HYBRID CRYPTOSYSTEM WITH DNA BASED KEY FOR WIRELESS SENSOR NETWORKS

Monika Poriye and Shuchita Upadhyaya

[1] Department of Computer Science and Applications, Kurukshetra University, Kurukshetra, 136118, Haryana, India

ABSTRACT

A number of various techniques have been already developed for providing security in sensor networks. It may be anticipated that these techniques provide less secure sensor network which has numerous adverse effects associated with them. Thus there is a sufficient scope for improvement of secure electronic communication, as the proficiency of attacks is growing rapidly in wireless sensor networks. DNA steganography is a technique of covered writing, which provides secure system in sensor network to some extent. Steganography is more effective over cryptography as later one only conceals information but steganography obscures the information, as well as camouflage the data to various attackers. DNA steganography is an inventive approach to reduce the popularity of public key cryptography over the wireless sensor networks. In the proposed work, a secret key is introduced which is purely based on DNA sequence named as DNA stego key and is only known to sender and receiver. This DNA stego key is used to hide information and is stored in a carrier. The proposed technique is implemented using java to verify its correctness.

KEYWORDS

Wireless sensor networks, DNA Computing, DNA Steganography, DNA Cryptography, Stego & Hybrid Cryptosystem.

1. INTRODUCTION

Wireless sensor networks (WSNs) use small sensor nodes with restricted capacity to sense, gather, and broadcast information in different types of applications. Sensor networks may have so many types of sensors, such as low sampling rate magnetic, seismic, thermal, visual, infrared, acoustic, and radar, which is used to observe temperature, humidity, vehicular movement, lighting condition, pressure, soil makeup, etc. [1]. Wireless sensor networks have been used in many areas like military, agriculture and homeland security etc. Many sensor networks having crucial task, like in military applications, thus it is obvious that security requirements should be taken into account at the time of design of the sensor networks and hence to impart security in sensor networks become a prominent task. On comparing the sensor node with conventional desktop computers, several limitations are associated with sensor nodes such as limited processing power, storage capacity and less battery power. A significant amount of work has been carried out in the direction of security in sensor networks to overcome these limitations [2-5]. In wireless sensor networks Steganography is a remarkable research area which embeds the secret information into a carrier image so that information can't be perceived by the human visual system (HVS) [6]. Historical examples of steganography systems include the usage of grills which mask out all of an

DOI: 10.5121/ijwmn.2016.8602

image except the sensitive data, micro-photographs situated inside the larger images, unnoticeable inks, etc. The cryptographic studies [7] broadly consider the traditional steganography techniques to get low security although there is controversy whether the steganography is an encryption in consideration of the plaintext is not actually hided here but instead undercover within other carrier and there are plentiful different cases in which steganography techniques already been broken [8] [9]. However, it is a very popular technique due to its easiness in implementation. There are so many methods available for applying steganography.

One of the steganographic method embed supplementary data in 802.15.4 data packets that increases signal to noise ratio (SNR) which improves communication quality between sensor nodes, but an attacker can use this method by differentiating the signal at receiver site against the link quality[10]. Although various steganographic methods have been proposed for better memory utilization and security in wireless networks [11-13], there are few methods concerning DNA steganography.

With the growing awareness in industry and academia for sustainable development, data processing with large scale compressed data storage required in sensor networks. Researches show that DNA based technique truly resolves the storage and security related problems in sensor network systems.

In the past decade DNA has been used for cryptography and is an attractive domain which manifests huge data density. Two cryptographic techniques are prominent which are based on DNA strands. In first, steganography use DNA binary strands as a technique of data hiding. The second technique was based on graphical subtraction of binary gel-images which is used to calculate a molecular checksum and then it is combined with the first approach to give strength to conceal the information [14]. A chip-based DNA micro-array for 2D data input/output for hiding natural DNA and artificial DNA to encode the binary data [15], provide better security than previous one. DNA steganography with vigenere keys and primer sequences are used to secure data but the main weakness of this method is not to provide fully secure system [16]. In another method, oligonucleotides are used for carrying the encrypted message and incorporated it with a huge amount of background DNA which would be retrieved by two secret primers. The main disadvantage of this method, is the possibility of brute-force attack although the time required is much high [17].

In the proposed cryptosystem, DNA stego key is used as a session key for secure transmission of information in an encrypted form. Thus both steganography and cryptography are used here which enhance the security to large extents. Here section 2 provides a brief overview of DNA computing. The proposed security framework is presented in section 3. Section 4 shows the results implemented in java language and section 5 presents the conclusion with the future work in section 6.

2. DNA COMPUTING

DNA computing is an interdisciplinary field that uses DNA and molecular biology hardware, rather than conventional silicon-based computer technologies. In the early stages it was evolved by Leonard Adleman of the University of Southern California, in 1994[18] [19]. The main objective of DNA computing is to acquire a biological technique, where data are expressed using DNA strands [20].

By reviewing the DNA computing, it was found that DNA cryptography become a newly emerged technique. In this technique, the biological based knowledge is required since the DNA is used as carrier data. The huge density and uniformity of data in the DNA molecules are tested for authentication, encryption, integrity and other related cryptographic schemes. All cryptography method has its own merits; demerits and each one compete with another for its regular practices.

To persuade the efficiency of DNA techniques and the cryptographic achievements, the huge data density available in the DNA molecules, are extremely beneficial. The DNA computing is also called biological computing. And this DNA computing techniques promotes to the innovation of DNA cryptography. As known in the traditional cryptography methods, which developed with the betterment of technical science it had enormous demand in the 20th century and is still in process [21].
Coding system in DNA of all living beings is based upon four key components of the DNA-molecule i.e. adenine, guanine, cytosine and thymine, abbreviated A; G; C and T, respectively, which used as a suitable medium for data processing [22]. Distinct estimations show that a DNA-computer having one liter of fluid incorporating six grams of DNA could probably have a memory capacity of 3072 exabytes [23].

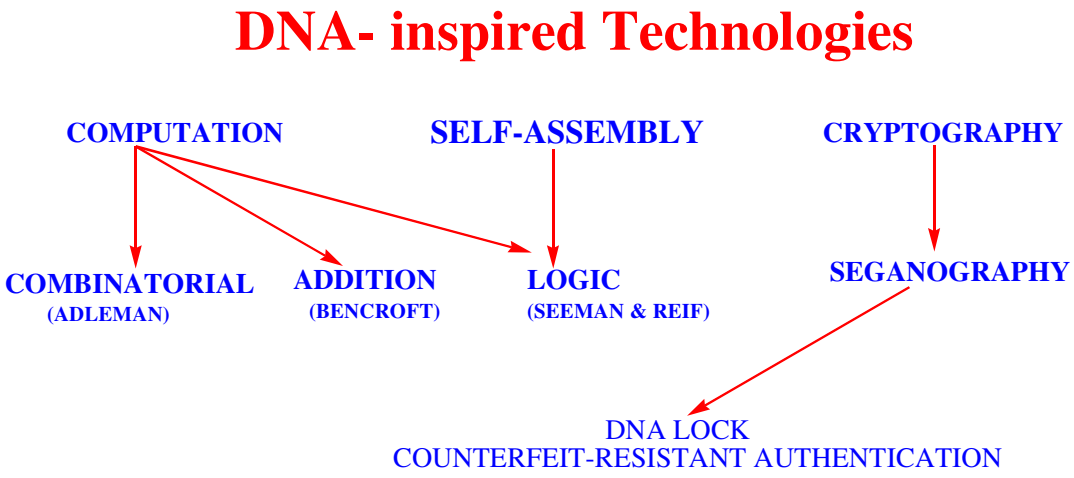


Fig. 1 DNA Technologies

Nowadays, with steganographic techniques, information security has been improved considerably, as in a steganographic system, the original data is not really encrypted but is hidded within the other data and combination of DNA with steganographic provides a new platform [24-26]. The theory of DNA steganography is based upon DNA sequences i.e. order of nucleotides within a DNA molecule. These nucleotides are linked to each other by phosphate groups. Scientist have done valuable work in the field of security associated with sensor network with DNA steganography, but still it may have some pitfalls which is the problem related to implementation of DNA system.

3. Proposed Work

3.1. Analysis

In the proposed method, DNA steganography is introduced for secure communication, which solves the security problem in wireless sensor networks. Here, a single key (DNA stego key) is used for communication between two parties. This DNA stego key consists of nucleotide bases i.e. Adenine, Guanine, Cytocine and Thymine, which is only known to sender and receiver before communication. A message is encrypted by using DNA stego key (a sequence of DNA i.e. ACGTTAACCC) with the usage of DES algorithm for the cryptographic process and then encrypted message is hidden within a digital image by steganography. Finally, stego image containing hidden data is used for transmission and at the receiver end the same process gets reversed to obtain the original message. The key feature of this technique is DNA stego key required for encryption and decryption. As the DNA of living being is unique, so it is not possible to guess or acquire the DNA sequence in any manner. Thus the system would be secure for communication. The following figure shows the framework of DNA based hybrid cryptosystem.

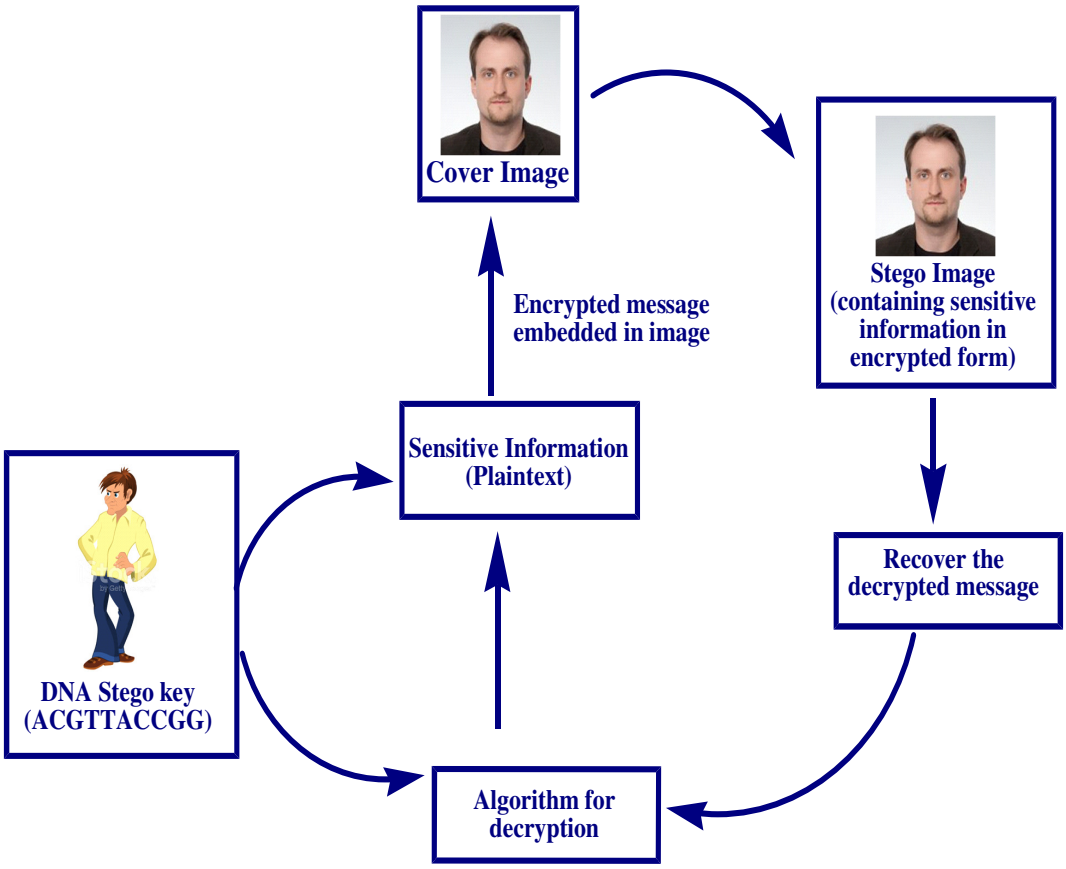


Fig. 2 DNA based Cryptosystem

3.2. Algorithm

Description process of DNA key

1. Take a DNA sequence ACGGTTCCAAAA (as a DNA key) of any living being.
2. Using DNA key, encrypt the sensitive data by using DES (Data Encryption Standards) algorithm. We get the data into encrypted form.

Embedding Process:

1. Create an array of cover image & store all pixels into that array.
2. Calculate the length of the encrypted message and let it be n. create a byte array b of size n.
3. Selects pixels of the cover image i.e. Red, Blue, Green & Alpha (transparency).(First 8 bits (0 to 7) of the pixel belong to Alpha value or the transparency value. The second 8 bits (8 to 15) represent red color, third 8 bits (16 to 23) represent green color and the last 8 bits (24 to 31) represent blue color.
4. Read the data from byte array b and segment 8 bit of characters into four parts.
5. Overwrite the LSB of Alpha, Red, Green & Blue components of pixel by segmented data bit.
6. Repeat steps 3 to 5 until byte array b become empty.
7. Reattain all the pixels of the cover image to form a stego image containing the encrypted data.

3.3. Algorithm (Extraction Process)

1.Extract the value n i.e. length of the message.
2. Read pixels from stego-image and store it in byte array b.
3. Pick up the pixels from array b & extract bit value from selected pixels.
4. Join these bits store it into any array c.
5. Repeat steps 3 &4 until n pixels are selected from b array.
6. Convert content of array c into string, the encrypted secret message.

4. Results and Implementation

JAVA language is used for the implementation of DNA based hybrid cryptosystem. Fig. 3 shows the results for encode an encrypted message. From this result it was inferred that the resulted stego image is completely secure for transmission because the DNA stego key which is used for encrypt the message is unique and cannot be notable by third party. For the encoded process ARGB system is used in which pixel data are stores in the form of alpha (transparency), red, green & blue. In ARGB system, first 8 bits (0 to 7) of the pixel concern with Alpha value. The second 8 bits (8 to 15) correspond to red colour, green colour represented by third 8 bits (16 to 23) and the blue colour represents the last 8 bits (24 to 31). If a change is made to the least significant bit of each parameter, the quality of the image will not be sacrificed as the change is very less i.e. the data bit stored every LSB of colour values which are 0,8,16 & 24 bit.

Here, the plain text is “harshvardhan singh” is encrypted by using DNA stego key and then encrypted data is covered in a carrier image. The carrier image which having the sensitive data is called stego image. Fig. 4 shows the decoded process in which the encrypted data can be acquired from the stego image which is then again processed for getting original information by decryption algorithm.

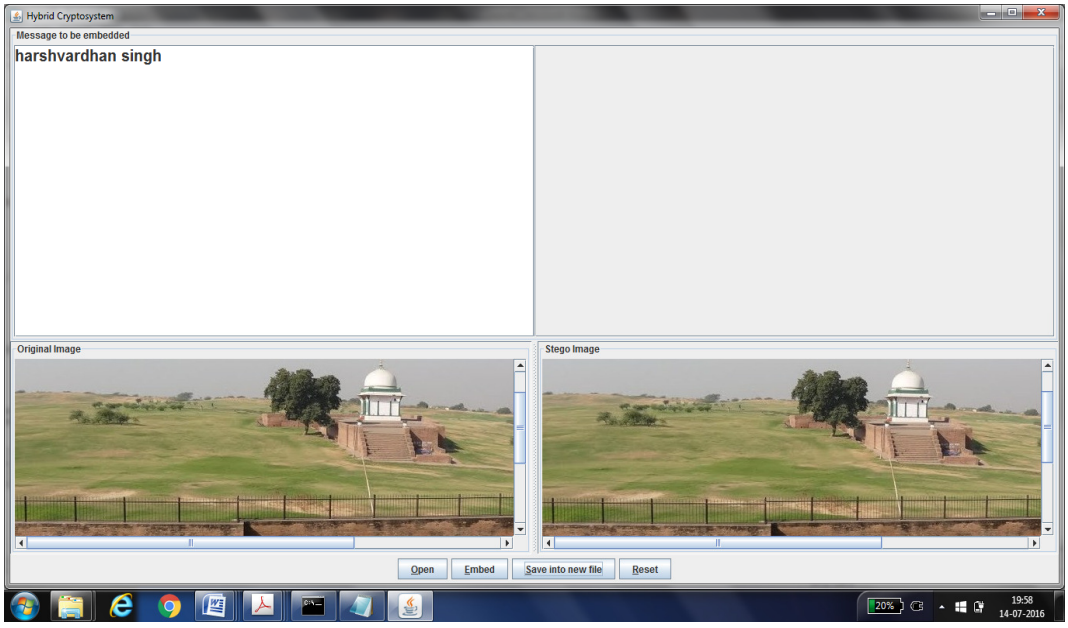
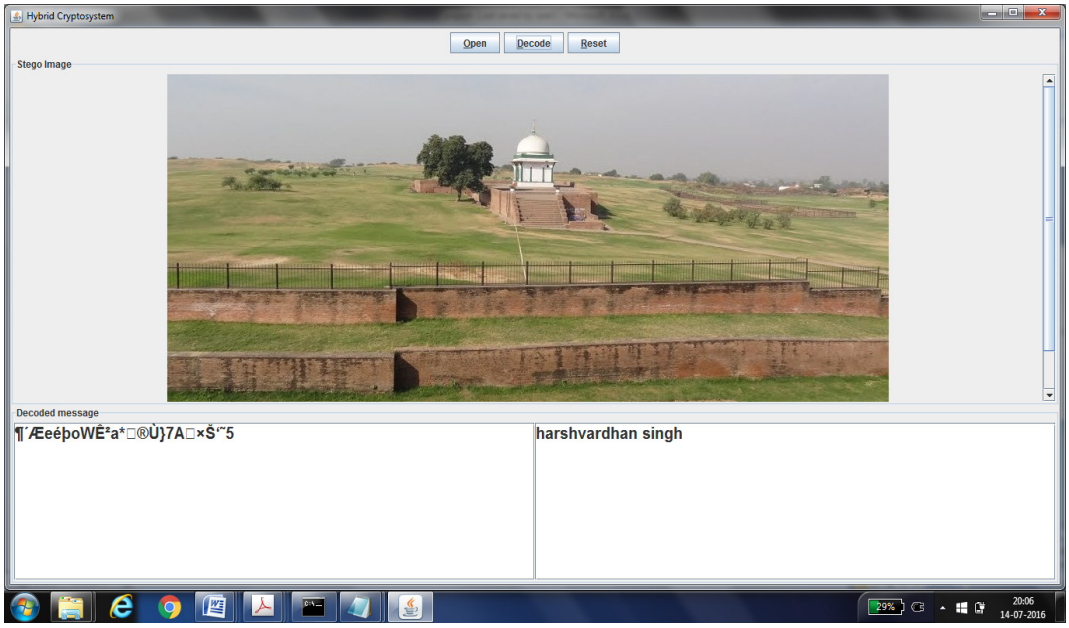


Fig. 3 Encode Process



5. CONCLUSION

DNA based key supports major applicability in DNA-based systems. For today's network, DNA based cryptographic algorithms provides satisfactory security and high performance in the applications of wireless sensor networks.

This technique shown that DNA based hybrid cryptosystem is a secure method for transmission of sensitive data by successful concealing and recovering. The length of a message depends upon the size of the image taken as carrier. It provides a very high level of security due to the usage of DNA stego key (a DNA sequence). Here, the sensitive data is encrypted with DNA stego key by applying DES algorithm. The cipher data is then hided inside a carrier image. In this work, DNA stego key is the attractive factor of the proposed framework which makes this cryptosystem totally secured.

6. FUTURE WORK

In our future research, we are going to apply compression technique before encrypted the sensitive data. By the use of compression algorithm more data can be hidden in the carrier image. Also, it will enhance the complexity with greater security. Finally, we are planning to compare performance measures of our algorithms with previous techniques by taking different parameters for wireless sensor networks.

ACKNOWLEDGEMENTS

The authors would like to thank everyone who offered support to this work and the publication of its results.

REFERENCES

[1] D. Estrin, R. Govindan, J. Heidemann, and S. Kumar, “Next century challenges: Scalable coordination in sensor networks,” in Proc. International Conf. Mobile Computing Networking, 1999, pp 263–270. doi: 10.1145/313451.313556.

[2] J. W. Gardner, V. Varadan, and O. Awadelkarim, Microsensors, MEMS and Smart Devices. New York: Wiley, 2001.

[3] H. Chan, A. Perrig, (2003) "Security and privacy in sensor networks," in Computer, IEEE Computer Society, Vol. 36, pp 103-105. doi: 10.1109/MC.2003.1236475.

[4] C. Karlof, D. Wagner, (2003) “Secure routing in wireless sensor networks: attacks and countermeasures,” Ad Hoc Networks, Vol. 1, pp 293-315. doi:10.1016/S1570-8705(03)00008-8.

[5] A. Abbasi, (2009) "Better Security for Wireless Sensor Networks," Future Networks, International Conference on, Bangkok, pp 100-103. doi: 10.1109/ICFN.2009.55.

[6] X. Du and H. h. Chen, (2008) "Security in wireless sensor networks," in IEEE Wireless Communications, Vol. 15, pp 60-66. doi: 10.1109/MWC.2008.4599222.

[7] D. Artz, (2001) "Digital steganography: hiding data within data," in IEEE Internet Computing, pp 75-80. doi: 10.1109/4236.935180.

[8] B. Schneier, (1996) “Applied Cryptography”, 2nd Edition, John Wiley.

[9] D. Kahn, (1967) “The Codebreakers: The Story of Secret Writing”, New York: Macmillan Pub. Comp.

[10] A. M. Mehta, S. Lanzisera, K. S. J. Pister, (2008)"Steganography in 802.15.4 wireless communication," 2nd International Symposium on Advanced Networks and Telecommunication Systems, Mumbai, pp 1-3.

[11] A. H. M. Kamal, (2013) “Steganography: Securing Message in wireless network” in International Journal of Computers & Technology, Vol. 4, pp 797-801.

[12] R. Vijayarajeswari, A. Rajivkannan, J. Santhosh, (2016) “A Simple Steganography Algorithm Based on Lossless Compression Technique in WSN. Circuits and Systems, Vol. 7, pp 1341-1351.

[13] A. Hassan, C. Bach, (2014) “Improving Security Connection in Wireless Sensor Networks” International Journal of Innovation and Scientific Research, Vol. 2, pp 301-307.

[14] A. Leier, C. Richter, W. Banzhaf, H. Rauhe, (2000)"Cryptography with DNA binary strands," Biosystems, Vol. 57, pp 13-22.

[15] A. Gehani, T. LaBean, J. Reif, (2004) "DNA-based Cryptography," Lecture Notes in Computer Science, Vol. 2950, pp 167-188.
[16] Z. Wang, X. Zhao, H. Wang, G. Cui, (2013) “Information Hiding Based on DNA Steganography” in Software Engineering and Service Science (ICSESS), 4th IEEE International Conference, pp 946-949.
[17] G. M. N. C. S. Gupta, "DNA Computing," 2001.
[18] V. I. Risca, (2001) “DNA-Based steganography” Cryptologia. Vol. 25, pp 37-49, DOI: 10.1080/0161-110191889761.
[19] L. M. Adleman, (1994) “Molecular computation of solutions to combinatorial problems,” Science, JSTOR, Vol. 266, pp 1021–1024.
[20] A. Martyn, G. Paun, G. Rozenberg, A. Salomaa, (2002) "Topics in the theory of DNA computing". Theoretical computer science Vol. 287, pp 3–38.
[21] G. Cui, C. Li, H. Li, X. Li, (2009) "DNA Computing and Its Application to Information Security Field," Fifth International Conference on Natural Computation, Tianjin pp 148-152. doi: 10.1109/ICNC.2009.27.
[22] Monika, S. Updhyaya, (2015) “Secure communication using DNA cryptography with secure socket layer (SSL) protocol in wireless sensor networks” Procedia Computer Science Vol. 70, pp 808-813. doi:10.1016/j.procs.2015.10.121.
[23] https://en.wikipedia.org/wiki/DNA_computing.
[24] M. Lu, X. Lai, G. Xiao, L. Qin, (2007) "Symmetric-key cryptosystem with DNA technology," Science China Information Sciences, Vol. 50, pp 324-333.
[25] C. T. Clelland, V. Risca, C. Bancroft, (1999) “Hiding messages in DNA microdots” Nature, Vol. 399, pp 533-534.
[26] Z. Wang, X. Zhao, H. Wang, G. Cui, (2013) "Information hiding based on DNA steganography," Software Engineering and Service Science (ICSESS), 4th IEEE International Conference on, Beijing, pp 946-949.