IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

STEGANOGRAPHY METHOD FOR EMBEDDING MESSAGE IN JPEG IMAGES

DR.D.PRASANNA M.E; PH.D[1],PRIYANKA M[2],PRIYADHARSHINI S[3],VINITHA T[4]
1 ASSOCIATE PROFESSOR, 2,3,4 UG STUDENTS
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
MAHENDRA ENGINEERING COLLEGE, TAMILNADU, INDIA

ABSTRACT

Content-based image retrieval is a process framework that applies computer vision techniques for searching and managing large image collections more efficiently. With the growth of large digital image collections triggered by rapid advances in electronic storage capacity and computing power, there is a growing need for devices and computer systems to support efficient browsing, searching, and retrieval for image collections.

We propose a RDH with triple DES block-based transformation algorithm to achieve the purpose of image content protection. More importantly, under the proposed image content protection framework, image retrieval and image convolution can also be performed directly on the content-protected images.

As a consequence, not only secure image storage and communication are accomplished, but also the computation efforts can be fully distributed, thus making it a perfect match for nowadays popular cloud computing technology. Security analyses are conducted to prove that the proposed image encryption scheme offers certain degree of security in both statistical and computational aspects.

Keywords : DES block, JPEG Image & Testing

INTRODUCTION

1.1 IMAGE PROCESSING

Image processing involves changing the nature of an image either improve its pictorial information for human interpretation or render it more suitable for autonomous machine perception. digital image processing, which involves using a computer to change the nature of a digital image. The digital image define as a two-dimensional function, f(x, y), where x and y are spatial (plane) coordinates, and the amplitude of f at any pair of coordinates (x, y) is called the intensity or gray level of the image at that point. When x, y, and the amplitude values of f are all finite, discrete quantities.

ENHANCING THE REPRESENTATION OF AN IMAGE

Enhancing the edges of an image to make it appear sharper. It Makes image as a more pleasant image. Sharpening edges is a essential component of printing , in order for an image to appear “at its best” on the printed page

(II) IDENTIFY MATCHING FROM AN IMAGE

Matching being random errors in the image. Matching is a very common problem in data transmission all sorts of electronic components may affect data passing through image, and the results may be undesirable. Matching may take many different forms each type of Matching requiring a different method

(III) IDENTIFY MOTION BLUR FROM AN IMAGE

Motion blur may occur when the shutter speed of the camera is too long for the speed of the object. The photographs of fast moving objects: athletes, vehicles for example, the problem of blur may be considerable

(IV) OBTAINING THE EDGES OF AN IMAGE

Obtaining the edges of an image necessary for the measurement of objects in an image. The edges are used for measure their spread, and the area contained within the image . The edge result is necessary to enhance the original image slightly, to make the edges clearer.

(V) IDENTIFY DETAIL FROM AN IMAGE

The measurement or counting purposes, all the details of an image is not necessary . Example, a machine inspected items on an assembly line, the only matters of interest may be shape, size or colour is used to simplify the image . Measure the size and shape of the animal without being distracted by unnecessary detail.

ASPECTS OF IMAGE PROCESSING

Image precession has three aspects

1.2 IMAGE MINING

Image mining deals with the extraction of implicit knowledge, image data relationship, or other patterns not explicitly stored in the images and Image mining is more than just an extension of data mining to image domain.Image mining has two main themes

- Mining large collection of images
- Combined data mining of large collections of image and associated alphanumeric data.

IMAGE MINING PROCESS

The three major image mining steps are as follows:

FEATURE EXTRACTION

Segment images into regions identifiable by region descriptors (blobs). Ideally one blob represents one object is also called segmentation.

OBJECT IDENTIFICATION AND RECORD CREATION

Compare objects in one image to objects in every other image. Label each object with an id.This step is the preprocessing algorithm.

Create auxiliary images

Generate images with identified objects to interpret the association rules and apply data mining techniques .

Image Copy Detection

The increasing availability of digital multimedia data, the integrity verification of image data becomes more and more important . Digital images distributed through the Internet may suffer from several possible manipulations . To ensure trustworthiness, image copy detection techniques have emerged to search duplicates and forgeries.Image copy detection can be achieved via image hashing or watermarking techniques. The current hashing techniques may be not very robust to some image manipulations while watermarking techniques will suffer from some distortions induced by data embedding. Recently, SIFT (scale invariant feature transform) has been exposed to be invariant to several image variability's, and efficient to image copy detection. Extract compact local feature descriptors via constructing the basis of the SIFT-based feature vectors extracted from the secure SIFT domain of an image. Image copy detection can be efficiently accomplished based on the sparse representations and reconstruction errors of the features extracted from an image possibly manipulated by

Image Retrieval

The most popular image retrieval approach is Content-based approach image retrieval (CBIR) . A query image, extract its Dictionary Score feature (with atoms) and transmits the features into an image database, the each image is stored together with its Dictionary Score feature and original SIFT feature vectors . The most common technique is to measure the similarity between two images

by comparing the extracted image features.

Content based image retrieval

Content-based image retrieval (CBIR) systems needed to effectively and efficiently use large image databases. A CBIR system, users will be able to retrieve relevant images based on their contents. CBIR systems followed two distinct directions

- Based on modelling the contents of the image as a set of attributes which is produced manually and stored, for example in a relational database.
- Using an integrated feature-extraction/object-recognition system.

Mainly the differences can be categorized in terms of image features extracted, their level of abstraction and the degree of domain independence. Certainly tradeoffs must be made in building a CBIR system. For example, having automatic feature extraction is achieved at the expense of domain independence. A high degree of domain indepence is achieved by having a semiautomatic (or manual) feature extraction component. With CBIR systems, querying is facilitated through generic query classes. Increasingly specialized grouping activities that produces a "blob world" representation of an image, which is a transformation from the raw pixel data to a small set of localized coherent regions in color and textual space.

SYSTEM ANALYSIS

3.1 EXISTING SYSTEM

This is the most common form of text search on the Web. Most search engines do their text query and retrieval using keywords. In early search engine that offered disambiguation to search terms. User intention identification plays an important role in the intelligent semantic search engine.

The similarity assessment is fundamentally important to many multimedia information processing systems and applications such as compression, restoration, enhancement and copy detection etc. The Peak signal-to-Matching ratio(PSNR),Human visual system(HVS)and Natural Scene Statistics(NSS) are efficient to measure the quality of an image evaluated with its original version, particularly for some image restoration applications. The existing methods mainly focus on evaluating the similarities between a reference image and its non-geometrically variation versions, such as decompressed and brightness/contrast-enhanced versions.

3.2 PROPOSED SYSTEM

The proposed system Content-Based Image Retrieval (CBIR) uses RDH with triple DES algorithm the visual contents of an image such as color, shape, texture, and spatial layout to represent and index the image. Active research in CBIR is geared towards the development of methodologies for analyzing, interpreting cataloging and indexing image databases. In addition to their development, efforts are also being made to evaluate the performance of image retrieval systems. This project proposes a novel approach for steganography using reversible texture synthesis. A texture synthesis process re-samples a small texture image drawn by an artist or captured in a photograph in order to synthesize a new texture image with a similar local appearance and arbitrary size.

The patch-based method is used to embed a secret message during the synthesizing procedure. This allows the source texture to be recovered in a message extracting procedure, providing the functionality of reversibility.

The quality of response is heavily dependent on the choice of the method used to generate feature vectors and similarity measure for comparison of features. In this paper we proposed an algorithm which incorporates the advantages of various other algorithms to improve the accuracy and performance of retrieval.

3.3 FEASIBILITY STUDY

Preliminary investigation examine project feasibility, the likelihood the system will be useful to the organization. The main objective of the feasibility study is to test the Technical, Operational and Economical feasibility for adding new modules and debugging old running system. All system is feasible if they are unlimited resources and infinite time. There are aspects in the feasibility study portion of the preliminary investigation:

- Technical Feasibility
- Operation Feasibility
- Economical Feasibility

3.4 ECONOMIC FEASIBILITY

A system can be developed technically and that will be used if installed must still be a good investment for the organization. In the economical feasibility, the development cost in creating the system is evaluated against the ultimate benefit derived from the new systems. Financial benefits must equal or exceed the costs.

The system is economically feasible. It does not require any addition hardware or software. Since the interface for this system is developed using the existing resources and technologies available at NIC, There is nominal expenditure and economical feasibility for certain.

3.5 OPERATIONAL FEASIBILITY

Proposed projects are beneficial only if they can be turned out into information system. That will meet the organization's operating requirements. Operational feasibility aspects of the project are to be taken as an important part of the project implementation. Some of the important issues raised are to test the operational feasibility of a project includes the following: -

- Is there sufficient support for the management from the users?
- Will the system be used and work properly if it is being developed and implemented?
- Will there be any resistance from the user that will undermine the possible application benefits?

This system is targeted to be in accordance with the above-mentioned issues. Beforehand, the management issues and user requirements have been taken into consideration. So there is no question of resistance from the users that can undermine the possible application benefits.

The well-planned design would ensure the optimal utilization of the computer resources and would help in the improvement of performance status.

3.6 TECHNICAL FEASIBILITY

The technical issue usually raised during the feasibility stage of the investigation includes the following:

- Does the necessary technology exist to do what is suggested?
- Do the proposed equipments have the technical capacity to hold the data required to use the new system?
- Will the proposed system provide adequate response to inquiries, regardless of the number or location of users?
- Can the system be upgraded if developed?
- Are there technical guarantees of accuracy, reliability, ease of access and data security?

Earlier no system existed to cater to the needs of 'Secure Infrastructure Implementation System'. The current system developed is technically feasible. It is a web based user interface for audit workflow at DB2 Database. Thus it provides an easy access to the users. The database's purpose is to create, establish and maintain a workflow among various entities in order to facilitate all concerned users in their various capacities or roles. Permission to the users would be granted based on the roles specified.

Therefore, it provides the technical guarantee of accuracy, reliability and security. The software and hard requirements for the development of this project are not many and are already available in-house at NIC or are available as free as open source. The work for the project is done with the current equipment and existing software technology. Necessary bandwidth exists for providing a fast feedback to the users irrespective of the number of users using the system.

SYSTEM ENVIRONMENT

4.1 HARDWARE REQUIREMENTS:

- System : Pentium Core 2 Duo
- Hard Disk : 80 GB
- RAM : 1 GB
- Key Board : LG
- Mouse : Logitech
- Monitor : 15 inch TFT Color monitor

4.2 SOFTWARE REQUIREMENTS:

- Operating System : Windows 10
- Front end : NetBeans8.1/JDK
- Coding lamguage : Java

SOFTWARE DESCRIPTION

5.1 FRONT END

FEATURES OF JAVA

Java platform has two components:

- The Java Virtual Machine (Java VM)
- The Java Application Programming Interface (Java API)

The Java API is a large collection of ready-made software components that provide many useful capabilities, such as graphical user interface (GUI) widgets. The Java API is grouped into libraries (packages) of related components.

The following figure depicts a Java program, such as an application or applet, that's running on the Java platform. As the figure shows, the Java API and Virtual Machine insulates the Java program from hardware dependencies.

As a platform-independent environment, Java can be a bit slower than native code. However, smart compilers, well-tuned interpreters, and just-in-time byte code compilers can bring Java's performance close to that of native code without threatening portability.

SOCKET OVERVIEW

A network socket is a lot like an electrical socket. Various plugs around the network have a standard way of delivering their payload. Anything that understands the standard protocol can “plug in” to the socket and communicate.

Internet protocol (IP) is a low-level routing protocol that breaks data into small packets and sends them to an address across a network, which does not guarantee to deliver said packets to the destination.

Transmission Control Protocol (TCP) is a higher-level protocol that manages to reliably transmit data. A third protocol, User Datagram Protocol (UDP), sits next to TCP and can be used directly to support fast, connectionless, unreliable transport of packets.

CLIENT/SERVER

A server is anything that has some resource that can be shared. There are compute servers, which provide computing power; print servers, which manage a collection of printers; disk servers, which provide networked disk space; and web servers, which store web pages. A client is simply any other entity that wants to gain access to a particular server.

A server process is said to “listen” to a port until a client connects to it. A server is allowed to accept multiple clients connected to the same port number, although each session is unique. To mange multiple client connections, a server process must be multithreaded or have some other means of

RESERVED SOCKETS

Once connected, a higher-level protocol ensues, which is dependent on which port user are using. TCP/IP reserves the lower, 1,024 ports for specific protocols. Port number 21 is for FTP, 23 is for Telnet, 25 is for e-mail, 79 is for finger, 80 is for HTTP, 119 is for Netnews-and the list goes on. It is up to each protocol to determine how a client should interact with the port.

JAVA AND THE NET

Java supports TCP/IP both by extending the already established stream I/O interface. Java supports both the TCP and UDP protocol families. TCP is used for reliable stream-based I/O across the network. UDP supports a simpler, hence faster, point-to-point datagram-oriented model.

INETADDRESS

The InetAddress class is used to encapsulate both the numerical IP address and the domain name for that address. User interact with this class by using the name of an IP host, which is more convenient and understandable than its IP address. The InetAddress class hides the number inside. As of Java 2, version 1.4, InetAddress can handle both IPv4 and IPv6 addresses.

The InetAddress class also has several other methods, which can be used on the objects returned by the methods just discussed.

Here are some of the most commonly used.

Boolean equals (Object other)-Returns true if this object has the same Internet address as other.

1. byte [ ] get Address ( )-Returns a byte array that represents the object's Internet address in network byte order.
2. String getHostAddress ( ) - Returns a string that represents the host address associated with the InetAddress object.
3. String get Hostname ( ) - Returns a string that represents the host name associated with the InetAddress object.
4. boolean isMulticastAddress ( )- Returns true if this Internet address is a multicast address. Otherwise, it returns false.
5. String toString ( ) - Returns a string that lists the host name and the IP address for convenience.

TCP/IP CLIENT SOCKETS

TCP/IP sockets are used to implement reliable, bidirectional, persistent, point-to-point and stream-based connections between hosts on the Internet. A socket can be used to connect Java's I/O system to other programs that may reside either on the local machine or on any other machine on the Internet.

There are two kinds of TCP sockets in Java. One is for servers, and the other is for clients. The Server Socket class is designed to be a "listener," which waits for clients to connect before doing anything. The Socket class is designed to connect to server sockets and initiate protocol exchanges.

The creation of a Socket object implicitly establishes a connection between the client and server. There are no methods or constructors that explicitly expose the details of establishing that connection. Here are two constructors used to create client sockets:

Socket (String hostName, int port) - Creates a socket connecting the local host to the named host and port; can throw an UnknownHostException or anIOException.

Socket (InetAddress ipAddress, int port) - Creates a socket using a preexisting InetAddress object and a port; can throw an IOException.

A socket can be examined at any time for the address and port information associated with it, by use of the following methods:

- InetAddress getInetAddress ( ) - Returns the InetAddress associated with the Socket object.
- Int getPort ( ) - Returns the remote port to which this Socket object is connected.
- Int getLocalPort ( ) - Returns the local port to which this Socket object is connected.

Once the Socket object has been created, it can also be examined to gain access to the input and output streams associated with it. Each of these methods can throw an IOException if the sockets have been invalidated by a loss of connection on the Net.

InputStream getInputStream ( ) - Returns the InputStream associated with the invoking socket.OutputStream getOutputStream ( ) - Returns the OutputStream associated with the invoking socket.

TCP/IP SERVER SOCKETS

Java has a different socket class that must be used for creating server applications. The ServerSocket class is used to create servers that listen for either local or remote client programs to connect to them on published ports. ServerSockets are quite different form normal Sockets.

When the user create a ServerSocket, it will register itself with the system as having an interest in client connections.

- ServerSocket(int port) - Creates server socket on the specified port with a queue length of 50.
- Serversocket(int port, int maxQueue) - Creates a server socket on the specified port with a maximum queue length of maxQueue.
- ServerSocket(int port, int maxQueue, InetAddress localAddress)-Creates a server socket on the specified port with a maximum queue length of maxQueue. On a multihomed host, localAddress specifies the IP address to which this socket binds.
- ServerSocket has a method called accept( ) - which is a blocking call that will wait for a client to initiate communications, and then return with a normal Socket that is then used for communication with

URL

The Web is a loose collection of higher-level protocols and file formats, all unified in a web browser. One of the most important aspects of the Web is that Tim Berners-Lee devised a scaleable way to locate all of the resources of the Net. The Uniform Resource Locator (URL) is used to name anything and everything reliably. URL provides a reasonably intelligible form to uniquely identify or address information on the Internet. URLs are ubiquitous; every browser uses them to identify information on the Web.

5.2 BACK END

MYSQL DEFINITION

A database is a separate application that stores a collection of data. Each database has one or more distinct APIs for creating, accessing, managing, searching and replicating the data it holds.

Other kinds of data stores can be used, such as files on the file system or large hash tables in memory but data fetching and writing would not be so fast and easy with those types of systems.

So nowadays, we use relational database management systems (RDBMS) to store and manage huge volume of data. This is called relational database because all the data is stored into different tables and relations are established using primary keys or other keys known as foreign keys.

A Relational DataBase Management System (RDBMS) is a software that:

- Enables you to implement a database with tables, columns and indexes.
- Guarantees the Referential Integrity between rows of various tables.
- Updates the indexes automatically.
- Interprets an SQL query and combines information from various tables.

RDBMS Terminology:

Before we proceed to explain MySQL database system, let's revise few definitions related to database.

- Database: A database is a collection of tables, with related data.
- Table: A table is a matrix with data. A table in a database looks like a simple spreadsheet.
- Column: One column (data element) contains data of one and the same kind, for example the column postcode.
- Row: A row (= tuple, entry or record) is a group of related data, for example the data of one subscription.
- Redundancy: Storing data twice, redundantly to make the system faster.
- Primary Key: A primary key is unique. A key value can not occur twice in one table. With a key, you can find at most one row.
- Foreign Key: A foreign key is the linking pin between two tables.
- Compound Key: A compound key (composite key) is a key that consists of multiple columns, because one column is not sufficiently unique.
- Index: An index in a database resembles an index at the back of a book.
- Referential Integrity: Referential Integrity makes sure that a foreign key value always points to an existing row.

PROJECT DESCRIPTION

6.1 PROBLEM DEFINITION

The keywords based searches they usually provide results from blogs or other discussion boards. The user cannot have a satisfaction with these results due to lack of trusts on blogs etc. low precision and high recall rate. The image similarity assessment is to design algorithms for repeated and objective evaluation of similarity in a consistent manner with individual human judgment. Image Quality of a test image is strongly related to the virtual information present in the image and that the information can be

6.2 OVERVIEW OF THE PROJECT

Assessment of image similarity is fundamentally important to numerous multimedia applications. The goal of similarity assessment is to automatically assess the similarities among images in a perceptually consistent manner. Specifically, a feature-based approach to quantify the information that is present in a reference image and how much of this information can be extracted from a test image to assess the similarity between the two images. Extract the feature points and their descriptors from an image, followed by learning the Dictionary Score /basis for the descriptors in order to interpret the information present in this image.

Represent all of the descriptors of an image via sparse representation and assess the similarity between two images via sparse coding technique. The main advantage is, a feature descriptor is sparsely represented in terms of a Dictionary Score or transferred as a linear combination of Dictionary Score atoms, so as to achieve efficient feature representation and robust image similarity assessment.

6.3 MODULE DESCRIPTION

6.3.1 IMAGE PREPROCESSING AND FEATURE EXTRACTION

In the input module, the feature vector from the input image is extracted and that input image is stored in the image dataset.

The feature vector of each image in the dataset is also stored in the dataset whereas in the second module i.e. query module, a query image is inputted. After that the extraction of its feature vector is done.

During the third module i.e. in the process of retrieval, comparison is performed. The feature vector of the query image is compared with the each vector stored in the dataset.

The features which are widely used involve: texture, color, local shape and spatial information.

There is very high demand for searching image datasets of ever-growing size, this is reason why CBIR is becoming very popular.

6.3.3 IMAGE ANALYSIS:

In this module that have two functions as below

Scale-space extrema detection

Searches over all scales and image locations.A difference-of-Gaussian function to identify potential interest points that are invariant to scale and orientation.

Key point localization

A key point has been found by comparing a pixel to its neighbors and is to perform a detailed fit to the nearby data for location, scale, and ratio of key curvatures. The low contrast points or poorly localized along an edges are removed by key point localization.

Color Retrieval Color retrieval system works in two stages.

1) In the first stage, Histogram based comparison is done and matching images are short listed.

2) In the second stage, the Color Coherence Vectors of the short listed images (stage 1) are used to refine the results.

Numbers of coherent and non-coherent pixels for all color intensities are calculated in the image.

Then size of coherency array, coherency array and no. of coherency pixels are stored as a vector.

1. Index Table Generation
2. Composition Image generation
3. Data Embedding
4. Data Extraction

6.3.7 DATA EMBEDDING AND EXTRACTION

This module embeds the secret message via the message-oriented texture synthesis to produce the final stego synthetic texture.

Compute ranks of all candidate patches. Select the candidate patch where its rank equals the decimal value of an *n*-bit secret message. In this way, a segment of the *n*-bit secret message has been concealed into the selected patch to be pasted into the working location.

The message extraction and authentication module contains three sub-steps.

The first sub-step constructs a candidate list based on the overlapped area by referring to the current working location.

The second sub-step is the match-authentication step.

The third sub step extracts all of the secret messages that are concealed in the stego synthetic texture patch by patch.

6.3.8 TRIPLE DES

In cryptography, Triple DES is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm. Triple DES uses a "key bundle" which comprises three DES keys, K1, K2 and K3, each of 56 bits (excluding parity bits).

Triple DES is simply another mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits. In Private

Encryptor, you simply type in the entire 192-bit (24 character) key rather than entering each of the three keys individually. The Triple DES DLL then breaks the user provided key into three sub keys, padding the keys if necessary so they are each 64 bits long. The procedure for encryption is exactly the same as regular DES, but it is repeated three times. The data is encrypted with the first key, decrypted with the second key, and finally encrypted again with the third key.

Consequently, Triple DES runs three times slower than standard DES, but is much more secure if used properly. The procedure for decrypting something is the same as the procedure for encryption, except it is executed in reverse. Like DES, data is encrypted and decrypted in 64-bit chunks. Unfortunately, there are some weak keys that one should be aware of: if all three keys, the first and second keys, or the second and third keys are the same, then the encryption procedure is essentially the same as standard DES. This situation is to be avoided because it is the same as using a really slow version of regular DES.

6.4 SYSTEM ARCHITECTURE **Data Embedding**

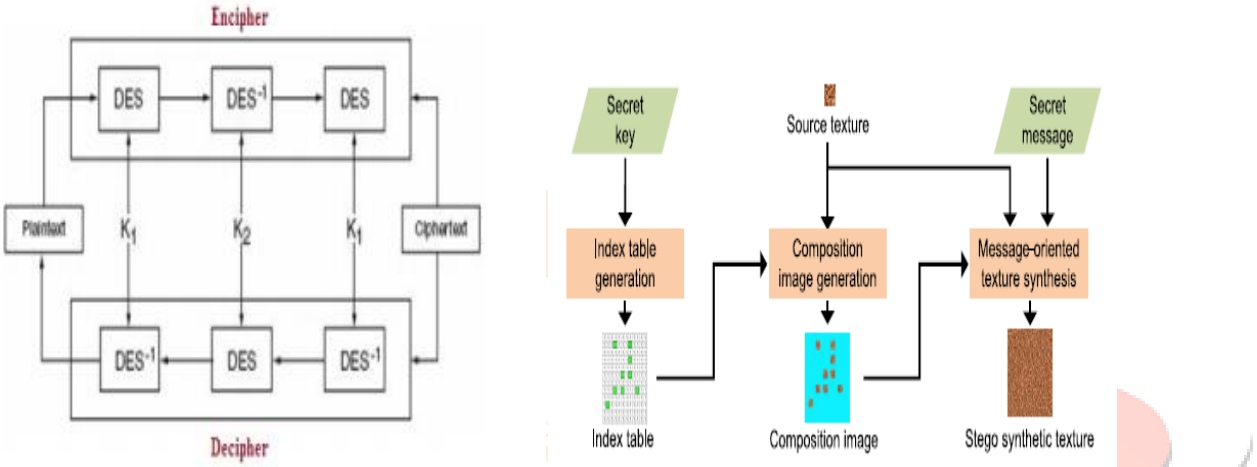

Figure 1.5

SYSTEM TESTING

SYSTEM TESTING

System testing is the stage of implementation, which is aimed at ensuring that the system works accurately and efficiently before live operation commences. Testing is vital to the success of the system. System testing makes a logical assumption that if all the parts of the system are correct, the goal will be successfully achieved. The candidate system is subject to a variety of tests.

A series of tests are performed for the proposed system before the system is ready for user acceptance testing.

The testing steps are:

- Unit testing
- Integration testing
- Validation testing
- Output testing
- User acceptance testing

7.1 UNIT TESTING

Unit testing focuses verification efforts on the smallest unit of software design, the module. This is also known as “module testing” .The modules are tested separately. This testing is carried out during programming stage itself. In this testing step, each module is found to be working satisfactorily as regard to the expected output from the module.

7.2 INTEGRATION TESTING

Data can be lost across an interface; one module can have an adverse effect on others; sub-functions when combined may not produce the desired major functions; integration testing is a systematic testing for constructing the program structure. While at the same

time conducting to uncover errors associated within the interface? The objective is to take unit tested modules and to combine them and test it as a whole. Here correction is difficult because the vast expenses of the entire program complicate the isolation of causes. This is the integration-testing step; all the errors encountered are corrected for the next testing step.

7.3 VALIDATION TESTING

Verification testing runs the system in a simulated environment using simulated data. This simulated test is sometimes called alpha testing. This simulated test is primarily looking for errors and monitions regarding end user and decisions design specifications hat where specified in the earlier phases but not fulfilled during construction.

Validation refers to the process of using software in a live environment in order to find errors. The feedback from the validation phase generally produces changes in the software to deal with errors and failures that are uncovered. Than a set of user sites is selected that puts the system in to use on a live basis. They are called beta tests.

The beta test suits use the system in day to day activities. They process live transactions and produce normal system output. The system is live in every sense of the word; except that the users are aware they are using a system that can fail. But the transactions that are entered and persons using the system are real. Validation may continue for several months. During the course of validating the system, failure may occur and the software will be changed. Continued use may produce additional failures and need for still more changes.

7.4 OUTPUT TESTING

After performing the validation, the next step is output testing of the proposed system, since no system could be useful if it does not produce the required output in the specified format. Asking the users about the format required by them tests the output generated or displayed by the system under consideration. Hence the output format is considered in two ways-one is on screen and another in printed format.

7.5 USER ACCEPTANCE TESTING

User acceptance of a system is the key factor for the success of any system. The system under consideration is tested for the user acceptance by constantly keeping in touch with the prospective system users at the time of developing and making changes whenever required. This is done in regard to the following point:

An acceptance test has the objective of selling the user on the validity and reliability of the system .it verifies that the system's procedures operate to system specifications and that the integrity of important data is maintained. Performance of an acceptance test is actually the user's show. User motivation is very important for the successful performance of the system. After that a comprehensive test report is prepared. This report shows the system's tolerance, Performance range, error rate and accuracy.

EXPERIMENTAL SETUP

The method used to evaluate the present technique is described in Fig. 2. The algorithm was applied on a bit mapped (bmp) image that has the size of 300 pixels x 300 pixels with 256 colors. In order to evaluate the impact of the number of blocks on the correlation and entropy, three different cases were tested. The number of blocks and the block sizes for each case are shown in Table I.

Each case produces three output images; (a) a ciphered image using the Blowfish algorithm, (b) a transformed image using the proposed algorithm, and (c) a ciphered image using the proposed algorithm followed by the Blowfish algorithm. For the rest of this paper, we use image A, image B, image C, and image D to denote the original image, the ciphered image using the Blowfish algorithm, the transformed image, and the ciphered image using the proposed algorithm followed by the Blowfish algorithm respectively.

Case Number	No.of.Blocks	Block Size
1	30*30	10*10
2	60*60	5*5
3	100*100	3*3

Table.1 Different Cases to Test the Impact of the Number of Blocks on the Correlation and Entropy.

CONCLUSION AND FUTURE ENHANCEMENT

In the RDH feature extraction, RDH transforms image data into scale-invariant coordinates virtual to local features and generates large numbers of features that compactly cover the image over the full range of scales and locations.

The low contrast points or poorly localized along an edges are removed by key point localization.

A key point has been found by comparing a pixel to its neighbors and is to perform a detailed fit to the nearby data for location, scale, and ratio of key curvatures.

To make the RDH feature more compact, the bag-of-words (BoW) representation approach quantizes RDH descriptors by vector quantization technique into a collection of visual words based on a pre-defined visual vocabulary or vocabulary tree .

REFERENCES

1. Y. Luo, X. Ouyang, J. Liu, and L. Cao, ‘‘An image encryption method based on elliptic curve elgamal encryption and chaotic systems,’’ IEEE Access, vol. 7, pp. 38507–38522, 2019, doi: 10.1109/access.2019.2906052
2. R. Zhang, S. Dong, and J. Liu, ‘‘Invisible steganography via generative adversarial networks,’’ Multimedia Tools Appl., vol. 78, no. 7, pp. 8559–8575, https://doi.org/10.1007/s11042-018-6951-z, Multimedia Tools and Applications (2019) 78: 8559–8575 springer
3. X. Duan, K. Jia, B. Li, D. Guo, E. Zhang, and C. Qin, ‘‘Reversible image steganography scheme based on a U-net structure,’’ IEEE Access, vol. 7, pp. 9314–9323, 2019, doi: 10.1109/access.2019.2891247.
4. Li-Wei Kang, Member, IEEE, Chao-Yung Hsu, Hung-Wei Chen, Chun- Shien Lu, Member, IEEE, Chih-Yang Lin, Member, IEEE, and Soo-Chang Pei, (2011) “Feature-Based Sparse Representation for Image Similarity Assessment”, IEEE Transactions on Multimedia, vol. 13, no. 5.
5. Sivic J and Zisserman A, (2003) “Video Google: A text retrieval approach to object matching in videos,” in Proc. IEEE Int. Conf. Computer Vision, Nice, France, vol. 2, pp. 1470–1477.
6.] C. Kim, “Content-based image copy detection,” Signal Process.: Image Commun., vol. 18, pp. 169–184, 2003
7. Lowe D. G, (2004) “Distinctive image features from scale-invariant keypoints,” Int. J. Comput. Vision, vol. 60, no. 2, pp. 91–110
8. Ke Y., Sukthankar R and Huston L, (2004) “Efficient near-duplicate detection and sub-image retrieval,” in Proc. ACM Multimedia.

.