DNA Computing Based Encryption Algorithm for Wireless Multimedia Communication System

A. Vyasa Bharadwaja, V. Ganesan

Abstract: ***Transmission of digital images for wireless multimedia communication system requires reliable security in storage which is a challenging task. So many works are carried out to develop and implement the cryptographic techniques for a wireless multimedia communication system. A traditional symmetric key cryptographic algorithm such as Light weight Data Encryption Standard cipher, Advanced Encryption Standard cipher, Triple-DES, Twofish, Blowfish, RC5 etc played a major role to transmit and receive the multimedia (text, image and video) data. Proposed DNA computing based authentication algorithm provides secure transmission of multimedia data by using symmetric key cryptography techniques. DNA computing techniques provides a higher level of security and enables the user to store a large amount of data. Finally, it shows the implemented result analysis the performance of different symmetric key cryptographic techniques using the simulation parameters such as power consumption, key size, processing time, memory space, speed and latency. It also improves the security level by incorporating the advantage of DNA cryptography to achieve a high level of security against various attacks.***

Keywords: ***Wireless multimedia communication, Symmetric key cryptography, DNA Cryptography, Secret key, Processing time, Key size, Communication Complexity and Computational overhead.***

I. INTRODUCTION

Nowadays, Wireless multimedia communication systemplays a major role on the internetfor hiding and security data transmission of digital Images. Through internet communication, medical and military imaging systems require the system to keep confidential images and data information to avoid security issues. To avoid all these problems, an image communication system for internet applications approaches a compressed sensing (CS) model that is used for reducing the image encryption and decryption time. It also provides various operations for secure transmission and the effective performance of the system[1].In today's growing world, it has been a challenging one for protecting the data information security from the intruders due to fast-developing technologies. Even though the industries and the business developers keep their information very confidentially, the hackers try to get the information which leads to the major security issues. Due to this, there is a need for hiding the data using various techniques. Steganography based data hiding technique avoids the intruder and also provides the additional usage of identifying the attacker. It shows the performance in terms of correlation technique, PSNR and MSE values [2].

High throughput is achieved by implementing the secure authentication AES-Counter with Chaining Mode (AES-CCM)algorithm on the asynchronous multicore processor and also it avoids various attacks. Key adjusting technique also has been played a vital role to protect against the secret key pattern attacks [3]. Universal security architecture is a novel design crypto processor for 4G long term evolution which consists of four cyphers that have been deployed on FPGA to achieve network level protection and security for wireless communications.Internet protocol network is used in the transmission of communication for authenticating different network protocols in the fast-growing technology. The data is processed to the cloud FPGA and the symmetric proxy re-encryption scheme (PRE) is used to support on internet operations to achieve higher security and for the enhancement of the security and authentication for wireless communication systems based on encryption and decryption [3] [4] [5]. Cloud computing has not become a secured process as there is developing a faster technology through internet and they attack the user resources and retrieve all the information required. The user data applications are secured using FPGA against potential attacks[6]. Rivest cypher (RC5) chaotic key scheduling algorithm is performed for health monitoring systems to protect against several attacks and to secure the patient's clinical reports. The chaotic image encryption algorithm and Bitwise operation are performed for wireless image transmission to reduce the complexity and for analyzing the security performance [7] [8].

II. RELATED WORK

In addition with bit-level scrambling, Pixel level based operations are used on an image to enhance the security level and DNA encoding to improve the performance of the cryptography against various attacks. User efficient authentication scheme uses different cryptography techniques like digital signatures, hashing and encryption for securing authentication server protocol that can resist password attacks. Diffusion process is ensured by the combination fiestel structure based SHA-3 technique and the DNA mapping process and also to encrypt the cypher text image for high security [1] [2] [3].

Revised Manuscript Received on January 05, 2020.
***** Correspondence Author
A. Vyasa Bharadwaja*, Department of ECE, Sathyabama Institute of Science and Technology, Chennai (Tamil Nadu) India.
E-mail: bharadwaja.akondi@gmail.com
V. Ganesan, Department of ECE, Sathyabama Institute of Science and Technology, Chennai (Tamil Nadu) India.
E-mail: vganesh1711@gmail.com

DNA encoding role performs matrix operations on scrambled DNA design based on CML and DNA sequences to encrypt a final output image to improve the security and statistical analysis performance [7]. User authentication technique on wearable devices is implemented using three combinations of biometrics such as physiological, hybrid and behavioral by SVM classifiers to improve the accuracy of the authentication by comparison of three biometrics [9]. Anonymous authentication is built on cloud service with the exchange of private keys for privacy-aware security attacks and it also used for location-based service for authentication protocol [10] [11].

The authentication for multiple servers is a difficult task for that BAN-logic is used for the effective security capability using multiple server architecture. The robust authentication scheme is used for Vehicle Sensor Networks (VSN) for continuous information of the vehicle and decentralized authentication for vehicle communication for fast efficient and security performance [12] [13]. The Proxy-based authentication scheme (PBAS) and Identity message-based authentication scheme (ID- MAP) is used for securing the message-related information which satisfies the Vehicular Ad-Hoc networks (VANETs) and edge computing scheme is also used for authentication of the further need of potential attacks. Dual authentication is for transmitting the secured data or messages based on the key management techniques [14] [15] [16]. The active authentication based on mobile devices uses four biometric characteristics such as GPS location, WiFi, web browsing and various application usage for protecting the overall performance system from the intruders[17]. Authentication based on the robust and efficient protocol by using biometrics and security key for E-Health services for the prevention of users identity and personal attacks. A scalable Video Coding (SVC) stream is used for secure and efficient authentication and also for a better quality of videos on decoding dependency graph for wireless multimedia systems [18] [19]. Mobile authentication based on touch screen devices using BEAT authentication scheme by signatures and gestures to improve the sensitive privacy information [20]. Authentication and the public key signature scheme is approached on ECDSA for vehicular application network to avoid privacy attacks and to prevent vehicle safety measures [21]. A two authentication mechanism such as AMAN and NRTT is used for securing authentication and login passwords for the web service [22]. The authentication scheme of biometrics is based on the wireless sensor networks to analyze the security performance against various attacks using a chaotic map [23]. A privacy-based authentication method for a vehicular ad hoc network to reduce the efficiency of network communication using an identity cryptography algorithm [24]. The Byzantine fault tolerance (PBFT) algorithm is used to improve the fifth generation of ultra-dense network and to evaluate the security to reduce the frequency of the user authentication in a network protocol [25].

III. TRADITIONAL SECURE AUTHENTICATION ENCRYPTION ALGORITHM FOR WIRELESS MULTIMEDIA COMMUNICATION SYSTEM

Traditional secure AES based authentication algorithm was implemented as an 8-bit asynchronous 9-core processor. It provides improved authentication speed by employing matrix multiplication to transfer the 16 plain texts into one plaintext. Secured AES authentication process is carried out by using parallel encryption techniques and provides high power dissipation, latency and throughput on a multicore processor implementation. Key adjusting technique is additionally added for the detection of pattern-based attacks and also to avoid the same secret key for one-time communication. Using the pattern detection, the variance distribution, power dissipation, time, electromagnetic dissipation (EM) and several cores are measured based on the core processor to predict the secret key against leakage pattern attacks. The performance of these techniques leads to high-level security and authentication process for various secured application.

IV. PROPOSED DNA COMPUTING BASED ENCRYPTION ALGORITHM FOR WIRELESS MULTIMEDIA COMMUNICATION SYSTEM

Proposed DNA mapping techniques combined with DES encipher methods gives security by two levels for data encryption and decryption [10]. DES algorithm uses the identical secret key for encryption process as well as decryption process to avoid the irrespective of a secured channel to obtain ciphertext as shown in Fig.1. It will be improved by employing the advantages of DNA computing techniques for text and image encryption method as shown below.

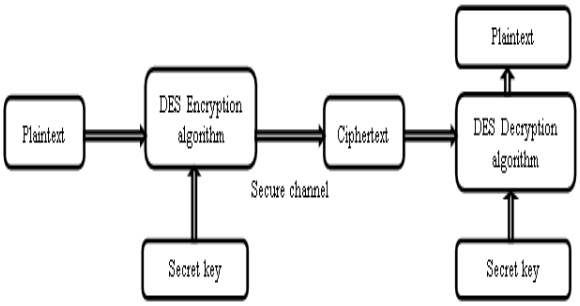

Fig.1: DES encryption and decryption algorithm

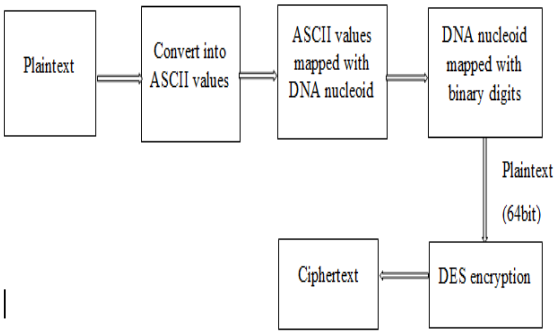

Fig.2 DNA mapping techniques for encryption process

DNA computing based text encryption algorithm

The following are the steps taken to convert plaintext into ciphertext using DES encryption algorithm and DNA computing techniques as given in fig.2

- First step, choose the plaintext of required size.
- Second, convert the chosen plaintext into ASCII values using table 1.
- Third step, map the ASCII values with DNA nucleoid by using table 3.
- Fourth step, use the table 2 for mapping the DNA nucleoid with binary digits.
- Fifth step, encrypt the binary digits using DES encryption algorithm [10].

Table 1: ASCII Code for Alphabets

Letter	ASCII Code	Letter	ASCII Code
a	097	A	065
b	098	B	066
c	099	C	067
d	100	D	068
e	101	E	069
f	102	F	070
g	103	G	071
h	104	H	072
i	105	I	073
j	106	J	074
k	107	K	075
l	108	L	076
m	109	M	077
n	110	N	078
o	111	O	079
p	112	P	080
q	113	Q	081
r	114	R	082
s	115	S	083
t	116	T	084
u	117	U	085
v	118	V	086
w	119	W	087
x	120	X	088
y	121	Y	089
z	122	Z	090

Table 2: DNA Mapping with Binary Values

DNA code	Binary values
A	0
T	1
C	10
G	11

Table 3: Number mapping with DNA Code

Numbers	DNA code
0	CAC
1	TAC
2	AGC
3	CTT
4	CGG
5	GAC
6	GAT
7	TTC
8	TTA
9	ATG

DNA computing based image encryption algorithm

The following are the steps taken to convert the image pixel values into ciphertext values using DES encryption algorithm and DNA computing techniques as shown in Fig.3

Step 1: Choose the image of size N x M

Step 2: Image pixel values is converted into DNA nucleoid using table 3.

Step 4: Use the table 2 to map the DNA nucleoid with binary digits.

Step 5: Encrypt the binary digits using DES encryption algorithm [10].

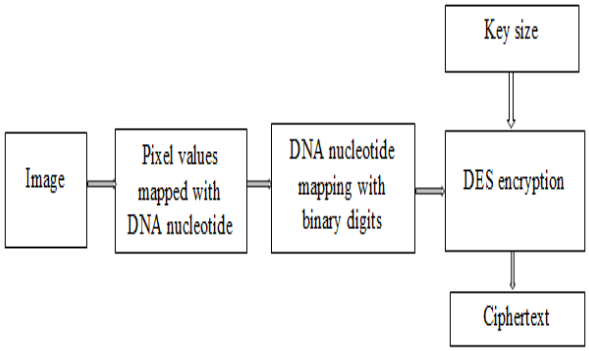

Fig. 3 DNA computing based image encryption algorithm

V. SIMULATION RESULTS

The proposed DNA computing based text and image encryption algorithm has been implemented by using MATLAB software and compares the performance in terms of communication and computational overheads.

DNA computing based text encryption algorithm

DNA computing based text encryption algorithm has been implemented by using different plaintext block size and constant secret key size = 48 bits. Simulated results provide the processing time taken to execute the DNA computing based DES encryption algorithm for key size = 48 bits and different block size of plaintext as shown in table 5 and table 6. Simulation results shows the variation of processing time with respect to different block size of plaintext and it proves that when size of the plaintext increases, processing time also increasing as shown in Fig.5.

Table 4: DNA computing based text encryption (Key size = 48 bit)

Plaintext (Block Size)	Processing time (ms)	
	DES Encryption & Decryption Algorithm	Proposed DNA computing based Encryption Algorithm
64	79	119
128	106	188
256	156	254
512	264	373
1024	407	460
2048	800	850

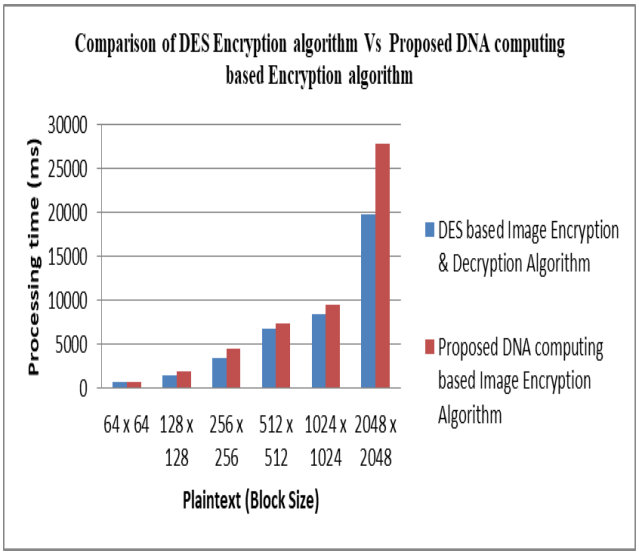

Fig. 4.Comparison of DES Encryption algorithm Vs Proposed DNA computing based Encryption algorithm

Table 5: Example of DNA computing based encryption algorithm

Letter	ASCII value	DNA Nucleotide	Binary values
H	72	TTCAGC	010110001110
E	69	GATATG	110001000111
L	76	TTCGAT	010110110001
L	76	TTCGAT	010110110001
O	79	TTCATG	010110000111

DNA computing based image encryption algorithm

DNA computing based image encryption algorithm has been implemented by using different size of the image and keeping constant secret key size = 48 bits. Simulated results provide the processing time taken to execute the DNA computing based image encryption algorithm for key size = 48 bits and the different size of an image as shown in table 6. As shown in Fig.6 and Fig.7, simulated results provide that if the size of the image increases, processing time also gets increase.

Table 6: DNA computing based image encryption algorithm (Key size = 48 bit)

Size of Image	Processing time (ms)	
	DES Image Encryption & Decryption Algorithm	Proposed DNA computing based Image Encryption Algorithm
64 x 64	689	697
128 x 128	1356	1838
256 x 256	3363	4388
512 x 512	6729	7373
1024 x 1024	8407	9460
2048 x 2048	19774	27850

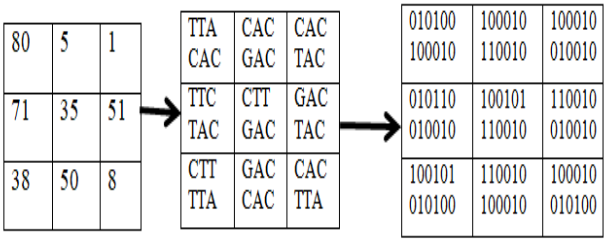

Fig.6 Example for DNA computing based image encryption algorithm

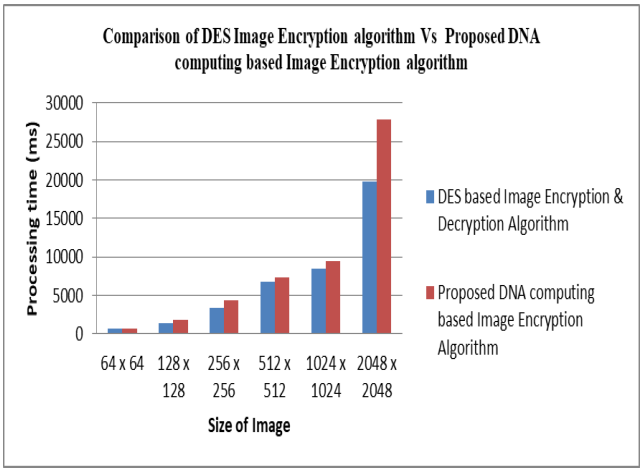

Fig. 5Comparison of DES Image Encryption algorithm Vs Proposed DNA computing based Image Encryption algorithm

VI. CONCLUSION

An efficient and secured data transmission using hybrid DNA mapping techniques with DES cryptographic technique. It proves that mapped DNA strands had the ability to handle numerous amounts of data and greater level of security.Simulation results shows the processing time for encrypting the mapped DNA strands and conversion of plaintext into ASCII values using the predefined table. Proposed idea enables the user to store the huge amount of encrypted data and safe transmission of data with less communication complexity.

In future, proposed idea will be implemented using different cryptographic algorithm and gives the proof of work by using attacks. Also, it will be helpful for image encryption algorithm in military two way communication system.

REFERENCES

1. L. Li, G. Wen, Z. Wang and Y. Yang, "Efficient and Secure Image Communication System Based on Compressed Sensing for IoT Monitoring Applications," in *IEEE Transactions on Multimedia*. Vol. 10, no. 9, pp. 1520- 9210, June 2019.
2. M. Rajput, M. Deshmukh, N. Nain and M. Ahmed, "Securing Data Through Steganography and Secret Sharing Schemes: Trapping and Misleading Potential Attackers," in *IEEE Consumer Electronics Magazine*, vol. 7, no. 5, pp. 40-45, Sept. 2018.
3. A. A. Pammu, W. Ho, N. K. Z. Lwin, K. Chong and B. Gwee, "A High Throughput and Secure Authentication-Encryption AES-CCM Algorithm on Asynchronous Multicore Processor," in *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 4, pp. 1023-1036, April 2019.
4. A. N. Bikos and N. Sklavos, "Architecture Design of an Area Efficient High-Speed Crypto Processor for 4G LTE," in *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 729-741, 1 Sept.-Oct. 2018.
5. R. Shahzadi, S. M. Anwar, F. Qamar, M. Ali and J. J. P. C. Rodrigues, "Chaos Based Enhanced RC5 Algorithm for Security and Integrity of Clinical Images in Remote Health Monitoring," in *IEEE Access*, vol. 7, pp. 52858-52870, April 2019.
6. S. Sun, "A Novel Hyperchaotic Image Encryption Scheme Based on DNA Encoding, Pixel-Level Scrambling and Bit-Level Scrambling," in *IEEE Photonics Journal*, vol. 10, no. 2, pp. 1-14, April 2018, Art no. 7201714.
7. A. Alhothaily, C. Hu, A. Alrawais, T. Song, X. Cheng and D. Chen, "A Secure and Practical Authentication Scheme Using Personal Devices," in *IEEE Access*, vol. 5, pp. 11677-11687, 2017.
8. X. Zhang, Z. Zhou and Y. Niu, "An Image Encryption Method Based on the Feistel Network and Dynamic DNA Encoding," in *IEEE Photonics Journal*, vol. 10, no. 4, pp. 1-14, Aug. 2018, Art no. 3901014.
9. O. Günlü, K. Kittichokechai, R. F. Schaefer and G. Caire, "Controllable Identifier Measurements for Private Authentication With Secret Keys," in *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8, pp. 1945-1959, Aug. 2018.
10. Y. Wang, Q. Han, G. Cui and J. Sun, "Hiding Messages Based on DNA Sequence and Recombinant DNA Technique," in *IEEE Transactions on Nanotechnology*, vol. 18, pp. 299-307, August 2019.
11. X. Wang, Y. Hou, S. Wang and R. Li, "A New Image Encryption Algorithm Based on CML and DNA Sequence," in *IEEE Access*, vol. 6, pp. 62272-62285, November 2018.
12. L. Lu *et al*., "Lip Reading-Based User Authentication Through Acoustic Sensing on Smartphones," in *IEEE/ACM Transactions on Networking*, vol. 27, no. 1, pp. 447-460, Feb. 2019.
13. S. Vhaduri and C. Poellabauer, "Multi-Modal Biometric-Based Implicit Authentication of Wearable Device Users," in *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 12, pp. 3116-3125, Dec. 2019.
14. H. Lin, "Traceable Anonymous Authentication and Key Exchange Protocol for Privacy-Aware Cloud Environments," in *IEEE Systems Journal*, vol. 13, no. 2, pp. 1608-1617, June 2019.
15. C. Shouqi, L. Wanrong, C. Liling, S. Qing and H. Xin, "An Improved Anonymous Authentication Protocol for Location-Based Service," in *IEEE Access*, vol. 7, pp. 114203-114212, July 2019.
16. H. Wang, D. Guo, Q. Wen and H. Zhang, "A Robust Authentication Scheme for Multiple Servers Architecture," in *IEEE Access*, vol. 7, pp. 111222-111231,August 2019.
17. X. Liu and R. Zhang, "A Robust Authentication Scheme With Continuously Updated Information for Vehicular Sensor Networks," in *IEEE Access*, vol. 6, pp. 70473-70486, November 2018.
18. M. R. Asaar, M. Salmasizadeh, W. Susilo and A. Majidi, "A Secure and Efficient Authentication Technique for Vehicular Ad-Hoc Networks," in *IEEE Transactions on Vehicular Technology*, vol. 67, no. 6, pp. 5409-5423, June 2018.
19. J. Cui, L. Wei, J. Zhang, Y. Xu and H. Zhong, "An Efficient Message-Authentication Scheme Based on Edge Computing for Vehicular Ad Hoc Networks," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 5, pp. 1621-1632, May 2019.
20. H. Tan, D. Choi, P. Kim, S. Pan and I. Chung, "Comments on "Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks"," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 7, pp. 2149-2151, July 2018.
21. L. Fridman, S. Weber, R. Greenstadt and M. Kam, "Active Authentication on Mobile Devices via Stylometry, Application Usage, Web Browsing, and GPS Location," in *IEEE Systems Journal*, vol. 11, no. 2, pp. 513-521, June 2017.
22. Z. Mehmood, A. Ghani, G. Chen and A. S. Alghamdi, "Authentication and Secure Key Management in E-Health Services: A Robust and Efficient Protocol Using Biometrics," in *IEEE Access*, vol. 7, pp. 113385-113397, August 2019.
23. Q. Ma, L. Xing and L. Zheng, "Authentication of Scalable Video Coding Streams Based on Topological Sort on Decoding Dependency Graph," in *IEEE Access*, vol. 5, pp. 16847-16857, August 2017.
24. M. Shahzad, A. X. Liu and A. Samuel, "Behavior Based Human Authentication on Touch Screen Devices Using Gestures and Signatures," in *IEEE Transactions on Mobile Computing*, vol. 16, no. 10, pp. 2726-2741, 1 Oct. 2017.
25. K. Shim, "Comments on "A Cross-Layer Approach to Privacy-Preserving Authentication in WAVE-Enabled VANETs" by Biswas and Mišić," in *IEEE Transactions on Vehicular Technology*, vol. 66, no. 11, pp. 10588-10589, Nov. 2017.

AUTHORS PROFILE

A. Vyasa Bharadwaja, working as an assistant professor in GIET Autonomous College of Engineering & Technology, Rajahmundry, Andhrapradesh**.** He completed his B.E from Anil Neerukonda Institute of Technology and M.Tech in VIT University, Chennai. He is currently researching at Sathyabama Institute of Science and Technology, Chennai for the past three years. He has a total of 5 years of teaching and research experience.

Dr. V. Ganesan, is currently working as Asst Professor in Dept of Electronics and Telecommunication Engineering at Sathyabama Institute of science and technology, Chennai. He received his PhD from Sathyabama University, Chennai on 25th April 2015 he is currently working as faculty of Electronics Engineeringin Sathyabama Institute of science and technology. He received his M.Sc. degree in Physics and M.E. Applied Electronics from Sathyabama University, Chennai in 2004 and 2007 respectively. His research interest focuses mainly on VLSI. He has published papers in international and national level Journals & IEEE conferences. Most of the papers are in the web of science and Scopus indexed publications.