Fuzzy Systems and Soft Computing
ISSN : 1819-4362

THE ROLE OF STEGANOGRAPHY IN SOCIAL MEDIA USING BIT PLANE ALGORITHM

Dr. N. Kalaivani, Assistant Professor, Department of Information Technology, Sri Krishna Adithya College of Arts and Science, Coimbatore : kalaivhani@gmail.com
GeethaDevi M, III B.Sc. Information Technology, Department of Information Technology, Sri Krishna Adithya College of Arts and Science, Coimbatore : geethadevimurugesan@gmail.com

ABSTRACT

Steganography or data hiding is used to protect the privacy of information in the transit; it has been observed that the information that flows through Online Social Networks (OSN) is very much unsafe. Therefore, people hesitate to communicate their sensitive data on social media. Most of the information on the online social network is not useful to users and appears to disregard such details. People's actions provided a possibility for digital Steganography through the Internet.. TCPIP covert channels were used for steganography until the last decade. People began to utilize social media as a covert conduit to communicate hidden messages to targeted users as social media grew in popularity. There are numerous Online Social Networks accessible nowadays, ranging from Facebook to the more contemporary Twitter and Instagram. All of them may be utilized as covert channels without the general public noticing. The primary characteristic of steganography is the protection of information privacy; nonetheless, it has been utilized more for illicit message transmission, which is a source of concern. To make matters worse, adversaries are using steganalysis techniques to mess with the concealed data. In this work we propose a novel approaches for cryprtography and stegonagraphy for Information Masking. We weave the texture synthesis process into masking with image to conceal secret messages using RSA algorithm for encryption. In contrast to using an existing cover image to hide messages, our proposed Bit Plane algorithm for steganography conceals the source texture image and embeds secret messages through the process of texture synthesis. This allows us to extract secret messages and the source texture from a stego synthetic texture. High volumetric data is embedded into bit-planes as low as possible to keep message integrity, but at the cost of an extra bit-plane encoding procedure and slightly changed compression ratio. The proposed method can be easily integrated into the JPEG2000 image coder, and the produced stego-bit stream can be decoded normally.

Keywords: - OSN, TCPIP, RSA, JPEG, DWT

I. INTRODUCTION

Steganography is a very old method that dates back about 2000 years, and digital steganography has just been around over the last two decades. People utilized covert channels to hide text, image, audio, video, and network protocols like TCP/IP in the early phases of the digital era.

In the recent decade, people began to use clandestine social media platforms. As the Internet grew in popularity, so did social media networks, which began to generate massive amounts of data on a regular basis. The majority of the data created is unimportant and unattended, and individuals prefer to ignore large chunks of social media data. People's attitudes influenced the development of social media steganography.

Social media has brought transformative changes in the individuals and it removed the barriers that were existed. The main idea of being the user of online social network is to stretch out to oneself to multiple communities of certain interest. Engaging in sharing the work with communities in social media, that facilitates connection with similar interest people, information, and discussions and so on.

Social media is described as forms of electronic Communication and it was initiated byWWWthrough a website, SIX DEGREES in 1997. In 2000, MySpace and LinkedIn two social media sites were released. Then in 2007, very famous Facebook and later hundreds of social media sites were released. Social media and networks made our lives lucrative; it is a huge evolution that helped globalization of education, business, culture, social life, etc. Though there are plenty of positive aspects, the negativity factors namely, cyber bullying, illegal content, harassment, stalking, Child abuse, health impact, terror utilization, are equally dominant.

Social networking (SNSs) has become an important part of the medium for communicating inside and around interpersonal relationships. The strongest SNS is Facebook in the United States and beyond. One theory why? Facebook is the most popular social networking site. It is the selection of services that consumers are offered. Online connections allow users to quickly interact with members of the network. Facebook may also have a negative effect on relationships that are romantic. Studies have shown that Facebook can foster romantic jealousy. Given that each participant has a major negative relationship and psychological experience linked to Facebook, social media management and its role in our relationships should be an important part of education in media literacy. It's nothing new to Steganography. It has got the history of usage in the malware as the first instance. This concept had used even before 440 BCE. Namely, the ancient royal people of Greece used to shave the slaves head, on their head tattooing some secret message, and then before sending them to the other destination; used to wait for hair to grow so that such an act could not be recognized by any enemies. This way, it has been transformed up to the age of digital Steganography. Steganography is a Greek word meaning ``covered writing". The sender of the message encodes the secret on an innocent text, and whoever receives decodes the same to get back the secret.

The process of data concealment and extraction is depicted in the Figure 1 below. Two users, Alice and Bob, function as transmitter and receiver, respectively. Alice and Bob need to communicate privately and invisibly via the Internet (Online Social Networks), and Steganography can enable them do so. Alice transmits the secret information to Bob by embedding it in a normal-looking cover file using a specific technique. Bob receives the Stego object and extracts the secret using the same technique. Between the source and the target, there would always be attackers known as `Steganalysts' (in our case, Wendy), who would study the messages and then attack them. Recently, people of social media are using the image and text Steganography more to send their messages. Steganography alone cannot provide complete anonymity; sometimes, it reveals the existence of the secret. Even attackers can come to know and tries to decode it; the certain time they may succeed in their mission as well. It is very important for a sender to protect their message and the second level of security in the form of encryption might be employed. GoogleC and Facebook today are recognized social media networks that are being used for secret sharing. Flickr is another similar kind of Social media for photo-sharing website.

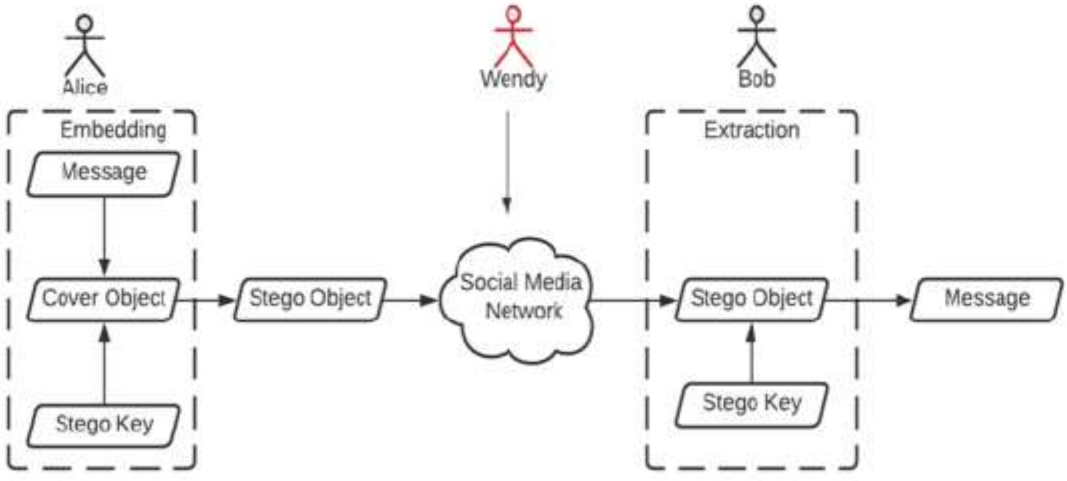


Figure 1: The process of data hiding in social media networks.

Purpose of the system

The main purpose of the system is to improve the security by using RSA algorithm and for hiding and compressing the capacity in JPEG2000 wavelet transform (DSP) is used.

Scope of the System

The system scope includes the following

- To reliably embed high-volume data into the JPEG2000 bit-stream
- To encryption data hide to image using wave let transformer. It is gives high performance
- To encryption data hide to image using wave let transformer. It is gives high level security

II. LITERATURE STUDY

System analysis will be performed to determine if it is flexible to design information based on policies and plans of organization and on user requirements and to eliminate the weakness of present system. This chapter discusses the existing system, proposed system and highlights of the system requirements.

EXISTING SYSTEM

For JPEG2000 compressed images, it is necessary to enlarge the hiding capacity because the available redundancy is very limited. In addition, the bitstream truncation makes it difficult to hide information.

In JPEG coding system, quantized DCT coefficients are entropy encoded without distortion to get the final compressed bitstream. Secure information hiding can be achieved simply by modification on the quantized DCT coefficients. A DCT domain hiding scheme can be applied in JPEG very conveniently.

DISADVANTAGES OF EXISTING SYSTEM

- A typical steganographic application includes covert communications between two parties whose existence is unknown to a possible attacker and whose success depends on detecting the existence of this communication
- Most image steganographic algorithms adopt an existing image as a cover medium. The expense of embedding secret messages into this cover image is the image distortion encountered in the stego image.
- No significant visual difference exists between the two stego synthetic textures and the pure synthetic texture.

III. DEVELOPMENT OF STEGANOGRAPHY ROLE IN SOCIAL MEDIA USING BIT PLANE ALGORITHM

As the latest still image coding international standard, JPEG2000 is based on discrete wavelet transform (DWT) and embedded block coding and optimized truncation algorithm. It offers superior compression performance to JPEG, and puts emphasis on scalable compressed representations.

In JPEG2000 coding system, bit stream is rate-distortion optimizing truncated after bit-plane encoding. The secret message will be destroyed by the truncating operation if it is embedded directly into the lowest bit-plane of quantized wavelet coefficients. Although there exist many kinds of DWT domain hiding schemes, most of them cannot be fitted into JPEG2000 directly.

An image reversible data hiding algorithm which can recover the cover image without any distortion from the stego image after the hidden data have been extracted. Here for encrypting the secret message we use RSA algorithm and for masking the encrypted message we use bit plane encoding algorithm.

ADVANTAGES:

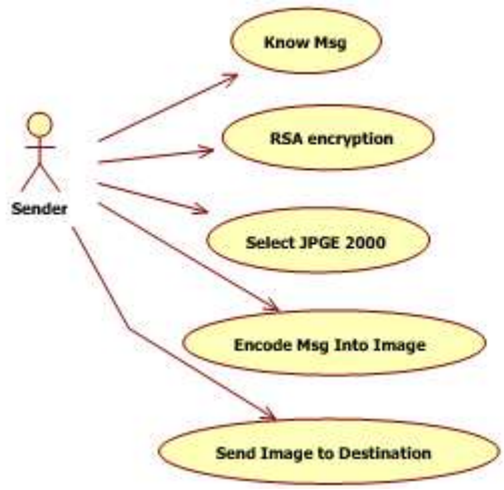
- It has verified that our proposed algorithm can provide various numbers of embedding capacities, produce a visually plausible texture images, and recover the source texture.
- We believe our proposed scheme offers substantial benefits and provides an opportunity to extend steganographic applications.

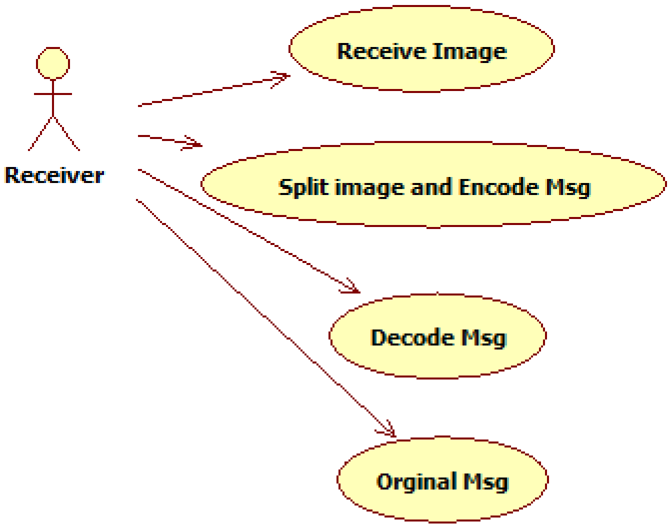
SYSTEM ANALYSIS AND DESIGN

Use Case Diagram:

A use case diagram is a graph of actors, a set of use cases enclosed by a system boundary, communication (participation) associations between the actors and users and generalization among use cases. The use case model defines the outside (actors) and inside (use case) of the system’s behavior.

Sender: **Reciever:**

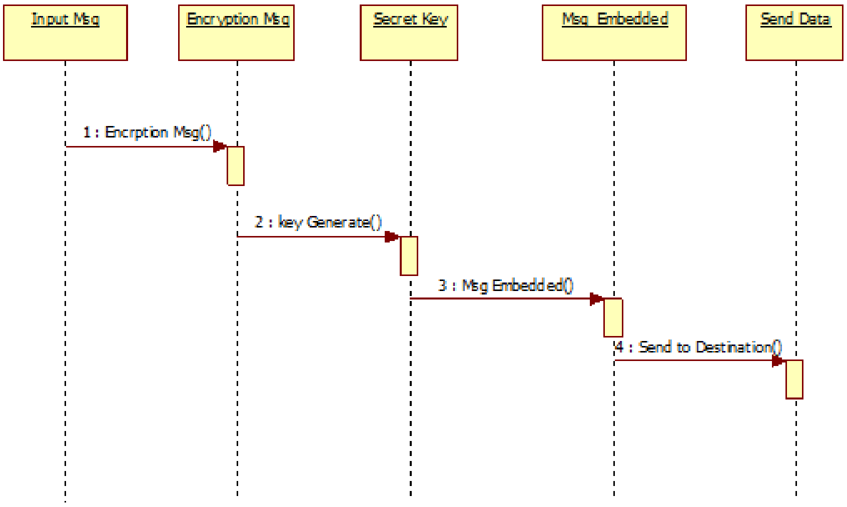




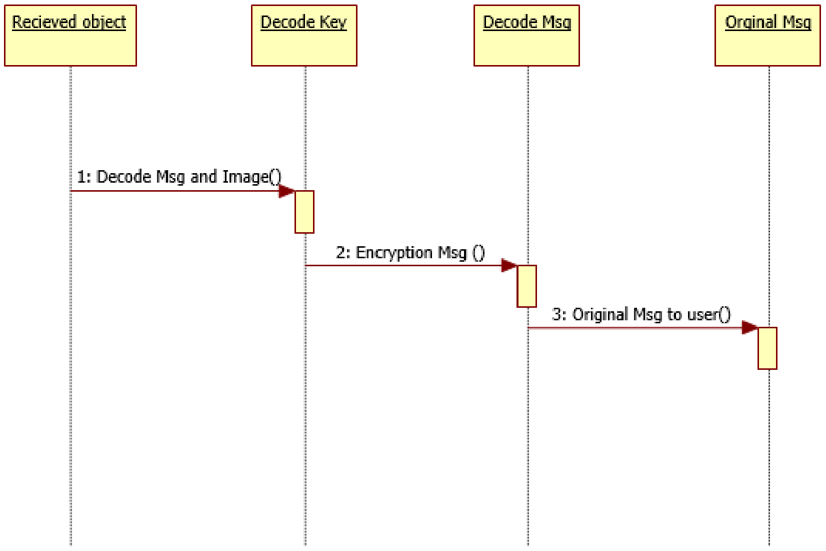
Sequence Diagram:

Sequence diagram are an easy and intuitive way of describing the behavior Of a system by viewing the interaction between the system and its environment. A Sequence diagram shows an interaction arranged in a time sequence. A sequence diagram has two dimensions: vertical dimension represents time; the horizontal Dimension represents different objects. The vertical line is called is the object's life line. The lifeline represents the object's existence during the interaction

Sender:

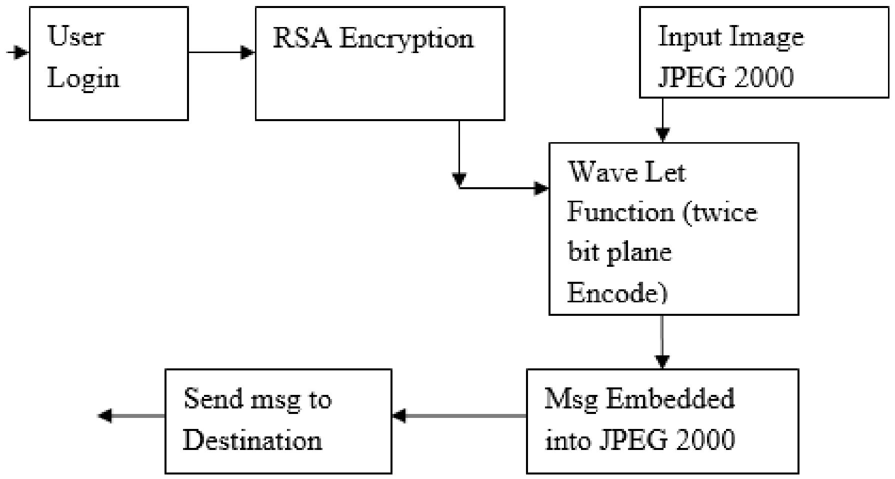


Receiver:

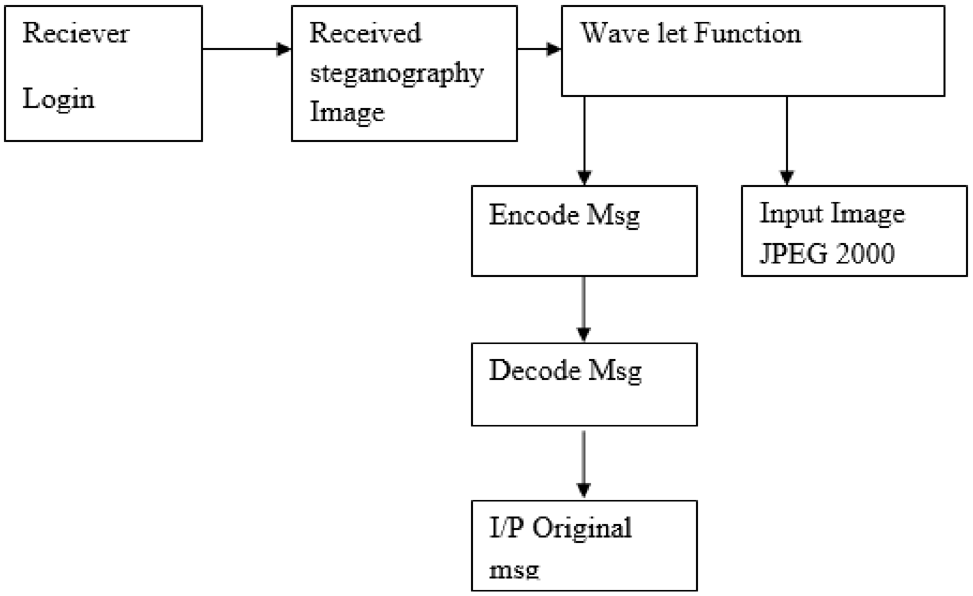


System Architecture:

Encode:


User Login
RSA Encryption
Input Image JPEG 2000
Wave Let Function (twice bit plane Encode)
Msg Embedded into JPEG 2000
Send msg to Destination

Decode:



MODULE DESIGN

Encoding side:

Message Encryption using RSA

Message Embedded into Image using Twice bit-plane encoding.

Decoding side:

Message Extraction

Decryption Message

1. RSA Encryption

The cryptographs depicts the simple concept that is: at the sender side, where the plaintext gets transformed into cipher textual content by the use of encryption algorithms, Cipher textual content is conveyed over the communicating channel and subsequently at the destination part the cipher textual content is transformed to the authentic plain textual content by using the use of decryption algorithm. It utilizes highly straightforward operations like growth and XOR expansion. The RSA algorithm is named after Ron Rivest, Adi Shamir and Len Adleman, who invented it in 1977. The basic technique was first discovered in 1973 by Clifford Cocks of CESG (part of the British GCHQ) but this was a secret until 1997. The patent taken out by RSA Labs has expired. The RSA cryptosystem is the most widely-used public key cryptography algorithm in the world. It can be used to encrypt a message without the need to exchange a secret key separately. The RSA algorithm can be used for both public key encryption and digital signatures. Its security is based on the difficulty of factoring large integers. Party A can send an encrypted message to party B without any prior exchange of secret keys.

2. Twice bit-plane encoding

Embedding points and embedding intensity for a code block.

• The wavelet coefficients greater than a given threshold are chosen as candidate embedding points.

• According to the rate-distortion optimization, the lowest bit-plane which keeps unabridged after bitstream truncation is determined as the lowest embed-allowed bitplane of the code block.

• The embedding points and embedding intensity are adjusted adaptively on the basis of redundancy evaluation.

Scrambled synchronization

Scrambled synchronization information and secret messages are embedded into the selected embedding points from the lowest embed-allowed bit-plane to higher ones. The synchronization information structure and the scrambling measure.

Rate-distortion optimization.

By doing this, messages are embedded into bit-planes that would not be truncated by rate-distortion optimization. The integrality of the embedded message is ensured at the cost of increased computational complexity and slightly changed compression ratio. The twice bit-plane encoding procedure is explained to execute the bit-plane encoding twice.

3. Message extraction

First, the lowest bit-plane with complete information of all its three coding passes can be determined easily in the procedure of entropy decoding. Then the embedding points and their intensity are determined by the method similar to the encoder. Finally, both synchronization information and secret messages are extracted.

IV. RESULTS AND DISCUSSION

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:'

- ➢ What data should be given as input?
- ➢ How the data should be arranged or coded?
- ➢ The dialog to guide the operating personnel in providing input.
- ➢ Methods for preparing input validations and steps to follow when error occur.

OBJECTIVES

1.Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.

2. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.

3.When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant.

Thus the objective of input design is to create an input layout that is easy to follow.

OUTPUT DESIGN

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
2.Select methods for presenting information.
3.Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

- ❖ Convey information about past activities, current status or projections of the
- ❖ Future.
- ❖ Signal important events, opportunities, problems, or warnings.
- ❖ Trigger an action.
- ❖ Confirm an action.

DATABASE DESIGN

Databases are normally implemented by using a package called a Data Base Management System (DBMS). Each particular DBMS has somewhat unique characteristics, and so such, general techniques for the design of database are limited. One of the most useful methods of analyzing the data required by the system for the data dictionary has developed from research into relational database, particularly the work of E.F.Codd. This method of analyzing data is called "Normalization". Unnormalized data are converted into normalized data by three stages. Each stage has a procedure to follow.

NORMALIZATION:

The first stage is normalization is to reduce the data to its first normal form, by removing repeating items showing them as separate records but including in them the key fields of the original record.

The next stage of reduction to the second normal form is to check that the record, which one is first normal form, all the items in each record are entirely dependent on the key of the record. If a data item is not dependent on the key of the record, but on the other data item, then it is removed with its key to form another record. This is done until each record contains data items, which are entirely dependent on the key of their record.

The final stage of the analysis, the reduction of third normal form involves examining each record, which one is in second normal form to see whether any items are mutually dependent. If there are any item there are removed to a separate record leaving one of the items behind in the original record and using that as the key in the newly created record.

BUSINESS MODELING:

The information flow among business function is modeled in a way that answers the following questions: what information drives the business process? What information is generated? What generate it? Where does the information go? Who process it?

DATA MODELING:

The information flow defined as a process of the business modeling is refined into a set of data objects that are needed to support the business. The characteristics (called attributes) of each object are identified and relationships between these objects are defined.

PROCESS MODELING:

The data objects defined in the data-modeling phase are transformed to achieve the information flow necessary to implement a business function. Processing description is created for addition, modifying, deleting, or retrieving a data object.

TABLE DESIGN:

This table is used to store the User Name and their Password.

ENCODING PART

S. NO	FIELD NAME	DATA TYPE
1	User name	Character
2	Password	Character

DECODING PART

S. NO	FIELD NAME	DATA TYPE
1	User name	Character
2	Password	Character

IMPLEMENTATION

The implementation phase focuses how the engineer attempts to develop the system. It also deals with how data are to be structured, how procedural details are to be implemented, how interfaces are characterized, how the design will be translated into programming and hoe the testing will be performed. The methods applied during the development phase will vary but three specific technical tasks should always occur.

- The software design
- Code generation
- Software testing

The system group has changed with responsibility to develop a new system to meet requirements and design and development of new information system. The source of these study facts is variety of users at all level throughout the organization.

Stage of Development of a System

- Feasibility assessment
- Requirement analysis
- External assessment
- Architectural design
- Detailed design
- Coding
- Debugging
- Maintenance

Feasibility Assessment

In Feasibility this stage problem was defined. Criteria for choosing solution were developed, proposed possible solution, estimated costs and benefits of the system and recommended the course of action to be taken.

Requirement Analysis

During requirement analysis high-level requirement like the capabilities of the system must provide in order to solve a problem. Function requirements, performance requirements for the hardware specified during the initial planning were elaborated and made more specific in order to characterize features and the proposed system will incorporate.

External Design

External design of any software development involves conceiving, planning out and specifying the externally observable characteristic of the software product. These characteristics include user displays, report formats, external data source and data links and the functional characteristics.

Internal Design Architectural and Detailed Design

Internal design involved conceiving, planning out and specifying the internal structure and processing details in order to record the design decisions and to be able to indicate why certain alternations were chosen in preference to others. These phases also include elaboration of the test plans and provide blue prints of implementation, testing and maintenance activities. The product of internal design is architectural structure specification.

The work products of internal design are architectural structure specification, the details of the algorithm, data structure and test plan. In architectural design the conceptual view is refined.

Detailed Design

Detailed design involved specifying the algorithmic details concerned with data representation, interconnections among data structures and packaging of the software product. This phase emphasizes more on semantic issues and less synthetic details.

Coding

This phase involves actual programming, i.e, transacting detailed design into source code using appropriate programming language.

Debugging

This stage was related with removing errors from programs and making them completely error free.

Maintenance

During this stage the systems are loaded and put into use. They also get modified accordingly to the requirements of the user. These modifications included making enhancements to system and removing problems.

V. CONCLUSION AND FUTURE ENHANCEMENT

Information masking using digital keys for image steganography has been implemented. An efficient steganographic method for embedding secret messages into cover images without producing any major changes has been accomplished through bit plane encoding method. In this work, a new way of hiding information in an image with less variation in image bits have been created, which makes our technique secure and more efficient. This technique also applies a cryptographic method i.e. RSA algorithm to secure the secret message so that it is not easy to break the encryption without the key.

RSA algorithm itself is very secure that’s why we used in this technique to increase the security of the secret message. A specified embedding technique uses hash function and also provide encryption of data uses RSA algorithm; makes our technique a very much usable and trustworthy to send information over any unsecure channel or internet.

This technique have been applied to.jpeg images; however it can work with any other formats with minor procedural modification like for compressed images. Performance analysis of the developed technique have been evaluated successfully.

SCOPE FOR FUTURE ENHANCEMENT

The future scope for the proposed method might be the development of an enhanced steganography that can have the biometric authentication module along with encryption and decryption. Meanwhile the work can be enhanced for other data files like video, audio, text. Similarly the steganography technique can be developed for 3D images. The further work may contain combination of this method to message digesting algorithms.

VI. BIBLIOGRAPHY

[1] M. Asikuzzaman and M. R. Pickering, “An overview of digital video watermarking,” IEEE Trans. Circuits Syst. Video Technol., vol. 28, no. 9, pp. 2131–2153, 2018.

[2] M. Asikuzzaman, M. J. Alam, A. J. Lambert, and M. R. Pickering, “Imperceptible and robust blind video watermarking using chrominance embedding: A set of approaches in the DT CWT domain,” IEEE Trans. Inf. Forensics Security, vol. 9, no. 9, pp. 1502–1517, 2014.

[3] M. Asikuzzaman, M. J. Alam, A. J. Lambert, and M. R. Pickering, “Robust DT CWT-based DIBR 3D video watermarking using chrominance embedding,” IEEE Trans. Multimedia, vol. 18, no. 9, pp. 1733–1748, 2016.

[4] J. Fridrich, Steganography in digital media: principles, algorithms, and applications. Cambridge University Press, 2009.

[5] T.-Y. Liu and W.-H. Tsai, “A new steganographic method for data hiding in microsoft word documents by a change tracking technique,” IEEE Trans. Inf. Forensics Security, vol. 2, no. 1, pp. 24–30, 2007.

[6] B. Li, S. Tan, M. Wang, and J. Huang, “Investigation on cost assignment in spatial image steganography,” IEEE Trans. Inf. Forensics Security, vol. 9, no. 8, pp. 1264–1277, 2014.

[7] C. Qin, C. C. Chang, Y. H. Huang, and L. T. Liao, “An inpaintingassisted reversible steganographic scheme using a histogram shifting mechanism,” IEEE Trans. Circuits Syst. Video Technol., vol. 23, no. 7, pp. 1109–1118, 2013.

[8] Y. Huang, C. Liu, S. Tang, and S. Bai, “Steganography integration into a low-bit rate speech codec,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 6, pp. 1865–1875, 2012.

[9] D. Xu, R. Wang, and Y. Q. Shi, “Data hiding in encrypted H.264/AVC video streams by codeword substitution,” IEEE Trans. Inf. Forensics Security, vol. 9, no. 4, pp. 596–606, 2014.

[10] S. Li and X. Zhang, “Towards construction based data hiding: From secrets to fingerprint images,” IEEE Transactions on Image Processing, doi:10.1109/TIP.2018.2878290.