Security in Ad-Hoc Network Using Encrypted Data Transmission and Steganography

Prof. Ravindra Ghugare, Ankita Patil, Ajay Jha, Dhiraj Kuslekar

Prof Ravindra Ghugare, Department of Computer Engineering, Bharati Vidyapeeth College of Engineering, Navi Mumbai, India.

Ankita Patil, Dept of Computer Engineering, Bharati Vidyapeeth College of Engineering, Navi Mumbai,India
Dhiraj Kuslekar, Dept of Computer Engineering, Bharati Vidyapeeth College of Engineering, Navi Mumbai, India
Ajay Jha, Dept of Computer Engineering, Bharati Vidyapeeth College of Engineering, Navi Mumbai, India.

Abstract-Currently, there is a growing trend of outsourcing data to a remote cloud, where people send their data to a Cloud Service Provider (CSP) that provides large storage space at a low cost. As a result, users can reduce the time and effort needed to manage local data storage. Meanwhile, once data is moved to the cloud, the owner loses ownership of it, which inevitably introduces new security threats to the integrity and confidentiality of the data. As a result, efficient and effective methods for ensuring the data integrity and confidentiality of outsourced data on untrusted cloud servers are needed. The previously proposed protocols fail to provide users with a high degree of security assurance. To resolve these problems, we propose an effective and reliable protocol in this paper. Our system enables a third-party auditor to check the data integrity on a regular basis.

Keywords — *Steganography, Cryptography, Cloud Service Provider, Elliptical Curve Cryptography, Least Significant Bit*

Introduction

With the invention of storage, the times of keeping all of your documents, photos, music files etc. On your computer's hardware square measure step by step coming back to a detailed. Today, the storage is fulfilling the necessity for additional cupboard space to carry all of your digital knowledge. Cupboard space suppliers operate giant knowledge centers, and folks united nations agency need their knowledge to be hosted purchase or lease storage capability from them.

Operators, within the background, virtualizes the resources consistent with the wants of the client and expose them as storage pools, that the purchasers will themselves use to store files or knowledge objects. Physically, the resource could span across multiple servers. Storage will be used from smaller computing devices to desktop computers and servers. Storage services is also accessed through an internet service api or through a web-based interface. The storage architectures build one virtual memory system. The info once keep on cupboard space has the subsequent threats:

1. Once knowledge is distributed, it's keep at multiple locations increasing the danger of unauthorized physical access to the info.
2. The amount of individuals with access to the info united nations agency may be compromised (i.E. Bribed or coerced) will increase dramatically.
3. It will increase the amount of networks over that the info travels. Rather than simply an {area|a neighborhood} area network (lan) or enclosure network (san), knowledge keep on a cupboard space needs a wan (wide space network) to attach them each.
4. Sharing of storage and networks with several alternative users/customers it's doable for alternative customers to access your knowledge.

To secure knowledge, most systems use a mix of techniques, including:

1. Encryption, which suggests they use a posh rule to write in code data. To rewrite the encrypted files, a user wants associate degree secret writing key. Whereas it's doable to crack encrypted data, most hackers haven't got access to the quantity of laptop process power they'd have to be compelled to decode data.
2. Authentication processes, that need making a user name and secret.
3. Authorization practices -- the consumer lists the people that square measure licensed to access data keep on the storage system. Several companies have multiple levels of authorization. As an example, a front-line worker might need terribly restricted access to knowledge keep on a storage system, whereas the top of human resources might need intensive access to files. Storage approach poses a possible security threat to your knowledge and furthermore, solely the secret access to storage isn't decent because the secret will be hacked by associate degree entrant. Conjointly the info will be captured en-

route to the storage services. The necessity to access storage on skinny shoppers and mobile
Devices is changing into associate degree rising application. However thanks to littleer processor speed associate degreed run time memory; these devices want an rule which may be utilized in such small computing devices. Security of keep knowledge and knowledge in transit is also a priority once storing sensitive knowledge at a cupboard space supplier.

I. PROBLEM STATEMENT

The problem statements area unit as follows:
User-id and arcanum don't seem to be lined in some applications. As a consequence, anyone un agency is curious about victimisation the programme will do thus. Causing a lucid text of knowledge to the receiver isn't secure. Since the info is decipherable, everybody will access it. Although the message is encoded before being sent, the hacker can decipher it with the assistance of a particular algorithmic rule. It's potential that the systems are not properly joined from time to time. As a consequence, the info being transmitted couldn't arrive within the correct format at its destination. Maintaining software package stability is very tough. The responsibility comes at a worth. Once the message falls into the hands of a hacker, the hacker has the power to insert, erase, or amendment the first message's content. If the message isn't adequately secured, the message's confidentiality is lost. A hacker will impersonate the sender and lead the recipient wide. As a result, a hacker will get round the authentication method. In bound cases, hackers area unit unable to get the first message's content. Therefore they perform the exponential attack. The hacker loses the content of the first message in associate in nursing exponential assault.

II. METHODOLOGY

The six main modules in this project are the User Interface, Insert Module, Retrieve Module, Sender Module, Receiver Module, and Support Module. These modules will be constructed individually first, and then all of them will be assembled together.

1) User Interface Module (Steganograph):
This module will effectively serve as the entry point for using the app's features. Since the application will be implemented as an MDI parent child property for user interface, this module will act as a parent type for other child types.

2) Embed Module:
This module enables you to add a message, as well as a text or data file, to an image, audio, or video file. It will also contain a "Encrypt" submodule, which will encrypt both the message and the data file. The embed module will use this encrypt module to encrypt data. The Embed File form's backend tasks will be handled by this module.

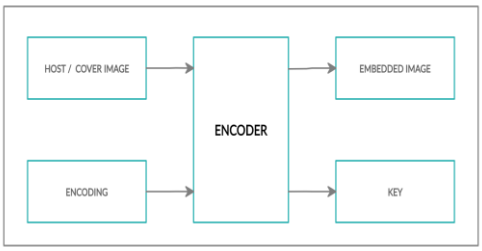


Figure 1 : Watermark Embedding

3) Retrieve Module:
This module will be able to extract the message, as well as the text or data file, from image, audio, and video files. It will also contain a "Decrypt" submodule, which will be responsible for decrypting the message and data file. The retrieve module will use this decrypt module to decrypt data. This module will be in charge of the Retrieve File type's backend function.

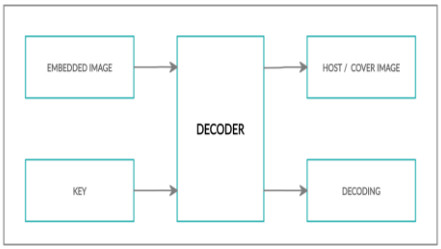


Figure 2 : Watermark Detection

4) Sender Module:

This module's main purpose will be to move files from one device to another. This module will use socket programming to transfer the file to other computers. This module will also have a user interface for children (Send File).

5) Receiver Module:
This module's primary function would be to accept files from other devices. This module can also use socket programming to accept files from other computers. This module will not have a user interface. It will run in the background quietly.

6) Help Module:

This module is responsible for providing help to the application. It will be introduced with both JAVA and HTML. The type for this module will be written in JAVA, and the support material will be written in HTML.

III. SYSTEM ARCHITECTURE

Overview of System Architecture

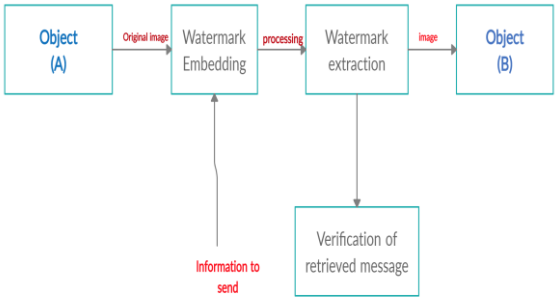


Fig 3 : Architecture Diagram

Hardware Requirement

1. A display drive that supports a 32-bit colour scheme is needed.

2. A display resolution of 1024 x 768 pixels is recommended.

3. A graphics drive capable of supporting a display resolution of 800 x 600 pixels.

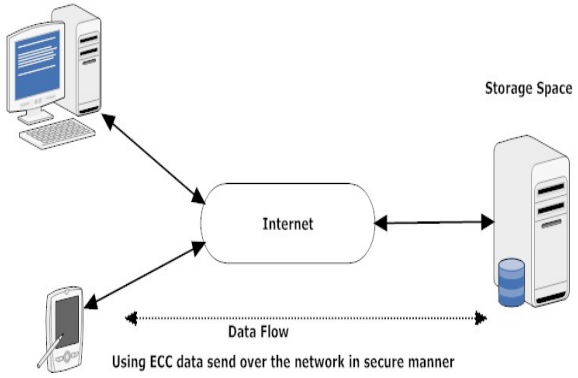
4. You'll need at least 128 MB of RAM.

5. The processor should hopefully be a Pentium III or higher/equivalent.

Software Requirement

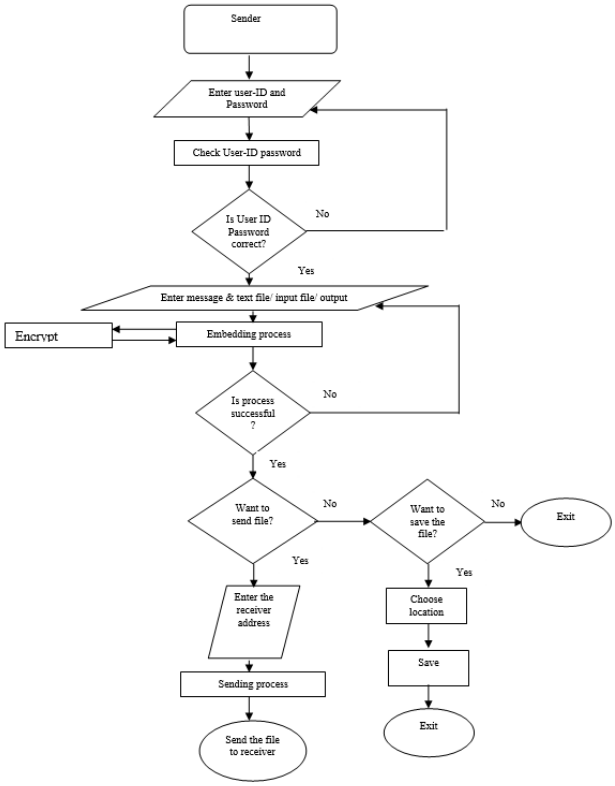
1. JDK 1.5 2. Any Windows, Macintosh, UNIX, or Solaris version

Figure 4 :

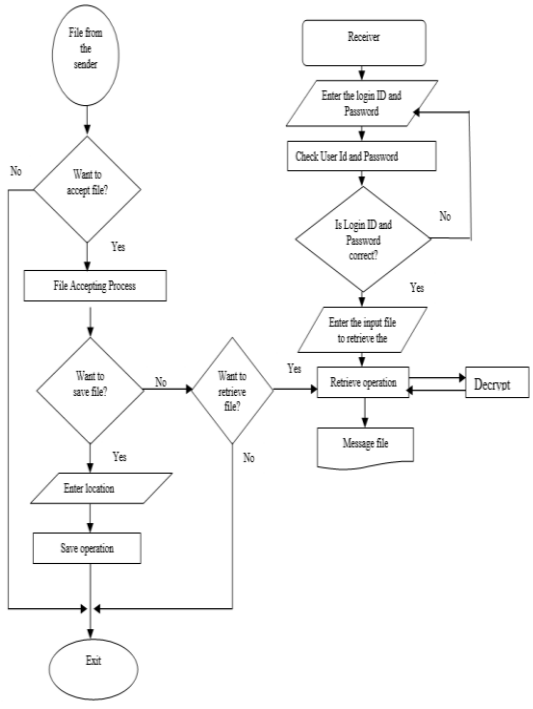


IV. SYSTEM DESIGN

System Flowchart



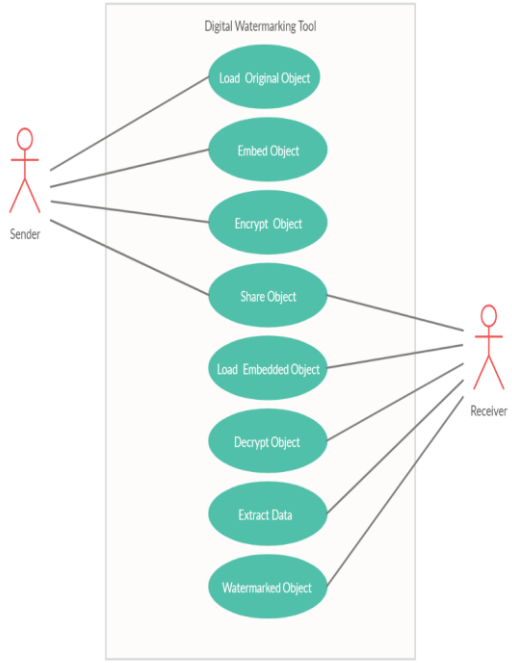
FLOW CHART OF SENDER



FLOWCHART OF RECEIVER

Use Case Diagram

Use Case Diagram involves the modular interactions between user and the system environment. Every Case is unique but is dependent on each other for interconnectivity and successful execution.



Use Case features the involvement of 2 actors:

1. **Customer/ Image Owner:**
   Customer is the user who requests for the watermarked Image. The entire project relies on proper execution and interaction of the customer with this Tool.
2. **Watermark Developer :**
   Watermark Developer is the person who processes the requests for the watermarked Image by the user.

Cryptography

Cryptography may be accustomed offer message confidentiality and integrity and sender verification. The essential functions of cryptography area unit encoding, secret writing and cryptanalytic hashing. So as to write and decipher messages, the sender and recipient have to be compelled to share a secret. Usually this is often a key, sort of a secret, that's employed by the cryptanalytic algorithmic program. The key's employed by the sender to write the message (transform it into cipher text) and by the recipient to decipher the message (reverse the cipher text back to clear text). This method may be done on a hard and fast message, like an e-mail, or a communications stream, like a tcp/ip affiliation. Cryptanalytic hashing is that the method of generating a fixed-length string from a message of capricious length. If the sender provides a cryptanalytic hash with the message, the recipient will verify its integrity. Trendy cryptanalytic systems area unit supported advanced mathematical relationships and processes. Let's specialise in the common cryptography standards accustomed secure pc communications and the way they're used.

The 3 basic kinds of cryptography in common use area unit radial key, uneven (public) key systems and cryptanalytic hash functions. Typically, the strength of a crypto system is directly associated with the length of the key. This assumes that there's no inherent weakness within the algorithmic program which the keys area unit chosen during a manner that totally utilizes the key area (the range of potential keys). There are a unit several types of attacks that may be used against crypto systems, however these area unit on the far side our scope here. That said, if you utilize public algorithms with no better-known vulnerabilities, use affordable key lengths and select smart keys (which area unit unremarkably chosen for you), your communications are terribly secure.

The components that area unit essential in cryptosystems area unit as follows :

1. Text in plain language (input)
2. Algorithm for encrypting data
3. The key to the vault
4. Text ciphered
5. Algorithm for decryption

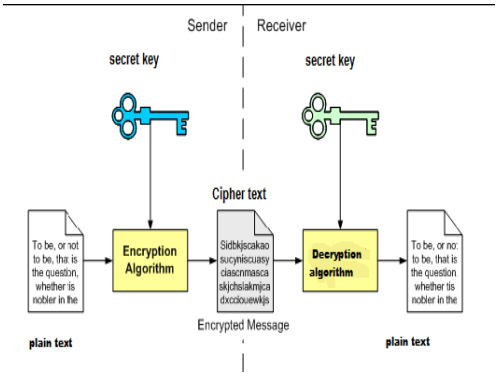


Figure 5 : General model of cryptographic system

Plain text: the initial piece knowledge|of knowledge|of information} needed to submit data to the supposed recipient. Plain text is that the name of the coding formula. Any cryptanalytic system's main secret's

referred to as it. The plain text is subjected to totally different substitutions and transformations during this coding formula. The key secret's used as associate degree input to the coding formula that the user specifies.

Various substitutions and transformations on the plain text will disagree supported this key. The performance of the coding formula is named cypher text. The disorderly text is that the cypher text. Every secret key that has been given to the coding formula ends up in a distinct cypher text. The "decryption formula" is that the inverse of the "encryption algorithm." it'll soak up cypher text and therefore the secret key as input and output plain text.

V. ANALYSIS

Basics of steganography:

Steganography aims to conceal data during a piece of cowl information in such a way that non-participating persons aren't able to discover the presence of this data by analysing the data detection. In contrast to watermarking, steganography doesn't mean to stop the hidden data by opponents of removing or dynamical the hidden message, that is embedded within the cowl information however it emphasizes on remains it undetectable. Steganography is especially attention-grabbing for applications during which the coding cannot accustom defend the communication of direction.

Image steganography

Hiding the info by taking the duvet object as an image is referred to as image steganography. In image steganography, constituent intensities area unit accustomed to hide the info. In digital steganography, pictures area unit wide used cowl supply as a result of there area unit range of bits presents in digital illustration of a picture.

Audio steganography

In audio steganography, the secret message is embedded into a digitized audio signal that result in slight sterilization of the binary sequence of the corresponding audio file. There area unit many ways area units out there for audio steganography. We have a tendency to area unit reaching to have a quick introduction on a number of them. It involves concealing information in audio files. This methodology hides the info in wav, au and mp3 sound files. There area unit totally different ways of audio steganography. These ways area unit

I) low bit coding

Ii) section committal to writing

Iii) unfold spectrum.

Video Steganography

It is a method of concealing any quite files or information into digital video format. During this case video (combination of pictures) is employed as carrier for concealing the info. Usually separate circular function remodel (dct) alter the values (e.G., 8.667 to 9) that is employed to cover the info in every of the photographs within the video, that is unnoticeable by the human eye. H.264, mp4, mpeg, avi area unit the formats utilized by video steganography.

In all of those strategies, the fundamental principle of steganography is that a secret message is to be embedded in another cowl object which can not be of any significance in such the way that the encrypted information would finally show solely the duvet information. Therefore it can not be detected simply to be containing hidden info unless correct cryptography is employed.

Functional Analysis

1. Login: login perform can demonstrate the sender if username and word area unit correct otherwise it'll exit the system.
2. Secret text message file: during this file you'll have to be compelled to write secret message to cover otherwise you will choose any computer file of secret message.
3. Cowl object: cowl object is that the object that is to be elect during which secret text message are often hidden.
4. Stego coding lsb implementation is performed on cowl object to cover secret text message by substitution bits of canopy object by the bits of message.
5. Sender during this sender send this stego object file to meant recipient to that he will wish to speak.
6. Receiver during this receiver receives the stego object and opens in decipherment choice for obtaining hidden text message within that image.

Non- Functional Analysis

1. Safety requirements: sender and receiver ought to certify that solely they're having an equivalent computer code to inscribe and decipher information within the image. Each ought to watch out of eavesdropping.
2. Security requirements: we tend to area units aiming to develop a computer code during which embedding secret

text information in the object(image, audio, video). Solely sender and receiver ought to bear in mind the encrypted file. The user shouldn't unfold the message concerning the sent image also as receiver info.

3. Computer code quality attributes: the standard of the computer code is maintained in such a way that solely sender and receiver will communicate through image, video, audio. There's no likelihood of knowing a secret object.

ADVANTAGES

1. Shorter keys are as strong as long key for RSA.
2. Low on CPU consumption.
3. Low on memory usage.
4. Size of encrypted data is smaller**.**

In today's world error correction code formula is employed just in case of key exchanges by certificate authority (ca) to share the general public key certificates with finish users. Elliptic curve cryptography could be a secure and a lot of economical coding formula than rsa

As it uses smaller key sizes for same level of security as compared to rsa. For e.G. A 256-bit error correction code public key provides comparable security to a 3072-bit rsa public key. The aim of this work is providing associate degree insight into the utilization of error correction code formula for encryption before uploading the documents on to the cloud. Elliptic curve cryptography (ecc) was discovered in 1985 by victor miller (ibm) and neil koblitz (university of washington) as an alternate mechanism for implementing

Public-key cryptography. Public-key algorithms produce a mechanism for sharing keys among massive numbers of participants or entities in an exceedingly complicated data system. In contrast to different well-liked algorithms like rsa, error correction code relies on separate logarithms that square measure far more tough to challenge at equivalent key lengths.

Every participant within the public key cryptography can have a try of keys, a public key and personal key, used for coding and secret writing operations. Public secret's distributed to all or any the participants wherever as non-public secret's notable to a selected

Participant solely.

Steganography With LSB Algorithm

Bytes of pixels unit ample to hold one message hardware unit. The rest of the bits inside the pixels remains

The same. Steganography is that the art and science of human action during a} very means hides the existence of communication. Steganography plays an important role in data security it is the art of invisible communication by concealing data inside completely different data. The term steganography comes from greek and just about suggests that lined writing. A steganography system consists of three elements: the cowl image (which hides the key message), the key message, and conjointly the stegano image(which is that the cowl object with a message embedded inside it). A digital image is drawn using a 2-d matrix of the color intestines at each grid purpose (i.E. Pixel). Generally, gray photos use eight bits, whereas colored utilizes 24 bits to clarify the color model, just like the RGB model. The steganography system uses an image as a result of the cowl, there unit several techniques to cover data inside cover-image. The abstraction domain techniques manipulate the cover-image part bit values to insert the key data. The key bits unit is written on to the quilt image part bytes. Consequently, the abstraction domain techniques unit easy and easy to implement. The tiniest quantity of significant bit (lsb) is one in every of the foremost techniques in abstraction domain image steganography.

The construct of lsb embedding is simple. It exploits the actual fact that the quantity of truth in many image formats is far larger than that perceivable by average human vision. Therefore, associate altered image with slight variations in its colours is indistinguishable from the initial by somebody's being, just by watching it. In customary lsb technique, that wants eight bytes of pixels to store 1byte of secret info but in planned lsb technique.

VI. CONCLUSION

Elliptic curve cryptography is a lot safe and reliable than first-generation public key techniques like RSA, which are presently in use. Once it involves upgrading their systems, vendors ought to seriously think about the elliptic curve possibility due to the procedure and information measure edges it provides whereas maintaining comparable security. Though the safety of ECC has not been absolutely assessed, it's expected to be widely utilized in the long run during a style of field. Once examination of the RSA and ECC cyphers, it had been discovered that ECC has considerably lower overheads than RSA. Since it will have an equivalent degree of protection as RSA by mistreatment shorter keys, the ECC features a ton of benefits. However, one flaw that might obscure its charm is its lack of maturity, as mathematicians conclude that not enough analysis has been worn out ecc. Since today's applications (smart cards, pagers, and cellular telephones, for example) cannot bear the overheads introduced by

RSA, ECC seems to own a far better future than RSA. ECC may be used for coding and coding in today's tiny computing devices as a result of it wants smaller key sizes and has less computing complexness than RSA. As a result, ECC is a superb possibility for compact, mobile, and low-power applications, still as cloud integration. The time taken by the 2 algorithms for key generation and coding is compared during this paper. The importance of this analysis is that it demonstrates the utilization of the ECC algorithmic rule in cloud storage, which provides improved protection. This analysis may be dilated to equate ECC with different algorithms for digital signatures, key exchanges, and information integrity.

VII. REFERENCES

[1] Study on Watermarking Techniques in Digital Images Purnima Pal1 M.Tech1(Communication Engineering) KNIT Sultanpur purnima22pal@gmail.com1

Harsh Vikram Singh2 Associate Prof.2(Electronics Department) KNIT Sultanpur harshvikram@gmail.com2

Sarvesh Kumar Verma3 M.Tech3(Communication Engineering) KNIT Sultanpur sarvesh24816@gmail.com3

[2] A Robust Double-Blind Secure High Capacity Watermarking and Information Hiding Scheme For Authentication and Tampering Recovery Via the Wavelet and Arnold Transforms

S. Swapnil and D. B. Megherbi - Center for Computer Man/Human Intelligence Networking and Distributed Systems (CMINDS),Department of Electrical and Computer Engineering, University of Massachusetts, Lowell, MA

[3] An Invisible Watermarking Technique For Image Verification.

Minewa M. Yeung and Fred Mintzer - IBM T.J. Watson Research Center, Yorktown Heights, NY 10598. {yeung,mintzer} @ watson.ibm.com

[4] Elliptic curve cryptography,

https://en.wikipedia.org/wiki/Elliptic_curve_cryptography

[5] RSA (algorithm),

http://en.wikipedia.org/wiki/RSA_(algorithm)

[6] JavaTM Cryptography Extension (JCE), Reference Guide.

http://docs.oracle.com/javase/1.5.0/docs/guide/security/jce/JCE

RefGuide.html