[4] Wilson, Phillip I , Mario Garcia, 2006, A Modified Version of the Vigenre Algorithm, IJCSNS *International Journal of Computer Science and Network Security.*

[5] Kabachinski, Jeff, 2007, DRM: Tales from the Crypt(ography), *Biomedical Instrumentation & Technology.*

[6] Rahmani, Md. Khalid Imam , Wadhwa Neeta, Malhotra Vaibhav, 2012, Alpha–Qwerty Cipher: An Extended Vigenere Cipher, *Advanced Computing: An International Journal (ACIJ).*

[7] Liss, Michael, Daniela Daubert, Kathrin Brunner, Kristina Kliche, Ulrich Hammes, Andreas Leiherer, Ralf Wagner, 2012, *Embedding Permanent Watermarks in Synthetic Genes*, Plos One.

[8] Mollin, Richard A.,2007, *An Introduction to Cryptography Second Edition*, Taylor & Francis Group LLC.

[9] Klima, Richard E., Neil P. Sigmon, Ernest Stitzinger., 1999, *Applications of abstract algebra with Maple*, CRC Press LLC.

[10] Gandino, Filippo, Bartolomeo Montrucchio, Maurizio Rebaudengo,2009, Tampering in RFID: A Survey on Risks and Defenses, *Springer Science and Business Media*, LLC.

[11] Lee, Yeuan-Kuen, Ling-Hwei Chen, 1999, *A High Capacity Image Steganographic Model*, National Chiao Tung University, Hsinchu, Taiwan, R.O.C.

[12] Curran, Kevin, Karen Bailey, 2003, An Evaluation of Image Based Steganography Methods Internet Technologies Research Group, *International Journal of Digital Evidence*, Ireland.

[13] Grantham, Beau, 2015, *Bitmap Steganography : An Introduction, Computer Science.*

[14] Ullas K, Chandrashekar H M, 2015, Implementation of Embedding Text in Audio using Randomized LSB Method for Secured Audio Steganography, *International Journal of Engineering Research & Technology.*

[15] Axelsson, E. Petter, Glenn R. Iason, Riitta Julkunen-Tiitto, Thomas G. Whitham, 2015, Host Genetics and Environment Drive Divergent Responses of Two Resource Sharing Gall-Formers on Norway Spruce: A Common Garden Analysis, *Plos One Journal.*

[16] Diposumarto, Ngadino Surip, 2012, *Metodologi Penelitian Teori dan Terapani.* Mitra Wacana Media.

[]