INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATION & MANAGEMENT

A Monthly Double-Blind Peer Reviewed (Refereed/Juried) Open Access International e-Journal - Included in the International Serial Directories
Indexed & Listed at:
Ulrich's Periodicals Directory ©, ProQuest, U.S.A., EBSCO Publishing, U.S.A., Cabell's Directories of Publishing Opportunities, U.S.A.,
Open J-Gage, India [link of the same is duly available at Inflibnet of University Grants Commission (U.G.C.)],
Index Copernicus Publishers Panel, Poland with IC Value of 5.09 & number of libraries all around the world.
Circulated all over the world & Google has verified that scholars of more than 3130 Cities in 166 countries/territories are visiting our journal on regular basis.
Ground Floor, Building No. 1041-C-1, Devi Bhawan Bazar, JAGADHRI – 135 003, Yamunanagar, Haryana, INDIA
http://ijrcm.org.in/

CONTENTS

CALL FOR MANUSCRIPTS

We invite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the areas of Computer Science & Applications; Commerce; Business; Finance; Marketing; Human Resource Management; General Management; Banking; Economics; Tourism Administration & Management; Education; Law; Library & Information Science; Defence & Strategic Studies; Electronic Science; Corporate Governance; Industrial Relations; and emerging paradigms in allied subjects like Accounting; Accounting Information Systems; Accounting Theory & Practice; Auditing; Behavioral Accounting; Behavioral Economics; Corporate Finance; Cost Accounting; Econometrics; Economic Development; Economic History; Financial Institutions & Markets; Financial Services; Fiscal Policy; Government & Non Profit Accounting; Industrial Organization; International Economics & Trade; International Finance; Macro Economics; Micro Economics; Rural Economics; Co-operation; Demography: Development Planning; Development Studies; Applied Economics; Development Economics; Business Economics; Monetary Policy; Public Policy Economics; Real Estate; Regional Economics; Political Science; Continuing Education; Labour Welfare; Philosophy; Psychology; Sociology; Tax Accounting; Advertising & Promotion Management; Management Information Systems (MIS); Business Law; Public Responsibility & Ethics; Communication; Direct Marketing; E-Commerce; Global Business; Health Care Administration; Labour Relations & Human Resource Management; Marketing Research; Marketing Theory & Applications; Non-Profit Organizations; Office Administration/Management; Operations Research/Statistics; Organizational Behavior & Theory; Organizational Development; Production/Operations; International Relations; Human Rights & Duties; Public Administration; Population Studies; Purchasing/Materials Management; Retailing; Sales/Selling; Services; Small Business Entrepreneurship; Strategic Management Policy; Technology/Innovation; Tourism & Hospitality; Transportation Distribution; Algorithms; Artificial Intelligence; Compilers & Translation; Computer Aided Design (CAD); Computer Aided Manufacturing; Computer Graphics; Computer Organization & Architecture; Database Structures & Systems; Discrete Structures; Internet; Management Information Systems; Modeling & Simulation; Neural Systems/Neural Networks; Numerical Analysis/Scientific Computing; Object Oriented Programming; Operating Systems; Programming Languages; Robotics; Symbolic & Formal Logic; Web Design and emerging paradigms in allied subjects.

Anybody can submit the **soft copy** of unpublished novel; original; empirical and high quality **research work/manuscript** ***anytime*** in ***M.S. Word format*** after preparing the same as per our **GUIDELINES FOR SUBMISSION**; at our email address i.e. infoijrcm@gmail.com or online by clicking the link **online submission** as given on our website (***FOR ONLINE SUBMISSION, CLICK HERE***).

GUIDELINES FOR SUBMISSION OF MANUSCRIPT

1. **COVERING LETTER FOR SUBMISSION:**

DATED: _____________

THE EDITOR
IJRCM

Subject: **SUBMISSION OF MANUSCRIPT IN THE AREA OF .**

(e.g. Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/Engineering/Mathematics/other, please specify)

DEAR SIR/MADAM

Please find my submission of manuscript entitled '____' for possible publication in your journals.

I hereby affirm that the contents of this manuscript are original. Furthermore, it has neither been published elsewhere in any language fully or partly, nor is it under review for publication elsewhere.

I affirm that all the author (s) have seen and agreed to the submitted version of the manuscript and their inclusion of name (s) as co-author (s).

Also, if my/our manuscript is accepted, I/We agree to comply with the formalities as given on the website of the journal & you are free to publish our contribution in any of your journals.

NAME OF CORRESPONDING AUTHOR:
Designation:
Affiliation with full address, contact numbers & Pin Code:
Residential address with Pin Code:
Mobile Number (s):
Landline Number (s):
E-mail Address:
Alternate E-mail Address:

NOTES:
a) The whole manuscript is required to be in ***ONE MS WORD FILE*** only (pdf. version is liable to be rejected without any consideration), which will start from the covering letter, inside the manuscript.
b) The sender is required to mentionthe following in the **SUBJECT COLUMN** of the mail:
New Manuscript for Review in the area of (Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/Engineering/Mathematics/other, please specify)
c) There is no need to give any text in the body of mail, except the cases where the author wishes to give any specific message w.r.t. to the manuscript.
d) The total size of the file containing the manuscript is required to be below **500 KB**.
e) Abstract alone will not be considered for review, and the author is required to submit the complete manuscript in the first instance.
f) The journal gives acknowledgement w.r.t. the receipt of every email and in case of non-receipt of acknowledgment from the journal, w.r.t. the submission of manuscript, within two days of submission, the corresponding author is required to demand for the same by sending separate mail to the journal.

2. **MANUSCRIPT TITLE**: The title of the paper should be in a 12 point Calibri Font. It should be bold typed, centered and fully capitalised.

3. **AUTHOR NAME (S) & AFFILIATIONS**: The author (s) **full name**, **designation**, **affiliation** (s), **address**, **mobile/landline numbers**, and **email/alternate email address** should be in italic & 11-point Calibri Font. It must be centered underneath the title.

4. **ABSTRACT**: Abstract should be in fully italicized text, not exceeding 250 words. The abstract must be informative and explain the background, aims, methods, results & conclusion in a single para. Abbreviations must be mentioned in full.

5. **KEYWORDS:** Abstract must be followed by a list of keywords, subject to the maximum of five. These should be arranged in alphabetic order separated by commas and full stops at the end.

6. **MANUSCRIPT:** Manuscript must be in ***BRITISH ENGLISH*** prepared on a standard A4 size ***PORTRAIT SETTING PAPER***. It must be prepared on a single space and single column with 1" margin set for top, bottom, left and right. It should be typed in 8 point Calibri Font with page numbers at the bottom and centre of every page. It should be free from grammatical, spelling and punctuation errors and must be thoroughly edited.

7. **HEADINGS**: All the headings should be in a 10 point Calibri Font. These must be bold-faced, aligned left and fully capitalised. Leave a blank line before each heading.

8. **SUB-HEADINGS**: All the sub-headings should be in a 8 point Calibri Font. These must be bold-faced, aligned left and fully capitalised.

9. **MAIN TEXT:** The main text should follow the following sequence:

   INTRODUCTION

   REVIEW OF LITERATURE

   NEED/IMPORTANCE OF THE STUDY

   STATEMENT OF THE PROBLEM

   OBJECTIVES

   HYPOTHESES

   RESEARCH METHODOLOGY

   RESULTS & DISCUSSION

   FINDINGS

   RECOMMENDATIONS/SUGGESTIONS

   CONCLUSIONS

   SCOPE FOR FURTHER RESEARCH

   ACKNOWLEDGMENTS

   REFERENCES

   APPENDIX/ANNEXURE

   It should be in a 8 point Calibri Font, single spaced and justified. The manuscript should preferably not exceed ***5000 WORDS***.

10. **FIGURES &TABLES:** These should be simple, crystal clear, centered, separately numbered &self explained, and **titles must be above the table/figure**. **Sources of data should be mentioned below the table/figure**. It should be ensured that the tables/figures are referred to from the main text.

11. **EQUATIONS:**These should be consecutively numbered in parentheses, horizontally centered with equation number placed at the right.

12. **REFERENCES:** The list of all references should be alphabetically arranged. The author (s) should mention only the actually utilised references in the preparation of manuscript and they are supposed to follow **Harvard Style of Referencing**. The author (s) are supposed to follow the references as per the following:

- All works cited in the text (including sources for tables and figures) should be listed alphabetically.
- Use (**ed.**) for one editor, and (**ed.s)** for multiple editors.
- When listing two or more works by one author, use --- (20xx), such as after Kohl (1997), use --- (2001), etc, in chronologically ascending order.
- Indicate (opening and closing) page numbers for articles in journals and for chapters in books.
- The title of books and journals should be in italics. Double quotation marks are used for titles of journal articles, book chapters, dissertations, reports, working papers, unpublished material, etc.
- For titles in a language other than English, provide an English translation in parentheses.
- The location of endnotes within the text should be indicated by superscript numbers.

PLEASE USE THE FOLLOWING FOR STYLE AND PUNCTUATION IN REFERENCES:

BOOKS

- Bowersox, Donald J., Closs, David J., (1996), "Logistical Management." Tata McGraw, Hill, New Delhi.
- Hunker, H.L. and A.J. Wright (1963), "Factors of Industrial Location in Ohio" Ohio State University, Nigeria.

CONTRIBUTIONS TO BOOKS

- Sharma T., Kwatra, G. (2008) Effectiveness of Social Advertising: A Study of Selected Campaigns, Corporate Social Responsibility, Edited by David Crowther & Nicholas Capaldi, Ashgate Research Companion to Corporate Social Responsibility, Chapter 15, pp 287-303.

JOURNAL AND OTHER ARTICLES

- Schemenner, R.W., Huber, J.C. and Cook, R.L. (1987), "Geographic Differences and the Location of New Manufacturing Facilities," Journal of Urban Economics, Vol. 21, No. 1, pp. 83-104.

CONFERENCE PAPERS

- Garg, Sambhav (2011): "Business Ethics" Paper presented at the Annual International Conference for the All India Management Association, New Delhi, India, 19–22 June.

UNPUBLISHED DISSERTATIONS AND THESES

- Kumar S. (2011): "Customer Value: A Comparative Study of Rural and Urban Customers," Thesis, Kurukshetra University, Kurukshetra.
- **ONLINE RESOURCES**
- Always indicate the date that the source was accessed, as online resources are frequently updated or removed.

WEBSITES

- Garg, Bhavet (2011): Towards a New Natural Gas Policy, Political Weekly, Viewed on January 01, 2012 http://epw.in/user/viewabstract.jsp

A ROBUST AUDIO STEGANOGRAPHY FOR HIDING ENCRYPTED DATA

R.VALARMATHI.
RESEARCH SCHOLAR
BHARATHIAR UNIVERSITY
COIMBATORE

DR. G.M.KADHAR NAWAZ
DIRECTOR& PROFESSOR
DEPARTMENT OF MCA
SONA COLLEGE OF TECHNOLOGY
SALEM

ABSTRACT

In the current information age, secure data transfer is limited due to its attack made on data communication. So more robust methods are chosen so that they ensure secured data transfer. One of the solutions which came to the rescue is the audio steganography. But existing audio steganographic systems have poor interface, very level implementation, difficult to understand and valid only for certain audio formats with restricted message size. This is one proposed system which is based on audio steganography and cryptography, ensures secure data transfer between the source and destination. This uses most powerful encryption algorithm in the first level of security, which is very complex to break. In the second level it uses a more powerful modified LSB(Least Significant Bit) algorithm to encode the message into audio. It performs bit level manipulation to encode the message. The basic idea behind this paper is to provide a good, efficient method for hiding the data from hackers and sent to the destination in a safe manner.

KEYWORDS
Steganography, LSB, Security, Cryptography.

1. INTRODUCTION
Security of information is one of the most important factors of information technology and communication. Security of information often lies in the secrecy of its existence and/or the secrecy of how to decode it. Cryptography techniques often use the worst approach assuming that only one of these two conditions holds. It was created as a technique for securing the secrecy of communication. Various methods have been developed to encrypt and decrypt data in order to keep the message secret[2]. Unfortunately, it is not enough to keep the content of the information/message secret, it may also be necessary to keep the existence of the information secret. The technique used to implement this, is called steganography. Steganography is the science and art of hiding information in another. The definition according to Neil Johnson "Steganography is the art of hiding information in a way that prevent the detection of hidden message". It is a useful tool that allows covert communication amongst acknowledged parties[3]. The word steganography is derived from the Greek words "stegos" meaning cover/hidden/roof and "grafia" meaning writing defining it as "covered writing" and essentially means "to hide in plain sight". In Audio steganography the information is hidden exclusively in Audio files. Hiding messages by masking their existence is nothing new. Before the digital era, simple steganography techniques have been in use for hundreds of years. However, with the emergence of networks and digital technologies and increasing use of communication and files in electronic format, new techniques for information hiding have become possible[4]. Steganography relies on hiding covert message in unsuspected text, protocols, images, and multimedia (audio/video) data which is generally used in secret communication between acknowledged parties. Steganography is a method of encryption that hides data among the bits of a cover file, such as a graphic or an audio file. The technique replaces bits with the secret data[5].

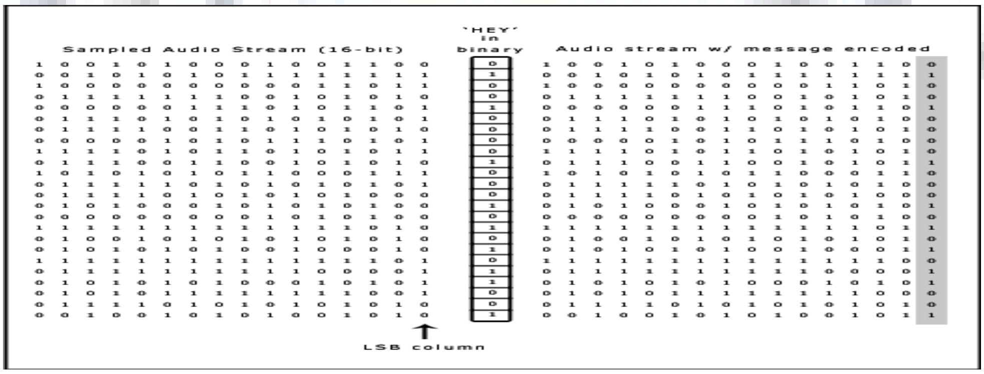
2. LITERATURE REVIEW
This section presents some common methods used in audio steganography[7].
* LSB coding
* Parity coding
* Phase coding
* Spread spectrum
* Echo hiding

LSB CODING

Least significant bit (LSB) coding is the simplest way to embed information in a digital audio file. By substituting the least significant bit of each sampling point with a binary message, LSB coding allows for a large amount of data to be encoded.

In LSB coding, the ideal data transmission rate is 1 kbps per 1 kHZ. In some implementations of LSB coding, however, the two least significant bits of a sample are replaced with two message bits. This increases the amount of data that can be encoded but also increases the amount of resulting noise in the audio file as well. Thus, one should consider the signal content before deciding on the LSB operation to use.

FIG 2.1: LSB CODING



To extract a secret message from an LSB encoded sound file, the receiver needs access to the sequence of sample indices used in the embedding process. Normally, the length of the secret message to be encoded is smaller than the total number of samples in a sound file. One must decide then on how to choose the subset of samples that will contain the secret message and communicate that decision to the receiver. One trivial technique is to start at the beginning of the sound file and perform LSB coding until the message has been completely embedded, leaving the remaining samples unchanged.

A more sophisticated approach is to use a pseudorandom number generator to spread the message over the sound file in a random manner. One popular approach is to use the random interval method, in which a secret key possessed by the sender is used as a seed in a pseudorandom number generator to create a random sequence of sample indices. The receiver also has access to the secret key and knowledge of the pseudorandom number generator, allowing the random sequence of sample indices to be reconstructed. Checks must be put in place, however, to prevent the pseudorandom number generator from generating the same sample index twice. If this happened, a collision would occur where a sample already modified with part of the message is modified again. The problem of collisions can be overcome by keeping track of all the samples that have already been used. Another approach is to calculate the subset of samples via a pseudorandom permutation of the entire set through the use of a secure hash function. This technique insures that the same index is never generated more than once[7].

PARITY CODING

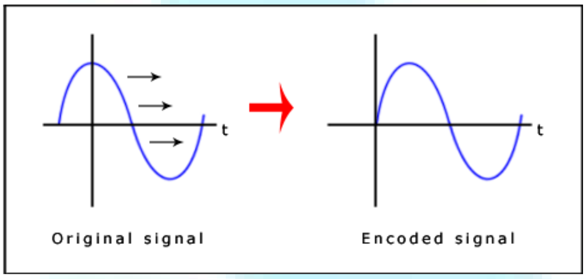
Instead of breaking a signal down into individual samples, the parity coding method breaks a signal down into separate regions of samples and encodes each bit from the secret message in a sample region's parity bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process flips the LSB of one of the samples in the region. Thus, the sender has more of a choice in encoding the secret bit, and the signal can be changed in a more unobtrusive fashion.

The decoding process extracts the secret message by calculating and lining up the parity bits of the regions used in the encoding process. Once again, the sender and receiver can use a shared secret key as a seed in a pseudorandom number generator to produce the same set of sample regions[7].

PHASE CODING

Phase coding addresses the disadvantages of the noise-inducing methods of audio steganography. Phase coding relies on the fact that the phase components of sound are not as perceptible to the human ear as noise is. Rather than introducing perturbations, the technique encodes the message bits as phase shifts in the phase spectrum of a digital signal, achieving an inaudible encoding in terms of signal-to-perceived noise ratio.

FIG. 2.2: PHASE CODING



Phase coding is explained in the following procedure:

1. The original sound signal is broken up into smaller segments whose lengths equal the size of the message to be encoded.
2. A Discrete Fourier Transform (DFT) is applied to each segment to create a matrix of the phases and Fourier transform magnitudes.
3. Phase differences between adjacent segments are calculated.
4. Phase shifts between consecutive segments are easily detected. In other words, the absolute phases of the segments can be changed but the relative phase differences between adjacent segments must be preserved. Therefore the secret message is only inserted in the phase vector of the first signal segment as follows:
5. A new phase matrix is created using the new phase of the first segment and the original phase differences.
6. Using the new phase matrix and original magnitude matrix, the sound signal is reconstructed by applying the inverse DFT and then concatenating the sound segments back together.

To extract the secret message from the sound file, the receiver must know the segment length. The receiver can then use the DFT to get the phases and extract the information[7].

SPREAD SPECTRUM

In the context of audio steganography, the basic spread spectrum (SS) method attempts to spread secret information across the audio signal's frequency spectrum as much as possible. This is analogous to a system using an implementation of the LSB coding that randomly spreads the message bits over the entire sound file. However, unlike LSB coding, the SS method spreads the secret message over the sound file's frequency spectrum, using a code that is independent of the actual signal. As a result, the final signal occupies a bandwidth in excess of what is actually required for transmission.

Two versions of SS can be used in audio steganography: the **direct-sequence** and **frequency-hopping schemes**. In direct-sequence SS, the secret message is spread out by a constant called the chip rate and then modulated with a pseudorandom signal. It is then interleaved with the cover-signal. In frequency-hopping SS, the audio file's frequency spectrum is altered so that it hops rapidly between frequencies[7].

ECHO HIDING

In echo hiding, information is embedded in a sound file by introducing an echo into the discrete signal. Like the spread spectrum method, it too provides advantages in that it allows for a high data transmission rate and provides superior robustness when compared to the noise inducing methods.

To hide the data successfully, three parameters of the echo are valid: amplitude, decay rate, and offset (delay time) from the original signal. All three parameters are set below the human hearing threshold so the echo is not easily resolved. In addition, offset is varied to represent the binary message to be encoded. One offset value represents a binary one, and a second offset value represents a binary zero.

If only one echo was produced rom the original signal, only one bit of information could be encoded. Therefore, the original signal is broken down into blocks before the encoding process begins. Once the encoding process is completed, the blocks are concatenated back together to create the final signal[7].

3. IMPORTANCE OF AUDIO STEGANOGRAPHY

In a computer-based audio steganography system, secret messages are embedded in digital sound. The secret message is embedded by slightly altering the binary sequence of a sound file. Existing audio steganography software can embed messages in WAV, AU, and even MP3 sound files[6].

Embedding secret messages in digital sound is usually a more difficult process than embedding messages in other media, such as digital images. In order to conceal secret messages successfully, a variety of methods for embedding information in digital audio have been introduced. These methods range from rather simple algorithms that insert information in the form of signal noise to more powerful methods that exploit sophisticated signal processing techniques to hide information[7].

4. PROPOSED SYSTEM

In the Audio Steganography with cryptography, the process of embedding secret message using Symmetric-Key algorithm[8], DES into the Audio file. The following gives the complete working of the Audio Steganogrpahy. This system contains Sender Side and Receiver Side. Both are connected with Trustcenter.

Both sides the user has to register their name. The system will generate secret key for the user. Using the login name both the users have to enter into their area. The system will generate Quantum Key. Both Sender and Receiver have to use the same quantum key to connect with each other through Trustcenter.

In the sender side, the text which has to be embedded into an audio file is encrypted using Symmetric Key cryptographic algorithm, DES. The cipher text obtained is then embedded using Steganographic algorithm. The resultant audio file contains the secrete message embedded into it. In the receiver side, the embedded audio file is selected to extract the secret message. The secret message is decrypted using DES decryption method.

5. ALGORITHMS AND RESULTS

I. SENDER SIDE ALGORITHM:

Step 1: Select the Text for encoding into Audio File.
Step 2: Encrypt the text using DES Algorithm.
Step 3: Select the Audio file for Encoding.
Step 4: Encode encrypted text into Audio File using modified LSB algorithm.

II. RECEIVER SIDE ALGORITHM

Step 1: Select the Encoded Audio file.
Step 2: Decode the text from Audio File using modified LSB algorithm.
Step 3: Decrypt the text using DES Algorithm.
Step 4: Display the secret text/message to the end user.

FOLLOWING FIGURES GIVES THE RESULTS OF THE ABOVE ALGORITHMS

FIG. 5.1 SENDER MAIN

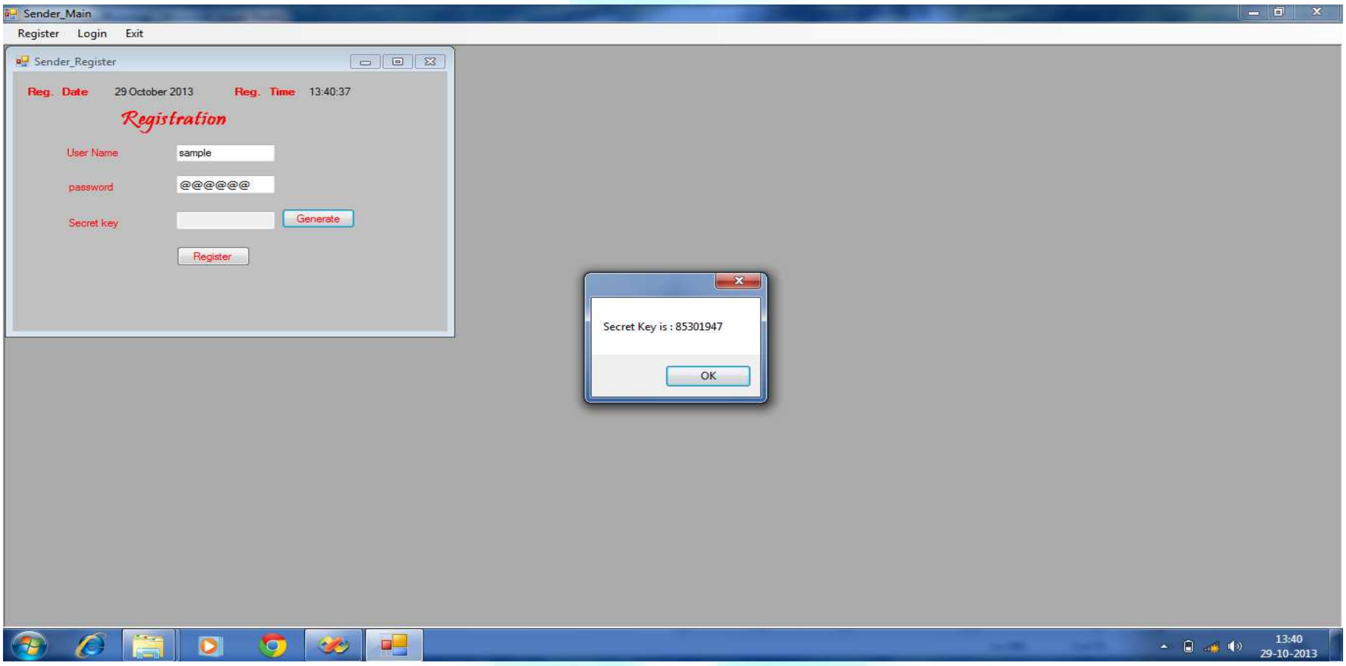


FIG. 5.2. RECEIVER MAIN

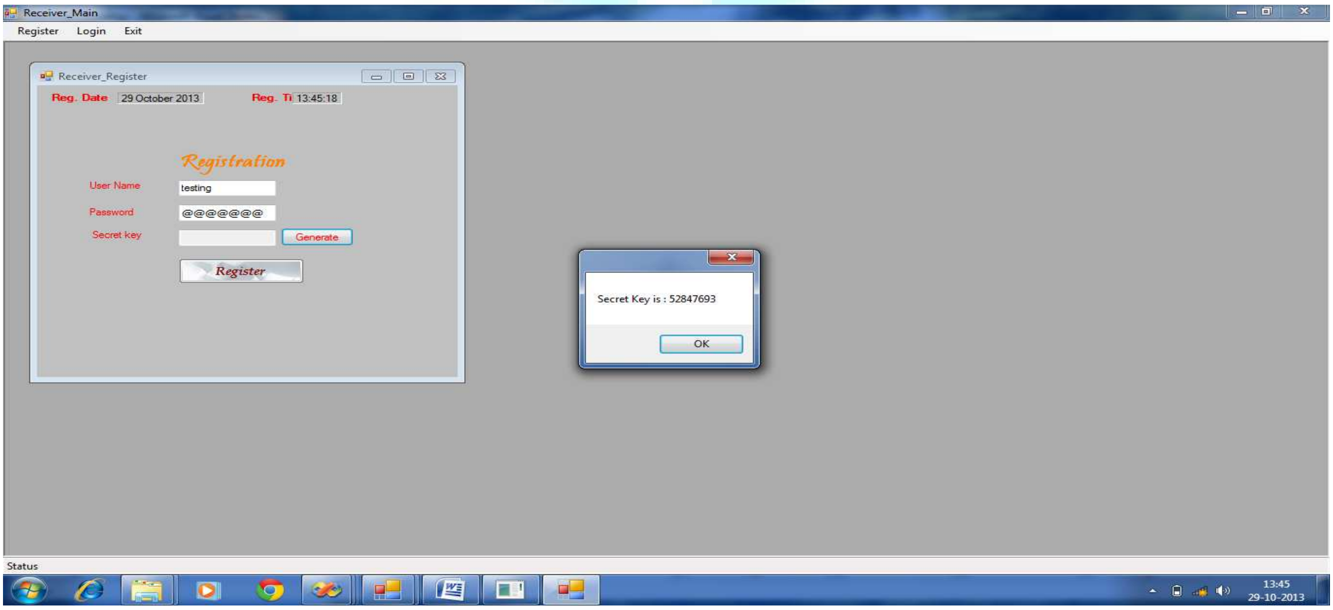


FIG.5.3 SENDER, RECEIVER AND TRUST CENTER

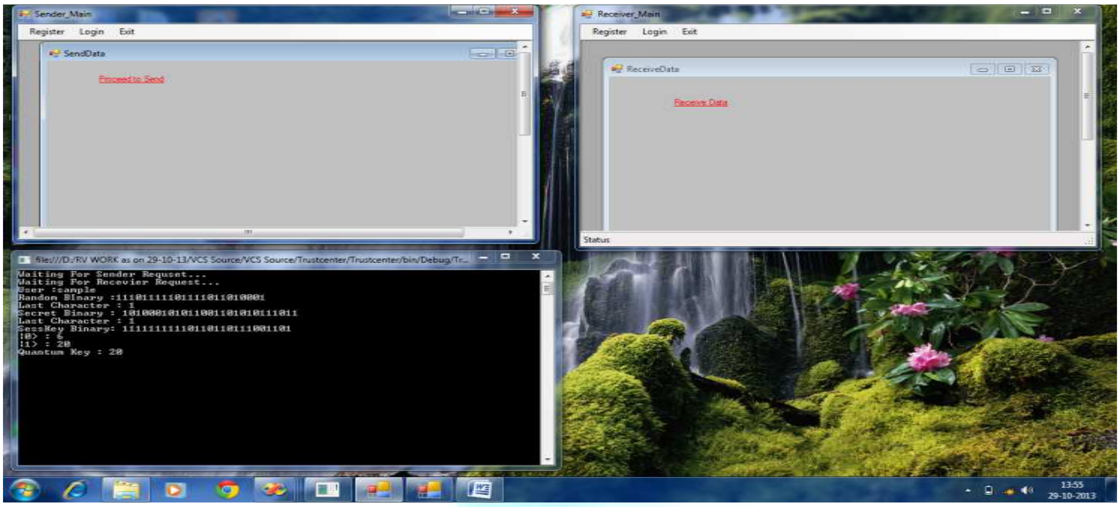


FIG.5.4: SENDING ENCODED FILE TO RECEIVER

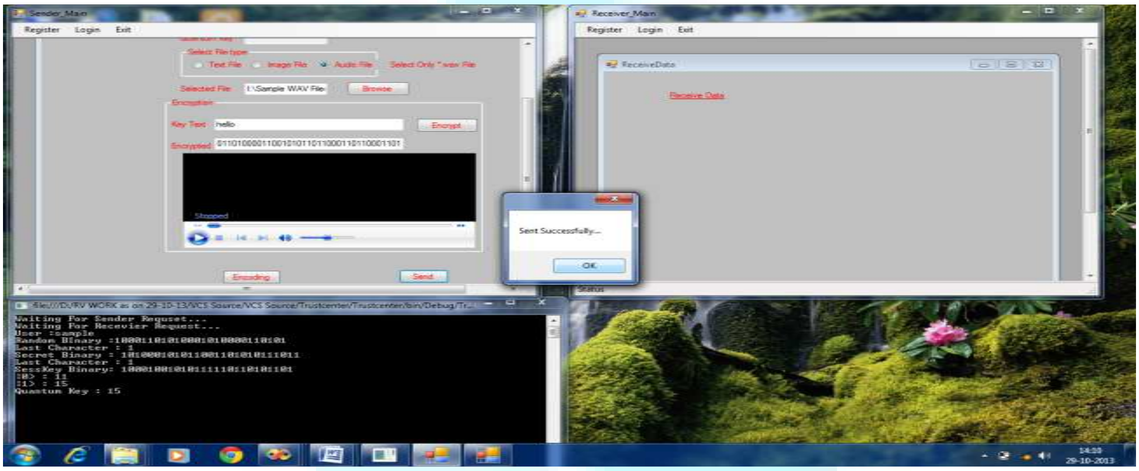
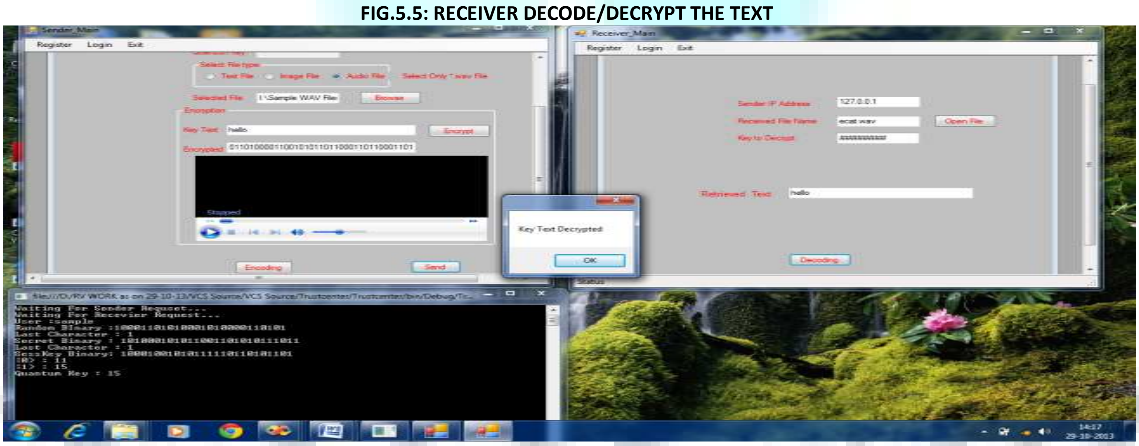


FIG.5.5: RECEIVER DECODE/DECRYPT THE TEXT



6. CONCLUSION

Audio Steganography with cryptography is to provide a good, efficient method for hiding the data from hackers and sent to the destination in a safe manner. This proposed system will not change the size of the file even after encoding. Encryption and Decryption techniques have been used to make the security system robust.

7. ACKNOWLEDGEMENT

My sincere thanks to Dr. G.M.Kadhar Nawaz M.C.A., Ph.D,. Director& Professor, Department of MCA, Sona College of Technology,Salem-5 for supporting and encouraging to do this research work and I extend my thanks to my friends who are in this circle and also the peer review committee members.

REFERENCES

1. R Sridevi, Dr. A Damodaram, Dr. Svl.Narasimham, "Efficient Method Of Audio Steganography By Modified LSB Algorithm And Strong Encryption Key With Enhanced", Journal of Theoretical and Applied Information Technology.
2. Deepak Singla, Rupali Syal /International Journal Of Computational Engineering Research/ ISSN: 2250–3005.Data Security Using LSB & DCT Steganography In Images -Deepak Singla1, Rupali Syal2
3. An Overview of Steganography for the Computer Forensics Examiner -Gary Kessler Associates,Burlington, Vermont ,February 2004 (updated June 2011)

4. International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, Issue-4, September 2011
   Optimum segment length for embedding in the LSB of JPEG images with Minimum MSE,Hamdy A. Morsy, Zaki B. Nossair, Alaa M. Hamdy, Fathy Z. Amer.
5. Secret Communication through Audio,Video and Image for Defence Application, Jun 26,2013.
6. Steganography| ClubHACK Magazine, Mar 8,2010.
7. Methods of Audio Steganography, Internet publication on www.Snotmonkey.com.
8. Padmashree G, Venugopala P S-Audio Stegnography and Cryptography: Using LSB algorithm at 4th and 5th LSB layers.

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, International Journal of Research in Computer Application & Management (IJRCM) acknowledges & appreciates your efforts in showing interest in our present issue under your kind perusal.

I would like to request you tosupply your critical comments and suggestions about the material published in this issue as well as on the journal as a whole, on our E-mail**infoijrcm@gmail.com** for further improvements in the interest of research.

If youhave any queries please feel free to contact us on our E-mail **infoijrcm@gmail.com**.

I am sure that your feedback and deliberations would make future issues better – a result of our joint effort.

Looking forward an appropriate consideration.

With sincere regards

Thanking you profoundly

Academically yours

Sd/-
Co-ordinator

DISCLAIMER

ABOUT THE JOURNAL

In this age of Commerce, Economics, Computer, I.T. & Management and cut throat competition, a group of intellectuals felt the need to have some platform, where young and budding managers and academicians could express their views and discuss the problems among their peers. This journal was conceived with this noble intention in view. This journal has been introduced to give an opportunity for expressing refined and innovative ideas in this field. It is our humble endeavour to provide a springboard to the upcoming specialists and give a chance to know about the latest in the sphere of research and knowledge. We have taken a small step and we hope that with the active co-operation of like-minded scholars, we shall be able to serve the society with our humble efforts.

Our Other Journals