Design and Analysis of Complex Data Security Algorithm Using Cryptography and Steganography Techniques

Paresh Kumar Pasayat, Soumya Ranjan Panigrahi, Chandan Kumar Padhy,

Manaswini Mishra, Trupti Mishra, Dr.G.Babu

Assistant Professor, Department of Electronics & Telecommunication Engineering, I.G.I.T., Sarang, India

B.Tech Student, Department of Electronics & Telecommunication Engineering, I.G.I.T., Sarang, India

B.Tech Student, Department of Electronics & Telecommunication Engineering, I.G.I.T., Sarang, India

B.Tech Student, Department of Electronics & Telecommunication Engineering, I.G.I.T., Sarang, India

B.Tech Student, Department of Electronics & Telecommunication Engineering, I.G.I.T., Sarang, India

B.Tech Student, Department of Electronics & Telecommunication Engineering, I.G.I.T., Sarang, India

ABSTRACT: This paper aims to provide a security solution for 256-bits digital data using Cryptography and Steganography techniques during its transmission over the digital network. The Cryptography technique has been implemented using a newly developed data security algorithm having various operations on the data and the keys and the Steganography technique has been implemented using data cover process. In order to check the integrity of the data, the data integrity check has been done so as to ensure that the data has not been modified by the attacker during its transmission. The proposed algorithm is found to be resistant towards various types of attacks such as Brute-force attack, timing attack etc. The maximum combinational path delay of the data security unit is 10.052ns.

KEYWORDS: Cryptography, Steganography, Combinational Path Delay

I. INTRODUCTION

In order to maintain the privacy of the data, different researches are carried out so as to avoid the hacking of the information / data. The privacy can be achieved by using data security techniques. The technique may be A Cryptography Technique or Steganography Technique or the combination of both the techniques. The Cryptography technique uses the concept of encryption process to achieve data security and the the Steganography technique uses the concept of data cover / imge cover / audio cover / video cover to achieve the privacy of the information. In the Proposed algorithm, the data cover has been used to provide privacy to the 256-bits data. In the encryption algorithm, four keys are used to achieve the data security.

II. PROPOSED ALGORITHM

The proposed algorithm used for the data security is given as follows:

Step 1: The 256-bits data and four keys (K1, K2, K3, K4-256, 512, 512, 256-bits) are given to the Cryptography unit which produces 256-bits middle encrypted data.

Step 2: The output of the Cryptography unit and the 256-bits covering data is given to the Steganography unit which produces 512-bits final encrypted data.

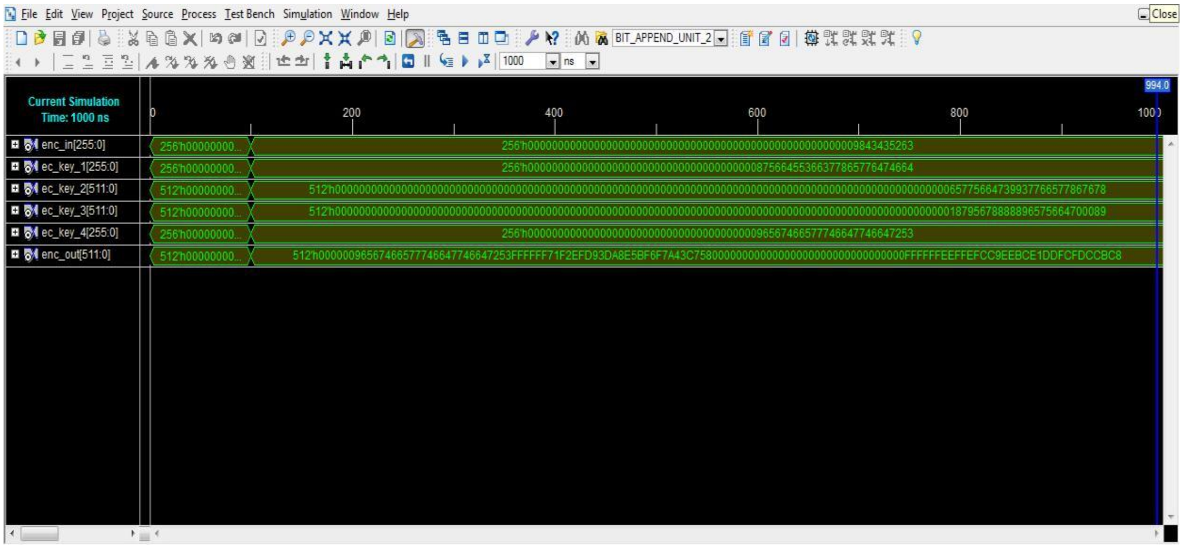
Step 3: The output of Steganography unit is given to the reverse Steganography unit which produces 256-bits middle decrypted data.

Step 4: The output of reverse Steganography unit is given to the reverse Cryptography unit which produces 256-bit final decrypted data which is the exact replica of the original data.

Step 5: The data integrity test has been done in order to check the integrity of the data (i.e. change in the data (if any)).

III. Simulation Results

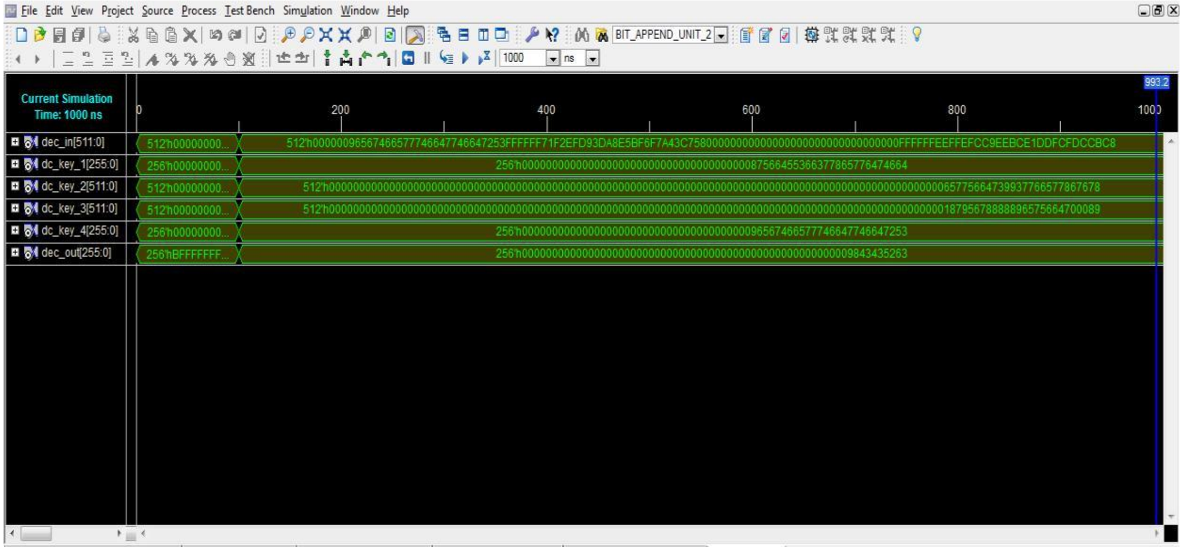
In the simulation result of the encryption unit, the original 256-bits data and four keys are used for the generation of the 512-bits encrypted data.


File Edit View Project Source Process Test Bench Simulation Window Help
Close
BIT_APPEND_UNIT_2
1000
ns
994.0
0
200
400
600
800
1000

```
Current Simulation
Time: 1000 ns
enc_in[255:0]      256'h00000000...   256'h0000000000000000000000000000000000000000000000000000009843435263
ec_key_1[255:0]    256'h00000000...   256'h0000000000000000000000000000000000000087566455366377865776474664
ec_key_2[511:0]    512'h00000000...   512'h00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000065775664739937766577867678
ec_key_3[511:0]    512'h00000000...   512'h00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000018795678888896575664700089
ec_key_4[255:0]    256'h00000000...   256'h0000000000000000000000000000000000000096567466577746647746647253
enc_out[511:0]     512'h00000000...   512'h0000096567466577746647746647253FFFFFF71F2EFD93DA8E5BF6F7A43C758000000000000000000000000000000000FFFFFFEEFFEFCC9EEBCE1DDFCFDCCBC8
```

Fig.1. Simulation Result of The Encryption Unit

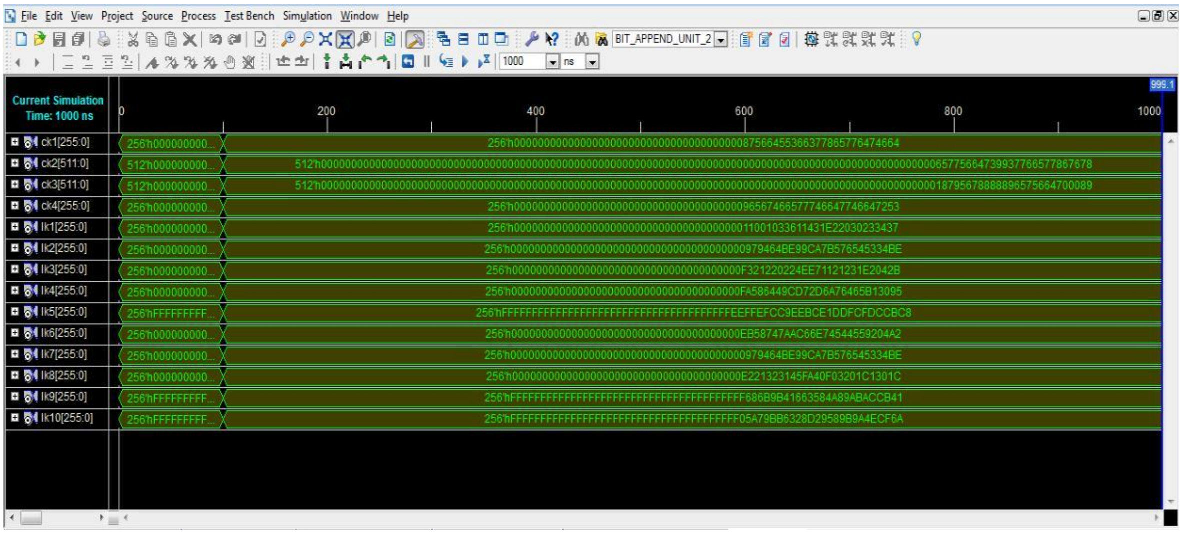
In the simulation result of the decryption unit, the 512-bits encrypted data and four keys are used for the generation of the 256-bits original / decrypted data.


File Edit View Project Source Process Test Bench Simulation Window Help
BIT_APPEND_UNIT_2
1000
ns
993.2
0
200
400
600
800
1000

```
Current Simulation
Time: 1000 ns
dec_in[511:0]      512'h00000000...   512'h0000096567466577746647746647253FFFFFF71F2EFD93DA8E5BF6F7A43C758000000000000000000000000000000000FFFFFFEEFFEFCC9EEBCE1DDFCFDCCBC8
dc_key_1[255:0]    256'h00000000...   256'h0000000000000000000000000000000000000087566455366377865776474664
dc_key_2[511:0]    512'h00000000...   512'h00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000065775664739937766577867678
dc_key_3[511:0]    512'h00000000...   512'h00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000018795678888896575664700089
dc_key_4[255:0]    256'h00000000...   256'h0000000000000000000000000000000000000096567466577746647746647253
dec_out[255:0]     256'hBFFFFFFF...   256'h0000000000000000000000000000000000000000000000000000009843435263
```

Fig.2. Simulation Result of The Decryption Unit

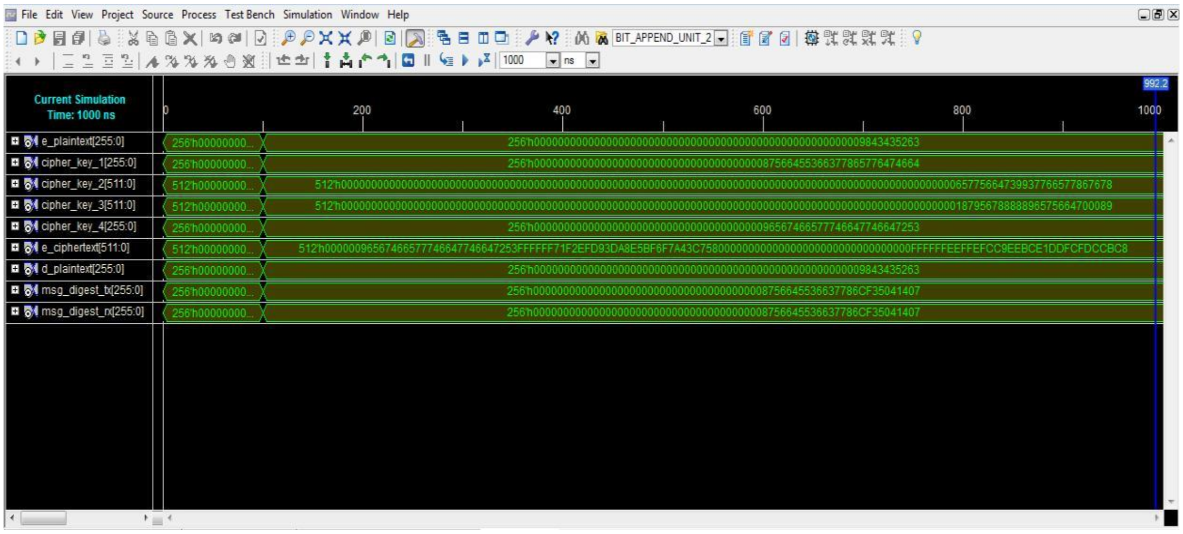
In the simulation result of the key generation unit, four cipher keys are used for the generation of the ten level keys.


File Edit View Project Source Process Test Bench Simulation Window Help
BIT_APPEND_UNIT_2
1000
ns
Current Simulation Time: 1000 ns
0
200
400
600
800
1000
999.1

```
ck1[255:0]   256'h000000000...  256'h0000000000000000000000000000000000000087566455366377865776474664
ck2[511:0]   512'h000000000...  512'h00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000065775664739937766577867678
ck3[511:0]   512'h000000000...  512'h00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000018795678888896575664700089
ck4[255:0]   256'h000000000...  256'h0000000000000000000000000000000000000096567466577746647746647253
lk1[255:0]   256'h000000000...  256'h0000000000000000000000000000000000000011001033611431E22030233437
lk2[255:0]   256'h000000000...  256'h000000000000000000000000000000000000000979464BE99CA7B576545334BE
lk3[255:0]   256'h000000000...  256'h00000000000000000000000000000000000000F321220224EE71121231E2042B
lk4[255:0]   256'h000000000...  256'h00000000000000000000000000000000000000FA586449CD72D6A76465B13095
lk5[255:0]   256'hFFFFFFFFF...  256'hFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEEFFEFCC9EEBCE1DDFCFDCCBC8
lk6[255:0]   256'h000000000...  256'h00000000000000000000000000000000000000EB58747AAC66E74544559204A2
lk7[255:0]   256'h000000000...  256'h000000000000000000000000000000000000000979464BE99CA7B576545334BE
lk8[255:0]   256'h000000000...  256'h00000000000000000000000000000000000000E221323145FA40F03201C1301C
lk9[255:0]   256'hFFFFFFFFF...  256'hFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF686B9B41663584A89ABACCB41
lk10[255:0]  256'hFFFFFFFFF...  256'hFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF05A79BB6328D29589B9A4ECF6A
```

Fig.3. Simulation Result of The Key Generator Unit

In the simulation result of the proposed model for providing the security solution, the original data and four cipher keys are used for the generation of encrypted data, decrypted data with data integrity test.


File Edit View Project Source Process Test Bench Simulation Window Help
BIT_APPEND_UNIT_2
1000
ns
Current Simulation Time: 1000 ns
0
200
400
600
800
1000
992.2

```
e_plaintext[255:0]      256'h00000000...  256'h0000000000000000000000000000000000000000000000000000009843435263
cipher_key_1[255:0]     256'h00000000...  256'h0000000000000000000000000000000000000087566455366377865776474664
cipher_key_2[511:0]     512'h00000000...  512'h00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000065775664739937766577867678
cipher_key_3[511:0]     512'h00000000...  512'h00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000018795678888896575664700089
cipher_key_4[255:0]     256'h00000000...  256'h0000000000000000000000000000000000000096567466577746647746647253
e_ciphertext[511:0]     512'h00000000...  512'h0000096567466577746647746647253FFFFFF71F2EFD93DA8E5BF6F7A43C75800000000000000000000000000000000FFFFFFEEFFEFCC9EEBCE1DDFCFDCCBC8
d_plaintext[255:0]      256'h00000000...  256'h0000000000000000000000000000000000000000000000000000009843435263
msg_digest_tx[255:0]    256'h00000000...  256'h00000000000000000000000000000000000000875664553663 7786CF35041407
msg_digest_rx[255:0]    256'h00000000...  256'h00000000000000000000000000000000000000875664553663 7786CF35041407
```

Fig.4. Simulation Result of The Proposed Algorithm

IV. Conclusion and Future Work

The proposed algorithm is tested using Xilinx software and it is designed in such a way that it provides not only privacy to the 256-bits data but also avoid hacking of data by the unauthorized user with data integrity test. The maximum combinational path delay is found to be 10.052ns. The proposed algorithm is found to be resistant towards Brute-force attack and timing attack. The proposed security solution can be used in the field of Telecommunication sector, Banking sector and Military sector to provide security the data.

REFERENCES

1. Adithya Vuppula.” Security Mechanisms for IOT Services and Differences between IOT and Traditional Networks”, Vol. 6, Issue 2, pp: 3127-3131,February 2017.
2. Satya Nagendra Prasad Poloju.”DATA MINING AS A SUPPORT FOR BUSINESS INTELLIGENCE APPLICATIONS TO BIG DATA”, Volume 7, Issue 2, pp:850-854,April 2019.
3. S.Ramana, N Bhaskar, C.R.K.Reddy, M.V.Ramana Murthy.” Three Level Gateway protocol for secure M Commerce Transactions”,Vol.63,No.6,(2020).
4. Satya Nagendra Prasad Poloju.”BIG DATA ANALYTICS: DATA PRE-PROCESSING, TRANSFORMATION AND CURATION”, Volume 5, Issue 2,pp:835-839,May 2017.
5. S. Ramana, N. Bhaskar , M. V. Ramana Murthy , G. R. Rama Devi.” A Two-Level Protocol For Secure Transmission Of Image Using IOT Enabled Devices”, Volume 18, No. 5,pp:1040-1050 ,2021.
6. Satya Nagendra Prasad Poloju.” APPLICATIONS OF BIG DATA TECHNOLOGY AND CLOUD COMPUTING IN SMART CAMPUS”, Volume 1, Issue 2,PP:840-844, September 2013.
7. Peddyreddy. Swathi, “A Study On Security Towards Sql Server Database”, JASC: Journal of Applied Science and Computation, Volume V, Issue II, February 2018
8. Satya Nagendra Prasad Poloju.” HACE THEOREM AND SOURCES OF BIG DATA”, Volume 1, Issue 2,pp:22-25,April 2011.
9. Peddyreddy. Swathi, “A Study on SQL - RDBMS Concepts And Database Normalization”, JASC: Journal of Applied Science and Computations, Volume VII, Issue VIII, August 2020
10. Adithya Vuppula.” Initiatives of 5G Vision and 5G Standardization”, Vol.6,Issue2, pp:1345-1348, February 2018.
11. Peddyreddy. Swathi, “An Overview on the techniques of Financial Statement Analysis”, **Journal of Emerging Technologies and Innovative Research, Volume 1, Issue 6, November 2014**
12. Adithya Vuppula.” An Overview on the Types of Wireless Networks”, Vol. 1, Issue 9, pp:2036-2041,November 2013.