DATA SECURITY USING CRYPTOGRAPHY, STEGANOGRAPHY AND LAN MESSAGING (DSCSL)

Agrawal Jayesh G.   Ashwini Gadge B.   Dawange Yogesh P.
Chaube Neha V .   Achaliya Parag N.

Abstract— **Data security using Cryptography, Steganography & LAN Messaging (DSCSL) is the newly proposed system in which cryptography and steganography are very popular techniques used worldwide. These widely used techniques helps to provide Dual security. These techniques is helpful for security purpose in Companies, Colleges, Organizations etc.The Technique of cryptography is to encrypts the sensitive data in some scrambled form & by using steganography data is hidden behind the image . At the receiver side hidden data is extracted & decrypts that data in readable form in between this LAN Messenger program serves the communication Medium. Various users can communicate with each other & transfer files easily.**

Keywords

Data security, Cryptography, Steganography LAN Messaging

I. INTRODUCTION

Cryptography and Steganography are well known and widely used techniques that manipulate information (messages) in order to cipher or hide their existence respectively. Steganography is the art and science of communicating in a way

Which hides the existence of the communication Cryptography scrambles a message so it cannot be understood and   Steganography hides the message so it Cannot be seen. In this paper we are focusing to develop such system that uses both Cryptography and Steganography Technique for better Confidentiality and Security.

The design for the combining two different techniques is purely based on the idea – Distort the Message and Hide the Existence of the Distorted Message and for getting back the Original Message – Retrieve the Distorted Message and regain the actual message by reversal of the distortion process. Here we design the system with three modules-

- For Cryptography - Crypto Module

- For Steganography - Stegno Module

- For Data transmission module – LAN Messaging
- The LAN Massaging module that we are providing is an easy way for data transmission after applying cryptography and steganography schemes.

II. BASIC CONCEPT

There are many aspects of Security and Applications. One essential aspect for Secure Communications is that of Cryptography.

It is important to note that Cryptography is necessary for secure communications but some factor such as Authentication, Privacy/confidentiality and Integrity Non-repudiation are also necessary with it.

The three types of algorithms are described:
(i)   Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption
(ii)   Public Key Cryptography (PKC): Uses one key for encryption and another for decryption
(iii) Block Functions: Uses a mathematical transformation to irreversibly "encrypt" information [2].

III. PROPOSING THEME

Many technology uses only Cryptography for Data Security. Proposed system can use the two technique for data Security like Cryptography and Stenography from   fig a .Suppose if only Cryptography is used then data hacking is so easy, but when these two technique combine together at that time Double Security is provided first encryption is done on given file by using cryptography and then hide that encrypted file behind the Image . After send this data file from one

node to another node waif LAN which can provide Transmission to our data. At
the Receiving end we do Stenography first and after that Cryptography and Regain the original message [1].
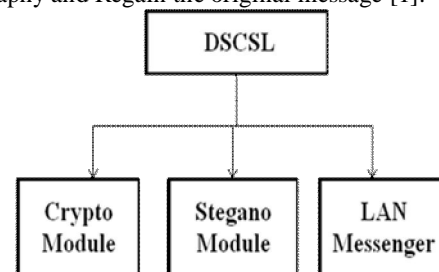
Fig a: Proposed system

IV .METHODOLOGY

The design for the combining two different techniques is purely based on the idea – Distort the Message and Hide the Existence of the Distorted Message and for getting back the Original Message – Retrieve the Distorted Message and regain the actual message by reversal of the distortion process. Here we design the system with three modules as:
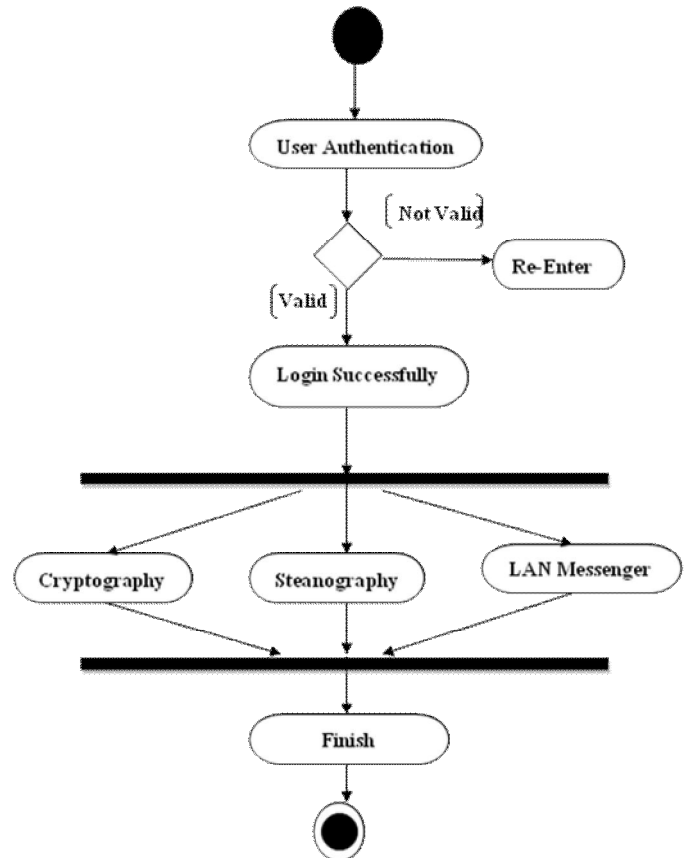
A. Cryptography Module

- It is a science of protecting information by encoding it into an unreadable format.

- Cryptography is an effective way of protecting sensitive information as it is stored on media or transmitted through network communication paths [2].

B.Steganography Module

- Steganography module facilitates hiding of a message that is to be kept secret inside other messages.

- It helps users to hide secret messages within Graphic Images.

Fig b: Flow diagram of DSCSL

C.LAN Messaging Module

- LAN Messenger (LM) is a form of real-time communication between two or more people based on typed text. The text is conveyed via computers connected over a network.
- LAN messaging offers real-time communication and allows easy collaboration, which might be considered more skin to genuine conversation than e-mail's "letter" format.

V. APPLICATION

DSCSL provide a specialized secured and easy way for sending files and messaging and provide security for networking related data.

.

1. DSCSL and their related modules services most of the following areas: small industrial environmental area & intranet, Collage and School, Computer System Related, Military for the security purpose.
2. DSCSL is very user friendly, as it having GUI (Graphical user interface) forms so that the users can easily operate to this software.
3. The military always need this kind of security Technique for their data Security.
4. In Banking Sector also this system is useful in any case such as in Transaction ID, Bank Statement and Account Detail etc.

VI. CONCLUSION

- So we conclude that Our System is the Solution of Providing Dual Security to Data.
- Since cryptography, steganography and LAN messenger are merged together for the first time it will be helpful and beneficial for all Secret message and Information sending.
- Transfer file in secure way in the network.

REFERENCES

[1]Neha Bajpai "Proposed System for Data Hiding Using Cryptography and Steganography", *International Journal of Computer Applications (0975 – 8887)*
[2]Cryptography and Network Security: Atul Kahate
[3]Westfield A. and Pitman A. "Attacks on Steganography Systems". *Lecture Notes in Computer Science*, Springer-Velar, Berlin 2000, pp. 61-75.
[4]Cvejic N. Seppanen, T., "Increasing robustness of LSB audio steganography using a novel

AUTHOR'S PROFILE

1.
Name: Agrawal Jayesh G.
E-mail: jayesh.agrawal2@gmail.com
Contact No.: 9421512661

Educational Detail:
Collage name: S.N.J.B. COE, Chandwad.
Qualification: Under Graduate (B.E. appearing).

Achievement:
Runner up in Robotic Compitition which is held at MET college of Engineering at Nasik

2.
Name: Ashwini Gadge B.
E-mail: ashwinig749@gmail.com

Educational Detail:
Collage name: S.N.J.B. COE, Chandwad.
Qualification: Under Graduate (B.E. appearing).

Achievement:
Won Frist Prize in Paper persentation at MIT colleage of engineering held in Pune

3.
Name: Dawange Yogesh P.
E-mail: ydawange@gmail.com
Contact No.: 9881227893

Educational Detail:
Collage name: S.N.J.B. COE, Chandwad.
Qualification: Under Graduate (B.E. appearing).

Achievement:
Runner up in Robotic Compitition which is held at MET college of Engineering at Nasik.

4.
Name: Chaube Neha V .
E-mail: sweetshreyasi.15@gmail.com

Educational Detail:
Collage name: S.N.J.B. COE, Chandwad.
Qualification: Under Graduate (B.E. appearing).

Achievement:
Won Frist Prize in Paper persentation at MIT colleage of engineering held in pune .

5.
Name: Achaliya Parag N.
E-mail: parag_achaliya143@yahoo.co.in
Contact No.: 9970077733

Education Detail:
Collage name: S.N.J.B. COE, Chandwad.
Qualification: Graduate (BE Computer).

Achievement:
1.
    "SmartTravelGuide : Application for Android Mobile" was selected in National Colloquium on "Novel Approaches in Computing Technology" at Indira College of Engineering and Management, Pune.

2.
    "DROID M-Learning" paper published in International Conference on "Global Economic Turmoil and Strategic Advantage (2012)" [ISBN: 978-81-910118-1-4]