iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** V **Month of publication:** May 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Highly Secured Quantum Genetic Based Encryption Method with Low Complexity

G.Ramadevi [#1]
Assistant Professor
[#]*Deparment of Electronics and Communication Engineering, Apollo Engineering College*

Abstract*— The security of digital images attracts attention recently, especially when these digital images are stored in some forms of memory or send through the communication systems like wireless sensor networks. Many different image encryption methods have been proposed to keep the secured images. Due to high complexity in hardware based implementation, and higher computational complexity many secured algorithms like AES, RC5 etc are not suitable for WSN nodes. To address these limitations, lightweight block cipher based on chaotic map and genetic operations have been proposed. An image encryption technique tries to convert an image to another image that is hard to understand with diffusion and confusion metrics. The proposed cryptographic scheme employs chaotic map parameters to generate the pseudorandom bit sequence. These sequences are used in XOR, mutation and crossover operations in order to encrypt the data blocks. In this proposed method, to reduce complexity, the quantum Genetic Algorithm (GA) is used to produce a new encryption method by using the powerful features of the Crossover and Mutation operations of (GA) and adoptive fused macro block selection process for better security. The efficiency of proposed encryption method is proved to be best for wireless sensor node based data transmissions.

Keywords*— Wireless Sensor Network, Pseudorandom bit sequence generator, Data Encryption, Elliptic curve, Chaotic map, Mutation, Crossover

I. INTRODUCTION

Wireless Sensor Networks (WSN), sometimes called Wireless Sensor And Actuator Networks (WSAN), are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, enabling control of sensor activity. he development of wireless sensor networks was motivated by military applications such as battlefield surveillance, today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, etc The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver , a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNS can vary from a simple star network to an advanced multi-hop wireless network.

The propagation technique between the hops of the network can be routing or flooding, in computer science and telecommunications, wireless sensor networks are an active research area with numerous workshops and conferences.

The rest of the paper is organized as follows. In Section 2, A Quantum Genetic Algorithm (QGA) is explained. In Section 3, Existing system is presented. In Section 4, Working methods of proposed QGA system is described. In Section 5, we give the Comparison between AES and QGA is discussed. In Section 6, we conclude the paper.

II. QUANTUM GENETIC ALGORITHM

A Quantum Genetic Algorithm (QGA) that exploits the quantum effects of superposition and entanglement. To begin, we start with N quantum registers, labelled reg10 through reg1n-1, where N will be the population size. Each of these registers is then placed in a superposition of all possible individuals. Thus, each register actually stores all possible individuals. Next, the fitness function is applied to each of the N quantum registers with the result stored in a second set of N quantum registers, labelled reg20 through reg2n-1. The fitness function is applied to produce an entanglement between the original registers and the second set of registers.

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

The set of N paired registers, half containing fitness values and half containing the superposition of individuals of those fitness , will represent our initial population. Crossover is applied normally. The contents of register reg1i are crossed with the contents of register reg1j. Because these registers contain a superposition of individuals, the result is two new superposition's . In particular, if reg1i contains all individuals of fitness fi and reg1j contains all individuals of fitness fj then the result is the superposition of all individuals that can be produced through crossover at the chosen location.

The final step is to obtain a result when the termination condition is reached. The final result will be N pair of registers, the first register of each pair will contain a set of superimposed individuals, all of the same fitness, entangled with the second register of the pair, which contains the measured fitness. A measurement of the first register will detect one of the individuals of the given fitness. This produces the desired result, a single quantum population is, at one level, much larger than a similar classical population.

III. EXISTING SYSTEM

A number of security mechanisms have been proposed for sensor networks.To provide the data (AES,KATAN,LED and TWINE).We proposed lightweight block ciphers based on chaotic map and genetic operations.The proposed cryptographic scheme employs to verify the communicating nodes. The Fig.1 show the AES system.

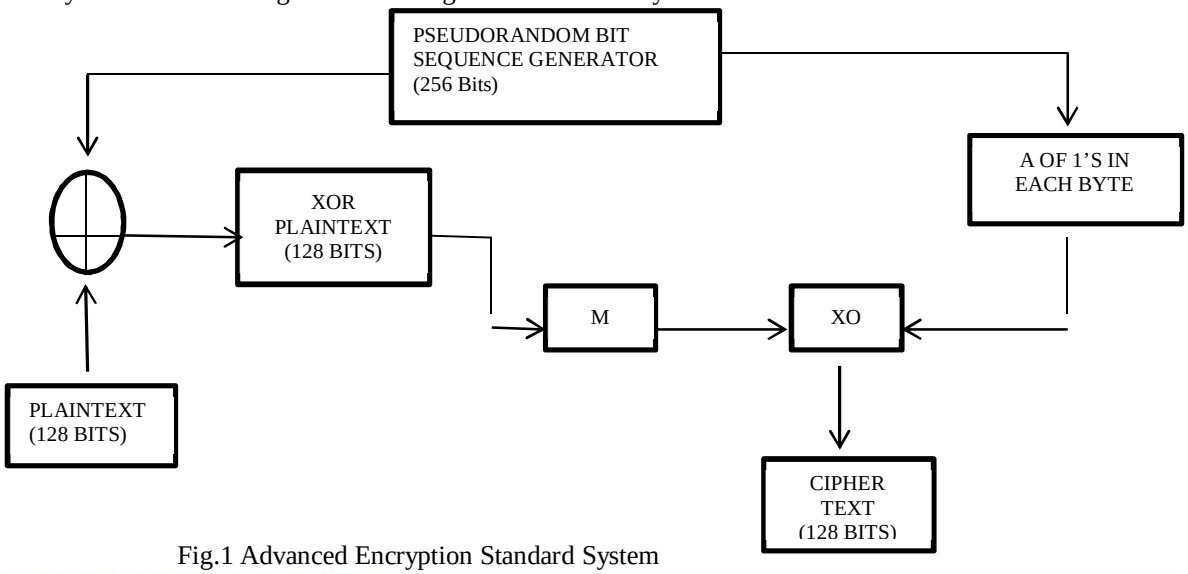


Fig.1 Advanced Encryption Standard System

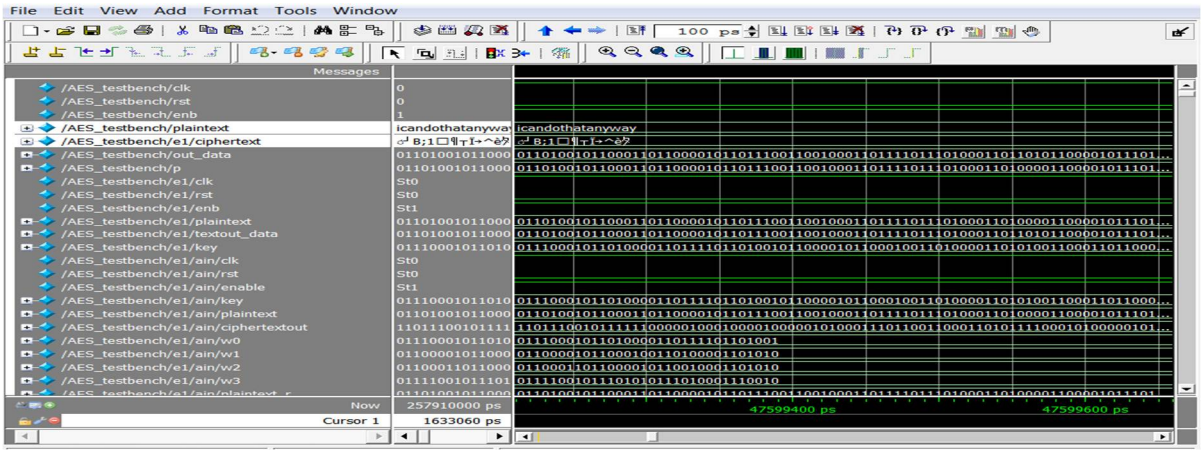


Fig.2 AES System Simulation Result

A. Conventional cryptosystems like AES, RC5,TEA are not suitable for WSN applications for following reasons:
B. Highly complex algorithms not supported by tiny sensor nodes.
C. Not applicable for real time because of its low speed .
D. Adjacent packets and pixels values in image pixels are highly correlated. This redundant nature needs genetic based approach for better encryption.
E. Requirement of RAM leads complexity.

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

F. All key length leads poor throughput rate.
G. The level of encryption is largely depends on a secret-key used on image block depends, which be easily encoded as a sequence of bits for decryption .
H. For any WSN data transmission between nodes should be secured one since these kind sensors nodes most widely used in nuclear power plants, aircrafts, and hospitals.
I. In most cases sensors nodes are smaller in size and deployed in short distances and operated with limited battery power.

IV. PROPOSED SYSTEM

The drawback of AES like high complexity, low speed, low secured have been overcome by the proposed Quantum Genetic Algorithm(QGA).The QGA over conventional approach is only for better security.Here The image is divided in overlapping blocks of desired size.The overlapping size and fashion is user defined.The proposed cryptography system makes different pseudo random bit sequence for every session.

Cross over & mutations are basic properties in genetic method. Confusion and diffusion are two general principles for any block ciphers. Chromosomes are represented as binary of sequence each belongs to unique state. Chromosome represents all quantum superposition states with equal probability. A cryptographic scheme that integrate of the elliptic curve for WSN applications. Crossover is the placement of two (or) more

and used to genetic recombine. A mutation is a permanent change of the nucleotide sequence of an organism. The proposed encryption scheme randomly selects different secret keys rather than fixed parameter .We plan to implement it in large scale sensor networks to evaluate overall message throughput and latency

Our proposed block cipher is divided into three phases:

A. Key establishment phase
B. Pseudorandom bit sequence generation phase
C. Encryption phase

The tools used in the project

A. Simulator- MODELSIM
B. Synthesizer- QUARTUS II
C. Pre & post processing- MATLAB
D. Microprocessor-AT mega 128L

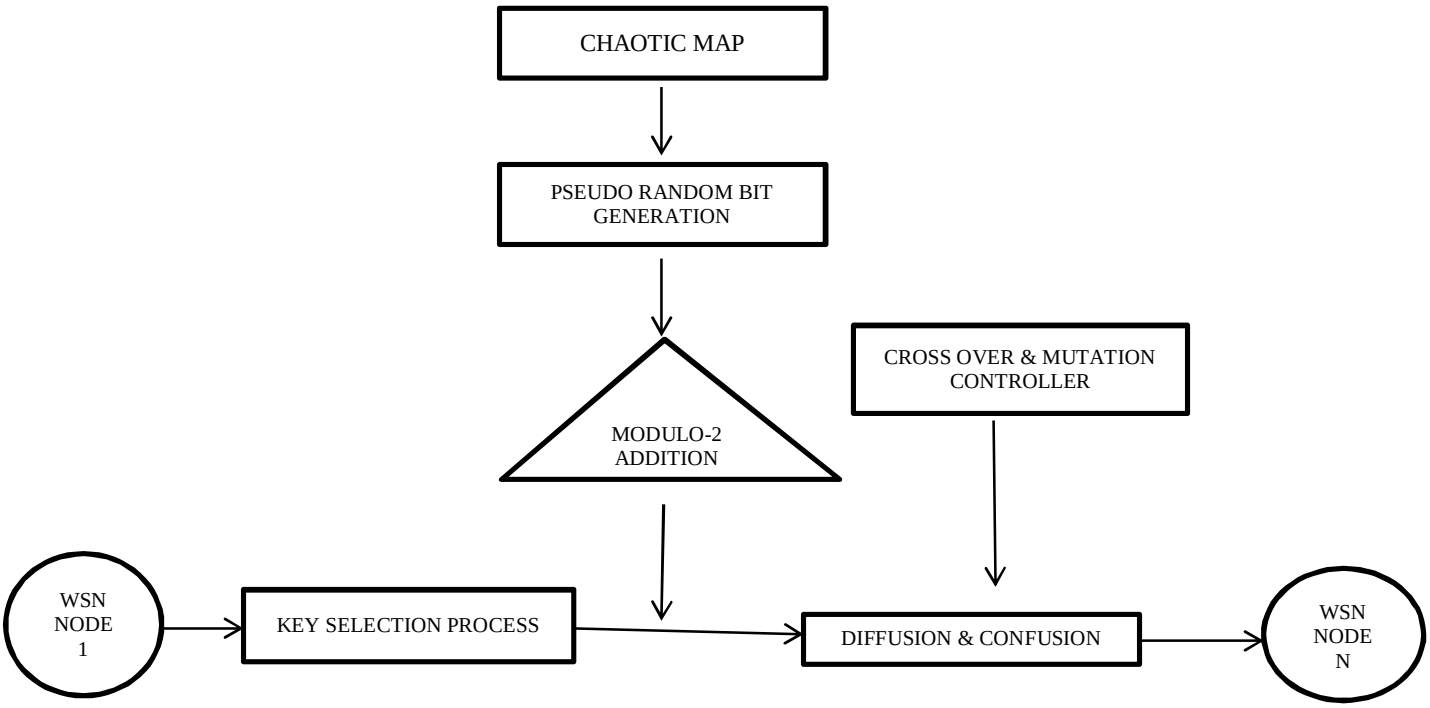


Fig.3 Proposed QGA System

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

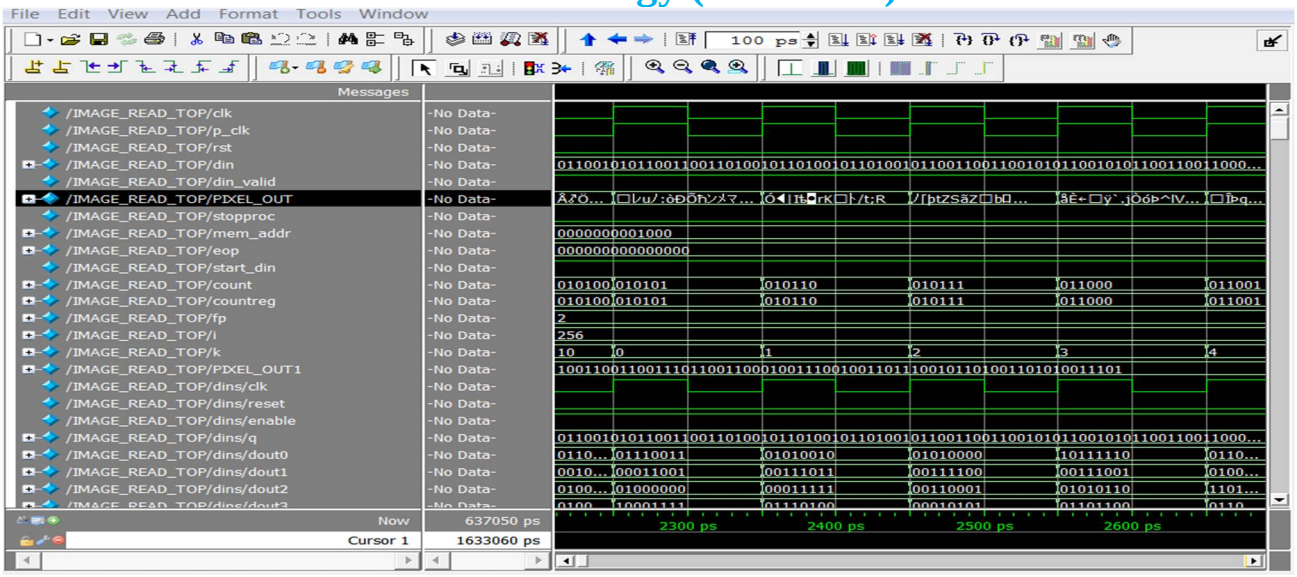


Fig.4 QGA System Simulation Result

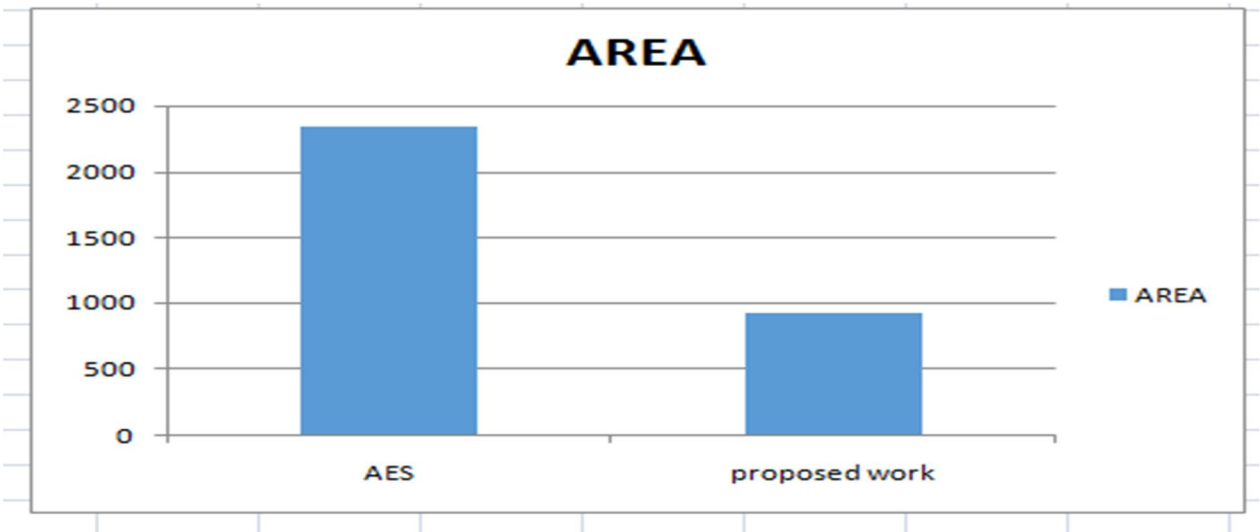
V. AES VS PROPOSED QGA

The following Table 1. and Graph 1. Shows the comparison between AES and QGA based on the Area . The advantages of QGA are as follows:

A. Packet reception rate in very high
B. Able to process high speed real time data with maximum payload
C. Quantum algorithm has less complexity
D. Outer level security is high

Crypto Type used	AREA
AES	2343
Proposed Work	930

Table 1. AES Vs Proposed QGA



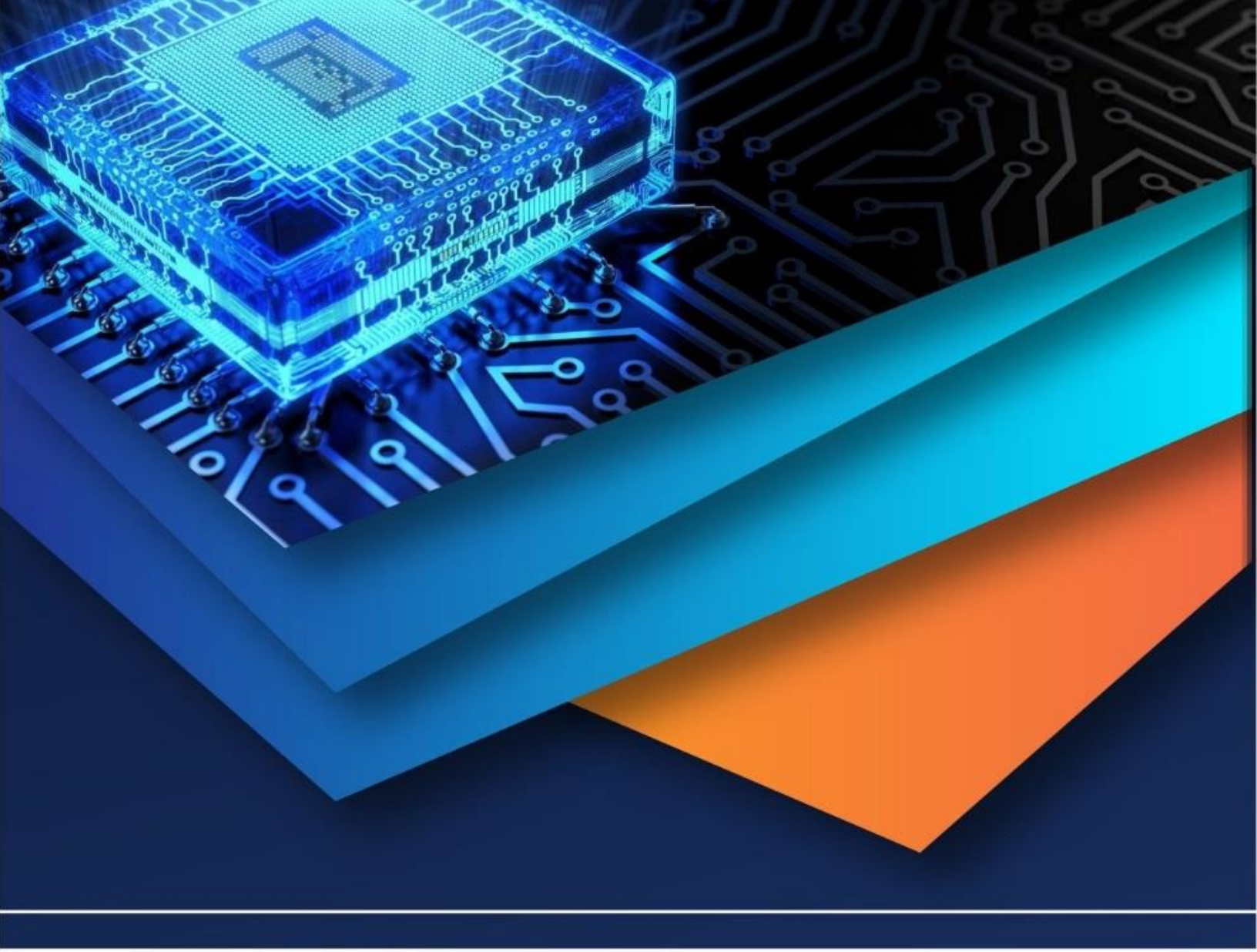
Graph 1. AES Vs Proposed QGA

VI. CONCLUSION

The Quantum Genetic Algorithm(QGA) have been used for cryptographic schemes in wireless environments,since it is highly secured for sensor networks.The implementation of lightweight block cipher based on chaotic map and genetic operations have been proposed. Thus this QGA has greatly reduced the complexity level of encryption scheme. Simple arithmetic is used for encryption since it has low complexity .Multilevel confusion metrics are added to have high security.Quantum cryptography can be a favoured choice for future applications that require long-term information security like Government agencies, Financial institutes, Health care providers

REFERENCES

[1] Yi-Chao Chen, Lili Qiu, Yin Zhang, Guangtao Xue, and Zhenxian Hu. Robust network compressive sensing. In Proceedings of the 20th annual international conference on Mobile computing and networking, pages 545–556. ACM, 2014.
[2] Cong Wang, Bingsheng Zhang, Kui Ren, Janet M Roveda, Chang Wen Chen, and Zhen Xu. A privacy-aware cloud-assisted healthcare monitoring system via compressive sensing. 2014.
[3] M. Cazorla, K. Marquet and M. Minier, Survey and benchmark of lightweight block ciphers for WSNs, SECRYPT, May 2013.
[4] Xinbing Wang X. Tian H. Zheng, S. Xiao. Energy and latency analysis for in-network computation with compressive sensing in wireless sensor networks. In INFOCOM, 2012 Proceedings IEEE, pages 2811 – 2815, 2012.
[5] G. R. Sakthidharan and S. Chitra, A survey on wireless sensor network: An application perspective, ICCCI, pp 1–5, 2012.
[6] Xinpeng Zhang, Yanli Ren, Guorui Feng, and Zhenxing Qian. Compressing encrypted image using compressive sensing. In Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2011 Seventh International Conference on, pages 222–225. IEEE, 2011.
[7] Yong Wang, Kwok-Wo Wong, Xiaofeng Liao, and Guanrong Chen. A new chaos-based fast image encryption algorithm. Applied soft computing, 11(1):514–522, 2011.
[8] Mikhail J Atallah and Keith B Frikken. Securely outsourcing linear algebra computations. In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, pages 48–59. ACM, 2010
[9] C. Karlof, N.Sastry and D. Wagner, TinySec: a link layer security architecture for WSNs, ACM SenSys, pp. 162–175, 2004.
[10] E. Yarrkov, Cryptanalysis of XXTEA, http://eprint.iacr.org/2010/254.pdf, 2010.
[11] Thomas M. Cover Joy A. Thomas. Elements of information theory. Wiley Series in Telecommunications and Signal Processing, pages 2021, 2006
[12] E. Biham, A. Biryukov and A. Shamir, Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials, J. of cryptology, vol. 18(4), pp. 291–311, 2005.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY