IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A New Reversible Data Hiding in Encrypted Image Based on Multi-Secret Sharing and Lightweight Cryptographic Algorithms

1Ms.M.Madhavi Latha, 2Ms.M.Nikitha, 3Ms.T.Geetha, 4Mr.M.Raja

1Student, 2Student, 3Student, 4Professor

1Kalasalingam University,

2Kalasalingam University,

3Kalasalingam University,

4Kalasalingam University

Abstract-The data hiding in an encrypted image (RDHEI) is being introduced for preserving an image privacy and the data embedding, RDHEI is usually involves in three parts, namely, 1. Image provider, 2. Data hider, and 3. Data receiver. Here for the security we used three keys theyare: Shared Independent Secret Key (SIK), Shared One Key (SOK), Shared No Secret Key (SNK).In Secret Key SIK, the image provider and data hider shares the secret keys with the data receiver independently. No secret key has been shared in SNK. The proposed SNK scheme uses homomorphic encryption with the computational cost is low. In the secret key SOK, image provider shares a key with the data receiver. Here we proposed a new technique multi secret sharing under encryption.

I. INTRODUCTION

The Reversible data hiding in an encrypted image allows the additional and secret message to cover media such as military or medical images, and to perform the reversible procedure that extracts hidden secret messages. Two seminal ideas in data hiding are difference expansion and histogram shifting. In difference expansion method, the difference between two adjacent pixels are doubled to release a Least Significant bit (LSB). In histogram shifting, method, zero and peak points are used to embedded the secret message by modifying the values of pixel. Medical images are encrypted for preserving the patient privacy. A database administrator embedded a few data into encrypted images. RDHEI technique not only ensures the accuracy of image but also preserves the privacy of the image. The receiver can also be divided into two steps, Decryption and Extraction. We can specify these two kinds of receivers as Rdec and Rext. Rdec performs decryption and rext takes the decrypted image to extract the secret message.

II. SYSTEM STUDY

II.1 FEASIBILITY STUDY:

Feasibility or the state of the project can be analyzed during this phase and have a general plan for the project and cost estimation. It ensures that the system which was newly proposed has not a burden to the organization. For the analysis of feasibility some major requirements are needed. In this feasibility study three key considerations are involved. II.1.1

Economic Feasibility II.1.2. Technical Feasibility and II.1.3. Social Feasibility.

II.1.1 ECONOMIC FEASIBILITY:

For the proposed system, organization needs to make a good investment so that the financial benefits are equal or less than the cost of the system but not exceeds the cost of the system. Each and every organization wants to reduce the cost and at the same time they wants to maintain the quality of service. The proposed system will reduces the cost, manual work and the speed of work is increased.

II.1.2 TECHNICAL FEASIBILITY:

Technical feasibility is nothing but the study of the software. Some technical issues were raised during feasibility study of the system. It evaluates the both hardware and software requirements. The proposed system uses the JSP as front end and Oracle as back end. It provides sufficient memory to process the data. The installation process of the system is very efficient. The system accepts the requests from the user and gives the responses without delay.

II.1.3 SOCIAL FEASIBILITY:

Social feasibility meets the requirements of an organization. The proposed system is beneficiary when an organization knows about the information system. Social feasibility also measures how the people can able to work with system. The system is more supported and friendly to the user. The techniques are defined in a proper manner to avoid the loss of data. The working will be more easier and flexible.

III. PROPOSED SYSTEM

To achieve better efficiency, we constructed an efficient scheme to create Shared Independent Key (SIK). For preserving privacy, the receiver shares only one secret key with the image provider. The advantages of this proposed system is High Security, no time elapsing and the Key field is allotted as text document.

IV. ALGORITHM

Cryptographic Algorithm used in this reversible data hiding in an encrypted image is Least Significant Algorithm (LSB)which is used to encrypt the data. It is a common and simple approach to embedded the information in an image. The Cryptographic algorithm LSB is used to convert the image into three parts such as Red, Green, Blue (RGB). Each color has 0 to 255 values and these three colors are used to collect the pixels that converts the image to encrypt. Least Significant Bit is a technique in which pixels of image is replaced with the data bits. This approach is easy to understand and implement.

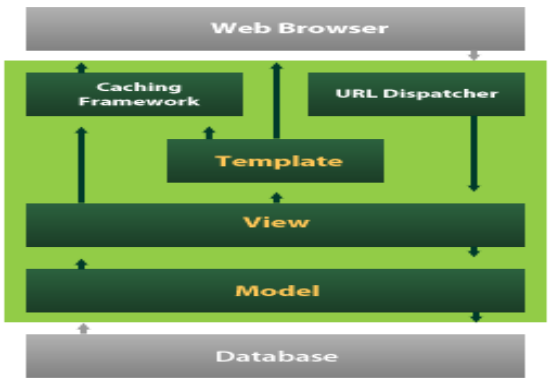
V.DETAIL DESCRIPTIONOF TECHNOLOGY

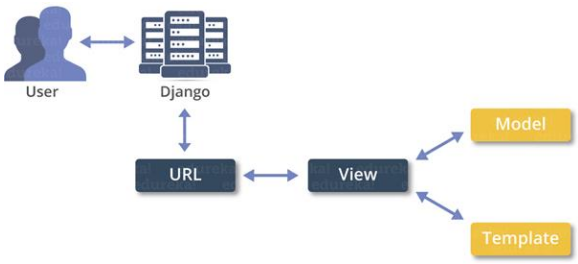
V 1.1 AN INTRODUCTION TO PYTHON:

Python isaobject-oriented,high-level, interpreted, interactive language. Python has a design philosophy that emphasizes code readability and a syntax that allows programmers to express codein languages such as C++ or java.Python interpreters are available for many operating systems. CPython is a open source software and it is the reference implementation of python. Python features are dynamic type systemand automatic memory management.

DJANGO:

Django is a high-level Python Web framework. Django encourages rapid development and clean,pragmatic design. It focuses on the Web development, and also writing your app without needing the wheel. It is a free and opensource framework. It's primary goal is to create of complex, database-driven websites. It also emphasizes reusability and pluggability of components. Python is used for settings files and data models. Django provides administrative create, read, update and delete interfaces and having introspection and configured admin models.





VI. SYSTEM DESIGN

VI 1.1 INPUT DESIGN:

Input design a link between the user and the information system. It procedures for data preparation and developing specification and put transaction data in to a usable form can be achieve by the inspecting the computer to read data from a written or document or occur by having people keying the data directly from the system.The input focus on the amount of input required, controlling the errors, avoiding extra steps.The input provides security and retaining the privacy.

OBJECTIVES:

Input Design is the converting process of user-oriented description of the input into a computer-based system.This design is more useful for avoiding errors and also it having the correct information from

the computerized system. It having user-friendly screens for data entry to handle large volume of data. The main goal of input is to make data easier and free from errors. It provides record viewing facilities. Validity is checked when the data is entered. With the help of Screens data can be entered. The objective of the input design is to create an input layout for easy follow.

VI 1.2 OUTPUT DESIGN:

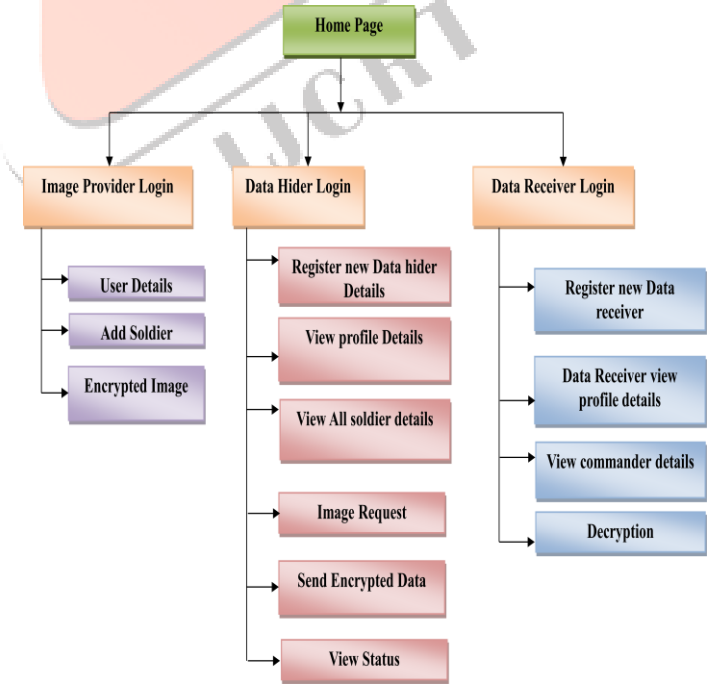
The output having quality is one, which presents the information clearly for end user. In any system the results are communicated to the users to the other systems through outputs. However, the information is displaced for the user through hard copy result. It is the most important and direct source information for the user. Output design improves the system's relationship with efficient and intelligent way to help users decision. Computer output is proceed in an organized well thought out manner. The right output must be developed while each output element is designed so that people will easily find the system. In analysis computer output the specific output should identify to meet the requirements. For presenting we use selective methods. Create document, report, or other formats contain information that can be produced by the system. The output should contain the following objectives. Convey information about past activities, current status or projections, future, signal important events, opportunities, problems, or warning, trigger an action, and confirm an action.

VII. SYSTEM ARCHITECTURE

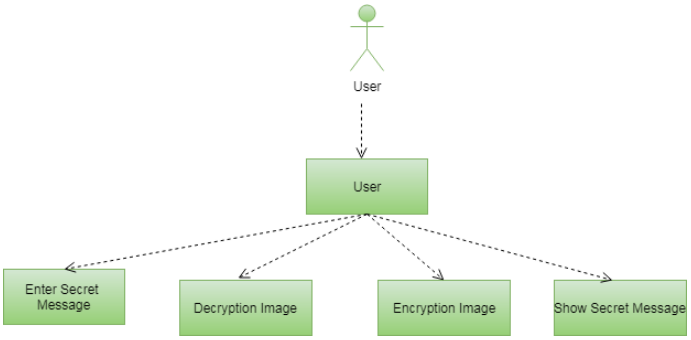
VII.1 SYSTEM ARCHITECTURE

A system architecture is the computational design that defines the structure and behavior of a system architecture description is a formal description of a system,that organized in a way that supports reasoning about the structural properties of the system. It defines the system components and provides the plan from which procured and system developed,that will work together to implement the overall system.

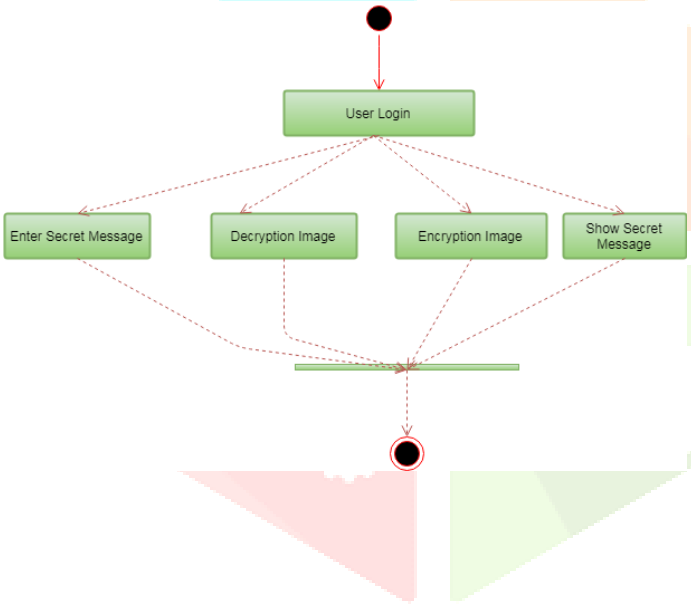
VII..2 DATA FLOW DIAGRAM



UML DIAGRAM



ACTIVITY DIAGRAM



VIII. SYSTEM IMPLIMENTATION

This is the stage where the theoretical design is turned into working system. The critical stage is to achieve a successful system and in giving confidence on this system for the users, it involves in careful planning, investing on the current system and constraints on implementation, design of methods to achieve the change in methods.

The process begins with preparing a plan of the system .According to these activities are to be carried out in this plans.

The coding step translate a design into a programming language.it is a communication between humans and system .The characteristics and coding style can profoundly affect software quality.The coding is done with the following characteristics.

- Ease of design to code translation
- Code efficiency
- Memory efficiency
- Maintainability

The user should be careful in implementing a project to ensure that whether it is implemented properly or not.The user should not change the purpose while implementing

This is the stage of the project which is considered as the critical stage in achieving a successful new system the new system will work effectively.it involves in careful planning, investigation on its constraints, design of methods to achieve changeover methods.

MODULES:

Encryption

Secret sharing acts as symmetric encryption to encrypt the cover image. In this method we use one shared key between P and R. However it does not construct shares for each pixel like Wu et also method. For preserving the total size, we pack t pixels and t random factors together to generate t shares and puts back as encrypted pixels and random factors as key. By using t random factors it avoid the size blow-up and also keeps decryption correctly. The technique is inspired by the multi secrete sharing but slightly modified for security.

Data embedding

We divide the message into several units then for embedding a unit we generate t shares without a key and then we use homomorphic evaluation and embedding procedure to embed message into the encrypted pixels.

Secret Sharing

It serves as the underlying primitive offering security, multiple secrete preserve complexity in size and inherently homomorphism realizes the data embedding. The formal description of the technique is provided and present a notion called OAMSS –operating addition homomorphism in multi

secret sharing. We also provide another technique to compare the key size used in OAMSS.

IX. SYSTEM TESTING

It is an important stage in any development life cycle.The main purpose of this testing is to find errors and it provides a way to check the functionality of components.There are various types in test in which each addresses a specific requirement.It is carried out to ensure that the system that not fail,that it meets the specifications and satisfies the user,here the system developed is tested with duplicate or original data

It is the critical process that consume half of the development time.The following are the attributes of good test.

- A good test should not be redundant
- Should be best of breed
- Should be neither simple nor complex

IX.1. UNIT TESTING

In this the analyst test the program. The software units in a system are the modules and routines are assembled to perform a specific function. In a large system modules on different levels are needed. It can be performed from the bottom up with the smallest and lowest level modules and proceeding at a time. In bottom up testing for each module a short program execute and provides the needed data

IX.2 INTEGRATION TESTING

Integration testing is a systematic technique for constructing the program structure while conducting test to uncover errors. Objectives are used to take unit testing and build program structure that has been directed by design.

The testing is performed when all the modules were to make it a complex system. The project will work successfully after integration.

IX.3. VALIDATION TESTING

Validation testing can be defined in many ways, but simply defined is that can be reasonably expected by the customer.

One of two possible condition exists after validation test

- The characteristics confirm to specification and accepted
- A deviation from specification is uncovered and deficiency list created
- In this project the validation test is performed against module. Then it is tested with valid and invalid inputs for the field id.

IX.4 WHITE BOX TESTING

It is sometimes called as glass box testing. It is test case design method that uses the control structure of the procedural design to derive test cases. By using this we can derive test cases that

- Guarantee that all independent paths with in a module have been exercised at least once.
- Exercise all logical decisions on their true or false side
- Execute all loops at their boundaries and within their operational bounds
- Exercise internal data structure to assure their validity

This test is performed against the patient module.without entering any text if we apply it displays the message"First add record and then save it".

IX.5 BLACK BOX TESTING

This method treats the coded module as a blackbox.It runs with inputs that are likely to cause errors.Then the output is checked to see the errors occurred. This method cannot used to test all errors because some of the errors may depend on the code or algorithm used to implement the module .

X. CONCLUSION

In this class only a image provider had a secret key with the receiver and if another knows the embedding procedure can hide.SOK is much weaker than SNK in flexibility. However existing SNK is rely on additive homomorphic encryption. We convert SNK scheme with some properties to a SOK version.

REFERENCES

- Tian, "A new technique for the Reversible embedding data by using expansion method," IEEE transactions on circuits and systems for video technology, vol. 13, no. 8, pp. 890–896, 2003.
- Y. Shi and N. Ansari "Protectively Reversible data hiding in an encrypted images," IEEE Transactions on circuits and systems for video technology, 2006.
- Mr.Hong, "Securily Data can be hiding based on the error energy control and histogram shifting," Optical communication,2012.
- W. Hong and T.S. Chen, "Reversible data hiding by using the prediction and the histogram shifting," Journal of Systems and Software,2010.
- S. Jung, S.-J. Ko et al., "Reversible data hiding algorithm by considering human visual system," IEEE Signal Processing Letters,2011.