ISSN No: - 2456 – 2165

Performance Enhancement in Security Using DNA-Eccsh Based Stego-Crypto for Secure Communication

Saurav Prasad
thapliyalsaurav@gmail.com
Department of Computer Science B.T.K.I.T. Dwarahat

Abstract—The most widely used techniques of secret writing are steganography and cryptography. Cryptography convert the plaintext into the cipher text. Steganography is a technique which is used to hide the information. Many steganography techniques are used to improve the security level for protect the information from an attacker. This paper describes the DNA steganography using elliptic curve cryptography secure hash technique, which improves the security level of image file and it also reduce the computational time.

Keywords— Steganography, Elliptic curve cryptography, secure hash algorithm, DNA.

I. INTRODUCTION

Steganography is a secret information hiding technique, which is used to prevent from an attacker. Existing techniques was also used to hide the information, like RSA, DES, and Triple DES. In these algorithms was the common disadvantages of the large key size, therefore the DNA computing is used with steganography and cryptography technique to provide a high level of security with less computational complexity.

DNA is a long linear polymer found in the core part of a cell.DNA is made up of several nucleotides. These nucleotides are used for mapping the plaintext. These are Adenine, Gunine, Cytosine and Thymine. Thus the proposed concept of an image encryption using DNA steganography using elliptic curve cryptography secure hash is a highly secured and reduces the computational time. The stego process generally involves placing a hidden message within some transport medium, called the carrier. The secret message is embedded within the carrier to form the stego medium. The use of the stego key may be employed for encryption of the hidden message and/or for randomization within the stego scheme. Image encryption algorithm aims to hide secret image/information in a larger carrier. Such that it does not discern the presence of the hidden image. It employees the advantage of both DNA crypto and stego. It attempts to hide an image in another image by converting it into DNA sequence using the nucleotides to binary conversion.

II. DNA STEGANOGRAPHY TECHNIQUE

DNA Nucleotide triplet	Alphabets	Numbers	DNA Nucleotide triplets
AAA	A	0	CAC
AAT	B	1	TAC
ATT	C	2	AGC
ATG	D	3	CTT
ACT	E	4	CGG
AGT	F	5	GAC
GCT	G	6	GAT
GGA	H	7	TTA
ACG	I	8	ATG
GAT	J	9	TTA
GCC	K		
ACC	L		
AGA	M		
GGT	N		
GTA	O		
CTT	P		
AGT	Q		
GTG	R		
GCG	S		

Table1.Characters to nucleotide triplet conversion

In DNA steganography technique we convert the image pixels (3*3) into DNA nucleotides bases of characters to nucleotide triplet conversion table.

After converting the pixel value of the image in the nucleotides we convert the DNA nucleotides into the binary digits. Which are represented as-

Nucleotide	Binary equivalent
A	00
C	01
G	10
T	11

Nucleotide to binary conversion table

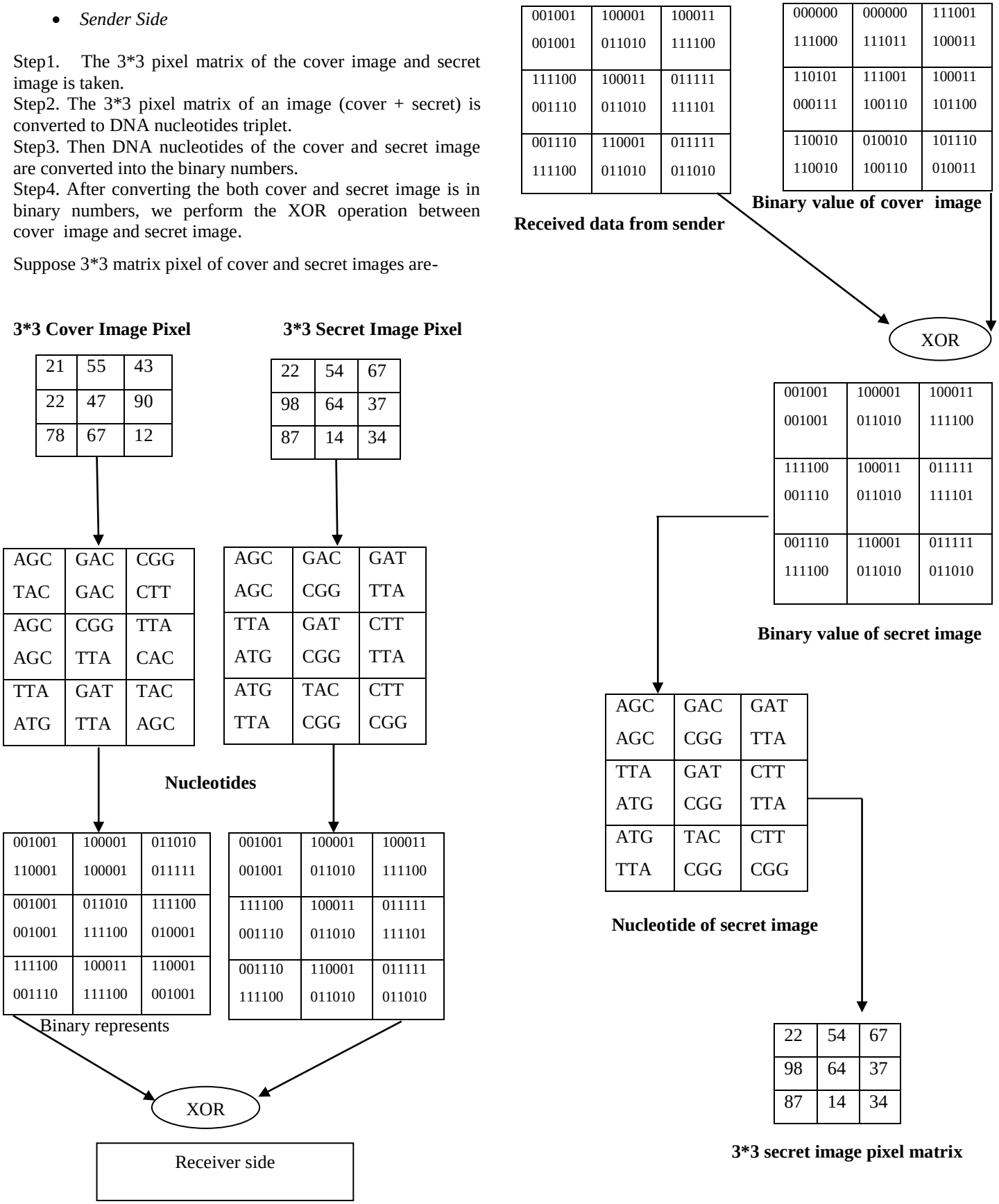
ISSN No: - 2456 – 2165

A. Steps in DNA steganography process

- *Sender Side*

Step1. The 3*3 pixel matrix of the cover image and secret image is taken.
Step2. The 3*3 pixel matrix of an image (cover + secret) is converted to DNA nucleotides triplet.
Step3. Then DNA nucleotides of the cover and secret image are converted into the binary numbers.
Step4. After converting the both cover and secret image is in binary numbers, we perform the XOR operation between cover image and secret image.

Suppose 3*3 matrix pixel of cover and secret images are-



21	55	43
22	47	90
78	67	12

22	54	67
98	64	37
87	14	34

AGC TAC	GAC GAC	CGG CTT
AGC AGC	CGG TTA	TTA CAC
TTA ATG	GAT TTA	TAC AGC

AGC AGC	GAC CGG	GAT TTA
TTA ATG	GAT CGG	CTT TTA
ATG TTA	TAC CGG	CTT CGG

001001 110001	100001 100001	011010 011111
001001 001001	011010 111100	111100 010001
111100 001110	100011 111100	110001 001001

001001 001001	100001 011010	100011 111100
111100 001110	100011 011010	011111 111101
001110 111100	110001 011010	011111 011010

001001 001001	100001 011010	100011 111100
111100 001110	100011 011010	011111 111101
001110 111100	110001 011010	011111 011010

000000 111000	000000 111011	111001 100011
110101 000111	111001 100110	100011 101100
110010 110010	010010 100110	101110 010011

AGC AGC	GAC CGG	GAT TTA
TTA ATG	GAT CGG	CTT TTA
ATG TTA	TAC CGG	CTT CGG

22	54	67
98	64	37
87	14	34

ISSN No: - 2456 – 2165

B. Receiver side

Receiver receive the cover and stego image, and perform the XOR operation to find the secret image.

Step1. The stego image is received by the receiver.

Step2. The XOR operation is performed by the receiver in between the cover image and stego image.

Step3. Then it convert in the nucleotides by using the binary to triplet form table.

Step4. Then in last receiver find the 3*3 image pixel matrix.

III. PREVIOUS TECHNIQUE

Previous technique was used with DNA steganography hyperelliptic curve cryptography, which was also used to provide the higher level of security. It uses 80 bit key size. HECC key size was small then ECC but it takes high processing time, that's why we used here elliptic curve cryptography secure hash technique, which provide less computational time to extract the original image or text.

IV. PROPOSED TECHNIQUE

Proposed technique provide higher level of security and we used here secure hash algorithm with elliptic curve cryptography which provide less computational time.

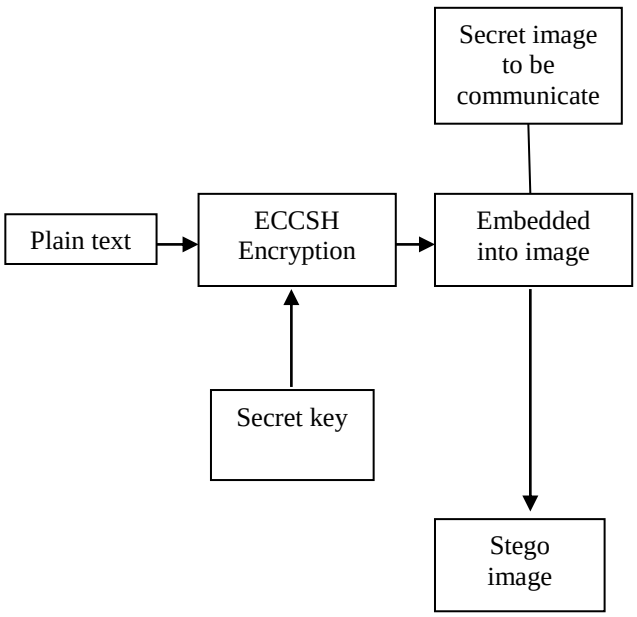
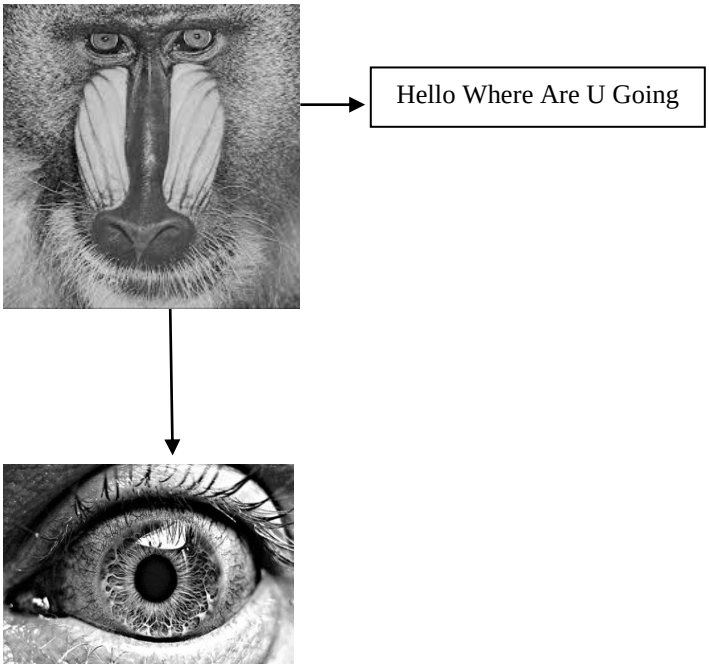


Fig. Hiding plaintext into secret image

In proposed technique after using the DNA Steganography we use the elliptic curve cryptography secure hash technique. Here we used 8*8 scrambled blocks and provide the hash keys for the particular location in the blocks where the data is store or hidden. It will be easy to find the location of the secure data where it is hidden.

Cover image

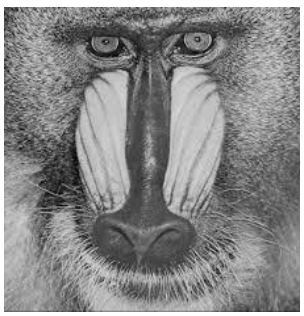
Hide Text Using ECCSH



Hide Secret Image

Fig 1. Hidden text/image with DNA-ECCSH

Suppose we have a cover image and we want to hide the image message inside the cover message. DNA- ECCSH techniques through it will be hide inside the cover image.



Stego Image

Receiver side- In the receiver side 8*8 scrambled blocks through receiver can easily extract the original information. Because user use in the particular blocks secure hash key where the data is hidden.

ISSN No: - 2456 – 2165

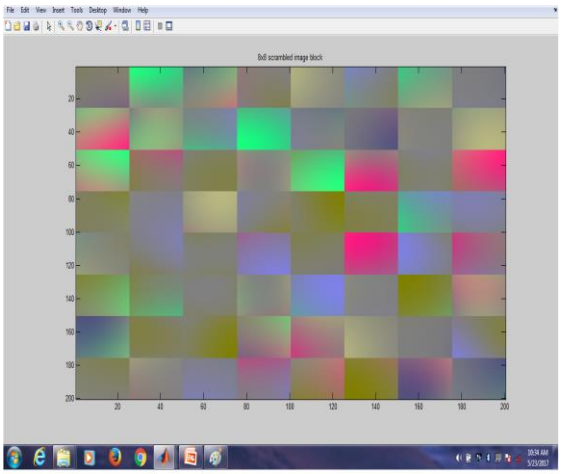


Fig.8*8 scrambled blocks

Fig. Extracting Image from the blocks

Hello where are u going

Extracting original text from the blocks

V. RESULTS

A. Time Complexity

DNA Steganography with elliptic curve cryptography secure hash provide less time complexity compare to the DNA Steganography with hyperelliptic curve cryptography. In our proposed approach base time complexity is 3.6582566 sec or in previous approach the time complexity was 5.9297479 sec for 3 channels.

B. Peak Signal Noise Ratio(PSNR):

Peak Signal Noise Ratio (PSNR) is a ratio between the largest and smallest possible values of the changeable quantity, we can say it is a ratio between original image and stego image. If the value of PSNR will be high the stego image will be secure. Here the PSNR value is high in proposed work. We represent the PSNR value in decibel.

$$\text{PSNR} = 10log_{10}\frac{255^2}{MSE}db$$

MAXf is the maximum signal value that exists in our known to be good image.

MAX f=2^8-1=255

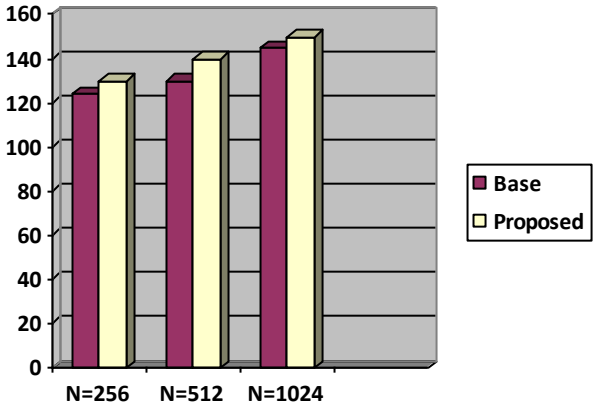


Fig. Peak Signal Noise Ratio

C. Mean Square Error (MSE)

The mean square error for our practical purpose allows us to compare the true pixels values of our original image to our degraded image. The MSE represents the average of the squares of the errors between our original image and stego image. The error is the amount by which the values of the original image image differ from the degraded image.

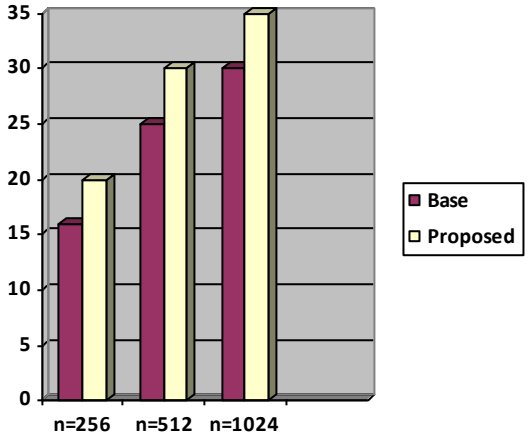


Fig. Mean Scqure Earror

$$MSE = [\frac{1}{m*n}]^2 \sum_{i=1}^{m} \sum_{j=1}^{n} (Xij - Xij')^2$$

VI. CONCLUSION

In this paper, a new technique used elliptic curve cryptography secure hash, This technique through user can easily find the particular location to extract the image. It provide higher level of security as well as it reduces the time complexity.

REFERENCES

[1]. G. Hamed et al., "DNA Based Steganography: Survey and Analysis for Parameters Optimization," in Applications of Intelligent Optimization in Biology and Medicine, Springer, 2015, ISSN: 1868–4394, pp. 47–89.
[2]. B. A. Mitras and A. K. Abo, "Proposed Steganography Approach using DNA Properties," International Journal of Information Technology and Business Management, ISSN: 2304–0777, vol. 14, Issue No. 1, pp. 96–102, June 2013.
[3]. M. R. N. Torkaman, N. S. Kazazi and A. Rouddini, "Innovative Approach to Improve Hybrid Cryptography by using DNA Steganography,"_International Journal of New Computer Architectures and their Applications (IJNCAA), ISSN: 2220–9085, vol. 2, Issue No. 1, pp. 224–235, 2012.
[4]. H. Kayarkar and S. Sanyal, "A Survey on Various Data Hiding Techniques and their Comparative Analysis," ACTA Technica Corviniensis, vol. 5, Issue No. 3, pp. 35–40, 2012.
[5]. A. Atito, A. Khalifa and S. Z. Rida, "DNA-based Data Encryption and Hiding using Playfair and Insertion Techniques," Journal of Communications and Computer Engineering, ISSN: 2090–6234, vol. 2, Issue No. 3, pp. 44–49, 2012.
[6]. A. K. Kaundal and A. K. Verma, "DNA based Cryptography: A Review," International Journal of Information and Computation Technology, ISSN: 0974–2239, vol. 04, Issue No. 7, pp. 693–698, 2014.
[7]. G. Hamed et al., "Hybrid Technique for Steganography Based on DNA with N-Bits Binary Coding Rule ," in 7th International Conference on Soft Computing and Pattern Recognition(SoCPaR), IEEE, 2015.
[8]. M. Skariya and M. Varghese, "Enhanced Double Layer Security using RSA over DNA based Data Encryption System," International Journal of Computer Science & Engineering Technology (IJCSET), ISSN: 2229– 3345, vol. 4, Issue No. 06, pp. 746–750, Jun 2013.
[9]. A. Siper, R. Farley and C. Lombardo, "The Rise of Steganography," Proceedings of Student/Faculty Research Day, CSIS, Pace University, May 6th, 2005.
[10]. M.M. Amin et al., "Information hiding using steganography," in Telecommunication Technology,2003, NCTT 2003 Proceedings, 4th National Conference, pp. 21–25, 2003.
[11]. M. K. Sharma, A. Upadhyaya and S. Agarwal, "Adaptive Stenographic Algorithm using Cryptographic Encryption RSA Algorithms," Journal of Engineering Computers and Applied Sciences, vol. 2, Issue No. 1, pp. 1–3, 2013.
[12]. T. Mandge and V. Choudhary, "A DNA encryption technique based on matrix manipulation and secure key generation scheme," in Information Communication and Embedded Systems (ICICES), pp. 47–52, 2013.
[13]. R. Terec et al., "DNA Security using Symmetric and Asymmetric Cryptography," International Journal on New Computer Architectures and Their Applications (IJNCAA), vol. 1, Issue No. 1, pp. 34–51, 2011.
[14]. B. Anam et al., "Review on the Advancements of DNA Cryptography,eprint arXiv:1010.0186, 2010.
[15]. Koblitz, "Elliptic curve cryptosystems," Mathematics of computation 48.177, 1987, pp. 203-209.
[16]. V. S. Miller, "Use of elliptic curves in cryptograph,." Advances in Cryptology—CRYPTO'85 Proceedings.
[17]. G. V. S. Raju and Rehan Akbani, "Elliptic curve cryptosystem and its applications," IEEE Systems, Man and Cybernetics, vol. 2, 2003.
[18]. M. Brown, et al., Software implementation of the NIST elliptic curves over prime fields. Springer Berlin Heidelberg, 2001.
[19]. H. Cohen, A. Miyaji, and T. Ono, "Efficient elliptic curve exponentiation using mixed coordinates," Advances in Cryptology—ASIACRYPT'98. Springer Berlin Heidelberg, 1998.
[20]. A. Miyaji, T. Ono, and H. Cohen, "Efficient elliptic curve exponentiation," Information and Communications Security, 1997, pp.282-290.
[21]. M. Rivain, "Fast and regular algorithms for scalar multiplication over elliptic curves," IACR Cryptology ePrint Archive, 2011, pp. 338.
[22]. P. Longa and C. Gebotys, "Efficient techniques for high-speed elliptic curve cryptography," Cryptographic hardware and embedded systems,CHES, 2010, pp. 80-94.