Indian Journal of Science and Technology, *Vol 8(31), DOI: 10.17485/ijst/2015/v8i31/87299, November 2015*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Protected Test Covering using Light Weight Block Cipher

V. Srinivasan*

Department of Electronics Tele Communication, Bharath University, Chennai-600073, Tamil Nadu, India;
srinivasan.etc@bharathuniv.ac.in

Abstract

In testing of single chip there are many approach were found to need their requirement. But for the SOCs we have less, in this paper a Protected Test Wrapper - PTW design introduce to protect SOCs that is compatible with IEEE 1500 standards. PTW protects internal scan chains and primary inputs, primary outputs, which may contain many critical data during the normal system operation like encryption keys. In the earlier system testing that is original IEEE 1500 standard will not concern about the Primary Input and Primary Output security, where as this PTW will secure the primary input and output in both scan mode and normal system functional mode. To achieve this protected test wrapper no extra larger component are required by changing the IEEE 1500 with some light weight block cipher we protect the core from the hacker.

Keywords: Boundary Scan, Design for Testing, Light Weight Block Cipher, Protection.

1. Introduction

Each primary input signal and primary output signal is supplemented with a multi-purpose memory element called a Boundary-scan Cell. Cells on device primary inputs are referred to as "Input cells;" cells on primary outputs are referred to as "Output cells." "Input" and "Output" is relative to the core logic of the device.

The following Figure 2 shows a basic universal Boundary-scan Cell, known as Boundary-scan Cells. The cell has four modes of operation: normal, update, capture, and serial shift. The memory elements are two D-type flip-flops with front-end and back-end multiplexing of data. During normal mode, Data In is passed straight through to Data Out. During update mode, the content of the Update Hold cell is passed through to Data Out.

During capture mode, the Data In signal is routed to the input Capture Scan cell and the value is captured by the next Clock DR. Clock DR is a derivative of TCK. During shift mode, the Scan Out of one Capture Scan cell is passed to the Scan In of the next Capture Scan cell via a hard-wired path. Both capture and shift operations do not interfere with the normal passing of data from the parallel-in terminal to the parallel-out terminal. This allows on the fly capture of operational values and the shifting out of these values for inspection without interference. This application of the boundary-scan register has tremendous potential for real-time monitoring of the operational status of system[2–3].

2. Existing Systems

2.1 Original IEEE 1500 Standards

The IEEE 1500 architecture[9] is characterized by flexibility and scalability. Careful consideration was given to the Plug-and-Play aspects of heterogeneous cores integrated into the same chip. The 1500 hardware architecture comprises an Instruction Register, and two data registers, the Wrapper Bypass Register and the Wrapper Boundary Register. The use of Core Data Registers is also anticipated by the standard. Access to these registers is provided via a set of wrapper interface ports. Figure 2.1 displays the mandatory components of the IEEE 1500 architecture[1].

To understand the operation of the IEEE 1500 standard the operations are divided into two types functional mode

*Author for correspondence

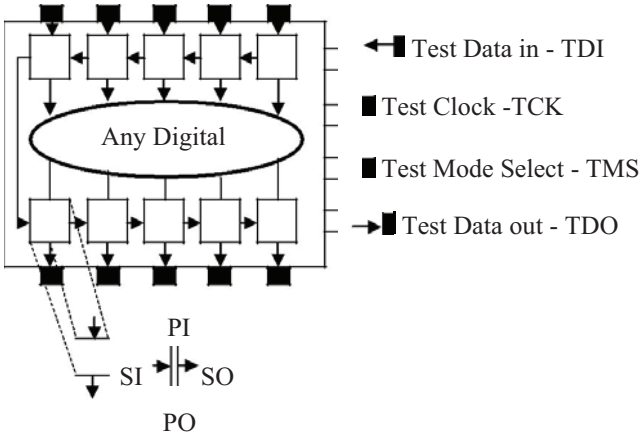

Figure 1. Principles of Boundary Scan.

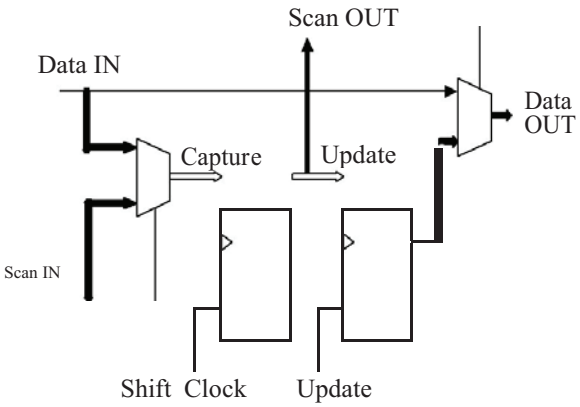

Figure 2. Basic Boundary Scan Cell.

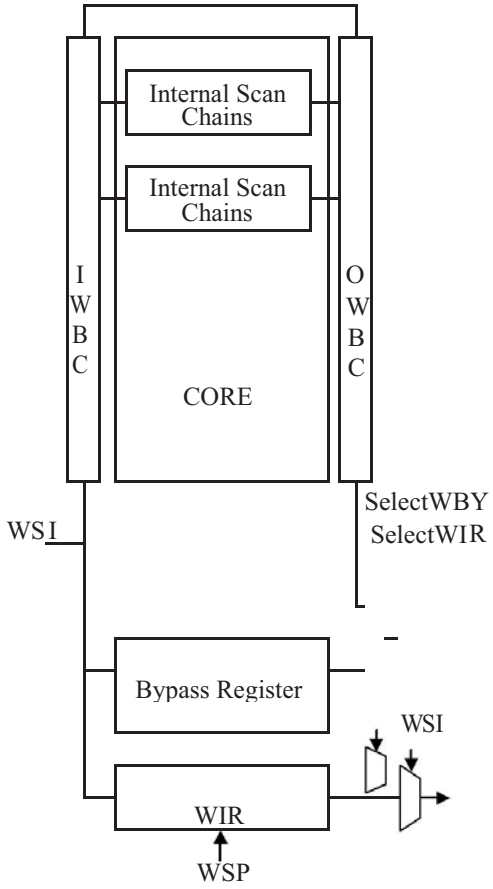

Figure 3. IEEE 1500 Standard.

and scan mode, in the functional mode the Primary Input is just transfer to the core to process the input and produces the output and the Primary Output is transfer in to the environment[4]. In this approach the primary input and output is not secured once the normal mode is chosen by the WSP signal the data can easily get in to the core for the operation. For any other normal SOCs this will not be a big problem where as in the most important secured SOCs like the AES or DES any other encryption core must be protected. Because the input of the core will be a plan text and the output will be a cipher text, so there are many chances to occur the internal attacks in the boundary scan[5].

To protect the core we proposed a new approach on this paper, protect test wrapper in opposition to boundary and internal attacks, the Primary Input of the core will not be process in to the chip until we unlock the wrapper by the unlock signal[6]. The signal will be generated after the comparison of the wrapper input with the light weight block cipher output. If the wrapper is unlocked then it gets it to the normal mode.

2.2 Advanced Encryption Standard

This method is used in the US government since in the year 2001. This is most popular technique which contains less hardware implementation with high security[2]. The cipher text cannot be hack with any kind of powerful algorithm like brute force etc. The AEC encryption contains many rounds to get the cipher text, each rounds consists of four basics operations: 1. the Sub Bytes transformation step, 2. The Shift Row transformation step, 3. The Mix Columns step and 4. The Add RoundKey step. In the Add RoundKey step, the subkey is combined with the state. The subkey is added by combining each byte of the state with the corresponding byte of the subkey using bitwise. For more details of AEC can be found in[10]. AES codes are secure most attacks expect the side channel attacks in the boundary scan. If anyone knows the details of the IP then it is easy to force the core in to the scan

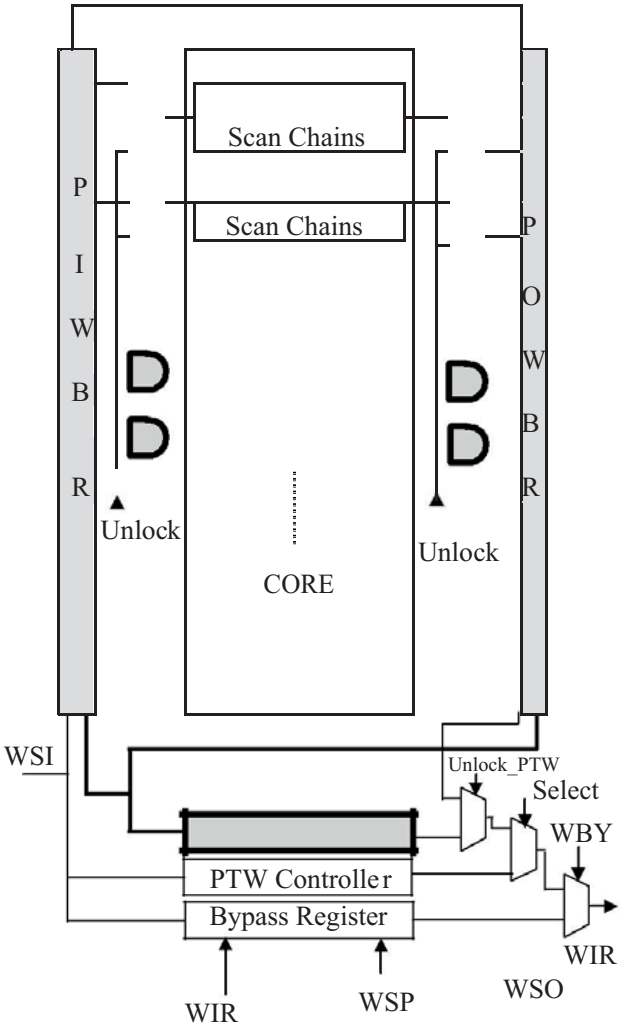

Figure 4. Protected Test Wrapper.

mode and the encrypted key will get out in the scan out. The IEEE 1500 wrapper will secure core[3].

3. Protected Secure Wrapper

3.1 Hardware Description

The Protected Test Wrapper is proposed with the technique instead of sending the functional input signal in to the boundary cell the wrapper will protect the input by having the locked gates[6, 7]. The gates will be unlocked until unless the authorized person will unlock the signal. The unlock signal will be generated by comparing the scan input signal and the light weight block cipher output when both gets match then the unlock signal[8] is generated. The following Figure no to defined the proposed protected test wrapper method in the diagram the original IEEE 1500 wrapper is not modified much just introducing the highlighted blocks to meet the protected test wrapper in against with the side channel attacks.

The SOC contains many separate blocks in it the chip will gets the input from the source pin or through from the memory the signal is protected for the IP based SOCs, it very important to get the sink without any side channel attacks in the core. The unlock signal is generated by many of the techniques where are each should have its own risk to have a chance of attacks[11]. The WSI will be generated according to the function which the boundary wrapper cell will perform. The WSP will contain much the major operation that is described in the introduction chapter, the WRCK continuously generated for the both system operation and the scan path operation[9, 10]. IEEE 1500 allows the WSI in to the PIWBR for the normal System operation and the signal will be performed as per the core which has its own task.

WSI signal the Wrapper compare the functional input with the Light weight block cipher output if it gets matches the unlock is generated.

The unlock signal generated after validating the input signal with the cipher text the wrapper allow the input in to the core, if validation fails then the wrapper get in to the idle mode as shown in the Figure 5.

3.2 Light Weight Block Cipher

The light weight block cipher KTANTAN[12] is a block cipher family designed for constrained devices and embedded systems, which has very small footprint and acceptable security levels. It consists of three versions with different block sizes, 32, 48 and 64 bits, which are thus named KTANTAN32, KTANTAN48 and KTANTAN64 respectively. In the following content, we use KTANTAN n to denote the KTANTAN version with n-bit block. Despite of different block sizes, they all accept 80-bit keys. The structure of KTANTAN n is shown in Figure 1. For encryption of KTANTAN n, the plaintext p is divided and then loaded into two registers, L1 and L2. Two nonlinear functions, defined by the Equations (1), are operated on L1 and L2 respectively.

The operation will further detail in the below diagram, the PTW controller Figure 5 denotes that the protected test wrapper will checks the follow the three stages of output and the PTW will,

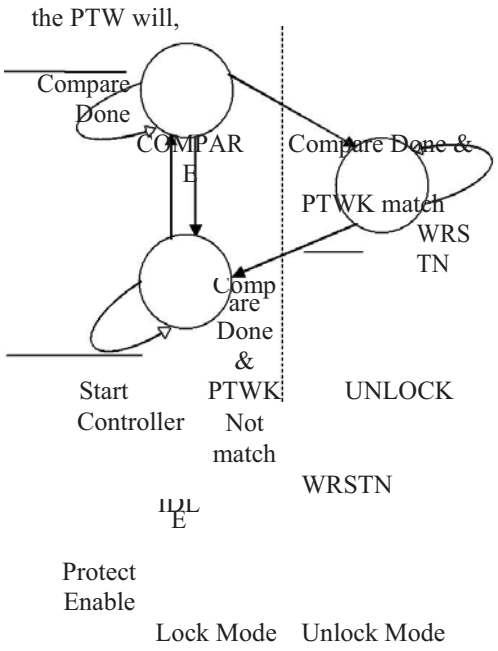

Figure 5. PTW Controller.

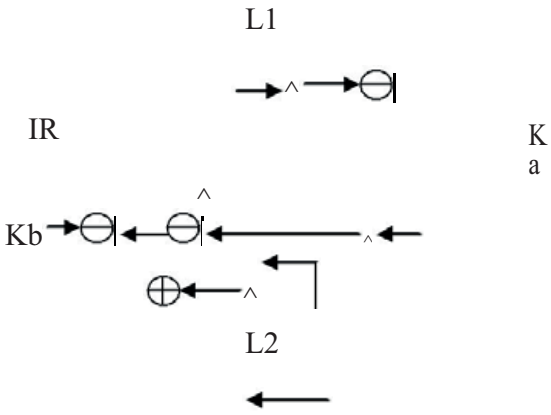

Figure 6. The Structure of KATANTAN.

Checks unlock signal, the Wrapper initial holds in the IDLE stage by checking the protected enable signal when the signal is generated through the

$$Fa\ [L1] = L1[x1] \wedge L2[x2] \wedge (L1[x3].L1[x4]) \wedge (L1[x5] . IR) \wedge Ka$$

$$Fb\ [L1] = L2[y1] \wedge L2[y2] \wedge (L2[y3].L2[y4]) \wedge (L2\ [y5] . L2[y6]) \wedge Kb \quad (1)$$

In the above equations, xi and yj are pre-defined indices for different versions of KTANTAN, IR is an irregular update sequence to prevent self-similarity attacks, and ka and kb are two bits chosen from the 80-bit master

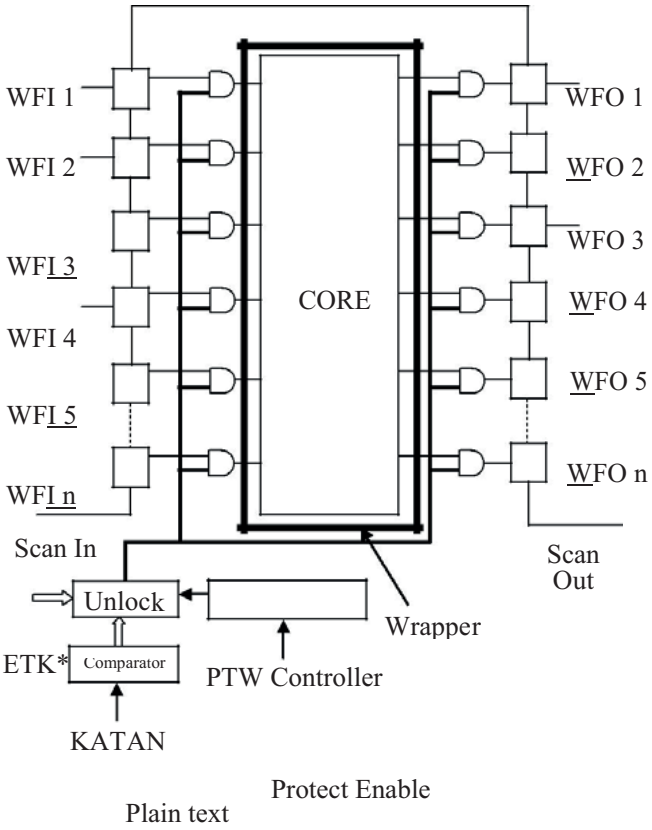

Figure 7. PTW with Light Weight Block Cipher.

key. The structure of KTANTAN is illustrated in Figure 6, and the parameters xi, yj, IR, and (ka, kb) used in each round. For KTANTAN32, after computing fa and fb, the registers L1 and L2 are shifted left once, and the most significant bits of L1 and L2 are discarded. Next, fa [L1] is fed into the least significant bit of L2, and fb [L2] is put into L1. After 254 such updating operations, the states of L1 and L2 are concatenated and outputted as a cipher text c. KTANTAN48 and KTANTAN 64 have the same structure as KTANTAN32, including the total number of rounds 254, but L1 and L2 of KTANTAN48 are updated twice in each round, and three times for KTANTAN64, by using same ka and kb. For more details, please refer to the original design specification[13].

The Figure 2.10 refers the PTW architecture this gives the complete details of the protected test wrapper how its functions, the wrapper functional input is given to both core input as well as in to the comparator then the polynomial sequence which is generated from the KATAN will compare to the input sequence and then this will be produce the output as per the condition if it's both get matches the unlock signal is generated[19-20].

Then the wrapper will be unlock that is the content of the wrapper input signal is given to the core input until unless the core wrapper is lock these information will not be passes through the input line by this core is protect although if it's in test mode nobody will know the core information till it get unlocks[14-16].

The unlock signal will be generated by the comparator but the process is starts when the secure enable signal will get active by the user side[17]. By this the whole system operation is in the secure mode and unsecure mode in other words lock mode and unlock mode.

4. Testing Of Protected Test Wrapper

The PTW is secured by the light weight block cipher and this will be tested by the following Figure explanation this Figure 8 shows the prototype model of the objective the SOC covers by the wrapper with an protected signal which is unlock, this signal is generated by the comparator and comparator checks the output of the server and the internal KATANs output. If SOC need to check the authorized person sends the plain text to both server and to the internal light weight block cipher. The server receives the plain text by means of nonce and the internal KATAN generates the cipher text as (ETX) and the server generates a cipher text as (ETK*). Both the data given to the server if it get match then the unlock signal is generated otherwise the wrapper remains lock. This function is clearly explained in the Figure 5. The server internal block is also a KATAN[18].

5. Discussion and Future Work

If more security is needed, the KATAN seed can be loaded from a unique, chip-specific code. Examples of chip-specific codes are die location on wafers, cache memory repair information, and etc. These codes are stored in the non volatile memory after a chip is tested. We cannot choose those chip-specific codes, like the microprocessor ID, that are accessible to users. We can choose the chip-specific codes, like the cache memory repair information, which is transparent to users. The cache memory repair information is caused by random defects during the manufacturing process so there is no correlation with the openly accessible microprocessor ID. Even if the attackers gain the seed by physically breaking into a chip, the information is useless for the other chip. It is an important assumption that, in normal operation, the chip never needs to enter test mode by itself. Otherwise, there could be a security hole. Because the JTAG interface it is not encrypted so the attacker could get the PTW key by recording data entering the TDI pin.

Our next step is to develop PTW for chips for protected the NOC chips which requires more security where as not important of area. The KATAN block cipher more efficient block cipher in the real environment.

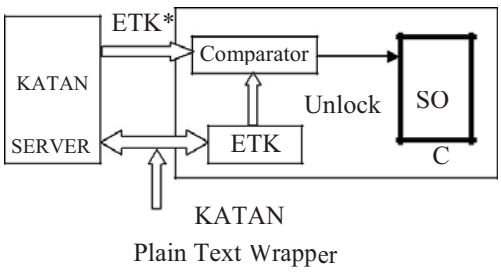

Figure 8. PTW design

6. References

1. Canniere CD, Dunkelman O, Knezevic M. Katan and Ktantan- A Family of Small and Efficient Hardware-oriented Block Ciphers. In Clavier C, Gaj K, editors. CHES. Lecture Notes in Computer Science. Springer: 2009; 5747:272–88z
2. Kulanthaivel L, Srinivasan P, Shanmugam V, Periyasamy BM. Therapeutic Efficacy of Kaempferol Against AFB1 Induced Experimental Hepatocarcinogenesis with Reference to Lipid Peroxidation, Antioxidants and Biotransformation Enzymes. Biomedicine and Preventive Nutrition. 2012; 2(4):252–59. ISSN: 2210-5239.
3. Schaumont P, Raghunathan A. Guest Editors' Introduction: Security and Trust in Embedded-Systems Design. IEEE Design and Test Computers. 2007 Dec; 24(6):518–20.
4. Verbauwhede I.M.R(Ed). Secure Integrated Circuits and Systems. Springer; Berlin: Germany. 2010.
5. Jayalakshmi T, Krishnamoorthy P, Kumar GR, Sivamani P. The Microbiological Quality of Fruit Containing Soft Drinks from Chennai. Journal of Chemical and Pharmaceutical Research. 2011; 3(6):626–30. ISSN: 0975 – 7384.
6. Tiri K. Design for Side-channel Attack Resistant Security ICs. Ph.D. dissertation, Electrical Engineering Dept; University of California; Los Angels. 2005.
7. Kalaiselvi VS, Prabhu K, Ramesh M, Venkatesan V. The Association of Serum Osteocalcin with the Bone Mineral Density in Post Menopausal Women. Journal of Clinical and Diagnostic Research. 2013; 7(5): 814–6. ISSN: 0973–709X.

8. Goering R. Scan Design called Portal for Hackers. EE Times 2004. Available from: http://www.eetimes.com/electronics-news/4050578/Scan-design-called-portal-for-hackers.
9. Kapur R. Security versus Test Quality: Are they Mutually Exclusive?. In Proceedings IEEE International Test Conference; 2004. p. 1414.
10. Chiu G-M, M JC, Li. IEEE 1500-Compatible Secure Test Wrapper for Embedded IP Cores. Proceedings IEEE International Test Conference; 2008. p. 1.
11. Lee J, Tehranipoor M, Patel C , Plusquellic J. Securing Scan Design using Lock and Key Technique. Proceedings IEEE International Symposium; Defect Fault Tolerance VLSI System; Monterey: CA: 2005. p. 51–62.
12. IEEE Computer Society, IEEE Standard Testability Method for Embedded Core-Based Integrated Circuits, IEEE Std. 1500-2005.
13. Daemen J, Rijmen R. The Design of Rijndael: AES–the Advance Encryption Standard. Springer-Verlag; Berlin: Germany. 2002. p. 31– 62.
14. B. Yang, K. Wu, and R. Karri, "Secure scan:
14. A design-for-Test Architecture for Crypto Chips. Proceedings IEEE/ACM Des. Automatic Conference; 2005. p. 135–140.
15. Udayakumar R, Khanaa V, Saravanan T, Saritha G. Retinal Image Analysis using Curvelet Transform and Multistructure Elements Morphology by Reconstruction. Middle - East Journal of Scientific Research. ISSN: 1990-9233. 2013; 16(12):1781–5.
17. Hely D, Flottes M-L, Bancel F, Rouzeyre B, Berard N, Renovell M. Scan Design and Secure Chip. Proceedings International, On-Line Test Symposium; 2004. p. 219–26.
18. Biryukov A, Khovratovich D. Related-Key Cryptanalysis of the Full AES-192 and AES-256. Available from: https://cryptolux. org/mediawiki/uploads/1/1a/Aes-192-256.pdf
19. Sharmila D, Muthusamy P. Removal of Heavy Metal from Industrial Effluent using Bio Adsorbents (Camellia sinensis). Journal of Chemical and Pharmaceutical Research. 2013; 5(2):10–3. ISSN: 0975 – 7384.
20. Kelsey J, Schneier B, Wagner D, Hall C. Side Channel Cryptanalysis of Product Ciphers. Proceedings European Symposium Research Computer Security; 1998.p. 97–110.
21. Kimio T, Natarajan G, Hideki A, Taichi K, Nanao K. Higher involvement of subtelomere regions for chromosome rearrangements in leukemia and lymphoma and in irradiated leukemic cell line. Indian Journal of Science and Technology. 2012 April; 5(1):1801–11.
22. Cunningham CH. A Laboratory Guide in Virology. 6th ed. Minnesota: Burgess Publication Company; 1973.
23. Sathish Kumar E, Varatharajan M. Microbiology of Indian Desert. In: Sen DN, editor. Ecology and Vegetation of Indian Desert. India: Agro Botanical Publishers; 1990. p. 83–105.
24. Varatharajan M, Rao BS, Anjaria KB, Unny VKP, Thyagarajan S. Radiotoxicity of Sulfur-35. Proceedings of 10th NSRP; India. 1993. p. 257–8.
25. 01 Jan 2015. Available from: http://www.indjst.org/index.php/vision