INTERNATIONAL JOURNAL • ENGINEERING RESEARCH •

International Journal for Innovative Engineering and Management Research

A Peer Revieved Open Access International Journal

www.ijiemr.org

IJIEMR Transactions, online available on 12th Febraury 2018. Link :
http://www.ijiemr.org/downloads.php?vol=Volume-7&issue=ISSUE-02

Title: Design And Implementation Of Dual Key Triple Encryption Text Based Message Using Cryptography

Volume 07, Issue 02, Page No: 340 – 344.

Paper Authors

***VALLEPU SUREKHA, K. SAM PRASAD.**

* Dept of ECE, St.Mary's Women's Engineering College.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

DESIGN AND IMPLEMENTATION OF DUAL KEY TRIPLE ENCRYPTION TEXT BASED MESSAGE USING CRYPTOGRAPHY

***VALLEPU SUREKHA, **K. SAM PRASAD**
*PG Scholar, Dept of ECE, St.Mary's Women's Engineering College, Budampadu, Guntur (Dt); A.P, India.
**Assistant Professor & HOD, Dept of ECE, St.Mary's Women's Engineering College, Budampadu, Guntur (Dt); A.P, India.
surekha.vallepu931@gmail.com syam1464@gmail.com

ABSTRACT:

Dual Key Triple Encryption Text Based Message Using Cryptography and Steganography is a modular encryption and decryption method for any type of file. It combines layer 1 and layer 2 encryption techniques with standard encryption like AES as layer 3 encryption. Dual symmetric key is required to encrypt or decrypt file, so it can be used by two different persons to encrypt or decrypt certain file. Layer 1 and Layer 2 can use independently to achieve higher security level and fast encrypt or decrypt processing time. We propose character mapping and window addition for level 1 encryption. This technique has better processing time more than 21 times faster than fair character mapping. For layer 2 encryption, we propose scrambling transpose position and dummy file insertion as steganography technique. This method has higher efficiency ratio compare to LSB technique. We can achieve 50% efficiency compare to 12.5% in LSB technique. Combining both methods, we can achieve higher security level by maintaining faster processing time and reduce chipper text size. It can also be used together with AES to increase security level, yet still maintaining fast overall processing time and high efficiency ratio.

Keywords— Dual Key, Encryption, Decryption, Cryptography, Steganography, Character, Window addition, Scrambling, Insertion, fast processing, high efficiency and AES

I. INTRODUCTION

Communication is a part of human life since before humans even know the language.There are times where the information is important and confidential. Therefore, the method of communication used to be made in the other way that no one who knows about such information. For these reasons, there is a confidential communications method called cryptography. Cryptography is a method for processing information with a certain algorithm that the information becomes vague and difficult to understand the meaning. However, this method often leads to suspicion of third person, which are difficult to understand because the message would have been processed in such a way and it shows that the message is important information.

To avoid the above problems, a new method called steganography has been introduced. Steganography is a method of hiding information in the other media, the media can be an image, sound or video. The method used in the other way that third person will not know that the media contain hidden information. The most important aspect of the level of security in steganography is concealment of information, which refers to how the third person can not to detect the presence of hidden information.

Standard cryptography method that applied encryption is AES. The Advanced Encryption Standard (AES) is an encryption algorithm for securing sensitive but unclassified material by U.S. Government agencies and, as a likely consequence, may eventually become the de facto encryption standard for commercial transactions in the private sector. Originally called Rijndael, the cipher was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, who submitted to the AES selection process.

Growing of cloud computing demand, where people can put important file in public server, make either concealing or simply encrypt the file is important. The most important aspect in security is how unauthorized people unable to read the file even they have full access to the file. It doesn’t matter they suspect to certain file or not, as long as they unable to reveal the content for valid time, it will be enough. Our Group see that the standard encryption like AES method is less secure to use for file encryption since this method is block based method and prone to known file attack. Therefore, this standard is the most secure encryption standard available today. We propose to combine it with our layer 1 and layer 2 encryption method, employing cryptography and steganography technique to achieve higher security level.

II. ENCRYPTION & DECRYPTION

Encryption is the conversion of data into a form, called a cipher text that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.

The use of encryption/decryption is as old as the art of communication. In wartime, a cipher, often incorrectly called a code, can be utilized to keep the enemy from obtaining the contents of transmissions. (Technically, a code is a means of representing a signal without the intent of keeping it secret; examples are Morse code and ASCII). Simple ciphers include the substitution of letters for numbers, the rotation of letters in the alphabet, and the "scrambling" of voice signals by inverting the sideband frequencies. More complex ciphers work according to sophisticated computer algorithms that rearrange the data bits in digital signals. In order to easily recover the contents of an encrypted signal, the correct decryption key is required. The key is an algorithm that undo the work of the encryption algorithm. Alternatively, a computer can be used in an attempt to break the cipher. The more complex the encryption algorithm, the more difficult it becomes to eavesdrop on the communications without access to the key.

A. Cryptography

Cryptography is a process of converting initial data by transforming it into unreadable format. It is known as encryption. The initial data is called a plaintext and unreadable format data is called a cipher text.

Cryptography is a kind of encryption by making sure that the secret data can be understood only by the right person. The information is converted from its normal comprehensible form into an incomprehensible format. This mechanism employs mathematical schemes and algorithms to scramble data into unreadable text.

B. Steganography

Steganography is a method of data encryption by hiding information in a cover. Source information will be cover with other media without leaving a remarkable trace. The main objective of Steganography is to hide the information under a cover media so that the outsiders may not discover the information contained in the cover media. The example of media for cover source data information is text or image. In this case we use text based message as source information then we conceal source information with other text as a cover media.

C. Dual Key

Keyword is a piece of information that used to authenticate and verify the secured information so only the intended user can read the document. Without key the information can’t be access by other users. In this system we use double authentication user for more secured information which each admin insert different password. It could be used by 2 different users that work together to open their shared important message for both.

D. Tipple Encryption

Data security is very important nowadays. Exchange of information can grow rapidly inline with the growth of internet. In this condition we must aware about data security which spread in the internet. Some information is critical such as information related to our national defence. Therefore, the confidentiality and data integrity are required to protect the information against unauthorized access. This has resulted in an explosive growth of the field of information security. Using triple encryption, it will increase our data safety

In this topic we use cryptography as first level encryption, then we combine and recompose the chipper text with other text using steganography. The Shuffled text then encrypted using AES standard encryption.

E. Symmetric Key Cryptography

Symmetric key cryptography is a type of key cryptography which use the same key to encrypt and decrypt data. User can get back the original data by using the key. The symmetric key cryptography usage as primitives to construct various cryptographic mechanisms and can be combined to produce stronger ciphers. The main fact is that the security of data depends on the security of the key. So, we should be more cautious on exchanging keys between the sender and the receiver.

III. PROPOSED ENCRYPTION METHOD

For the encryption process, Dual password will be used to encrypt data, so two different person in different institution can encrypt share importance message. Triple encryption by mean:

- First Encryption by character substitution and employ window addition.
- Second level using steganography by shuffle composition and character of the original chipper text inserted into shuffled encrypted dummy file.
- Third encryption using standard AES encryption.

A. Level 1 Encryption Algorithm

Proposed of first level encryption is developed to aim faster processing time but still maintaining high security level. The technique use character substitution for every 32 character and employ window substitution to another 31 character of the plain text and the dummy text. Both methods are correlated with our dual key properties

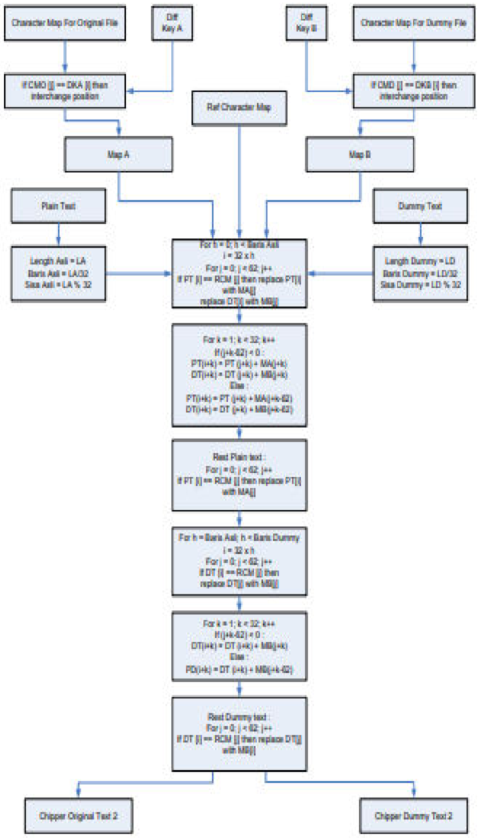

Character Map For Original File
Diff Key A
Diff Key B
Character Map For Dummy File
If CMO [j] == DKA [j] then interchange position
Ref Character Map
If CMD [j] == DKB [j] then interchange position
Map A
Map B
Plain Text
Dummy Text
Length Asli = LA
Baris Asli = LA/32
Sisa Asli = LA % 32
For h = 0; h < Baris Asli
i = 32 x h
For j = 0; j < 62; j++
If PT [i] == RCM [j] then replace PT[i] with MA[j]
replace DT[i] with MB[j]
Length Dummy = LD
Baris Dummy = LD/32
Sisa Dummy = LD % 32
For k = 1; k < 32; k++
If(j+k-62) < 0 :
PT(i+k) = PT (j+k) + MA(j+k)
DT(i+k) = DT (j+k) + MB(j+k)
Else :
PT(i+k) = PT (j+k) + MA(j+k-62)
DT(i+k) = DT (j+k) + MB(j+k-62)
Rest Plain text :
For j = 0; j < 62; j++
If PT [i] == RCM [j] then replace PT[i] with MA[j]
For h = Baris Asli; h < Baris Dummy
i = 32 x h
For j = 0; j < 62; j++
If DT [i] == RCM [j] then replace DT[j] with MB[j]
For k = 1; k < 32; k++
If(j+k-62) < 0 :
DT(i+k) = DT (j+k) + MB(j+k)
Else :
PD(i+k) = DT (j+k) + MB(j+k-62)
Rest Dummy text :
For j = 0; j < 62; j++
If DT [i] == RCM [j] then replace DT[j] with MB[j]
Chipper Original Text 2
Chipper Dummy Text 2

Figure 1: Algorithm first level encryption

Differentiated Key A is used to rearrange character map for the original file. In this project, we use original CMO Map. The Character Map for Original File (CMO Map) than be rearranged using Diff Key A. If we found that characters Key A[i] match with character CMO Map[j] than CMO Map[j] will be interchanged with CMO Map [i]. Let say, by employ Diff Key A with a value = 5IWE, we can rearranged CMO Map. A correlated MAP A with Diff Key A than is used to character substitution and window addition method. Plain text will be arranged in 32 columns. The plain text of the first column [i] in the substitution method will be compared with RCM, if the PT [i] match with RCM [j] than PT [i] replaced with MAP A [j]. The character in column 2 until 32 than add with window MAP A. The whole process will produce chipper original text 1 (COT 1).

Differentiated Key B is used to rearrange character map for dummy file. In this project, we arrange character map for dummy file which called CMO Map. The Character Map for Dummy File (CMD Map) than will be rearranged using Diff Key B. If we find character of Key B[i] match with character CMD Map[j] than CMD Map[j] will be interchanged with CMD Map[i]. Let say, by employ Diff Key B with a value IWF6, we will rearranged CMD Map become MAP B. Next step is the dummy plain text will be rearranged in 32 column. For every match first column of plain text, dummy text will be replaced with the associated MAPB and the 2nd until 32nd column will be add with window MAP B.

B. Level 2 Encryption Algorithm

Second Level Encryption using shuffle and text insertion (steganography). The method employs matrix transpose reposition and insertion original chipper text to dummy chipper text technique. Both methods are correlated with our dual key properties also.

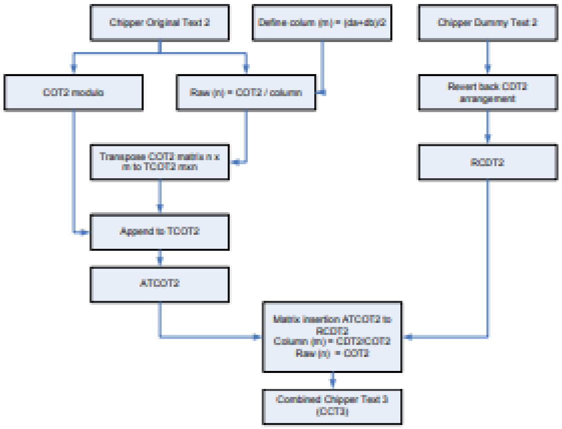
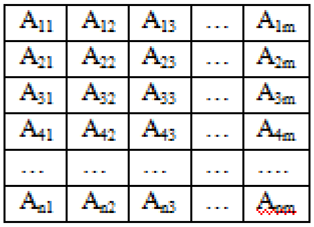
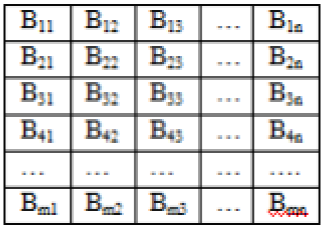

Chipper Original Text 2
Define colum (m) = (da+db)/2
Chipper Dummy Text 2
COT2 modulo
Raw (n) = COT2 / column
Revert back CDT2 arrangement
Transpose COT2 matrix n x m to TCOT2 mxn
RCDT2
Append to TCOT2
ATCOT2
Matrix insertion ATCOT2 to RCDT2
Column (m) = CDT2/COT2
Raw (n) = COT2
Combined Chipper Text 3 (CCT3)

Figure 2: Algorithm Second Level Encryption
Define matrix COT2, n x m, where m is a factor of function f(da,db) and n is size of COT2 divided by factor.



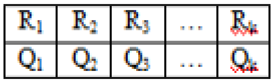
A_{11}	A_{12}	A_{13}	…	A_{1m}
A_{21}	A_{22}	A_{23}	…	A_{2m}
A_{31}	A_{32}	A_{33}	…	A_{3m}
A_{41}	A_{42}	A_{43}	…	A_{4m}
…	…	…	…	….
A_{n1}	A_{n2}	A_{n3}	…	A_{nm}

Figure 3: Matrix nxm of COT2



B_{11}	B_{12}	B_{13}	…	B_{1n}
B_{21}	B_{22}	B_{23}	…	B_{2n}
B_{31}	B_{32}	B_{33}	…	B_{3n}
B_{41}	B_{42}	B_{43}	…	B_{4n}
…	…	…	…	….
B_{m1}	B_{m2}	B_{m3}	…	B_{mn}

Figure 4: Transpose Matrix mxn of TCOT2
Remaining COT2 directly substitute and appended to TCOT2:



R_1	R_2	R_3	…	R_k
Q_1	Q_2	Q_3	…	Q_k

Figure 5: Remaining COT2 appended to TCOT2

Next step is insert COT2 chipper text to chipper dummy text CDT2, the insertion uses reverse arrangement method. The last COT2 chipper text will be inserted first. Let's define matrix n x m, where n is COT2 and m is TCOT2/COT2. We have dummy chipper text as follow :

D_{11}	D_{12}		D_{1n}
D_{21}	D_{22}		D_{2n}
D_{31}	D_{32}		D_{3n}
D_{n1}	D_{n2}		D_{nm}

Figure 6: Matrix dummy chipper text CDT2

We also have a matrix column of COT2.

B_{11}
B_{21}
B_{31}
....
B_{k1}

Figure 7: Matrix COT2

COT2 then inserted to CDT2 using reverse arrangement become combined chipper text 3 (CCT3).

D_{nm}	...	D_{n2}	D_{1n}	B_{n}
...	...	...	...	...
D_{3n}	...	D_{32}	D_{31}	B_{31}
D_{2n}	...	D_{22}	D_{21}	B_{21}
D_{1n}	...	D_{12}	D_{11}	B_{11}

Figure 8: Insertion and reverse arrangement chipper text

C. Level 3 Encryption Algorithm (AES)

All chipper text will be encrypted using AES standard. With Key1+key2.

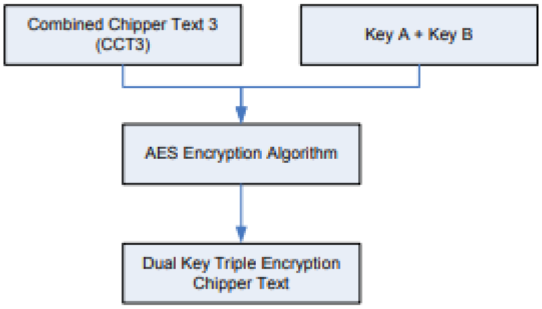

Combined Chipper Text 3 (CCT3)
Key A + Key B
AES Encryption Algorithm
Dual Key Triple Encryption Chipper Text

Figure 9: AES Encryption

IV. PROPOSED DECRYPTION METHOD

For the decryption process, dual password will be used to decrypt the encrypted data, so two different persons from different institution could read their share importance message. Triple decryption will be done through inverse of the encryption process:

- First decryption using standard AES encryption.
- Second decryption to recompose original file that stored in dummy file.
- Third level encryption by character substitution and employ window subtraction.

A. Level 1 Decryption (AES)

The chipper text look like standard AES chipper text, but actually need further decryption process to be able reveal the original text. T be able to decrypt the chipper text, first we should use AES standard algorithm using match key, a combining dual key.

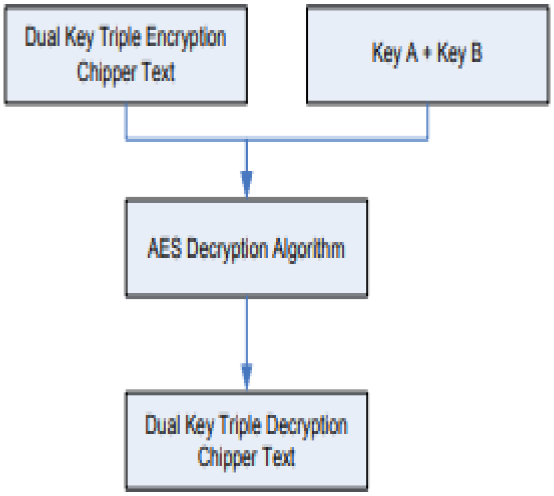

Dual Key Triple Encryption Chipper Text
Key A + Key B
AES Decryption Algorithm
Dual Key Triple Decryption Chipper Text

Figure 10: AES decryption

B. Level 2 Decryption

Second Level using reshuffle and text reveal (steganography). Algorithm that we use in second level decryption.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

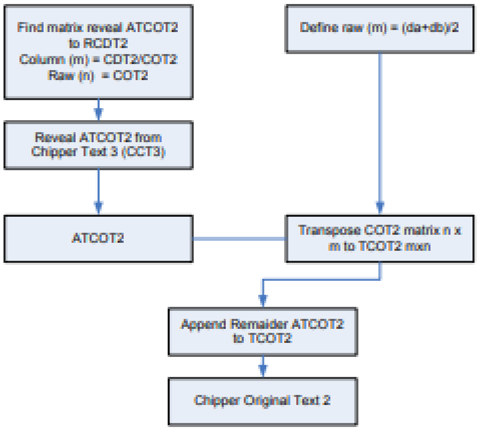
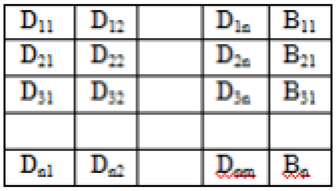

Find matrix reveal ATCOT2 to RCDT2
Column (m) = CDT2/COT2
Raw (n) = COT2
Define raw (m) = (da+db)/2
Reveal ATCOT2 from Chipper Text 3 (CCT3)
ATCOT2
Transpose COT2 matrix n x m to TCOT2 mxn
Append Remaider ATCOT2 to TCOT2
Chipper Original Text 2

Figure 11: Remaining COT2

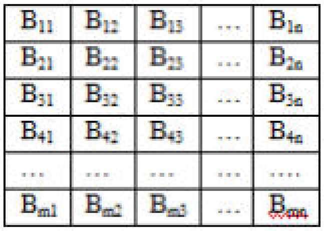
We should find original ATCOT2 size to define column of matrix combine dummy chipper text and original chipper text.



D_{11}	D_{12}		D_{1n}	B_{11}
D_{21}	D_{22}		D_{2n}	B_{21}
D_{31}	D_{32}		D_{3n}	B_{31}
D_{n1}	D_{n2}		D_{nm}	B_{n}

Figure 12: combined dummy chipper text and original chipper text

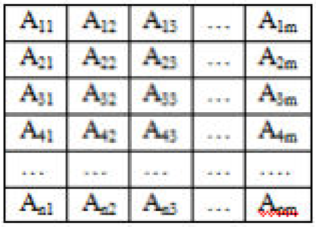
Column matrix of B then arranged to new matrix m x n, where m is a factor of function f(da,db) and n is size of COT2 divided by factor.



B_{11}	B_{12}	B_{13}	...	B_{1n}
B_{21}	B_{22}	B_{23}	...	B_{2n}
B_{31}	B_{32}	B_{33}	...	B_{3n}
B_{41}	B_{42}	B_{43}	...	B_{4n}
...	...	...	...	....
B_{m1}	B_{m2}	B_{m3}	...	B_{mn}

Figure 13: ATCOT2 Matrix

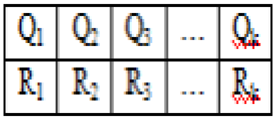
Transpose Position :Bmn =>Anm



A_{11}	A_{12}	A_{13}	...	A_{1m}
A_{21}	A_{22}	A_{23}	...	A_{2m}
A_{31}	A_{32}	A_{33}	...	A_{3m}
A_{41}	A_{42}	A_{43}	...	A_{4m}
...	...	...	...	....
A_{n1}	A_{n2}	A_{n3}	...	A_{nm}

Figure 14: COT2 Matrix

And remaining ATCOT2 will be substituted directly to COT2 :



Q_1	Q_2	Q_3	...	Q_k
R_1	R_2	R_3	...	R_k

Figure 15: Remaining COT2 will be append to COT2

C. Level 3 Decryption

Third Level decryption using resifting and re-substitution

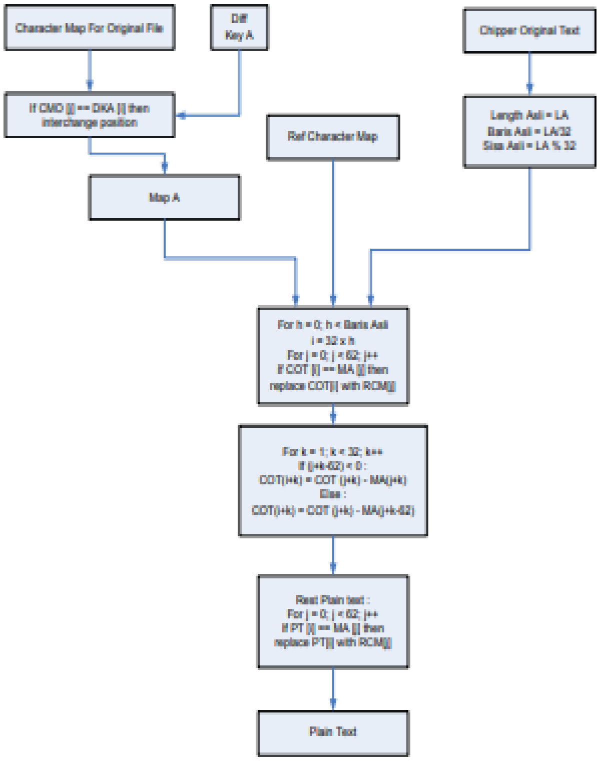


Figure 16: Level 3 Decryption process

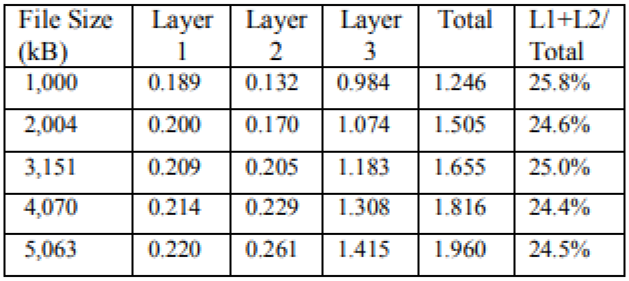
Differentiated Key A is used to rearrange character map for the chipper text. In this project, we use original CMO Map which arranged same as encryption method.

A correlated MAP A with Diff Key A than is used to character substitution and window subtraction method. Chipper original text (COT) will be arranged in 32 columns. The every first column COT[i] will be compared with MAP A, if the COT[i] matched with MAP A[j] than COT[i] will be replaced with RCM[j]. The COT in column 2 until 32 than will be subtracted with window MAP A. The whole process will produce original text.

V. RESULTS AND DISCUSSION

Proposed layer 1 encryption, using character substitution for every 32 character and employ window substitution is developed to aim faster processing time but still maintaining high security level. We will compare the processing time using this method again fair character mapping method.

Table 1: Percentage of L1 and L2 encryption processing time to overall process

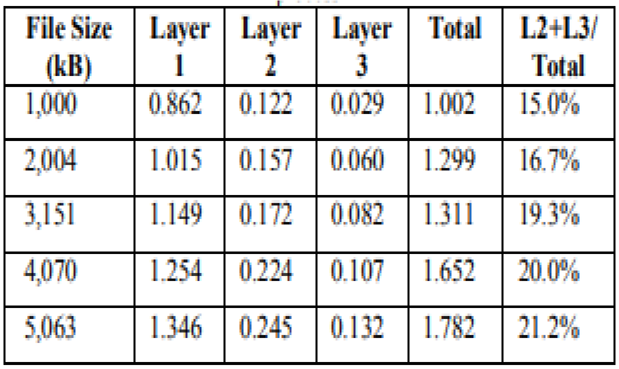


File Size (kB)	Layer 1	Layer 2	Layer 3	Total	L1+L2/ Total
1,000	0.189	0.132	0.984	1.246	25.8%
2,004	0.200	0.170	1.074	1.505	24.6%
3,151	0.209	0.205	1.183	1.655	25.0%
4,070	0.214	0.229	1.308	1.816	24.4%
5,063	0.220	0.261	1.415	1.960	24.5%

Comparing to overall process, the proposed layer 1 and layer 2 take about 25% of overall process. As we can see in Figure 26 below, encryption process of layer 1 and layer 2 is much faster than standard AES encryption.

Similar with the encryption process, in decryption side, our L2 and L3 proposed decryption method only take about 20 % of overall decryption process as can be seen in Table 5 below.

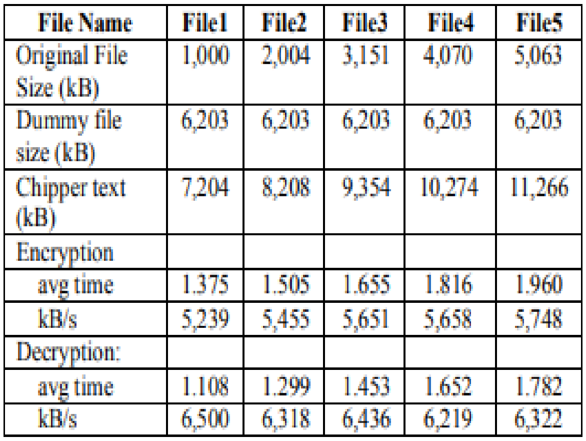
Table 2: Percentage of L2 and L3 decryption processing time to overall process



File Size (kB)	Layer 1	Layer 2	Layer 3	Total	L2+L3/ Total
1,000	0.862	0.122	0.029	1.002	15.0%
2,004	1.015	0.157	0.060	1.299	16.7%
3,151	1.149	0.172	0.082	1.311	19.3%
4,070	1.254	0.224	0.107	1.652	20.0%
5,063	1.346	0.245	0.132	1.782	21.2%

We found that processing time, either encryption or decryption using dual key triple encryption is correlated with the total size of chipper text file. The chipper text is combination between original file and dummy file. The bigger of the chipper text file, processing time take longer. But as depicted and Table 3 below, processing speed in term of kB/second for encryption and decryption is tend to stable.

Table 3: Average processing speed of Dual Key Triple Encryption



File Name	File1	File2	File3	File4	File5
Original File Size (kB)	1,000	2,004	3,151	4,070	5,063
Dummy file size (kB)	6,203	6,203	6,203	6,203	6,203
Chipper text (kB)	7,204	8,208	9,354	10,274	11,266
Encryption					
avg time	1.375	1.505	1.655	1.816	1.960
kB/s	5,239	5,455	5,651	5,658	5,748
Decryption:					
avg time	1.108	1.299	1.453	1.652	1.782
kB/s	6,500	6,318	6,436	6,219	6,322

VI. CONCLUSION

Using Dual Key Triple Encryption program, we can show that the proposed layer 1 encryption can achieve much faster time than fair character mapping. This technique has better processing time more than 21 times faster than fair character mapping. In decryption process the same method can achieve about 20 times faster than fair character mapping. Proposed steganography technique in layer 2 encryption has higher efficiency compare to LSB method. We can achieve 50% efficiency compare to 12.5% in LSB technique. Combining both proposed methods, we can achieve higher security level by maintaining faster processing time and reduce chipper text size. It can also be used together with AES to increase security level, yet still maintaining fast overall processing time and high efficiency ratio. Employ layer 1 and layer 2 encryption to AES encryption process, only take 25 % of total overall process. Meanwhile in decryption process only take less than 22% of the overall process

REFERENCE

[1] Behrouz A. Forouzan, ―Cryptography and Network Security‖, McGraw-Hill International edition, 2008.

[2] S. Usha, G.A.S.Kumar, K. Boopathybagan, ―A Secure Triple Level Encryption Method Using Cryptography and Steganography ‖, ICCSNT, vol. 2, 2426 December 2011, Chennai, India, Page(s): 1017– 1020.

[3] D. Bhattacharyya, P. Das, ; D. Ganguly, S. Mukherjee, S.K. Bandyopadhyay, and Taihoon Kim, " A Multi Layer Security Model for Text Messages‖, IACC, 67 March 2009, Kolkata, India, Page(s): 603–608.

[4] N.V. Rao, and J.T.L. Philjon, ―Metamorphic cryptography — A paradox between cryptography and steganography using dynamic encryption‖, ICRTIT, 35 June 2011, Chennai, India, Page(s): 217 – 222.

[5] Joseph Raphael, and Dr.V. Sundaram, ―Cryptography and Steganography – A Survey‖, IJCTA, vol.2, 03 February 2011,Coimbatore, India, Page(s) : 626-630.

[6] DiptiKapoorSarmah, and NehaBajpai, ―Proposed System for data hiding using Cryptography and Steganography‖, IJCA, vol. 2, No. 9, 710 October 2010, India

[7] AESCrypt company, ―Program AESCrypt 3.08‖, 2011, www.aescrypt.com

MS. VALLEPU SUREKHA M.TECH received B.tech from jntuk university and now pursuing M.Tech in the stream of VLSI at St.Mary's Women's Engineering College, Budampadu

Mr.NARESH BANDI received B.Tech and M.Tech. Currently working as a Assistant Professor in St.Mary's Women's Engineering College, Budampadu.. And his areas of interest are Applications of Power electronics in "VLSI& CHIP DESIGNINGS".