

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

9940 572 462

🕥 6381 907 438

🛛 🖂 ijircce@gmail.com

🛛 🙆 www.ijircce.com

| 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 / 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/LJIRCCE.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.

🚺 <u>F</u> ile <u>E</u> dit <u>V</u> iew P <u>r</u> oject	<u>Source</u> Process <u>T</u> est E	Bench Sim <u>u</u> lation <u>W</u> indow <u>H</u> el	р							Close
🗋 🖻 🖥 🕼 🐰	₽ 6 X 10 @	🖸 🔎 🔎 🗙 🗶 🔎 📓	3 2 8 0 0	🗅 🌽 😽 🕺 🕅	BIT_APPEND_UNIT	_2 🖃 📑 🗭 🕢 🗄	9 R R R R R	9		
(→ 글림콜월	A % % % @ ž	(±± †Å¢↑	⊡ ∥ ≦ ⊧ ⊳ ∡[[1000 💌 ns 💌						
Current Simulation Time: 1000 ns	p	200		400		600		800		994.0 100)
E 🛃 enc. in[255:0]	256%0000000		I	256500000000000000000000000000000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000	00000009843435263	1		A
C key 1(255:0)	256'500000000			256'h000000000000000	000000000000000000000000000000000000000	00000000087566455	366377865776474664	, 1		
E M ec_key_2[511:0]	512'h00000000	512'h0000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000)0000006577566473!	9937766577867678	
Rec_key_3[511:0]	512'h00000000	512'h00000000000		000000000000000000000000000000000000000		000000000000000000000000000000000000000		0000001879567888	8896575664700089	
E 🕅 ec_key_4[255:0]	256'h00000000			256'h0000000000000		00000000096567466	577746647746647253	3		
🗉 😽 enc_out[511:0]	512'h00000000	512'h00000096567466	5777466477466472	53FFFFFF71F2EFD93	BDA8E5BF6F7A43C7	580000000000000000000000000000000000000	0000000000000000000	FFFFFEEFFEFCC9EE	EBCE1DDFCFDCCBC	3
										~
< >	*									P.

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.

Wiew Project Edit View Project	t <u>S</u> ource <u>P</u> rocess <u>T</u> es	st Bench Sim <u>u</u> lation <u>W</u> indow <u>H</u> elp							
🗋 🌶 🖥 🕼 🐇	X h h X 10 0	• 🖸 🔎 🄎 🗙 🗶 🔎 📓 💆	A 🔁 🗉 🖸 🗁 🎤 😽 🕅	BIT_APPEND_UNIT	_2 💽 📑 🗹 🕢 🗄	\$ X X X X	9		
 ↓]]]]]]]] 	: 🔺 🌤 🌤 🎘 🕘	🛞 🗠 🖆 🕇 🍐 🗂 🖾	🔙 🕨 📲 1000 💌 ns 💌						
Current Simulation									993.2
Time: 1000 ns	0	200 I	400		600		800		1000
🖬 😽 dec_in[511:0]	512'h00000000	512'h0000096567466577	746647746647253FFFFFF71F2EFD930	DA8E5BF6F7A43C75	800000000000000000000000000000000000000	0000000000000000000	FFFFEEFFEFCC9EE	BCE1DDFCFDCCBC8	^
dc_key_1[255:0]	256'h00000000		256'h00000000000000	000000000000000000000000000000000000000	00000000875664553	6377865776474664			
dc_key_2[511:0]	512'h00000000	512h000000000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000	00000065775664739	937766577867678	
dc_key_3[511:0]	512'h00000000	512h000000000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000	00000018795678888	896575664700089	
dc_key_4[255:0]	256'h00000000		256%000000000000000000000000000000000000	000000000000000000000000000000000000000	000000000965674665	7746647746647253			
🖽 😽 dec_out[255:0]	256'hBFFFFFFF	X	256%000000000000000000000000000000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000	0000009843435263			
									-

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.

🚹 Eile Edit View Pro	oject <u>S</u> ource <u>P</u> rocess	Test Bench Simulation Window H	<u>H</u> elp						_ # ×			
L 🖌 🗑 🕼 🖁 🖗 🗶 🖄 🕲 🖉 🖉 🗩 🗩 🗩 🗶 📉 🗩 🖲 🖪 🗖 🔁 🗖 🛄 🖓 🕺 🕅 🐼 🐻 T_APPEND_UNIT_2 💽 🗑 🖉 🖄 🖏 🖏 🏹 🏌 💡												
< ▶ 글 일 철 일 / A % % % ④ 测 ☆ ☆ 書 內 今 圖 極 ▶ ▶ [1000 ▼ 10 ▼												
									999.1			
Current Simulation	0	200	400		600		800		1000			
Time. Tooo iis												
ck1[255:0]	256'h000000000	(256'h00000000	000000000000000000000000000000000000000	0000000008756645536	66377865776474664			^			
ck2[511:0]	512'h000000000	512'h000000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000	0006577566473993	7766577867678				
ck3[511:0]	512'h000000000	512'h000000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000	0001879567888889	6575664700089				
ck4[255:0]	256'h000000000		256'h00000000	000000000000000000000000000000000000000	00000000009656746657	7746647746647253						
🗉 🚮 lk1[255:0]	256'h000000000		256'h00000000	000000000000000000000000000000000000000	00000000001100103361	1431E22030233437						
🗉 😽 [k2[255:0]	256'h000000000		256'h000000000	000000000000000000000000000000000000000	0000000000979464BE9	9CA7B576545334BE						
🗄 🚮 [k3[255:0]	256'h000000000		256h000000000000000000000000000000000000									
🖽 😽 lk4[255:0]	256'h000000000		256'h000000000	000000000000000000000000000000000000000	0000000000FA586449CE	72D6A76465B13095						
Ik5[255:0]	256'hFFFFFFFFF		256'hFFFFFFFFFFF	FFFFFFFFFFFFFFFFFFF	FFFFFFFFEEFFEFCC9E	BCE1DDFCFDCCBC8						
🖽 😽 [k6[255:0]	256'h000000000		256'h000000000	000000000000000000000000000000000000000	0000000000EB58747AAC	C66E74544559204A2						
🖬 🚮 lk7[255:0]	256'h000000000		256'h000000000	000000000000000000000000000000000000000	0000000000979464BE9	9CA7B576545334BE						
🖶 💏 lk8[255:0]	256'h000000000		256'h000000000	000000000000000000000000000000000000000	0000000000E221323145	FA40F03201C1301C						
🗉 😽 [k9[255:0]	256'hFFFFFFFFF		256'hFFFFFFFF	FFFFFFFFFFFFFFFFFFFFFFFFF	FFFFFFFFF686B9B416	63584A89ABACCB41						
🖶 🚮 lk10[255:0]	256'hFFFFFFFFF		256"hFFFFFFFFF		FFFFFFFFF05A79BB632	8D29589B9A4ECF6A						
									Ţ			
< >									- F			



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 Sou	urce Process Test Ber	ch Simulation Window Help								_ # ×
🗋 🌶 🖥 🕼 🖕 🗶 🖻	``X ∞ @ .) 👂 👂 🗙 🗶 🔎 🖻 [2 2 2 2	1 🎤 😽 🕅 🕷	BIT_APPEND_UNIT_2	. 🛛 📑 🗹 🕢 👹	x x x x 9)		
(→) Ξ Ξ Ξ Ξ] A	124 24 24 69 28	ቀ ቀ † 📥 ሶ ኅ 🗳	5⊒ ▶ ,¤ [1000 💌 ns 💌						
Current Simulation										992.2
Time: 1000 ns	0	200 I		400		600		800 		100 <mark>0</mark>
🗉 🚮 e_plaintext[255:0]	256'h00000000			256'h000000000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000	000009843435263			^
cipher_key_1[255:0]	256'h00000000			256'h000000000000000	000000000000000000000000000000000000000	0000000087566455366	377865776474664			
cipher_key_2[511:0]	512'h00000000	512'h000000000000000000000000000000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000	0000006577566473	39937766577867678	
cipher_key_3[511:0]	512'h00000000	512'h000000000000000000000000000000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000	0000001879567888	8896575664700089	
🗉 😽 cipher_key_4[255:0]	256'h00000000			256'h000000000000000	000000000000000000000000000000000000000	00000000096567466577	746647746647253			
🗉 😽 e_ciphertext[511:0]	512'h00000000	512'h0000096567466	5777466477466472	253FFFFFF71F2EFD93	BDA8E5BF6F7A43C75	580000000000000000000000000000000000000	0000000000000000	FFFFEEFFEFCC9E	EBCE1DDFCFDCCBC	3
🗉 😽 d_plaintext[255:0]	256'h00000000			256'h000000000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000	000009843435263			
msg_digest_b(255:0)	256'h00000000			256'h0000000000000000	000000000000000000000000000000000000000	0000000087566455366	37786CF35041407			
🗉 😽 msg_digest_rx(255:0)	256'h00000000			256'h0000000000000000	000000000000000000000000000000000000000	0000000087566455366	37786CF35041407			
	4									
	-									· · · ·



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| <u>www.ijircce.com</u> | |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.











INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

🚺 9940 572 462 应 6381 907 438 🖂 ijircce@gmail.com



www.ijircce.com