Performance Analysis of DES Algorithm and RSA Algorithm with Audio Steganography

A. Gambhir and R. Arya

Delhi Technical Campus (GGSIP University) India

{a.gambhir@delhitechnicalcampus.ac.in; rajeev.arya.iit@gmail.com}

Abstract. In today's era data security is an important concern. It is most demanding issue now days. It is essential for people using online banking, e-shopping, reservations etc. The two major techniques that are used for secure communication are Cryptography and Steganography. Cryptographic algorithms scramble the data so that intruder will not able to retrieve it; however steganography covers that data in some cover file so that presence of communication is hidden. There are some techniques that integrate cryptography and steganography to provide multi layer security. This paper shows the comparison of such two techniques. These are 'RSA cryptography with audio steganography' and 'DES cryptography with audio steganography'. The coding has been done in MATLAB and stimulated results have been shown.

Keywords: ***Cryptography, steganography, data security, intruder, RSA, DES, audio steganography.***

1 Introduction

Internet users in India have increased enormously. In this digital era people are glued to internet. From money transfer to shopping, movie ticket booking to railway ticket booking, food ordering to bill payments all activities required transfer of confidential data like ATM pin, OTP, user ids etc. Information security is crucial now days. Cryptography and Steganography are the techniques used for information security. Cryptography [1] defines as the art and science of transforming data into a sequence of bits that appears as random and meaningless to a side observer or attacker. It comes from Greek words; crypto (secret) and graphy (writing or drawing) [2]. Cryptanalysis is the reverse process of cryptography. The process of converting message (plain text) into unreadable form (cipher text) is called encryption and the reverse process is called decryption. Steganography[2] also comes from the Greek steganos (covered) and graphy (writing or drawing). Steganography [1] can be defined as the hiding of information by embedding messages within other, seemingly harmless messages, graphics or sounds.. So far both the techniques are independently used to secure information. However there are some research papers available that merge both the techniques to provide multi layer security. In [17], RSA cryptography algorithm is integrated with audio steganography so that more level of security is maintained and risk of intruder is mitigated. In this paper, combination of 'DES cryptography algorithm and audio steganography' and combination of 'RSA cryptography algorithm and audio steganography' is implemented and results have been shown.

2 Related Work

2.1 RSA Algorithm [18]

It is developed by Ron Rivest, Adi Shamir and Len Adlemen in 1977. RSA algorithm is based on the fact that 'two prime numbers can be easily multiplied by cannot be easily factorize'. RSA is asymmetric key cryptographic algorithm i.e. keys used for encryption and decryption are different.

B. Iyer, S. Nalbalwar and R. Pawade (Eds.)
ICCASP/ICMMD-2016. Advances in Intelligent Systems Research.
Vol.137, Pp. 333-340.
© 2017- The authors. Published by Atlantis Press
This is an open access article under the CC BY-NC license (http://creativecommons.org/licens)es/by-nc/4.0/).

Procedure of RSA algorithm:

- Select two large prime numbers A and B (say) such that A is not equal to B.
- Determine K, by multiplying A and B.
- Determine L by formula L= (A-1)*(B-1).
- Choose a public key E such that E is not the factor of L.
- To select the private key D such that (D*E)modM=1.
- To determine cipher text (C): $C=M^{E}$modK.
- To determine plain text (M): $M=C^{D}$modK.

2.2 DES Algorithm [18]

DES is data encryption standard. Same key is used for encryption and decryption.

- 64 bit plain text is taken as input and 56 bit key and creates output 64 bit block.
- The plaintext goes through an initial permutation, (IP). It experiences an inverse final permutation at the closing stages (IP^{-1}).
- The plain text that passes through an IP to produce the permutated bit.
- 2 halves of permuted block are produced by IP - left plain text and right plain text.
- With its own keys, 16 rounds of encryption are done.
- The output of 16 rounds of encryption consists of 64 bits consist of plain text and key.

64 bit cipher text is produced at the last stage when the output undergoes inverse final permutation (IP^{-1}).

2.3 Audio Steganography

Steganography is an art of hiding data in some cover file. Cover file could be text, image, audio and video similarly Message can be plain text, image, audio or any type of file. A very well-liked method is LSB i.e. Least Significant Bit algorithm. In this LSB of cover file is replaced by bytes of data file.

3 Implementation

Case 1: RSA Algorithm and Audio Steganography

Message that has to be covered in an audio file is first converted in to cipher text by using RSA cryptography algorithm.

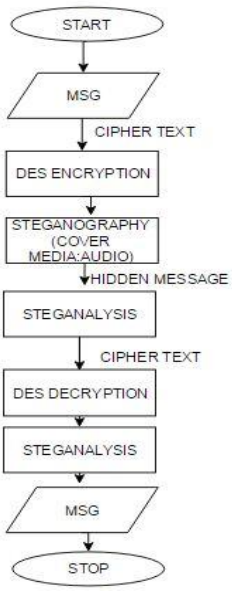

Fig. 3 (a). Flow Chart Case 1

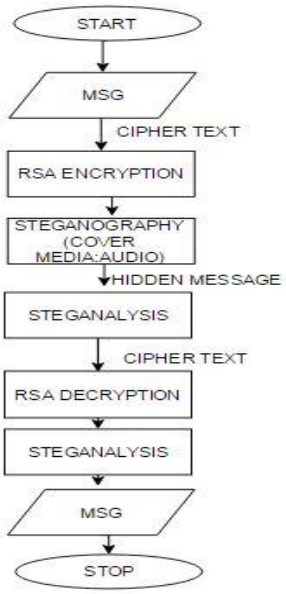

Fig. 3 (b). Flow Chart Case 2

Case 2: DES Algorithm and Audio Steganography

Message that has to be covered in an audio file is first converted in to cipher text by using DES cryptography algorithm.

3.1 Case 1

RSA Algorithm and Audio Steganography

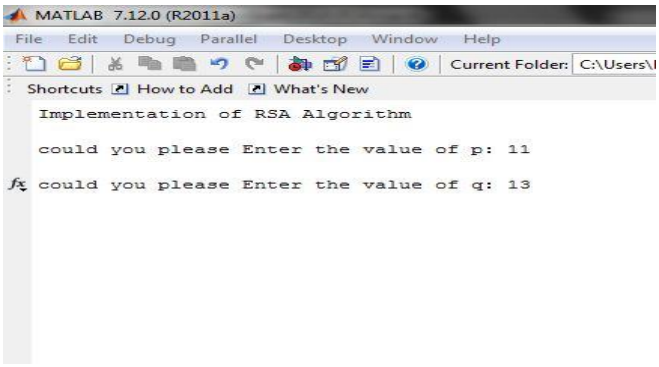

Fig. 3.1 (a). RSA Encryption Output

Here entered message is "**Galgotias University**" and value of p and q is taken as 11 and 13 respectively. The corresponding cipher text evaluated by RSA algorithm is "**38 59 4 38 45 129 118 59 80 98 39 33 79 62 49 80 118 129 121**" .

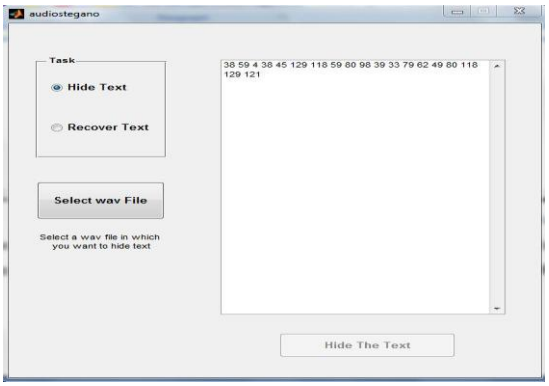

Fig. 3.1(b). GUI for Audio Steganography

Outcome of RSA algorithm (cipher text) is taken as input and hidden in an audio.

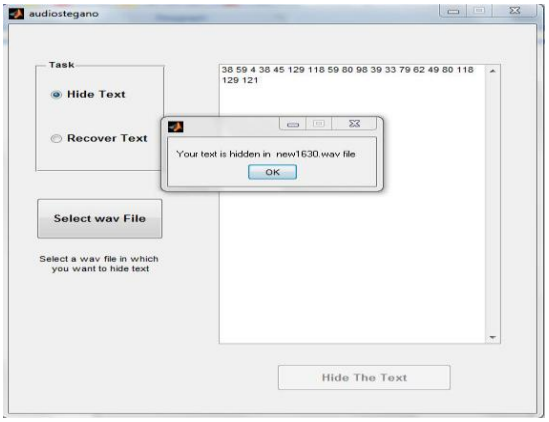

Fig. 3.1(c). GUI for Audio Steganography

To recover cipher text from audio, click recover text and select audio in which cipher text is hidden.

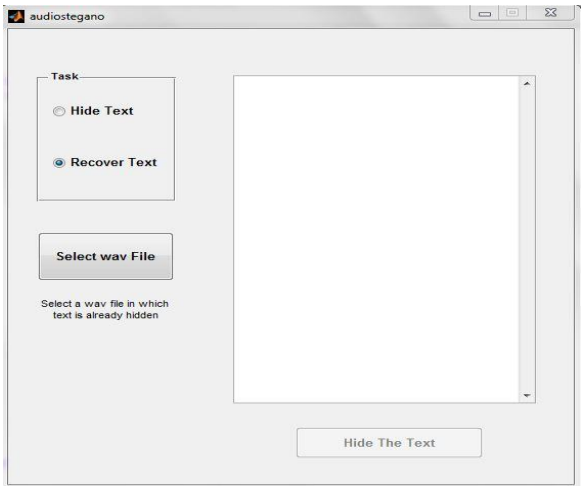

Fig. 3.1(d). GUI for Audio Steganography

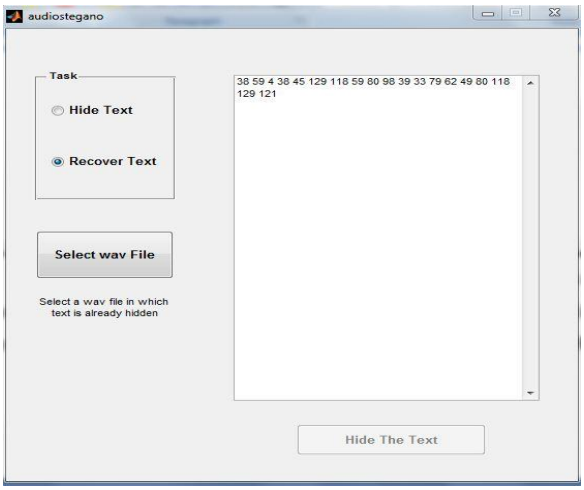

Fig. 3.1(e). GUI for Audio Steganography (Recover)

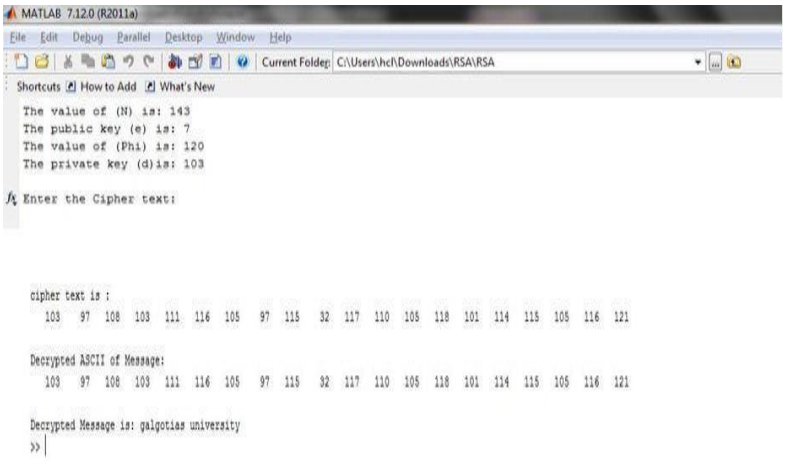

Fig. 3.1(f). RSA Decryption Output

Decrypted message is '**galgotias university'.**

3.2 Case 2

DES Algorithm and Audio Steganography

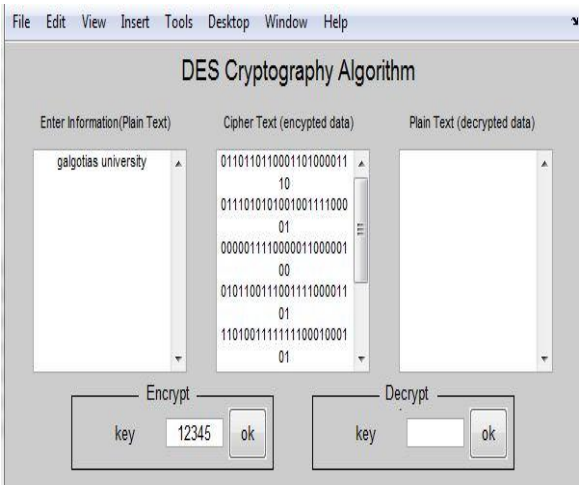

Fig. 3.2 (a). GUI for DES Cryptography Algorithm

Here entered message is again "**galgotias university**" and selected key is '12345'. Corresponding cipher text is obtained.

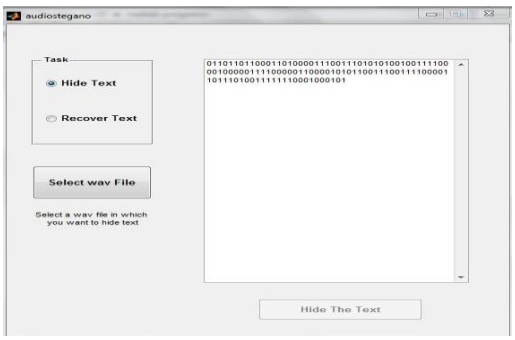

Fig. 3.2 (b). GUI for audio steganography

Cipher text obtained by DES algorithm is entered to hide it in cover (audio) file. The cipher text is saved in an audio 'new254'

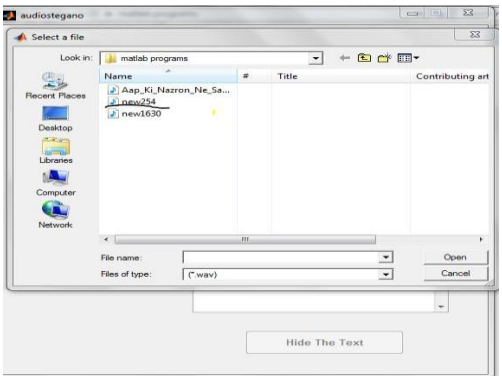

Fig. 3.2 (c). GUI for audio steganography

To recover cipher text from audio, recover text option is clicked and audio 'new254' is selected in which cipher text is hidden.

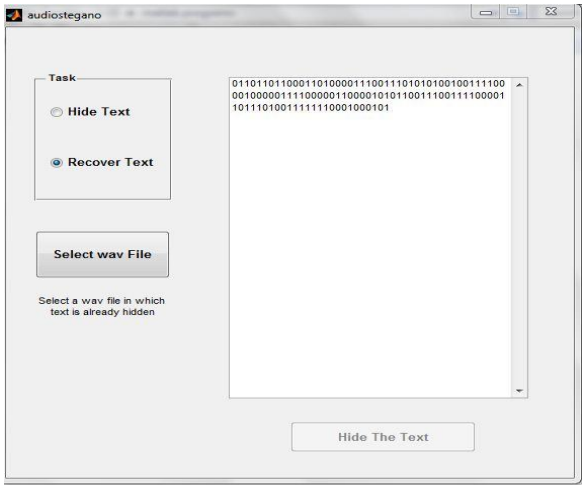

Fig. 3.2 (d). GUI for audio steganography

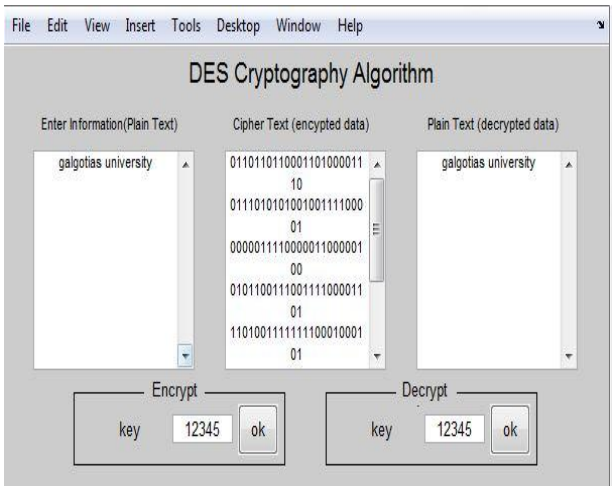

Fig. 3.2 (e). GUI for DES Cryptography Algorithm

The recovered cipher text is entered in GUI of DES Algorithm and same key is used to decrypt as DES is symmetric key algorithm. Same message i.e "**galgotias university**" is retrieved.

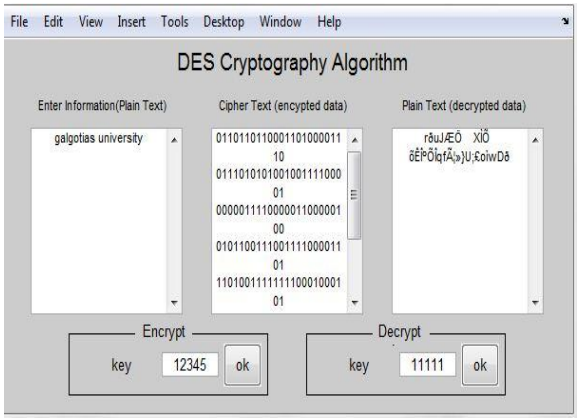

Fig. 3.2 (f). GUI for DES Cryptography Algorithm

If key does not match then message '**galgotias university**" will not retrieved.

4 Result Analysis

Result analysis of all audios; without data, with RSA cipher text & with DES cipher text.

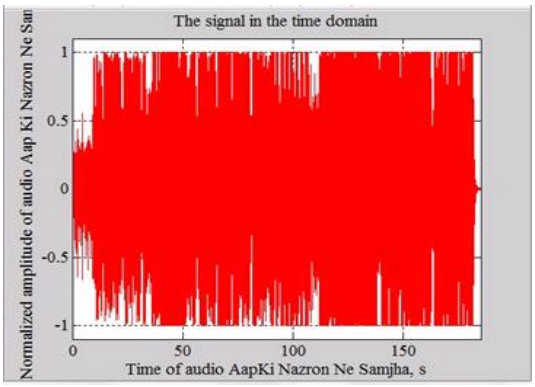

Fig. 4 (a). Representation of audio in time domain (without hidden data)

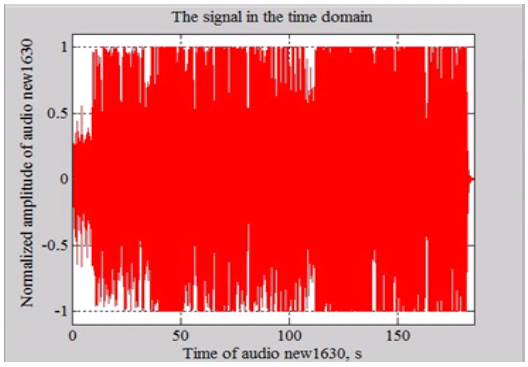

Fig. 4 (b). Representation of Audio in Time Domain (with Hidden RSA Cipher Text)

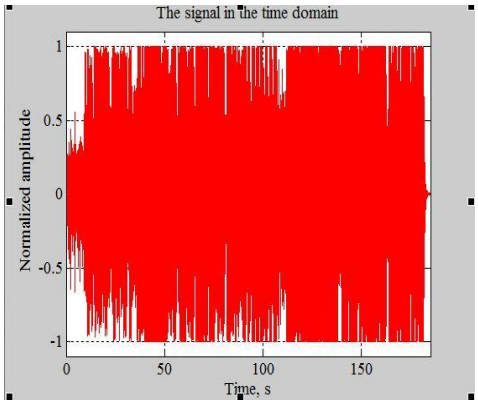

Fig. 4(c). Representation of Audio in Time Domain (with Hidden DES Cipher Text)

It can be observed from the Fig4 (a), Fig.4 (b) & Fig.4(c) that all the waveforms are identical. Means there is no change in characteristics of audio signal after embeds with data.

5 Conclusion

In this paper 'RSA cryptography algorithm with audio steganography' and 'DES cryptography algorithm with audio steganography' have been studied and implemented. Stimulated results have been shown. All three waveforms are identical. These techniques are better than individual techniques. The risk of unauthorized access is alleviated up to a certain extent by using these techniques. These techniques could be used in Banks, RAW agencies etc, where highly confidential data is transferred. There is a broad scope of future work such as a novel

algorithm can de design by amending RSA, DES or AES cryptographic algorithm, amendment can also be made in LSB embedding technique to make it robust.

References

[1] R Joseph and V Sundaram. : Cryptography and Steganography- A Survey, IJCTA, vol 2(3), 626-630. (2011)

[2] Liddell and Scott's Greek- English Oxford University Press.

[3] R. Krenn.: Steganography and steganalysis, An Article, Santa Barbara, California, January 2004, available from: http://www.krenn.nl/univ/cry/steg/article.pdf.

[4] Behrouz A. Forouzan.:Textbook on Data Communications & Networking , McGraw-Hill Forouzan Networking Series.

[5] A. Pye Pye and N.Min Tun.: A Novel Secure Combination Technique of Steganography and Cryptography IJITMC vol.2, no.1,pp 55-62, Feb 2014.

[6] K Harish and Anuradha.: Enhanced LSB Technique For Audio Steganography In: IEEE Computing Communication and Networking Technologies (ICCCNT) pp 89-95 IEEE Conference Publications ,(2012).

[7] M. Piyush and M. Paresh.: Visual Cryptographic Steganography in Images In: IEEE Computing Communication and Networking Technologies (ICCCNT) pp 1-6. IEEE Conference Publications ,(2010)

[8] S.Usha , K. Satish and K. Boopathybagan.: A Secure Triple Level Encryption Method Using Cryptography and Steganography. In: IEEE Computing Communication and Networking Technologies (ICCCNT) pp 1017-1020. IEEE Conference Publications, (2011).

[9] K. Manoj, U. Amit and A. Shalini. :Adaptive Steganographic Algorithm Using Cryptographic Encryption RSA Algorithms, JEC&AS: vol 2, no.1, pp 1-3 (2013).

[10] S. Arfan, S. Kirankumar, U. Vishal and V. Neeraj.: Audio Steganography and Security Using Cryptography ,IJETAE vol.4, issue 2, pp 317-319 (2014).

[11] S. Prakash Chandra, S Ramneet and K. Abhishek. : Enhance Security in Steganography with Cryptography, IJARCCE vol. 3 issue 3 , pp 5696-5699 (2014)

[12] G. Ankit , M. Anant.: CRYPTICSTEGANOGRAPHY: A New Data Hiding Technique with Multilayer Security System, IJIACS, ISSN 2347 – 8616 Vol 4,special issue pp 134-136 (2015)

[13] S. Roy and P. Venkateswaran.: Online Payment System using Steganography and Visual Cryptography. In: IEEE Student's Conference on Electrical, Electronics and Computer Science. pp.1-6 IEEE Conference Publications (2014)

[14] M. Mishra, G.Tiwari and A. Yadav.: Secret Communication using Public key Steganography. In: IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014) pp. 2389 - 2393 IEEE Conference Publications (2014)

[15] B Raja Rao, P. Anil Kumar, K Rama Mohana Rao and M. Nagu.: A Novel Information Security Scheme using Cryptic Steganography, IJCSE Vol. 1 No. 4, pp.327-332. (2010)

[16] A.Gambhir .: RSA Algorithm or DES Algorithm? (A Comparative Analysis) JECAS, Vol. 3, No.4, pp.27-29. (2014)

[17] Jayaram P, Ranganatha H R and Anupama H S.: Information Hiding Using Audio Steganography, IJMA Vol.3, No.3,pp 86-96. (2011)

[18] P. Deshpande, S.Sharma, P. Satteshkumar and A. Abhraham: Efficient Multimedia Data Storage in Cloud Environment. Informatica 39 (2015) 431–442.

[19] Prachi Deshpande, S.C.Sharma and Sateesh K. Peddoju, "Implementation of a private cloud: A case study", Advances in Intelligent Systems and Computing(Springer), vol. 259, pp. 635−647, 2013.

[20] Prachi Deshpande, S.C.Sharma, Sateesh K. Peddoju and A. Abraham, "Security threat analysis in Cloud computing environment", International Journal of System assurance and Management(Springer), In Press. doi: 10.1007/s13198-016-0525-0. Aug. 2016.

[21] Prachi Deshpande, S.C. Sharma and Sateesh K. Peddoju, "Security threats in cloud computing", IEEE International Conference on Computing, Communication and Automation (ICCCA−2015), Noida, India, May 2015, pp. 632−636.

[22] M. Patil, B. Iyer and R. Arya: Performance Evaluation of PCA and ICA Algorithm for Facial Expression Recognition Application. Proceedings of Fifth International Conference on Soft Computing for Problem Solving, 436, 2016:965-976.