J. Integr. Sci. Technol. 2022, 10(2), 168-172 Article

Journal of Integrated
SCIENCE & TECHNOLOGY

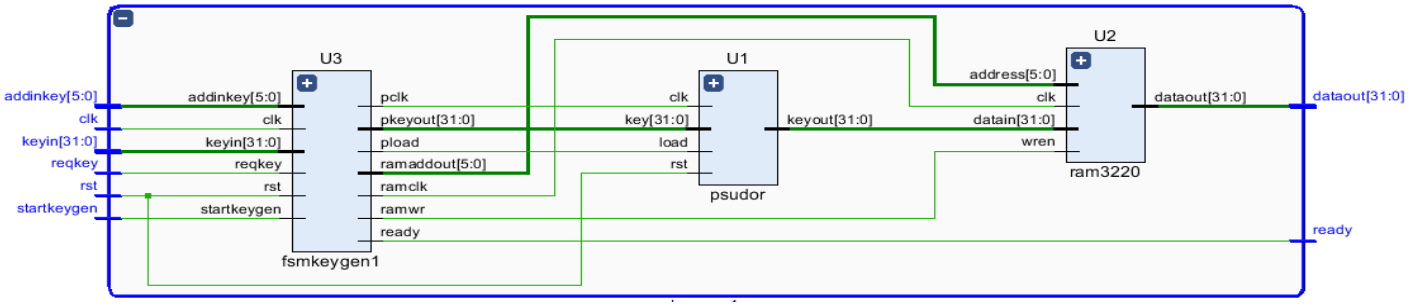
Field Programmable Gate Array (FPGA) based implementation of efficient RC6 block cipher

Sarita Sanap,[1*] Vijayshree More[2]

[1]Department of Electronics and Telecommunication Engineering, Maharashtra Institute of Technology, Dr. B.A. Marathwada University, Aurangabad. Maharashtra, India. [2]Department of Electronics and Computer Engineering, Jawaharlal Nehru Engineering College, MGM University, Aurangabad, Maharashtra, India.

Received on: 10-May-2022, Accepted and Published on: 14-Aug-2022

ABSTRACT



The efficient encryption system is required to achieve goal of security services. Rivest cipher 6 is a symmetric key block cipher which incorporates data dependent rotations. RC6 is specified as RC6-w/r/b, where the parameters w, r, and b respectively express the word size (in bits), the number of rounds, and the size of the encryption key (in bytes). In current work, optimized RC6 is implemented using xc7vx330t-2-ffg1157 field programmable gate array with proposing of inclusion of RC6-32/20/16. High value of rounds creates more diffusion and enables more security. Proposed system is synthesized and implemented on virtex7 field programmable gate array. The proposed method has less resource utilization and high throughput. Resource utilization in terms of slices is only 1% and in terms of fully used LUT-FF pair is 15%. Throughput of proposed system is 99.22 Gbps and efficiency is 50.596 Mbps/slice. Security analysis by performing avalanche test and strict avalanche criterion is also done. Average Avalanche effect of 54.71 is achieved, which satisfies criteria of SAC.

Keywords: RC6, Avalanche effect, Field programmable gate array, throughput, barrel shifter

INTRODUCTION

The deployment of computer-based information system is continuously increasing in various sectors like e-commerce, health care, eduaction, smart agricultural and social networks. Advances in internet of things (IoT) and big data eanbles data sharing for different applications.[1–4] Next generatin cellular systems also leades to high data rate due to which data exchange also increases. For all such cases data privacy and security is a major concern.[5] At various levels from indivdual, group, organization and society there is big concern of security and privacy of information.[6] Efficient secure and privacy scheme is the solution to this issue.[7] Such efficient RC6 algorithm is proposed in this work. RC6 is symmetric key[8] modern block cipher derived from RC5. Field Programmable Gate Arrays (FPGA) implementaion of encryption algorithm for various applications is preferred.[3,9–11] Encryption process mainly envolves pre-whitening, an inner loop of rounds, and post-whitening.[12] Reconfigurable architecture and processor-based design gives a strong system level design[13] which is used to handle networking. Virtex7[14] Field programmable gate array is used to implement proposed work and optimization is carried out to get high throughput and high efficiency. Synthesis and implementation of RC6-32/20/16 using xc7vx330t-2-ffg1157 is done. Very-large-scale integration (VLSI) design constants in terms of area, speed and memory usage were achieved efficiently.

Corresponding Author: Mrs. Sarita D Sanap, Assistant Professor, Department of Electronics and Telecommunication, Maharashtra Institute of Technology, Aurangabad.
Email: saritawagh1@gmail.com

Cite as: *J. Integr. Sci. Technol., 2022, 10(2), 168-172.*

 ISSN: 2321-4635 http://pubs.iscience.in/jist

The review of related work conducted to is given in second section.Description of proposed methodology with details of each process is elaborated in next section.Later results obtained after synthesis and implementation process are discussed.Results of avalanche effect test and SAC are also discusssed. Last section gives comprative analysis and conclusion of research work.

Related work

RC6 modules

RC6 encrypts plaintext in fixed-size 128-bit blocks. RC6 is a fully parameterized family of encryption algorithms. A version of RC6 is more accurately specified as RC6-w/r/b where the word size is w bits, encryption consists of a non-negative number of rounds as r, and b denotes the length of the encryption key in bytes. RC6 works with 4 w-bit registers A, B, C, D which contain the initial input plaintext as well as the output cipher text at the end of encryption process. For high security higher value of round is selected. RC6 working is divided into three main modules as key generation module, encryption module and decryption module. The key expansion algorithm is used to expand the user-supplied key to fill an expanded array S, so S resembles an array of *r* random binary words. Encryption process as shown in figure 1. Register B and D undergoes process of pre whitening.The resulting value of B after rotation has an exclusive-or operation with A, and D with C respectively. In the final stage of the round, the register values are permuted. At last stage registers A and C undergo post-whitening process using S array.

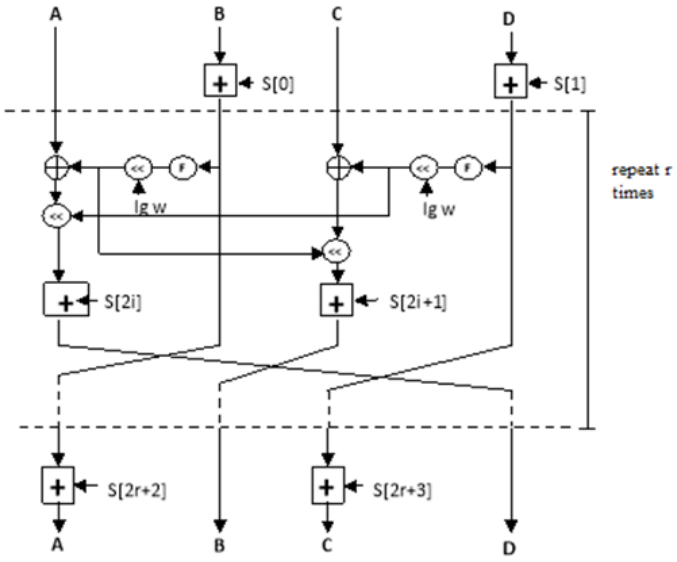


Figure 1. RC6 encryption process

Many reseacher had work on RC6 using various hardware and software platforms. Author designed RC6-Cascade which is 320-bits RC6 like block cipher and its implementaion on Altera FPGA gives improved avalanche efffect. Plaintext is divided into five parts and cascaded design is used.[15] Author had proposed light version of RC6 , RC6 8/5/b as RC6-lite and implemented using Microsoft Visual Basic Express Edition.[16] Compact hardware design of RC6 is propsed by author[17] using VirtexII FPGA. Resuse of same units for identical operation is done. Investigation and implementations of the f(X) operator of RC6 on Virtex-E and Virtex-II devices is done by authors. Design for feedback or non-feedback chaining modes is also done. Due to appropriateness for real-time applications RC6 is used for color image cryptosystem.[18] Cipher block chaining, cipher feedback, and output feedback modes can efficiently and effectively be used for color image encryption. RC6 technique is implemented in Cipher Feedback mode of operation as a first step for encrypting the multiple 3D video frames.[19] The mode of cipher-block chaining used by author. The practical performance was measured on a 2.40GHz Intel(R) Core(TM) i3 CPU with 4GB of RAM running Windows XP. Confusion, CPU utilization and memory utilization for Rijndael and RC6 algorithms is compared by author. RC6 is mostly suitable for these occasions where high encryption speed is required while Rijndael is useful where memory resource is key concern.[20,21] Author had proposed dynamic keys generation from the RC6 algorithm mixed with RC4 to create dynamic S-box and permutation table which preventes several known attacks during the real-time data transmission.[22]

Proposed methodology

Implementation of RC6 using pipeline structure is proposed in this work. As pipeline method includes a register in between two rounds, data is fetched continously which increases speed of operations. Design, implementation, simulation and synthesis is done on xc7vx330t-2-ffg1157 Field programmable Gate array using Xilinx 14.7 ISE and Aldec active HDL. Comparative analysis with existing work in terms resource usage, throughput and efficiency is done. Proposed modules are elaborated in following section.

Key expansion module

Key expansion module is used to expand the used defined key to fill an expanded array S, so S resembles an array of random binary words. Initially selection of two constants P and Q is done as

$$P = Odd((e-2)2^w) \quad (1)$$

$$Q = Odd((\phi-1)2^w) \quad (2)$$

Where e is base of natural logarithms and ø is golden ratio whose values are 2.718 and 1.6180 respectively. Odd(x) is the least odd integer greater than or equal to |x|. Process of key expansion is as per pseudocode 1.Output of this module is w-bit round keys S[0,…, 2r + 3]. In proposed work round r is 20, hence output is round keys S[0,1,--,43].

Pseudocode 1:

```
S[0]=P
for i=1 to 43 do
S[i]=S[i-1]+Q
X=Y=i=j=0
v=3*max{4,44}=132
for s=1 to 132 do
{
X=S[i]=(S[i]+X+Y)<<<3
Y=L[j]=(l[j]+X+Y)<<<(X+Y)
i=(i+1) mod 44
j=(j+1) mod 4
}
End
```

This module is implemented using vivado 17.4,Aldec active-HDL and synthesis is done using xilinx 14.7.Fig 2 shows RTL schematic of key generation module.

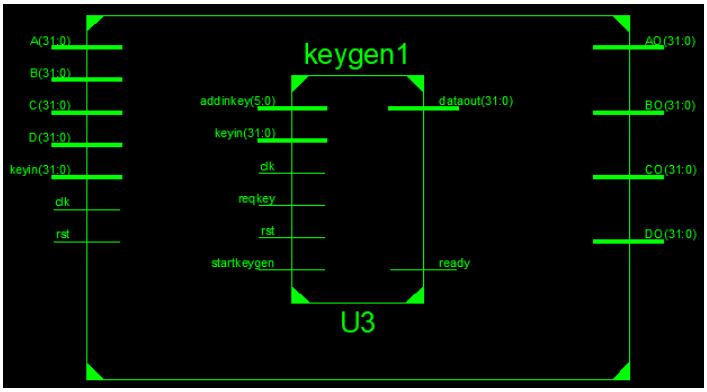


Figure 2. RTL schematic of key generation process

Encryption module

The processes of encryption and decryption are both composed of three stages: pre-whitening, an inner loop of rounds, and post-whitening. Main focus of proposed method is reuse of modules for compact design. So efficient design of the intermediate stages is done. Encryption process is as given pseudocode 2. Input given is plaintext stored in four w-bit input registers A,B,C,D number r of rounds and w-bit round keys S[0,…,2r + 3] where r is 20.

Pseudocode 2.

```
 B=B+S[0]
D=D+S[1]
for i=1 to 20
{
t=(B*(2B+1))<<<5
u=(D*(2D+1))<<<5
A=((A xor t)<<<u)+S[2i]
C=((C xor u)<<<t)+S[2i+1]
(A,B,C,D) = (B,C,D,A)
}
A=A+S[42]
C=C+S[43]
End
```

The registers B and D uses quadratic equation and rotated ($\log_2$ w) bits to the left, respectively. The resulting value of B has an exclusive-or operation with A, and D with C respectively. This value *t* is then left-rotated *u* bits and added to round key. The resulting value of D and C is left-rotated *t* bits and added to round key S[2i + 1]. In the final stage of the round, the register values are permuted, using parallel assignment process.

Decryption Module

Decryption module exhibits structure similarity with encryption module whereas reverse procedure is performed. Intially pre whitening process on C and A registers is carried out. Loop execution is in reverse for the r rounds. In loop execution firstly parallel assignment is done. Qurdratic equation is applied on D and B and resulting values are stored in u and t subregisters. These values are then left rotated. Steps performed are as per Pseudocode 3. After performance of all iterations finally D and B undergoes post-whitening process.

Pseudocode 3:

```
C=C-S[43]
B=B-S[42]
for i=20 downto 1
{
(A,B,C,D) = (D,A,B,C)
u=(D*(2D+1))<<<5
t=(B*(2B+1))<<<5
C=((C-S[2i+1])>>>t) xor u
A=((A-S[2i])>>>u) xor t
}
D=D-S[1]
B=B-S[0]
End
```

Implementation of operators used in RC6

Main operators used in RC6 implementation are given in table 1. Efficient design of these repetative operators is done in the proposed work. Implementation of carry look ahead adder and subtractor is done. The carry term is expanded recursively to each step to provide a 32-bit carry look-ahead adder substractor. The carry expression for each individual stage can be implemented in a two-level AND-OR expression. For rotation operation 32 bit right-left rotate by concatenating 1'b0 with 32-bit input word. Implementation of shift and add multiplication algorithm consists of looking at each successive bit of the multiplier in turn, starting with the lsb. A barrel shifter is a circuit which can shift a data word by a specified number of bits in one clock cycle. Implementation of barrel shifter is done as a cascade of parallel 2×1 multiplexers. RTL schematic of barrel shifter is as shown in figure 3. For a 4-bit barrel shifter, an intermediate signal is used which shifts by two bits, or passes the same data based on value of s[0] or s[1].

Table 1 Operators used in RC6

Operation	Description
a $\oplus$ b	Bitwise exclusive-or of w-bit words
a x b	Integer multiplication modulo 2^w
a <<< b	Rotate the *w*-bit word a to the left by the amount given by the least significant ($\log_2 w$) bits of *b*
a >>> b	Rotate the *w*-bit word a to the right by the amount given by the least significant ($\log_2 w$) bits of *b*
Enc: (A,B,C,D) = (B,C,D,A) **Dec:** (A,B,C,D) = (D,A,B,C)	Parallel assignment of values on the right to registers on the left.

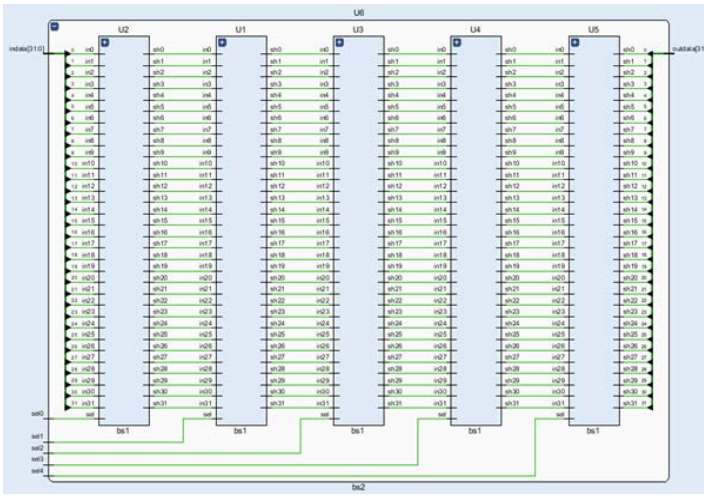


Figure 3: Barrel shifter RTL schematic

RESULTS AND DISCUSSION

The simulation and synthesis was performed to check correctness of the proposed design. Synthesis, simulation and Implementation results for proposed optimized method were analyzed. Resource utilization is as shown table 2. Simulation of modules done individually and then complete pipeline RC6 system is simulated using Aldec active HDL. Simulation waveform is shown in figure 4.

Figure 4. Output simulation waveforms

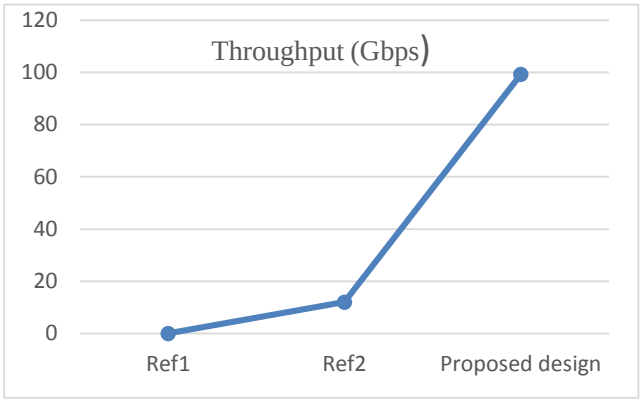
Table 2. Resource utilization

Parameters	Used in the proposed design	Available	% Utilization
No.of slice registers	1961	408000	1%
No.of slice LUTs	2145	204000	1%
No.of fully used LUT-FF pair	558	3548	15%
No of bonded IOB	289	600	45%

As given in table 2, only 1% slices are used which satisfies area constraints very effectively. Number of slice LUTs utilization is only 1%. Look up table- flip flop pair utilization is 15%. Bonded input output buffer utilization is 45%. Other parameters which plays very important role in analysis of algorithm are listed in table 3. Throughput is the ratio of number of processed bits and critical delay. Throughput also decides efficiency of system. It is calculated as ratio of throughput and number of slices used. Proposed design gives throughput 99.22 Gbps which is very high as compared to existing reference work ref 1 and ref 2,[23,24] where throughput is 0.0039 Gbps and 12 Gbps respectively. Efficiency of the design is 50.596 Mbps/Slice.

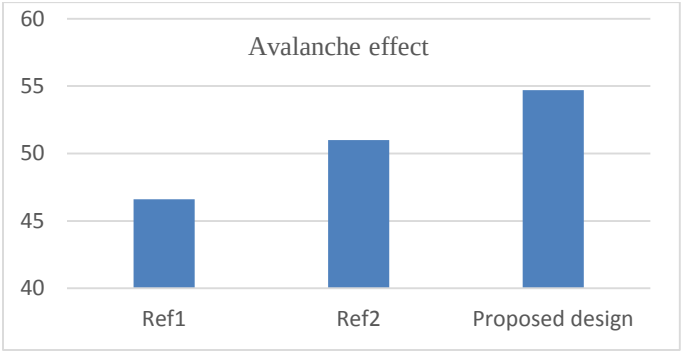
Table 3. Result summary

Parameters	Proposed design
Memory	480 MB
Critical Delay	1.29 ns
Frequency	770.89 MHz
Throughput	99.22 Gbps
Efficiency	50.596 Mbps/Slice
Plaintext Avalanche effect (Average)	54.12
Key Avalanche effect (Average)	55.3



Graph 1.Comparative analysis of throughput

Security of encryption method is analyzed by avalanche effect test. Avalache effect measues changes in ciphertext that occur when plaintext or key changes by one bit.[25] High avalanche effect guarantees security of plaintext. Tests have been carried out by change in key and change in plaintext. Average avalanche effect of 54.12 and 55.3 is obtained for one bit change in key and one bit change in plaintext respectively. More avalanche effect is obtained in this work as compared to existing work[26,15] where avalanche effect of 46.6 and 51 is obtained.



Graph 2. Avalanche effect analysis

As avalanche effect is more than 50% it satisfies strict avalanche criterion. It proves that proposed method has good diffusion

characteristics. Proposed system also passess frequency test and runs test which are used for validation. Statistical analysis gives P-Value 0.7. High p-Value indicated randomness in the output.

CONCLUSIONS

High throughput and efficiency are key features of encryption algorithms. In proposed work optimized RC6 implementation on FPGA device is done. Pipeline method and efficient modules design achieves constraints of area and speed. Only 1% slice registers and 1% slice LUTs are used in the design. LUT-FF pair usage is 15%. Critical delay observed is 1.29 ns. Maximum frequency achieved is 770.89MHz. High throughput of 99.22 Gbps is achieved. Average avalanche of 54.71 proves that method is secure and strict avalanche criterion is satisfied. High efficiency makes proposed work suitable for real time applications. Tests specified by National Institute of Standard and Technology(NIST) are performed and executed effectively to validate proposed work.

CONFLICT OF INTEREST

Authors declared no conflict of interest.

REFERENCES

1. X. Yang, L. Shu, J. Chen, et al. A Survey on Smart Agriculture: Development Modes, Technologies, and Security and Privacy Challenges. *IEEE/CAA J. Autom. Sin.* **2021**, 8 (2), 273–302.
2. A. Koohang, C.S. Sargent, J.H. Nord, J. Paliszkiewicz. Internet of Things (IoT): From awareness to continued use. *Int. J. Inf. Manage.* **2022**, 62 (October 2021), 102442.
3. H. Tao, M.Z.A. Bhuiyan, A.N. Abdalla, et al. Secured Data Collection with Hardware-Based Ciphers for IoT-Based Healthcare. *IEEE Internet Things J.* **2019**, 6 (1), 410–420.
4. D. Singh, S. Sinha, V. Thada. A novel attribute based access control model with application in IaaS cloud. *J. Integr. Sci. Technol.* **2022**, 10 (2), 79–86.
5. I. Torre, B. García-Zapirain, M. López-Coronado. Analysis of Security in Big Data Related to Healthcare. *J. Digit. Forensics, Secur. Law* **2017**.
6. M. Wang, T. Zhu, T. Zhang, et al. Security and privacy in 6G networks: New areas and new challenges. *Digit. Commun. Networks* **2020**, 6 (3), 281–291.
7. E. Bertino. Data Security and Privacy: Concepts, Approaches, and Research Directions. *Proc. - Int. Comput. Softw. Appl. Conf.* **2016**, 1, 400–407.
8. A.N. Tentu. A Review on Evolution of Symmetric Key Block Ciphers and Their Applications. *IETE J. Educ.* **2020**, 61 (1), 34–46.
9. M. Al-Asli, M.E.S. Elrabaa, M. Abu-Amara. FPGA-Based Symmetric Re-Encryption Scheme to Secure Data Processing for Cloud-Integrated Internet of Things. *IEEE Internet Things J.* **2019**, 6 (1), 446–457.
10. H. Hamadeh, A. Tyagi. An FPGA Implementation of Privacy Preserving Data Provenance Model Based on PUF for Secure Internet of Things. *SN Comput. Sci.* **2021**, 2 (2), 1–11.
11. P. Babu, E. Parthasarathy. Reconfigurable FPGA Architectures: A Survey and Applications. *J. Inst. Eng. Ser. B* **2021**, 102 (1), 143–156.
12. S.D. Sanap, V. More. Design of efficient S-box for Advanced Encryption Standard. *J. Integr. Sci. Technol.* **2022**, 10 (1), 39–43.
13. B. Xing, D.D. Wang, Y. Yang, et al. Accelerating DES and AES Algorithms for a Heterogeneous Many-core Processor. *Int. J. Parallel Program.* **2021**, 49 (3), 463–486.
14. A. Boutros, V. Betz. FPGA Architecture: Principles and Progression. *IEEE Circuits Syst. Mag.* **2021**, 21 (2), 4–29.
15. A.T. Hashim, A.M. Hasan, H.M. Abbas. Design and implementation of proposed 320 bit RC6-cascaded encryption/decryption cores on altera FPGA. *Int. J. Electr. Comput. Eng.* **2020**, 10 (6), 6370–6379.
16. A. Subandi, M.S. Lydia, R.W. Sembiring. Analysis of RC6-Lite Implementation for Data Encryption; Scitepress, **2021**; pp 42–47.
17. F. Fawwaz, A. Hashim, W. Fawwaz Shareef. Compact Hardware Implementation of FPGA Based RC6 Block Cipher. *J. Eng. Appl. Sci.* **2008**, 3, 598–601.
18. O.S. Faragallah, A. Afifi, W. El-Shafai, et al. Efficiently Encrypting Color Images with Few Details Based on RC6 and Different Operation Modes for Cybersecurity Applications. *IEEE Access* **2020**, 8, 103200–103218.
19. M. Helmy, W. El-Shafai, S. El-Rabaie, I.M. El-Dokany, F.E.A. El-Samie. Efficient security framework for reliable wireless 3D video transmission; Springer US, **2022**; Vol. 33.
20. N. Liu, J. Cai, X. Zeng, G. Lin, J. Chen. Cryptographic Performance for Rijndael and RC6 Block Ciphers. *Anti-counterfeiting, Secur. Identif.* **2017**, 36–39.
21. S.M. Noor, E.B. John. Resource Shared Galois Field Computation for Energy Efficient AES/CRC in IoT Applications. *IEEE Trans. Sustain. Comput.* **2019**, 4 (4), 340–348.
22. R. Maharjan, A. Alsadoon, P.W.C. Prasad, N. Giweli, O.H. Alsadoon. A novel secure solution of using mixed reality in data transmission for bowel and jaw surgical training: markov property using SHA 256. *Multimed. Tools Appl.* **2021**, 80 (12), 18917–18939.
23. F.F. Shareef, A.T. Hashim, W.F. Shareef. Compact Hardware Implementation of FPGA Based RC6 Block Cipher. *J. Eng. Appl. Sci.* **2008**, 3 (7), 598–601.
24. K. Aggarwal. Comparison of RC6, modified RC6 & enhancement of RC6. *Conf. Proceeding - 2015 Int. Conf. Adv. Comput. Eng. Appl. ICACEA 2015* **2015**, 444–449.
25. S.D. Sanap, V. More. Performance analysis of encryption techniques based on avalanche effect and strict avalanche criterion. *2021 3rd Int. Conf. Signal Process. Commun. ICPSC 2021* **2021**, 676–679.
26. S. Aljawarneh, M.B. Yassein, W.A. Talafha. A resource-efficient encryption algorithm for multimedia big data. *Multimed. Tools Appl.* **2017**, 76 (21), 22703–22724.