Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 1, January 2017, pg.23 – 29

An Efficient Hybrid Approach for Secure Speech Cryptography

Er. Jyoti Sharma[1], Prof. Jyoti Rani[2]

M.Tech Research Scholar, GZSCCET, Bathinda[1]

Assistant Professor, GZSCCET, Bathinda[2]

ABSTRACT: The ability to protect and secure information is vital to the growth of electronic commerce and to the growth of the Internet itself. Many people need or want to use communications and data security in Different areas. In this paper a hybridization technique of cryptography is proposed for the better security of the data. The message is initially encrypted with DES and the keys of DES are encrypted with RSA then the hybrid of both DES-RSA is embedded inside the speech with help of genetic algorithm. Results of the technique provide a stronger security. The encryption time is also faster than the previous techniques as well as brute force attack to this technique is almost not possible.

KEYWORDS: DES, RSA, Hybridization, Genetic Algorithm, Neural network and SVM.

1. INTRODUCTION

Since, the growing demand for data safety, image encryption as well as decryption has turn out to be an essential research zone and also it has wide-ranging application visions. The arena of encryption is becoming quite significant in the current years. Image safekeeping is of extreme apprehension as various kinds of network attacks have turn out to be progressively more severe. Image encryption as well as decryption has apps in multimedia systems, telemedicine, internet communiqué, medical imaging, military communication, and so on [1].

Several image content encryption procedures have been recommended [1]. In the direction of making the information secure from numerous attacks as well as for the integrity of information we need to encode the information before it is conveyed or deposited. Government, hospitals, military, private business as well as financial institution, contracts with private images regarding their financial status, patient (in Hospitals), enemy positions (in defence), geographical areas (in research), product, and so on. Maximum of this data is now composed together and stowed on electronic PCs as well as communicated across system to further computer. If these personal images regarding nemesis locations, patient as well as geographical regions drop into the incorrect hands, than such a type of breach of security could possibly lead to declaration of war, wrong treatment and so on. Guarding secret images is a virtuous as well as legitimate necessity.

Cryptography is actually participating in a major purpose throughout data protection throughout applications managing inside a network environment. The idea enables individuals to ply their trade in an electronic form without having problems associated with deceit and also lies besides guaranteeing this sincerity in the information and also authenticity in the sender. They have be a little more important to our day-to-day lifestyle simply because 1000s of folks have interaction in an electronic form every day; through e-mail, e-commerce, ATM equipment, cell phones, and so forth. This particular geometric increase associated with data carried in an electronic form has produced elevated reliability with cryptography and also authentication by consumers [2]. Although secured connection has been around since then, the key supervision issue has averted that coming from popular software. The actual development associated with public-key cryptography has allowed large-scale circle associated with network of users that may communicate safely with one another even when that they never communicated before [3].

2. PROBLEM FORMULATION AND OBJECTIVES

2.1 Problem Formulation

Now a day's computers and mobile have become common medium for communication between people separated by long distances. This also make it security vulnerable to use those speech processing. A speech communications become more and more widely used and even more vulnerable, the importance of providing a high level of security is dramatically increasing. Earlier various methods has been implemented like RSA, Diffie method, AES, Hybrid method, But none of the method has provided good security results.

So, in proposed work, by applying cryptography on audio file security mechanism has been implemented. In proposed work the audio files security is enhanced by applying hybridization of DES-RSA and Genetic Algorithm. Then classification of files are compared using neural network (NN) as well as Support Vector Machine (SVM) Algorithm. This file holds meaning only to the person who has knowledge about the decryption process and access to the keys. Then results are evaluated using MSE and PSNR parameters to check the validation of the proposed method.

2.2 Objectives

1. To study and analyse the existing series based on the security of English speech processing as well as cryptography and to implement related ones.
2. To formalize the design principles into an algorithmic description that can be applied on English Speech Processing, implementation of proposed algorithm to predict better results.
3. To analyse the experimental results by embedding and extracting cryptography on speech processing using proposed algorithm which are by using RSA, DES, GA, SVM , NN algorithm.
4. To evaluate the performance of the proposed system using parameters like PSNR, and MSE.

3. RESEARCH METHODOLOGY

The methodology goes in the following manner:

Step 1 : First start with English speech words acquisition.
Step 2 : Then prepare database for the system.
Step 3 : After this pre-processing and data extraction process is applied to extract wave data.
Step 4 : Start cryptography process.
   a) Apply RSA algorithm
   b) Apply DES algorithm
   c) Apply RSA in addition to DES algorithm
Step 5 : Encrypt the speech message.
Step 6 : Apply Genetic Algorithm for optimization purpose.
Step 7 : Extract original speech word.
Step 8 : Classify between various speech using SVM
Step 9 : Valuate results using MSE and PSNR.

4. SIMULATION RESULT AND DISCUSSION

The implementation of proposed work is as following:

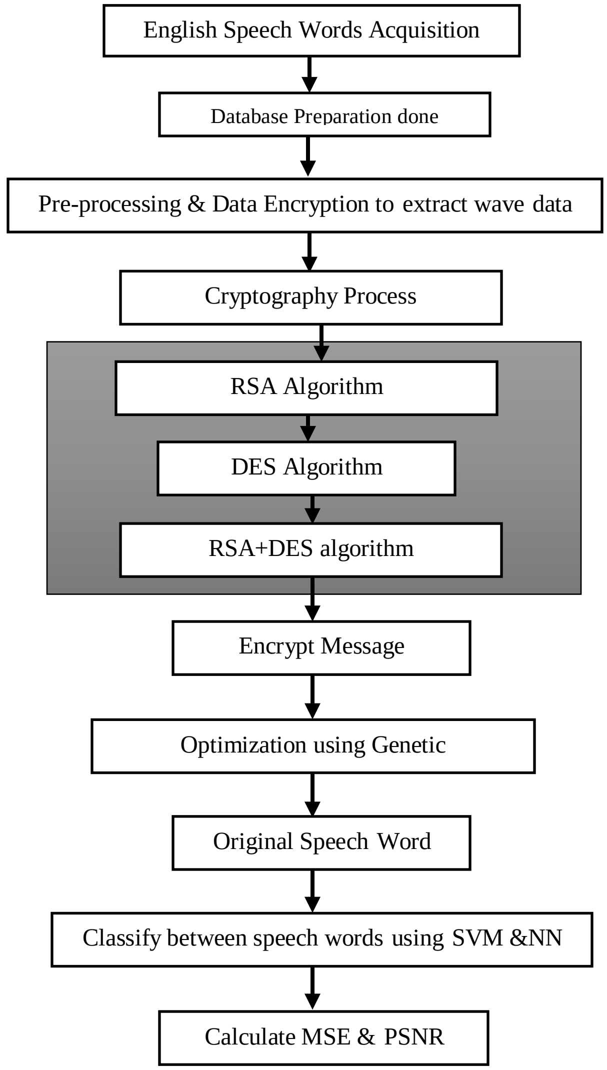
1. The speech has been converted into their equivalent crypted speech in order to provide more secured communication using the hybridization of RSA and DES methods.

2. This has been done using SVM and NN machine learning algorithms and then compilation and simulation algorithms applied with the help of MATLAB 2010a software.

3. After simulation we analyzed the result with help of various parameters like PSNR and MSE.

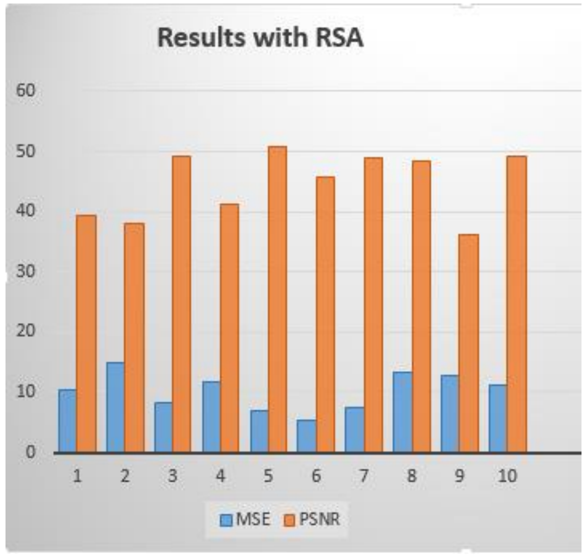
4. From result simulation it has been concluded that results obtained by hybridization of DES-RSA are better.

PROPOSED FLOWCHART



4.1 Result in case of RSA

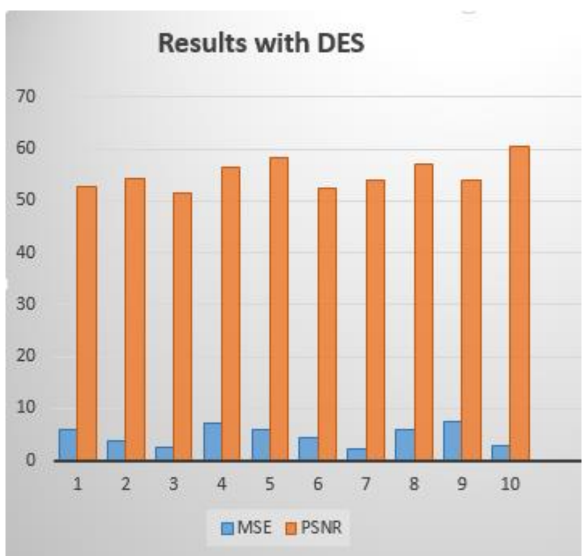
This section shows the results of RSA algorithm in terms of mean square error and peak signal to noise ratio parameters.



Graph 1.1: Result of RSA

4.2 Results in case of DES

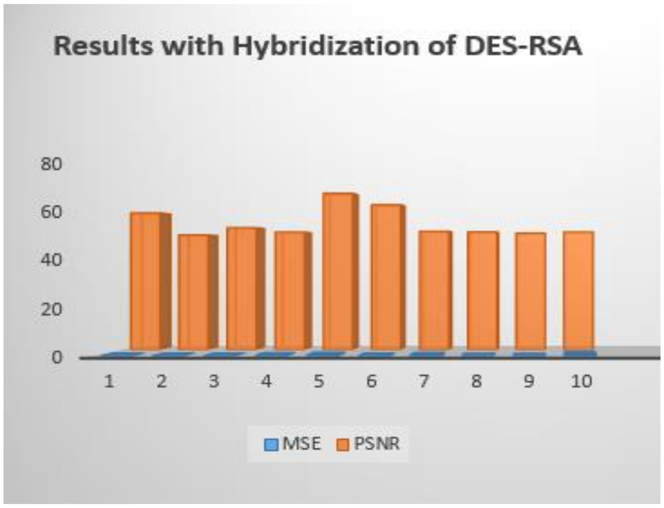
This section shows the results of DES algorithm in terms of mean square error and peak signal to noise ratio parameters.



Graph 1.2: Results of DES

4.3 Results with Hybridization DES-RSA

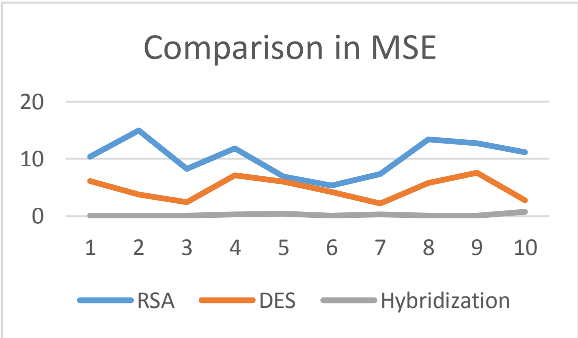
This section shows the results of our proposed scheme for execution in terms of mean square error and peak signal to noise ratio parameters.



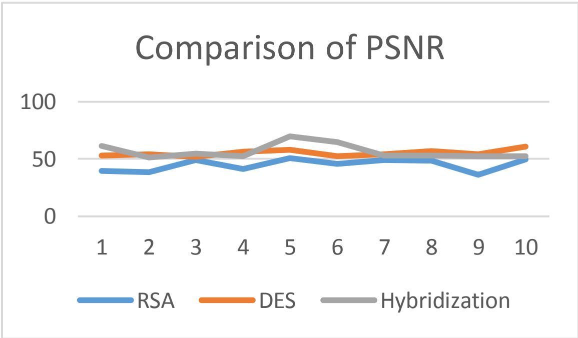
Graph 1.3: Results of Hybridization

4.4 *Comparative Analysis of all approaches*

The comparative analysis of mean square error and peak signal to noise ratio parameters in case of RSA, DES and Hybridization algorithms concludes that The mean square error is less in case of Hybrid algorithm than the other algorithms. Similarly, the peak signal to noise ration percentage is better in case of Hybrid algorithm than the other algorithms.



Graph 1.4: Comparison of MSE for all algorithm



Graph 1.5: Comparison of PSNR for all algorithm

5. CONCLUSION AND FUTURE WORK

A new and innovative algorithm for speech cryptography is proposed in this work which provides a security at different levels. Various techniques for identification of the encryption method of the cipher texts encrypted using the block ciphers. Secure communication is the prime requirement of every organization. In today's world the security has become the major aspect of life. It can be achieved by various techniques such as password, cryptography and biometrics. There are several ways of classifying the cryptographic algorithms. Based on the number of keys used in encryption and decryption there two types of cryptography.

But these results are not enough and there are several hybrid techniques for encryption. Therefore, future scope of work is:

1. To test the proposed model for checking it against its fault tolerant power.
2. The QOS (quality of service) of proposed model may be determined in terms of some availability, throughput and delay.

REFERENCES

[1] Kamal et al., 2014, "Enhancement Key Of Cryptography And Steganography Using RSA And Neural Network", IJARCET, vol. 3, pp. 1707-1710.

[2] Akshay et al., 2013, "Steganography Technique using Neural Network", International Journal of Computer Applications", Vol. 82, pp. 39-42.

[3] Ell effly et al., 2013 "Detecting pixel-value differencing steganography using Levenberg-Marquardt neural network", IEEE, Computational Intelligence and Data Mining (CIDM), pp. 160-165.

[4] Youssef, 2012, "A Generation-based Text Steganography Method using SQL Queries", IJCA, Vol. 57, pp. 27-31.

[5] Babloo Sha et al, 2012, "Steganographic Techniques of Data Hiding using Digital Images", DESIDOC, Vol. 62, pp. 11-18.

[6] Mohit Garg, 2011, "A Novel Text Steganography Technique Based on Html Documents", JJAST, Vol. 35, pp.129-135.

[7] Jisna et al., 2011, "Audio Steganography in Wavelet Domain – A Survey, IJCA, Vol. 52, pp. 33-37.

[8] Bidyut Jyoti Saha, Kunal Kumar Kabi, Arun and Chittaranjan Pradhan, "A Robust Digital Watermarking algorithm using DES and ECC in DCT Domain for Color pictures" 2014 International Conference on Circuit, Power and Computing Technologies [ICCPCT]

[9] Makarand L. Mali "Implementation of Text 2013 International Conference on Communication Systems and Network Technologies Watermarking Technique Using Natural Language Watermarks.

