

{tag}

International Journal of Computer Applications

Foundation of Computer Science (FCS), NY, USA

[Volume 144](#)

-  
[Number 4](#)

Year of Publication: 2016

Authors:

Anjana Yadav, Pankaj Rakheja

10.5120/ijca2016910287

{bibtex}2016910287.bib{/bibtex}

## Abstract

Cryptography is a science of encrypting data to make it non readable and secure. But with time traditional cryptography is not that reliable because of multiple types of attacks on it. So, to make it effective it can be integrated with latest techniques available. Here in this paper a new mechanism has been proposed which integrates RSA and steganography with elliptical cryptographic technique along with biometric authentication as an addition security measure. This method provides good security with small key size too.

## References

1. V.Miller, "Uses of elliptic curves in cryptography", Advances in cryptology-crypto'85, pp.417-426, 1986.
2. N.Koblitz, "Elliptic curve cryptosystems," Mathematics of Computation, vol.48, no.177, pp.203-208, 1987.

3. Lifang Wu et al., "A novel key Generation Cryptosystem based on Face Features", Proc. of the IEEE on pp.1675-1678 on oct.2012.
4. Fabian et al., "Cryptographic key Generation from Voice", 2001, IEEE, pp.202-213.
5. Nikita Gupta et al., "Elliptic curve Cryptography for CIPHERING Images", 2015, IEEE.
6. Leca, Cristian-Liviu and Cristian-Iulian Rincu. "Combining Point Operations for Efficient Elliptic curve Cryptography Scalar Multiplication", Communications (COMM), 2014 10th International Conference on. IEEE, 2014.
7. Ali Makki Sagheer, "Elliptic curves Cryptography Techniques", 2012, IEEE.
8. Christina Thomas and Dr. K. Gnana Sheela, "Analysis of Elliptic curve Scalar Multiplication in Secure Communication" Proc. of the IEEE in Global conference on Communication Technologies, pp.623-627, 2015.
9. H. El-din, H. Ahmed, H. M. Kalash, and O. S. F. Allah, "An efficient chaos-based feedback stream cipher (ECBFSC) for image encryption and decryption", Informatica, vol. 31, pp. 121-129, 2007.
10. M. Salleh, S. Ibrahim, and I. F. Isnin, "Image encryption algorithm based on chaotic mapping", Journal Technologies, vol. 39(D), pp. 1-12, 2003.
11. I. A. Ismail, M. Amin, and H. Diab, "A digital image encryption algorithm based a composition of two chaotic logistic maps", International Journal of Network Security, vol. 11, no. 1, pp. 1-10, July 2010.
12. Williams Stallings, Cryptography and Network Security, Prentice Hall, 4th Edition, 2006.
13. Ali Soleymani, Md Jan Nordin, and Zulkarnain Md Ali, "A Novel Public key Image Encryption based on Elliptic curves over Prime Group Fields", Journal of Image and Graphics, vol. 1, no. 1, pp.43-49, March 2013, Engineering and Technology Publishing.
14. Matthew England "Elliptic Curve Cryptography" dissertation MSc Applied Mathematical Sciences, Heriot-Watt University, 2006.
15. N. F. Johnson, S. Katzenbeisser. "A Survey of steganographic techniques." in Information Hiding Techniques for Steganography and Digital Watermarking, S. Katzenbeisser and F. Petitcolas, Ed. London: Artech House, 2000, pp. 43-78.
16. M. Juneja and P.S. Sandhu. "Designing of robust image steganography technique based on LSB insertion and encryption." IEEE International Conference on Advances in Recent Technologies in Communication and Computing, 2009, pp. 302-305.
17. Manoj Prabhakar, "Elliptic Curve Cryptography in securing networks by mobile authentication", International Journal on Cryptography and Information Security, ISSN 2013.3304, vol 3 no 3, September 2013.
18. Ms. Manali Dubal, Ms. Aaradhana Deshmukh, "Achieving authentication and integrity using Elliptic Curve Cryptography architecture", International Journal of Computer Applications, ISSN 0975 – 8887, vol 69 no 24, May 2013.

## Index Terms

Computer Science

Security

## **Keywords**

Elliptic Curve Cryptography (ECC), Rivest Shamir Adleman (RSA), Biometric Encryption (BE).