Enhancement of 128-bits Data Security through Steganography and Cryptography Techniques

Gyanaranjan Samal[1], Paresh Kumar Pasayat[2]

[1]PG Student, Dept. of ETC Engineering, IGIT, Odisha, India
[2]Assistant Professor, Dept. of ETC Engineering, IGIT, Odisha, India

---***---

Abstract – *The proposed paper deals with the combined effect of Steganography and Cryptography data security techniques on 128-bits digital data so as to avoid the stealing of information by the attackers. The information consists of 128-bit plaintext which needs to be protected from the attacker by using a newly developed data security algorithm. The algorithm uses Steganography and Cryptography techniques which have been implemented by using text/data cover and Hamming Code respectively. The algorithm protects the data by performing various operations on the 128-bits plaintext and 128-bits covering data and obtains a 448-bits encoded data with a 128-bits message digest to check the integrity of the message. This encoded data is sent towards the receiver end through a secure channel and received by the receiver. At the receiver end, the reverse operations are performed on the 448-bits received data to retrieve the 128-bits original data and 128-bits covering data with the generation of the new 128-bits message digest. Then, the message digest at the transmitter end and the receiver end are compared to check the integrity of the message. The proposed work can be implemented in the banking sector, telecommunication sector and military sector etc.*

Key Words: Steganography, Cryptography, Plaintext, Ciphertext, Message digest.

1. INTRODUCTION

Now-a-days, the information security plays an important role in most of the Government, Private and Public sector Organizations. The security of information can be achieved by using Steganography technique or Cryptography technique or using both the techniques. The Steganography means covered writing where as the Cryptography means Secret writing. The proposed paper aims to provide a better security solution by using both Steganography and Cryptography data security techniques.

1.1 Project Model

The project model describes the flow chart for the proposed project work. Each number in the model signifies the no. of bits in the input and output of each block. The diagrammatic representation of the proposed work is given as follows:

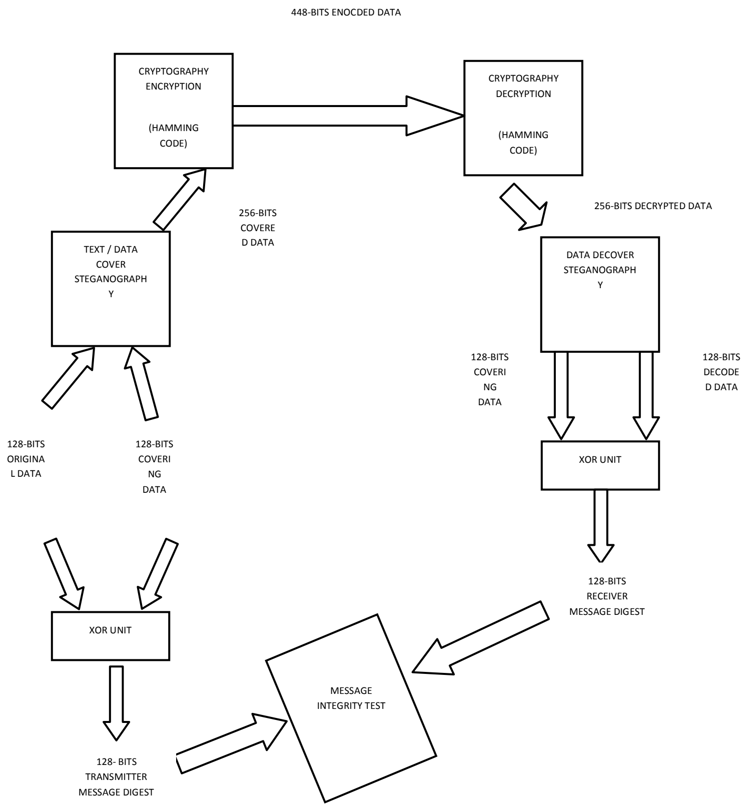


Fig 1: Project Model

2. ALGORITHM OF THE PROPOSED DESIGN

The logic used in the proposed design has been described in different steps as follow:

Step 1: First, the 128-bits original input data is covered by the 128-bits covering data using the text cover steganography technique to produce 256-bits covered data.

Step 2: At the transmitter end, the 128-bits message digest (MD1) is produced by performing the logical xor operation between the 128-bits original input data and the 128-bits covering data.

Step 3: The 256-bits covered data is given to the hamming (448,256) code encryption unit which uses Hamming (7,4) code encryption algorithm to produce 448-bits encrypted data.

Step 4: The 448-bits encrypted data is transmitted at the transmitter end and received by the receiver.

Step 5: At the receiver end, the error in the 448-bits received encrypted data is checked using parity bits and the error (if any) is corrected to produce 448-bits corrected data.

Step 6: The 448-bits corrected data is decrypted using Hamming (256,448) code decryption unit which used Hamming (4,7) code decryption algorithm to produce 256-bits decrypted data.

Step 7: The 128-bits original input data and the 128-bits covering data at the receiver end are produced from the 256-bits decrypted data using steganography text decover technique.

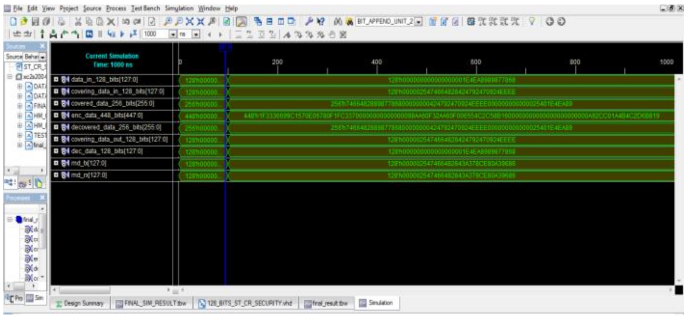
Step 8: At the receiver end, the new 128-bits message digest (MD2) is created by performing the logical xor operation between the 128-bits original input data and the 128-bits covering data generated at the receiver end.

Step 9: The message digests created at the transmitter end and the receiver end are compared and the integrity of the message (128-bits original input data) is verified. So, if MD1is equal to MD2, the integrity of the message is preserved and if MD1 is not equal to MD2, then the integrity of the message is lost.

3. SIMULATION RESULT

The VHDL code of the proposed work has been simulated using Xilinx ISE 9.2i software and the desired results have been obtained.

The simulation result of the proposed design is given as follows:



```
data_in_128_bits[127:0]              128'h00000...  128'h00000000000000001E4EA8989877868
covering_data_in_128_bits[127:0]     128'h00000...  128'h000002547466482842479247 0924EEEE
covered_data_256_bits[255:0]         256'h00000...  256'h7466482889877868000000004247924709 24EEEE00000000000025401E4EA89
enc_data_448_bits[447:0]             448'h00000...  448'h1F336699C1570E06780F1FC3370000000000000009AA60F32A460F006554C2C58E16000000000000000000000A82CC01A4B4C2D6B819
decovered_data_256_bits[255:0]       256'h00000...  256'h7466482889877868000000004247924709 24EEEE00000000000025401E4EA89
covering_data_out_128_bits[127:0]    128'h00000...  128'h000002547466482842479247 0924EEEE
dec_data_128_bits[127:0]             128'h00000...  128'h00000000000000001E4EA8989877868
md_tx[127:0]                         128'h00000...  128'h000002547466482843A378CE80A39686
md_rx[127:0]                         128'h00000...  128'h000002547466482843A378CE80A39686
```

Fig 2: Simulation result of the proposed design

4. CONCLUSION

It is concluded that the work is best suited in the field of data security to provide protection to the 128-bits digital data from unauthorized access using the concept of Steganography and the Cryptography data security techniques. The proposed work can be used to check the integrity of the message in order to satisfy the goal of data security. The proposed algorithm is resistant to the timing attack, pattern attack, statistical attack which makes the algorithm more robust. The combinational path delay required to convert 128-bits plaintext into 448-bits ciphertext is 4.468ns which obtained from the Xilinx software.

REFERENCES

[1] W.Stallings,"Cryptography and Network Security", 2nd Edition, Prentice Hall.

[2] Douglas L. Perry. "VHDL Programming by Examples", TMH.

[3] Karthikeyan B, Asha S, Poojasree B, "Gray Code Based Data Hiding in an Image using LSB Embedding Technique", IJRTE, Vol.8,2019.

[4] Deena Nath Gupta, Rajendra Kumar, "Lightweight Cryptography: an IoT Perspective", IJITEE, Vol. 8, 2019.

[5] Alpa Agath, Chintan Sidpara, ''Critical analysis of cryptography and steganography", JSRSET, Vol. 4, 2018.

[6] Achmad Solichin, Erwin wahyu Ramadhan, ''Enhancing data security using DES-based cryptography and DCT-based steganography", ICSITECH, 2017.

[7] Abhishek Anand, Abhishek Raj, Rashi Kohli, ''Proposed symmetric key cryptography algorithm for data security", IEEE, ICICCS, 2016.

[8] Cem Sahin, Brandon Katz, Kapil R.Dandekar, ''Secure and Robust symmetric key generation using physical layer techniques under various wireless environment", IEEE, 2016.