PERFORMANCE ENHANCEMENT IN VERIFIABLE SECRET USING ECC-DNA BPCS BASED STEGNO-CRYPTO FOR SECURITY

[1]Priya Jain, [2]Somesh Kumar and [3]Raj Kumar Goel
[1]M. Tech Student, [2]Assistant Professor
Department of Computer Science Engineering,
Noida Institute of Engineering & Technology, Greater Noida, U.P., India

Abstract: Steganography is the art of science of hiding information which is more useful in many social networks, digital media, and printing material. Many hiding algorithms are used to flourish the security level of the recent wireless multimedia system to protect the data from an attacker. The Cryptology is the learning of techniques for ensuring the privacy and verification of the data. PKE systems are safe only if the validity of the public-key is guaranteed. ECA (elliptic curve arithmetic) is used to grow a diversity of ECC systems plus key altercation, encryption and decryption. In this paper we suggest a new encryption algorithm Elliptic Curve over DNA and BPCS. This is an effective method, which delivers security for wireless communication and many more security application. In this study enhance the security level by the BPCS methods.

Keywords: Stegnography, BPCS, ECA (elliptic curve arithmetic)

I. INTRODUCTION:

These days more and more people are making use of internet to perform daily activities such as reading newspaper, searching information, online shopping, making bill payments and other activities than earlier. Though Internet brings different ways for helping end user, it also brings risk associated with it Making payment online, sending secure information over the web, using passwords and user ids for secure access are such deleterious works [1]. Therefore, steganography and cryptography is most important requirements for information protection in order to transmit information securely. Cryptography is a data hiding method for changing message is encoded into different form which is not understandable. There has been increase in number of online communication frauds; so it must be hide the very being of cognizance facts transmission must obscured [2]. cryptography and steganography together provides two level of security [3]. From many years a lot of research has been done to contrive new techniques and applications for encoding and decoding of data to be transferred, These algorithms can be enhanced by using DNA based computing method which provides better data security [4]. The DNA computing techniques because of its huge storage capacity and randomness allows the application to have large number of users [5, 9].

II. LITERATURE REVIEW:

Ushl et al. in proposed an encrypting technique which combines cryptography and steganography for data hiding. The message is encrypted two times for providing data security. The cipher text is hidden inside the image. It makes use of a reference matrix in order to select passwords depending on the image properties.

Xing Wang in applied computing theories in cryptography which will solve many hard problems successfully. He proposes a new way to use Cryptography with DNA Computing to transmit message securely and effectively. The RSA algorithm combined with DNA computing technique to encrypt and decrypt the message which requires more key size for providing same level of security as ECC.

Guangzhao Cui in can realize several security technologies such as encryption, Steganography, signature and authentication by using DNA molecular as information medium. He introduces the basic idea of DNA computing, and then discusses the information security technology in DNA computing.

Jiechen In this paper author used the random nature of DNA for creation the cryptographic system indestructible. They will be used for carbon nano tubes as a average for message broadcast. Plaintext messages also converted to cipher text by addition message with one time wads. The DNA arrangements act as one time pads. But this method is costly.

III. BPCS

The main principle of BPCS technique is that, the binary verifiable secret is divided into informative region and noise-like region. The secret data is hidden into noise-like region of the vessel verifiable secret without any deterioration. In our experiment, we used the BPCS Principle and experimented by using two verifiable secrets

i) Vessel verifiable secret of 512 x 512 size
ii) Secret verifiable secret of 256 x 256 sizes.

We performed this experiment for 3 different sets of verifiable secrets and calculated verifiable secret hiding capacity. In this module, BPCS-Steganography (Bit-Plane Complexity Segmentation Steganography) is a type of digital Steganography. Digital Steganography can hide confidential data (i.e., secret files) very securely by embedding them into some media data called "vessel data." The vessel data is also referred to as "carrier, cover, or dummy data". In BPCS-Steganography true color verifiable secrets (i.e., 24-bit color verifiable secrets) are mostly used for vessel data.

IV. PROPOSED ECC-DNABPCS METHOD

ECC-DNABPCS hash purpose changes a big and variable-sized quantity of DNA information addicted to a single number value in instruction to be help for numerous bioinformatics examines. A sequence of experiments was leading on affectedly produced chromosome structures and organic DNA orders from NCBI site. Investigational consequences demonstration which is proposed technique is well-organized in creating exceptional keys without impacts. The proposed method ECC-DNABPCS for repetitive sequence explore not if explore segment-based arrangements and database applications. A relative speed investigation accompanied alongside other three hashing functions, MD-5, SHA-1 and SHA-256, presented considerable qualities of ECC-DNABPCS technique, specifically the speed and the output size. In instruction to attain a real and balanced result, all functions have been applied in the similar program design language (MATLAB) and stayed tested on a process or containing a 2.8 GHz computer. Every hash function produced 1000 hash ethics for the similar order (a small chromosome order of 20b), afterward the response time was dignified. Frequent group of hash ethics for the similar chromosome classification showed to be a composed test, permitting for precise quantity of dispensation time for each purpose independently.

V. RESULT AND DISCUSSION

The Elliptic curve cryptography is a method to PKC founded on the arithmetical construction of elliptic curves completed finite grounds [6]. One and only of the core assistances in assessment with SHA cryptology is that ECC offers the similar side by side of security providing by keys of smaller size. To extent the efficiency of the planned secure hash purpose with DNA method, it separated three collections of experimentations that measured the production variety, the consistency of hash values and information dispensation (sending and receiving). For vocabulary, we definite all probable values that can be reverted by ECC-DNABPCS function as a “area range”.

The proposed method is tested on different sets of cover verifiable secrets as well as messages. The best suited type of verifiable secret for DNA steganography is png or bmp file because both type of verifiable secret uses lossless compression. While applying DNA Steganography data will not be lost. Below shows the result of proposed approach

Figure 5.1: Input image for simulation

At the sender side, the input secret verifiable secret generates shares based on proposed algorithm which done in the first phase. At the receiver side, the extracted verifiable secrets can be processed to extract the covering verifiable secrets from the generated shares and the secret verifiable secrets can be retrieved by overlapping the shares in the correct order.

Figure 5.2: Encrypted data hide with 3 channels for cover image (DNA stego-HECC)

Figure 5.3: Hiding text file after encryption

Following figures shows mean square error, PSNR in db between base and proposed data which enhance the security level in the proposed data**.**

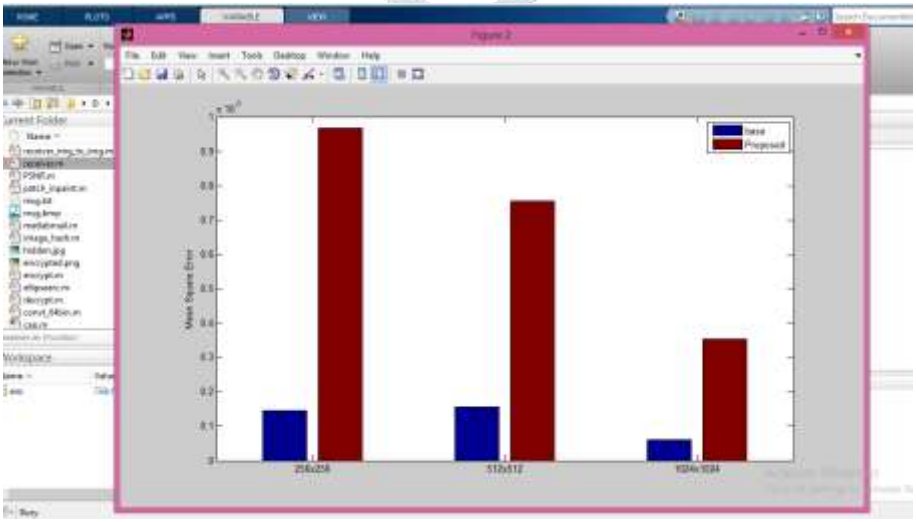

Figure 5.4: Mean square error between base and proposed (after technique)

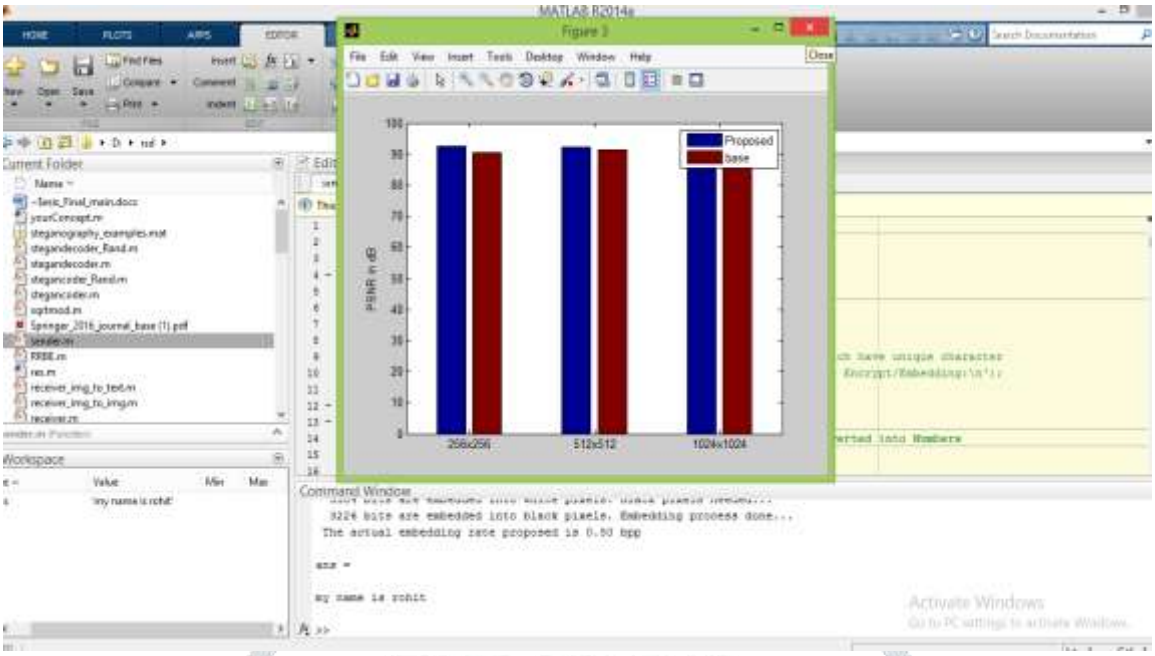

Figure 5.5: PSNR (peak signal noise ratio) between base and proposed (after technique)

VI. CONCLUSION

In current years, elliptic curve cryptography has increased extensive revelation and receipt, and has previously comprised in numerous safety values. In this Thesis, ECC-DNABPCS implementation proposed as a projecting for the comparatively new correction of cryptographic engineering. In specific, it will show that the necessities of effectiveness and security measured at the application stage technical features but also, meaningfully, complex level selections, ranging from finite field mathematics up to HECC method arithmetic. Elliptic and hyper elliptic curves are public key cryptographic protocols created on discrete logarithm problem. In this work we have conducted a study on DNA-ECCSH based primitives in the field of cryptography as with steganography with counter and block based verifiable secret matrix phase cryptographic primitives have been designed based on elliptic curve. Using our proposed approach it is proved to be easy and secure way to transfer information over simple mail transfer protocol. In HECCSH data is encrypted using HECC and is embedded in the verifiable secret using DNA Steganography to send through e-mail system over secure socket layer(SSL).

REFERNCES

[1]. Amritpal Singh, “An Improved LSB based Image Steganography Technique for RGB Images”, Electrical, Computer and Communication Technologies (ICECCT), 2015 IEEE International Conference on. IEEE, 2015.,pp 1-4.

[2]. Mehdi Hussain, “A Survey of Image Steganography Techniques”, International Journal of Advanced Science and Technology Vol. 54, May, 2013, pp 113-124.

[3]. T. Morkel, “AN OVERVIEW OF IMAGE STEGANOGRAPHY”, ISSA. 2005, pp 1-11

[4]. Usha, S., Kumar, G. A. S., and Boopathybagan, K., A secure triple level encryption method using cryptography and steganography, 0Computer Science and Network Technology (ICCSNT), International Conference,pp.

[5]. Bharti, P. and Soni, R., A New Approach of Data Hiding in Images using Cryptography and Steganography, International Journal of Computer Applications,Vol.58,No.18,pp1-5,2012.

[6]. Catherine Taylor Clelland. Hiding Messages in DNA Microdots. Nature, 399:533–534, June 1999.

[7]. Xing Wang and Qiang Zhang, “DNA computing-based cryptography”, in the IEEE proceeding of BIC-TA ’09. Fourth International Conference on Bio-Inspired Computing, Page(s): 1 - 3 , Oct. 2009.

[8]. Guozhen Xiao, Mingxin Lu, Lei Qin and XuejiaLai, “New field of cryptography: DNA cryptography”, in the Journal on Chinese Science Bulletin , vol.51, Issue 12 , pp.1413-1420, June 2006.

[9]. Guangzhao Cui, Cuiling Li, Haobin Li and Xiaoguang Li, "DNA Computing and Its Application to Information Security Field", in the IEEE proceedings of Fifth International Conference on Natural Computation, pp.148-152, June 2007.

[10]. R. Poornima, "AN OVERVIEW OF DIGITAL IMAGE STEGANOGRAPHY", (IJCSES) Vol.4, No.1, February 2013, pp 23-31.

[11]. Anil Kumar, "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique", IJARCSSE, Volume 3, Issue 7, July 2013, pp 363-372.

[12]. Shaveta Mahajan, "A Review of Methods and Approach for Secure Steganography", IJARCSSE, Volume 2, Issue 10, October 2012, pp 67-70.

[13]. Jasleen Kour, "Steganography Techniques –A Review Paper", International Journal of Emerging Research inn Management &Technology, Volume-3, Issue-5, May 2014, pp 132-135.

[14]. Andre Leier. Cryptography with DNA Binary Strands. Bio Systems, 57:13–22, April 2000.

[15]. Jie Chen. A DNA-based, bio-molecular cryptography design. In Circuits and Systems, 2003. ISCAS '03. Proceedings of the 2003 International Symposium on, volume 3, pages III–822-825 vol.3, May 2003.