ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

"Transmission of Data Through Images Using Encrypted Spread Spectrum Method"

Devyani M. Dugar[1], Laxmi Y. Attarde[2], Neelam N. Ramchandani[3], Ms. Sweta Pandey[4]

UG Student, Dept., of Information Technology, SSBT'S College of Engineering and Technology, Jalgaon, India [1,2,3]

Assistant Professor, Dept of Information Technology, SSBT'S College of Engineering and Technology, Jalgaon, India[4]

Abstract: In today's era, internet is the mean of convenience for sharing information over distance. Our day to day transactions completely relies on sharing of information and digital media. The sharing of confidential data can be done by using digital media such as images, audio and video etc. Certain technique has been brought forward to accomplish this sharing scenario. The enormous developments in the field of multimedia and internet technology easily let us do the distribution of digital media and data. Nowadays sharing of confidential data over network is a major issue, as there is a possibility of having threat to the information that we are delivering in terms of privacy and security. Hence it is necessary to find appropriate solution because the information that we are delivering needs to be delivered securely and safely. Considering this aspect, here we have implemented a system that hides the vital data behind an image in encrypted format by using multi-carrier/signature iterative generalized least-squares (MIGLS) algorithm, considering the fact that the quality of the image should not be differed, deflected or reduced.

Keywords: Digital media, Embedding, Encryption, MIGLS, Spread spectrum, Transaction.

I. INTRODUCTION

The development in the field of science and technology is growing day by day. Huge development and research is being carried out since the inception of science and technology. With advent in these fields, industrial sector also emerged out as well. Today, our business activities and processes demands use of technical approaches such as sharing etc. This sharing typically involves sharing of multimedia and data. Sometimes the data that we are sharing is highly confidential. Most of the time, it is relatively necessary to send sensitive data or information over network to complete our business functions. During such process, it is possible that the sensitive information that we are delivering over network may get in the hands of unauthorized person.

Hence it is a drastic need to find an approach to handle such situations. Existing techniques provides a bit of such facility that includes hiding of data and data encryption. Both techniques provide a way out through such situations but up to an extent. Till so far, such techniques has been implemented separately. Initially hiding of data behind image was considered as a secure approach to maintain very existence of data whereas data encryption approach was also the popular one. But nowadays several techniques have been in existence that can be followed to extract the hidden data in an image for example- Multi Carrier Spread Spectrum Embedding etc. [1] In case of encryption of data, the encrypted data can be made in the hands of unauthorized person or hacker by following certain techniques for example- Brute Force Attack. [2] It is the need of situation that there needs to be a system which can easily transmit sensitive and vital data over network among parties involved communication in such a way that the data should remain secure, private and unassessed during transfer. So to overcome on these aspects, here we have implemented a system that uses a collaborative approach. The above mentioned possibilities can be well handled by applying data hiding and encryption techniques together. The data hiding is nothing but steganography and data encryption is nothing but cryptography. [1]

A. Steganography

It is a simple method of hiding data. It is easy to make our data seems invisible by using steganography approach. If we apply steganography approach to the vital data then it causes no harm to our data because this approach makes our data seems invisible only. [3]

B. Cryptography

It is popular method of converting normal data or information into such format that it can't be understood or identified. If we encrypt our data then it is very hard to identify our real data contents. [4]

II. EXISTING SYSTEM

Till so far, it is observed that if we hide data behind an image then one can try to extract it by applying certain techniques such as spread spectrum embedding. Spread spectrum embedding is a technique that helps to identify hidden data and by using this technique we simply can extract the hidden data. [1] Also we known to this fact that if we hide data behind an image then it is possible that the image get deflected or its size get maximized or image get flattered.

III. OUR CONTRIBUTION

Here we have identified overall problematic aspects that arises while transferring vital data from one place to another place over network by implementing either one of the mentioned approach. We known to the fact that problem arises in the existing system if we use either technique of data hiding or data encryption. We took into

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

account the extracting data problem and built a solution on this. We built a system that allows us to transmit vital data over network by hiding it behind image. We built a system that easily fulfils the user's privacy and security requirement while he sends data over network. For this we have implemented a novel multi-carrier/signature iterative generalized least-squares core procedure algorithm. [1] Our system constituting this approach easily negotiated the possibility of extraction of hidden data and ensures safer delivery of confidential data without compromising its privacy.

C. Implementation Phase

We implemented MIGLS (multi- carrier/signature iterative generalized least-squares) approach for building our system. Hence now the system yields better output. This system now first accepts confidential information i.e. a file (.txt file) as an input. Once the input is given then the system applies the MIGLS (multi- carrier/signature iterative generalized least-squares) algorithmic approach/procedure in such a way that at first this input file is encrypted and then this file is hidden behind selected image. This way security, privacy and authentication of the confidential data is maintained. [5] Following figures shows the complete structure of the proposed system.

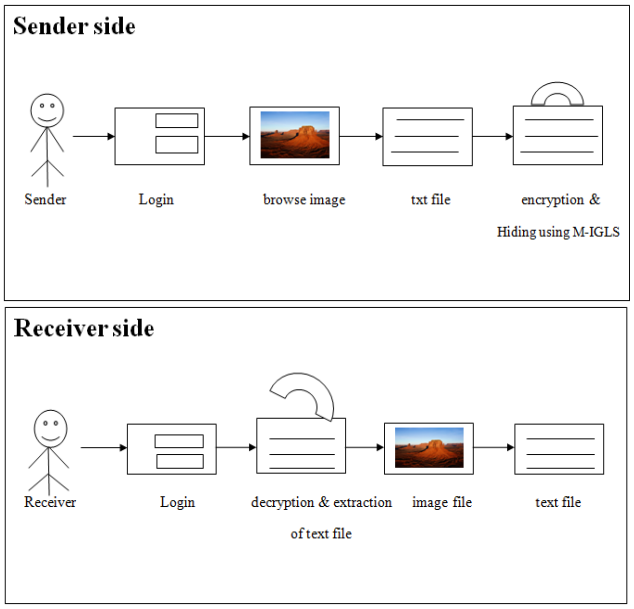

FIG. 1. PROPOSED SYSTEM

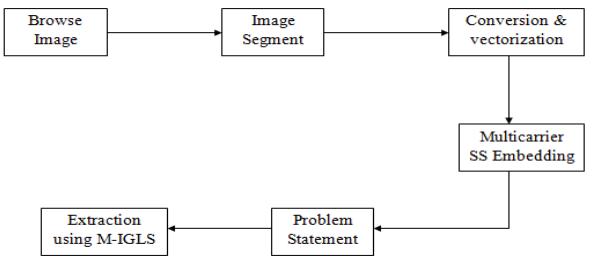

FIG. 2. MODULES OF DATA HIDING

FLOWCHARTS:

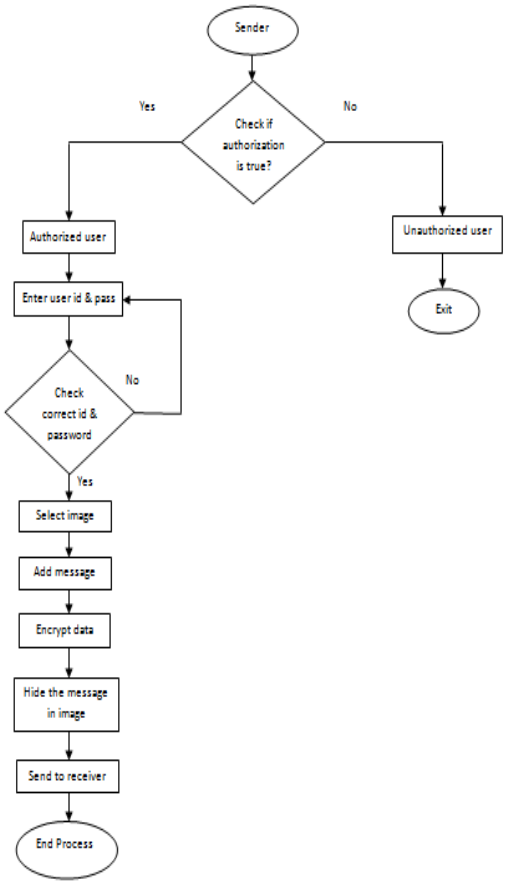

FIG. 3. SENDER SIDE

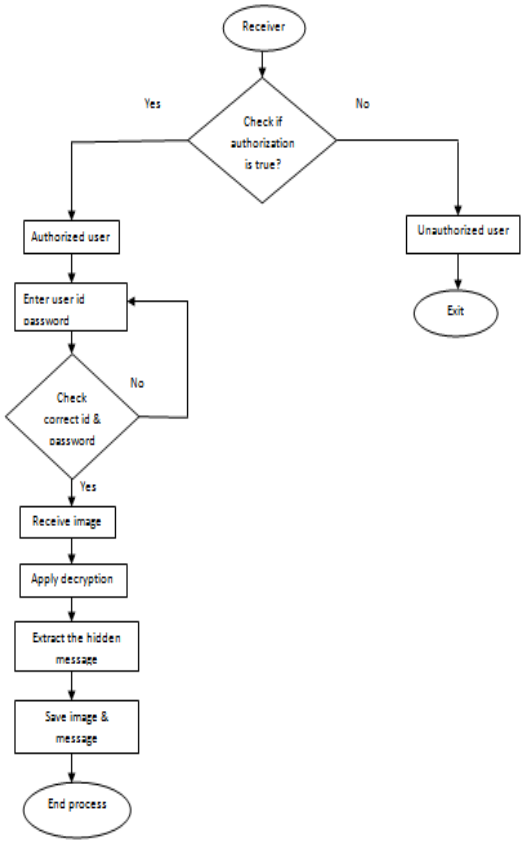

FIG. 4. RECEIVER SIDE

DOI 10.17148/IJARCCE.2015.4237

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

D. System Requirements

Hardware Requirements-

Processor-	Pentium –III
Speed-	1.1 GHz
RAM-	256 MB (min)
Hard Disk-	20 GB
Floppy Drive-	1.44 MB
Key Board-	Standard Windows
Mouse-	Two or Three Button
Monitor-	SVGA

Software Requirements-

Operating System-	Windows XP / 7
Front End-	JAVA, RMI, SWING

E. MIGLS Algorithm

Initialize B^ irrationally and swap step wise step among (1) and (2) to accomplish at every pace conditionally indiscriminate least squares rough of one matrix bound particular the further. The equations used for this is-

$$V\text{^}GLS=\arg V_{\epsilon R}{}^{LxR} \|Rz^{-1/2}(Y-VB)\|^2_F = YB^T(BB^T)^{-1} \text{ ----(1)}$$

$$B\text{^}{}^{binary}_{GLS}=\arg_{B\epsilon\{\pm1\}}{}^{KxM} \min \|Rz^{-1/2}(Y-VB)\|^2_F \approx sgn\ \{(V^TR_y^{-1}V)^{-1}V^TR_y^{-1}Y\} \text{ --------(2)}$$

$$R\text{^}y = 1/M\Sigma^M_{m=1}\ y(m)y(m)^T$$

Steps-

1) d := 0; initialize B^(0) 2 {±1}K×M arbitrarily.

2) d := d + 1;

$$V\text{^}(d) := Y(B\text{^}^{(d-1)})^T[B\text{^}^{(d-1)}(B\text{^}^{(d-1)})^T]^{-1};$$
$$B\text{^}(d) := sgn\{(V\text{^}^{(d)})^TR_y\text{^}^{-1}\ (V\text{^}^{(d)}))^{-1}(V\text{^}^{(d)})^T\ R_y\text{^}^{-1}\ Y\}$$

3) Repeat Step 2 until B^(d) = B^(d−1).

This algorithm is well known for extracting hidden data from the image and can be well used to provide security. [5]

IV. RESULT

This implemented system is used to maintain very existence of the data. Sender browses desired image, adds confidential text and sends it to the destination. At the other end receiver extracts and decrypts the hidden data from the image. It is observed that the size and quality of the image is not being compromised during data transfer as follows-

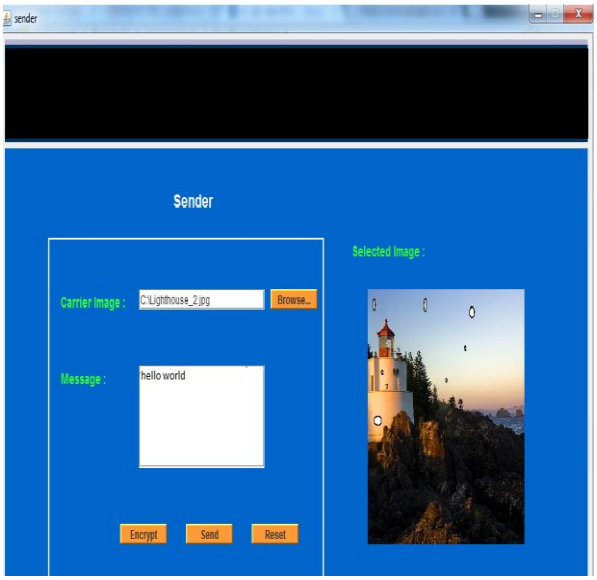

FIG. 5. ANALYSIS 1

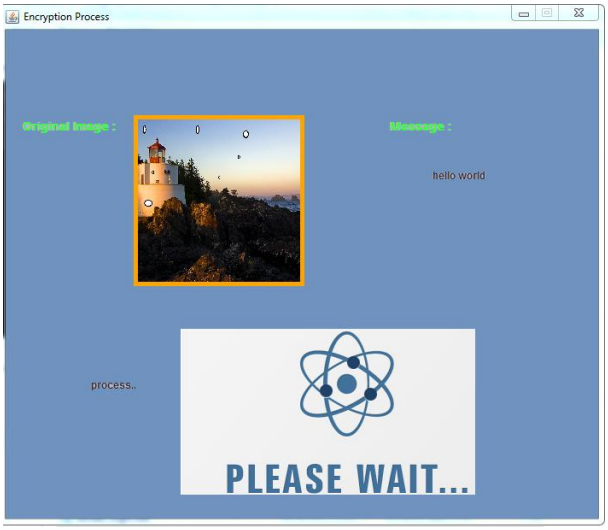

FIG. 6. ANALYSIS 2

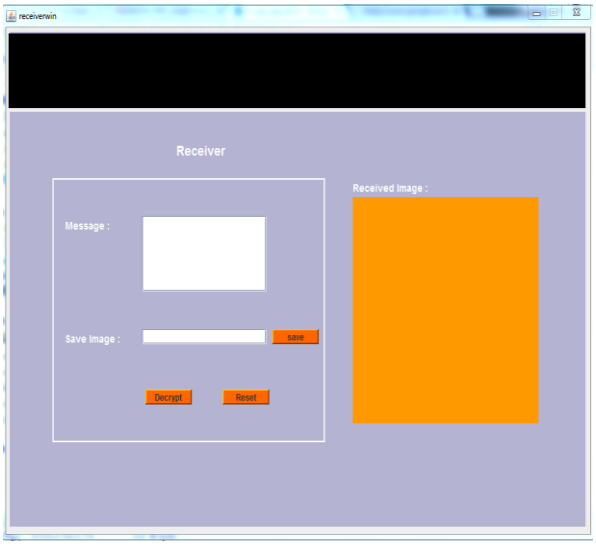

FIG. 7. ANALYSIS 3

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

V. CONCLUSION

Though extraction of data from the images can be made possible easily, yet we can put a security major to it by enhancing the data sharing facility by applying the steganography and cryptography approach together. This collaboration definitely adds a positive impact in data sharing facility.

ACKNOWLEDGMENT

We would like to thank our Head of Department, Principal and North Maharashtra University for their constant support and encouragement.

REFERENCES

[1]. Ming Li, Michel Kulhandjian, Dimitris A. Pados, Stella N. Batalama and Michael J. Medley, "Extracting Spread-Spectrum Hidden Data from Digital Media", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. X, NO. X.

[2]. Akansha Tuteja and Amit Shrivastava, " Faster Decryption and More Secure RSA Cryptosystem", Ijarcsse, Volume 4, Issue 11, November 2014 ISSN: 2277 128X.

[3]. Debnath Bhattacharyya, Poulami Das, Samir Kumar Bandyopadhyay, and Tai-hoon Kim, "Text Steganography: A Novel Approach", International Journal of Advanced Science and Technology Vol. 3, February, 2009.

[4]. Tanmaiy G. Verma, Zohaib Hasan and Dr. Girish Verma, "A Unique Approach for Data Hiding Using Audio Steganography", ijmer, Vol. 3, Issue. 4, Jul - Aug. 2013 pp-2098-2101 ISSN: 2249-6645.

[5]. Ch. Anusha and V. Sireesha, "Eliminating Hidden Data from an Image Using Multi Carrier-Iterative Generalized Least Squares", International Journal of Science and Research (IJSR), ISSN (Online): 2319-7064.

BIOGRAPHIES

Miss. Devyani M. Dugar, UG student, Department of Information Technology, Shram Sadhna Bombay Trust's College of Engineering and Technology, Bambhori, Jalgaon. Area of Interests: Network Security, IT Infrastructure Management and Software Development.

Miss. Laxmi Y. Attarde, UG student, Department of Information Technology, Shram Sadhna Bombay Trust's College of Engineering and Technology, Bambhori, Jalgaon. Area of Interests: Machine Learning, Software testing and analysis.

Miss. Neelam N. Ramchandani, UG student, Department of Information Technology, Shram Sadhna Bombay Trust's College of Engineering and Technology, Bambhori, Jalgaon. Area of Interests: Database Management, Software testing and Information Analysis.

Miss. Shweta Pandey is an active researcher in the field of image processing, currently working as Assistant Professor in Department of Information Technology at SSBT COET, Jalgaon India. She has done her BE IT from Apeejay College of engineering, Gurgaon, M. Tech from Banasthali University (Rajasthan) and undergoing PhD from Banasthali University (Rajasthan), India.