VLSI Implementation Of Encryption Algorithm Based On Regions

[1] M. VENUGOPALA RAO, [2]P. BALA KRISHNA, [3]S. KISHORE BABU

[1]M.Tech – Scholar,[2]Assistant Professor,[3]Head Of The Department,
1,2,3.Department Of ECE, Vikas Group Of Institutions,Nunna, Krishna District

Abstract-** This work proposes a novel scheme for encryption algorithm based data security hiding. In the first work, a content owner encrypts the original uncompressed text using an encryption key. Then, it may compress the least significant bits of the encrypted text using a data-hiding key to create a sparse space to accommodate some additional data. The communication processes are still used in many applications today. The existed system we have three based encryption and decryption but not having capable for international system and flat encryption process is used. When we are using flat encryption we do not provide either high security to international system or loss the encryption process for local level. So to overcome this we provide different key selection for different encryption process is proposed. There are four stages one for local, national, international and special case depends on their length. As the number of hackers are less. So, we provide less bits to choose combination cases. This process of security will be high in national, higher in international, very high in special case.

I.INTRODUCTION

Due to the increasing use of computers, security is an important issue for digital information. Intruder is an unwanted person who reads and changes the information while transmission occurs. This activity of intruder is called intrusion attack. To avoid such attack data may be encrypted to some formats that is an unreadable by an unauthorized person.

Most of the work on reversible data hiding focuses on the data embedding/extracting on the spatial domain. But, in some applications, a channel administrator hopes to append some additional message, such as the origin information, text notation or authentication data, within the encrypted text though he does not know the original text content.

It is also hopeful that the original content should be recovered without any error after text decryption and message extraction at receiver side. Reference presents a practical scheme satisfying the above-mentioned requirements. The owner of the information encrypts the original text using an encryption key, and a data hacker can embed additional data into the encrypted text using a data-hiding key though he does not know the original content. With an encrypted text containing additional data, a receiver may decrypt it according to the encryption key, and then take the embedded data and recover the original information according to the data-hiding key. Encryption has long been used by militaries and governments to facilitate secret communication.

II. RELATED WORKS

2.1. USER REGISTRATION

If the user desires to access the info from the server, they ought to have associate account there with server. While not having associate account them area unit not ready to access the files are read the small print. Therefore 1st the user can produce associate account therewith server by providing the required info like Username, Password, DOB, Address and signal. Once this info is provided by the user, server can get that info and keep it into the information for future purpose.

2.2. CLOUD SERVER

Cloud information Service supplier can contain the big quantity of information in their information Storage. Conjointly the Cloud Service supplier can maintain the all the User info to evidence the User once area unit login into their account. The User info is keep within the information of the Cloud Service supplier. Conjointly the info Server can send the User requested job to the Resource assignment Module to method the User requested Job. The Request of all the Users can method by the Resource assignment Module. To speak with the consumer and therefore the with the opposite modules of the Network, the info

Server can establish association between them. For this Purpose we have a tendency to area unit reaching to produce associate computer program Frame. Conjointly the Cloud Service supplier can send the User Job request to the Resource Assign Module in paw In 1st Out (FIFO) manner.

2.3. DATA UPLOAD WITH DATA SHARING PROVISION (SENSITIVE)

Although the Cloud Computing is huge developing technology, in security purpose of read the it want a lot of growth. To beat this disadvantage, we have a tendency to implementing 2 styles of Cloud. Once is Public Cloud and another one is non-public Cloud. In camera the patient can set the access privileges' for each and every user they need. Publicly Cloud, the Cloud Server can set the access privileges' for each and every user based mostly on their designation. So legitimate users will read the info keep within the cloud solely up to their privilege level. They aren't allowed to look at the info on the far side their privileges'.

III. PROPOSED SYSTEM

In existing system they used attribute-based encryption and decryption. As they are using three levels user, role, attribute so depends on that they are providing security and efficiency.

As we are using user, role and attribute they have their own disadvantages. To overcome this we introduced proposed system in that we divide key-selection into four sub dividing.

Key- one used for local level encryption with limited number of bits. The total probability of chances depends on the number of bits. As the bits are changing we are getting the number of combination. In local level the total channels are low. So we are using key-one as limited number of bits.

Key-two used for national level encryption with more number of bits compared with local level. The total wanted channels in national level is more compared with local level. So we use more bit length than local level.

Key-three used for international level with high security. So here we have high bit length compared with national level.

Key-four used for VIP-level encryption with more number of bits compared with international level to provide very high security for their data.

The total description of key-selections depends on their register use. The key is given to key-register to store the key and that key is encrypted with data and gives the output. The output of the encryption is taken as input for decryption part.

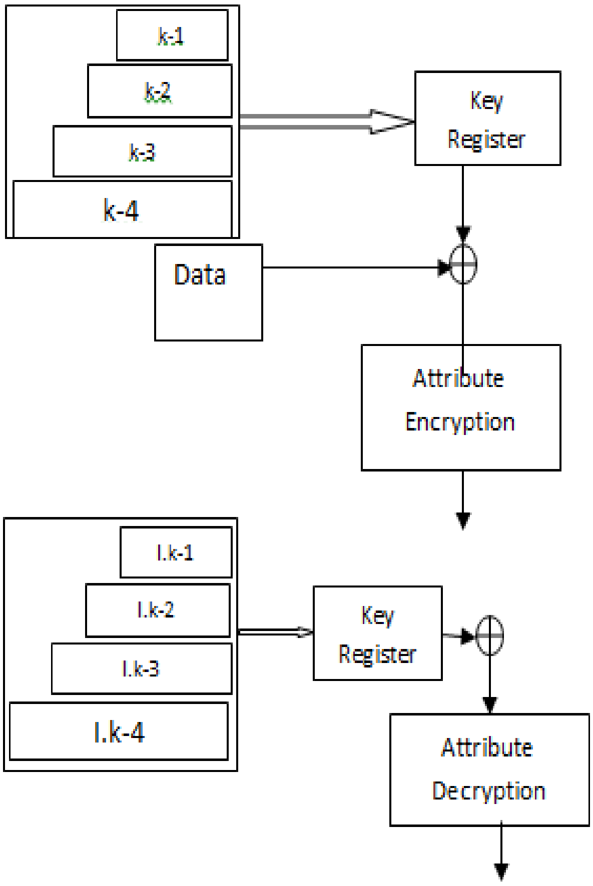


FIG. 1: PROPOSED SYSTEM

In decryption the receiver key-selection is selected with synchronization with encryption key. The recover key-selection is stored in key register and that key is decrypted the input data which is taken as decryption input and that decryption data is taken as finalized output.

IV. RESULTS

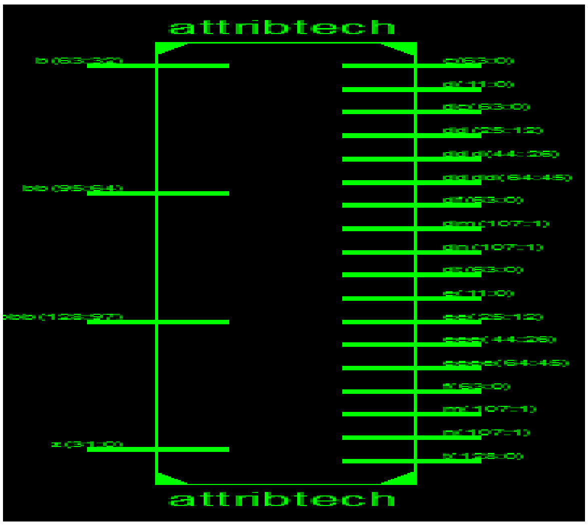
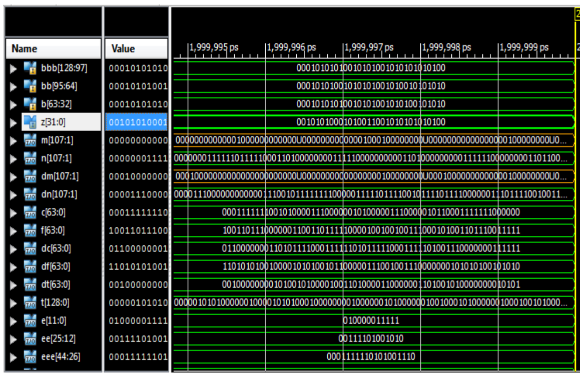


FIG. 2: RTL SCHEMATIC



```
Name          Value        |1,999,995 ps  |1,999,996 ps  |1,999,997 ps  |1,999,998 ps  |1,999,999 ps
bbb[128:97]   00010101010  00010101010010101001010101010100
bb[95:64]     00010101001  00010101001010101001010010101010
b[63:32]      00010101010  00010101010010101001010100101010
z[31:0]       00101010001  00101010001010011001010101010100
m[107:1]      00000000000  000000000000010000000000000U0000000000000100010000000000U0000000000000000000100000000U0...
n[107:1]      00000001111  0000000111111011111000110100000000011111000000000001101000000000111111000000001101100...
dm[107:1]     00010000000  000100000000000000000000000U000000000000000000100000000U000100000000000000100000000U0...
dn[107:1]     00001110000  0000111000000000000011100101111111110000011111011110010111101111000000111011110010011...
c[63:0]       00011111110  0001111111001010000111000000101000001110000010110001111111000000
f[63:0]       10011011100  1001101110000001100110111110000100100100111000101001101110011111
dc[63:0]      01100000001  0110000000110101111000111111010111110001111101001110000000111111
df[63:0]      11010101001  11010101001000010101001011100000111001001110000000101010100101010
dt[63:0]      00100000000  0010000000010100101000010011010000110000001101001010000000010101
t[128:0]      00000101010  000001010100000001000010101000100000000100000010100000010010001010000001000100101000...
e[11:0]       01000001111  010000011111
ee[25:12]     00111101001  00111101001010
eee[44:26]    00011111101  00011111110101001110
```

FIG. 3: OUTPUT WAVEFORM

V. CONCLUSION

The existed system we have encryption and decryption but not having capable for international system and flat encryption process is used. When we are using flat encryption we do not provide either high security to international system or loss the encryption process for local level. So to overcome this we provide different key selection for different encryption process is proposed. There are four stages one for local, national, international and special case depends on their length. As the number of hackers are less. So, we provide less bits to choose combination cases. This process of security will be high in national, higher in international, very high in special case. So finally I am concluding that proposed system provides different security level depends on application and it is better than Existed system.

REFERENCES

[1] A. Sahai and B. Waters, "Fluffy personality based encryption," in Progresses in Cryptology EUROCRYPT 2005, ser. Address Notes in Software engineering, R. Cramer, Ed. Springer Berlin Heidelberg, 2005, vol. 3494, pp. 457–473.

[2] D. Boneh, A. Sahai, and B. Waters, "Utilitarian encryption: Definitions what's more, difficulties," In principle of Cryptography, ser. Address Notes in Software engineering, Y. Ishai, Ed. Springer Berlin Heidelberg, 2011, vol. 6597, pp. 253–273.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Trait based encryption for fine-grained access control of scrambled information," in Procedures of the thirteenth ACM meeting on PC

and correspondences security, ser. CCS '06. New York, NY, USA: ACM, 2006, pp 89–98.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Figure content approach trait based encryption," in Procedures of the 2007 IEEE Symposium on Security and Protection, ser. SP '07. Washington, DC, USA: IEEE PC Society, 2007, pp. 321–334.

[5] M. Green, S. Hohen berger, and B. Waters, "Outsourcing the unscrambling of ABE figure writings," IN: Procedures of the twentieth USENIX Meeting on Security, SEC 2011. San Francisco, CA, USA: USENIX Affiliation, Berkeley, 2011.

[6] E. Fujisaki and T. Okamoto, "Secure combination of unbalanced what's more, symmetric encryption plans," in Advances in Cryptology - CRYPTO '99, ser. Address Notes in Software engineering, M. Wiener, Ed. Springer Berlin Heidelberg, 1999, vol. 1666, pp. 537–554.

[7] R. Canetti, O. Goldreich, and S. Halevi, "The arbitrary prophet system, returned to (preparatory rendition)," in Procedures of the Thirtieth Yearly ACM Symposium on Hypothesis of Figuring, ser. STOC '98. New York, NY, USA: ACM, 1998, pp. 209–218.

[8] J. Lai, R. Deng, C. Guan, and J. Weng, "Property based encryption with obvious outsourced unscrambling," IEEE Exchanges on Data Legal sciences and Security, vol. 8, no. 8, pp. 1343–1354, Aug 2013.

[9] B. Waters, "Figure content strategy characteristic based encryption: an expressive, proficient, and provably secure acknowledgment," in Procedures of the fourteenth global meeting on Practice and hypothesis out in the open key cryptography gathering on Open key cryptography, ser. PKC'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 53–70.

[10] S. Yamada, N. Attrapadung, G. Hanaoka, and N. Kunihiro, "Bland developments for picked ciphertext ecure quality based encryption," Out in the open Key Cryptography - PKC 2011, ser. Address Notes in Software engineering, D. Catalano, N. Fazio, R. Gennaro, also, A. Nicolosi. Ed. Springer Berlin Heidelberg, 2011, vol. 6571, pp. 71–89.

[11] T. Pedersen, "Non-intelligent and data theoretic secure unquestionable mystery sharing," in Advances in Cryptology - CRYPTO '91, ser. Address Notes in Software engineering, J. Feigenbaum, Ed. Springer Berlin Heidelberg, 1992, vol. 576, pp. 129–140.

[12] D. Boneh and J. Katz, "Enhanced proficiency for CCA-secure cryptosystems assembled utilizing personality based encryption," in Themes in Cryptology - CT-RSA 2005, ser. Address Notes in Software engineering, A. Menezes, Ed. Springer Berlin Heidelberg, 2005, vol. 3376, pp. 87–103.

[13] J. A. Akinyele, C. Garman, I. Miers, M. W. Pagano, M. Rushanan, M. Green, and A. D. Rubin, "Charm: a system for quickly prototyping cryptosystems," Diary of Cryptographic Designing, vol. 3, no. 2, pp. 111–128, 2013.

[14] R. Ostrovsky, A. Sahai, and B.Waters, "Characteristic based encryption with non-monotonic access structures," in Procedures of the fourteenth ACM Meeting on PC and Correspondences Security, ser. CCS '07. New York, NY, USA: ACM, 2007, pp. 195–203.

[15] L. Cheung, J. A. Cooley, R. Khazan, and C. Newport, "Collusion resistant bunch key administration utilizing property based encryption," Bunch Situated Cryptographic

[1] MAREEDU VENUGOPALA RAO studied his B.Tech in Ramachandra College Of Enginnering, Eluru. His area of interest is V.L.S.I.

[2]P. BALA KRISHNA studied B.Tech in Prakasam Engineering College - Kandukur and M.Tech in Dr. Samuel George Institute of Engineering and Technology, Markapur. He has 4 years of teaching experience and present working as Assistant Professor in Vikas Group of Institutions, Nunna, Vijayawada, Andhra Pradesh.

[3]S.KISHORE BABU studied diploma in Sir C.R.R Polytechnic College, Eluru, B.Tech in S.R.K.R Engineering College, Bhimavaram and M.Tech in J.N.T.U ananthapur. He is Pursuing PH.D in Acharya Nagarjuna University, Guntur