IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 12, December 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 12, December 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0912019 |

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, Ajay Kumar Manadhata

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)).

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 12, December 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0912019 |

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.

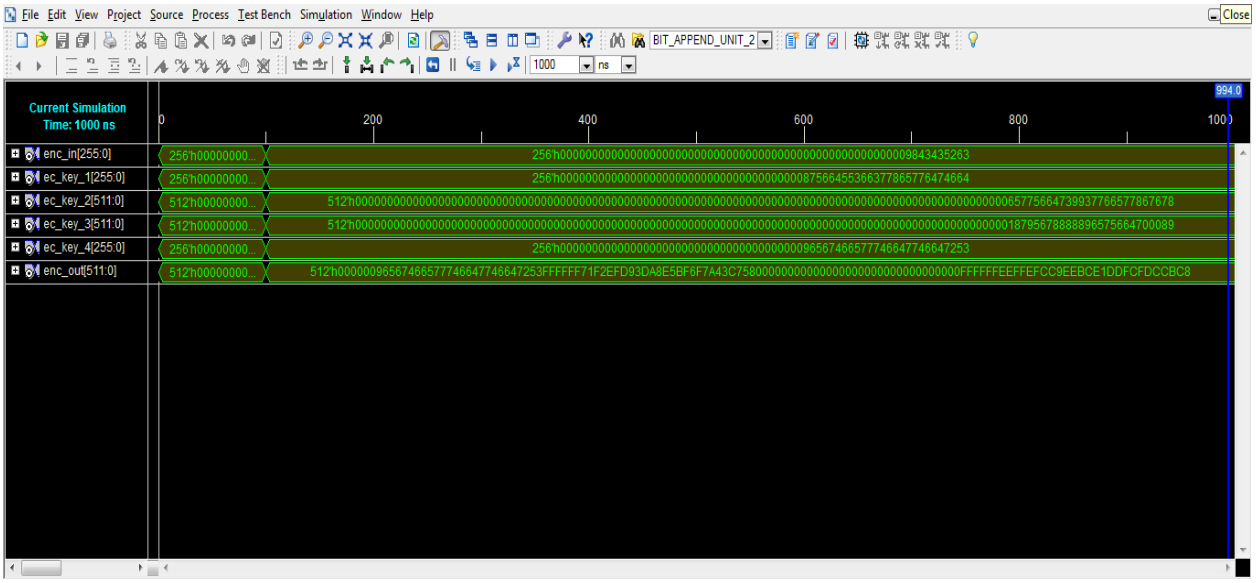

Fig.1. Simulation Result of The Encryption Unit

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.

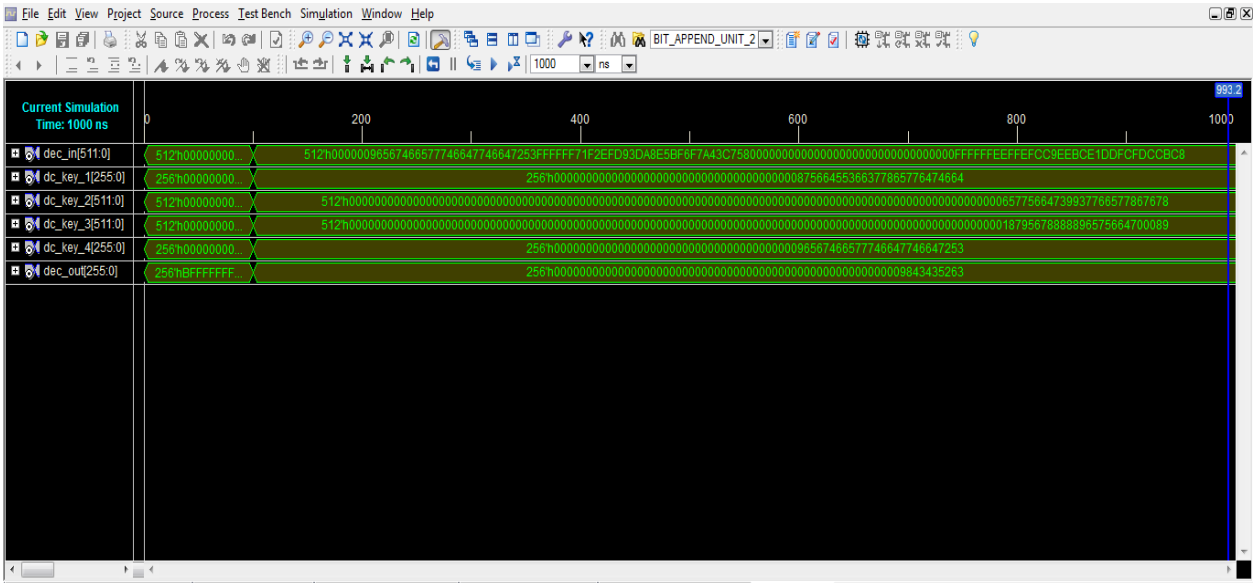

Fig.2. Simulation Result of The Decryption Unit

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 12, December 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0912019 |

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

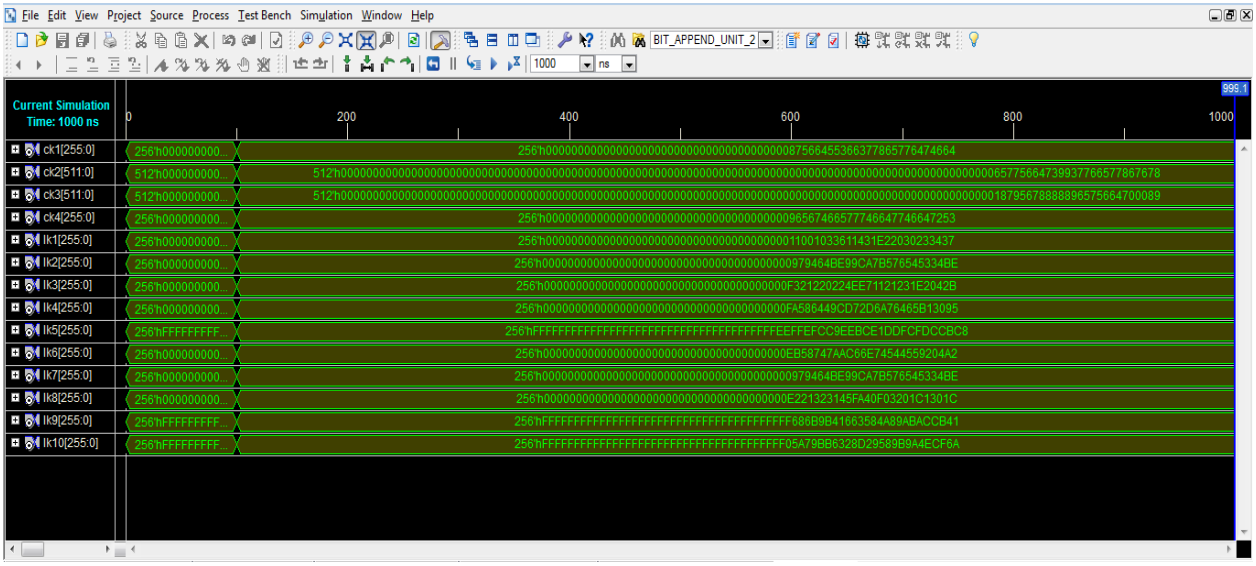

Fig.3. Simulation Result of The Key Generator Unit

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.

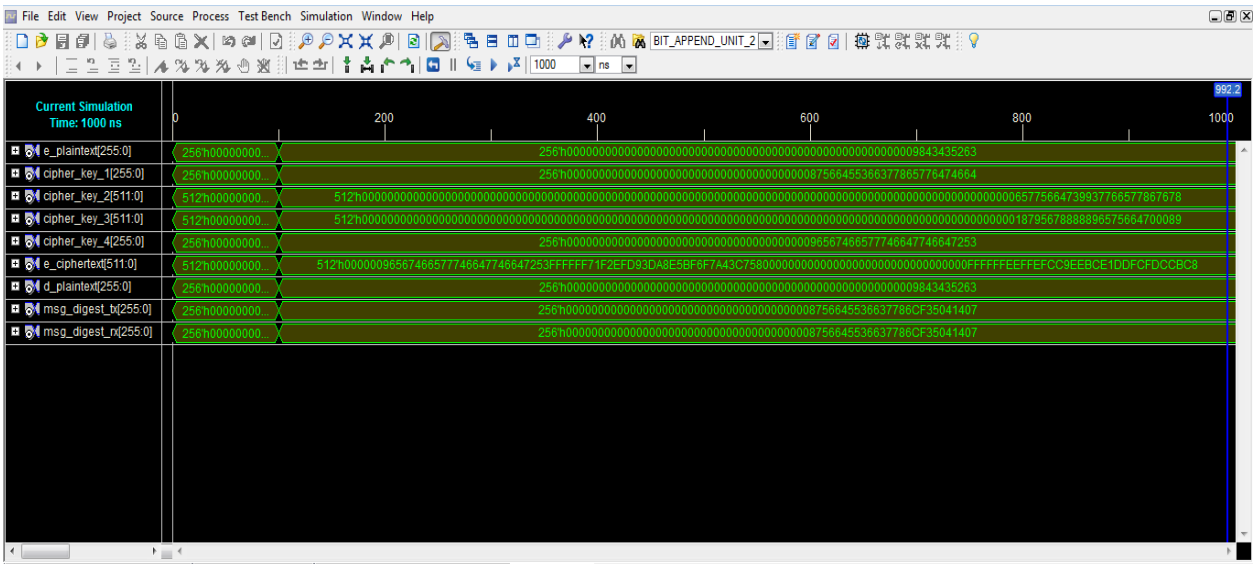

Fig.4. Simulation Result of The Proposed Algorithm

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.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 12, December 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0912019 |

REFERENCES

1. P. Chinnasamy, S. Padmavathi, R. Swathy, and S. Rakesh,'Efficient Data Security Using Hybrid Cryptography on Cloud Computing', Inventive Communication and Computational Technologies', 2021.
2. W.Xiaoyu, G.Zhengming,'Research and development of data security multi dimensional protection system in cloud computing environment', ICAACI, 2020.
3. S.Riaz, A.H. Khan, M.Haroon, S.Latif, S.Bhatti,'Big data security and privacy', ICIMTECH, 2020.
4. Chunli Su,'Big Data Security & Privacy Protection', International Conference on Virtual Reality & Intelligent Systems', 2019.
5. K.G. Kharade, S.K.Kharade, S.V.Katkar,'Cyber Security - A Method of Generic Authentication of Data with Ip Security', International Journal of Information Systems, 2019.
6. Dr. Prerna Mahajan, Abhishek Sachdeva, 'A study of Encryption AES, DES & RSA for Security', Global journal of computer science & technology, 2015.
7. Rachna Arora, AnshuParashar,'Secure User Data in Cloud Computing Using Encryption Algorithms', International Journal of Engineering Research and Applications, 2013.
8. W. Stallings, 'Cryptography and Network Security ', Prentice hall, 2011.
9. Douglas L. Perry,'VHDL Programming by Examples', TMH, 2010.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 7.542

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details