Steganographic and Watermarking Using Masking with Face Recognition by using Hash Algorithm

M. Dhivyalakshmi
PG Student
Department of Computer Applications
IFET College of Engineering

K. Chitra
PG Student
Department of Computer Applications
IFET College of Engineering

M. Jayabharathy
PG Student
Department of Computer Applications
IFET College of Engineering

S. Sivachandiran
Assistant Professor
Department of Computer Applications
IFET College of Engineering

R. Aktharunisa Begum
Assistant Professor
Department of Computer Applications
IFET College of Engineering

Abstract

The world is going day by day towards digital thing due to easy handling, usage and best quality of work. The protection of digital identities is getting more and more crucial. Steganography is an art to hide the important data from the unauthorized user during transferring or communication through any medium. There are many algorithms for image steganography but this paper intends to show an overview of image steganography using secure hash algorithm, techniques and its uses, it also merges a watermarking using masking. It also attempts to determine the requirements of a better steganography algorithm that briefly display that which steganography techniques are more suitable for which applications.

Keywords: Face Recognition, Masking, Steganography, Secure hash algorithm, Watermarking

I. INTRODUCTION

Steganography and cryptography both are similar used to protect important information from unauthorized user. But the difference between these is Steganography hides and protect the information so it makes appearance that there is no existence of information is hidden in particular file or data. Steganography is a method for covering important data inside the image. The main purpose and aim of steganography is hidden communication between the parties. This paper is used to describe a new perfect hashing algorithm for steganography in the color images and also going to add watermarking to provide more protection to important data. There are two functions performed first hiding the information in the colorful image second is retrieving the information from the image without the leakage of the information. This operation encryption and decryption mechanism has also used for protection of data and also watermarking for the authorized user.

II. EXISTING SYSTEM

Data security basically means protection of data from unauthorized users or hackers and providing high security to prevent data modification. Some of the following algorithms like International Data Encryption Algorithm (IDEA) , Advanced Encryption Standard (AES) , Data Encryption Standard (DES) , are efficient and good for small amount of data but not sufficient for massive information sets as these algorithms involves more complex computation and required much fast processing machines.

A. Literature Survey:

Several steganography methods have been proposed in literature and most of which are performed in pixel domain. However major contribution is in the domain of Image Steganography. The existing methods are mainly based on LSB where LSBs of the cover file are directly changed with message bits.

Tseng and Pan presented a data hiding scheme in 2-color images, it embeds the information in any bit where at least one of the adjacent bits is the same as the original unchanged bit.

The Syntactic Approach relies on the syntactic structure of text to embed the watermark. At Allah et al. first proposed the natural language watermarking scheme by using syntactic structure of text.

Meral et al. provided an overview of available syntactic tools for text watermarking. Meral et al. also performed morpho-syntactic alterations to the text to watermark it.

All rights reserved by *www.ijste.org*

III. PROPOSED SCHEME

Information security has become very important for many purposes, sharing information between parties, mail, and private information, business deal, and protection from unauthorized user. There are many algorithms for image steganography. Some steganography techniques uses perfect hash function others are not. Steganography using hash function can be used for image, audio or video steganography by slightly changing work and selection of carrier. These are following some steganography algorithms.

Facial recognition is a process of verifying a person's identity by comparing the facial features of the person with those already stored in a database. It is most widely used in security systems. Every face has numerous, distinguishable landmarks called as nodal points. Each human face has many nodal points.

A. Hashing Based Approach For Secure Steganograph:

A perfect hashing approach used for important information hiding in the grey-scale images. This approach is based on a robust perfect hash-function algorithm. This approach is secure and more efficient that presents a more secure method of data transmission at higher Speed. This approach is effective in many ways that multiple file formats such as bmp, gif, jpeg, and tiff are also supported. Here used hashing-based algorithm for data hiding for grey-scale image steganography. but this is not proper secure for information authentication so in proposed approach ,some extra feature that is water marking and also steganography will be done in colorful image.

B. Watermarking Using Masking:

Watermarking is used to verify the identity and authenticity of the owner of a digital image. It is a process in which information which verifies the owner is embedded into the digital image or signal. These signals could be either videos or pictures or audios.

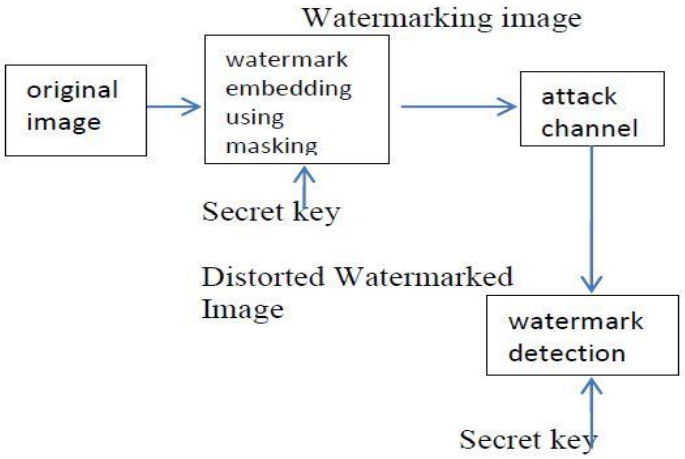

Fig.1: Watermarking Process

In embedding, an algorithm accepts the host and the data to be embedded and produce a watermarked image.

The person makes a modification is called an attack. The modification is not being malicious; the term attack arises from copyright protection application, where third parties may attempt to remove digital watermarking through modification.

Detection or extraction is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it.

C. Facial Recognition

Facial recognition is a process of verifying a person's identity by comparing the facial features of the person with those already stored in a database. Every face has numerous, distinguishable landmarks called as nodal points. Each human face has many nodal points. Few of the nodal points are as follows:

1. Width of the nose.
2. Distance between eyes.
3. Length of jaw line.
4. Shape of chin.

1) Acquisition:

Image acquisition module seeks and then extracts a region which contains only the face from the image picked up from the webcam. The image will then be resized and corrected geometrically and will eliminate the background and scenes which are unrelated to the face so that it is suitable for recognition.

2) Preprocessing:

The purpose of the preprocessing module is to reduce or eliminate some of the variations in face due to illumination. It performs normalization and filtering, improves image clarity, adjusts brightness and sets the default image size.

3) Feature Extraction (Principal Component Analysis):

The purpose of the feature extraction is to extract the feature vectors (Eigen vectors) which represent the face. This feature vector denotes the signature of the image. Signature matrix for the whole database is then computed. Euclidian distance of the image is then

All rights reserved by *www.ijste.org*

computed with all the signatures in the database. Image is identified as the one which gives a least distance with the signature of the image to recognize.

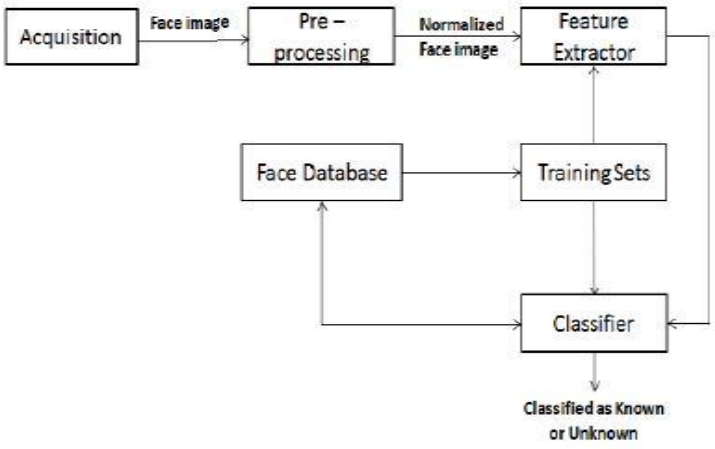

Fig.2: Facial Recognition Process

4) Classifier:

The purpose of the classification sub-module is to map the feature space of a test data to a discrete set of label data that serves as template. It compares the Eigen vectors with those already stored in the database library.

5) Training Sets:

It adjusts the feature extraction parameters to ensure optimization and accuracy.

D. The ∑ Hash Scheme:

Let M denote the original message that will be ∑ Hashed. During the first step M is hashed using any hashing algorithm fh , to produce the hash value H:

$$fh(M) = H$$

In the second step I embed the hash value H to M. This can be done by using an efficient and simple steganography algorithm called Selected LSB denoted by fs.The stego-key for the embedding process will be again the hash value H that was produced in the first step. The output of this step will be a stego-object called MS as follows:

$$fh(MS) = HS$$

By choosing H as a key eliminate the need for a key exchange and maintenance, as the hash value will be exchanged anyway. Furthermore, the steganography process ensures that the secret message, in our case the hash value, will be spread across the original message, regardless of its size and without affecting its appearance and functionality. Thus, the original object will remain function regardless of the embedded message.

$$fs(M, H, H) = MS$$

IV. OPERATIONS

A. Step 1:

Input the target image with any file format such as bmp, gif, jpeg, and tiff that has to use for hide information. The image provide user interface for the user to input an image to hide the personal data.

B. Step 2:

Input the target text to be hidden in the image in the form of the text file. This is the second input in the textual data that is stored in the text (.txt) file. Count characters in the message A. Let it is B. This input file will be read by the system and chunks of 3 characters will be made including space character. So, one chunk of data will be stored in place of one pixel in 8-bit color image.

As for example

Hi satya! How are you? [Hi][sat][ya!][ho][w a][ar][e y][ou][?]

To show end of the message, at the end of the message an End .of-file (EOF) character is stored using ASCII value of EOF that is 00.

C. Step 3:

Add this length B of message in the starting of message A and separate with #. Hide the target text in the target image for hiding the textual data in the image, hashing algorithm is used, this is used to pick the pixel randomly to store chunk of input data. This is done due to hash algorithm because it randomly produces a hash key that is later used by the algorithm to produce a pattern of pixel, where the data will be stored.

All rights reserved by *www.ijste.org*

D. Step 4:

Retrieve the hidden text back from the target image by scanning data from left to right. Starting character # defines length of information and after that scan right of information that is our message. For this same hash key will be used that was generated during the hiding information. By using the hash key same pattern will generate what was used at the time of hiding the data. The pixels value of each position are read one by one and generated characters concatenated to construct the whole message what had hidden.

E. Step 5:

Compare computed hash value with hash value stored in the message a, both are equal and same therefore message is intercepted. Output is the retrieved text. This is the original message.

V. WORKING OF PROPOSED SYSTEM

The proposed system aims to provide a high degree of security for the confidential message in bank transaction. The proposed system can be divided into 2 phases,(i)Hiding phase (ii) Extraction phase.

A. Hiding Phase:

1) Input a text (.txt) file containing textual data and count length of message and input (.jpg, .gif, .bmp or .tiff) image.
2) Input image is secured by using watermarking with masking using secret key.
3) Read text file b, tokenize the text and makes chunks of the text of 3 characters.
4) Each and stores each chunk of data in an array-list (lc). Total count of data chunks are represented as n. count a=b. //b is message and a is length of message.
5) Generate a random number that is used as a hash key and hash-key is represented using h. string Hash (#)=h(b);
6) The hash-function (H).1 uses the hash-key (h) and total number of chunks (n) to generate a pattern i.e. sequence of numbers (hash-values) those are position of the pixels where data will be stored. New message length b= a#b; new message=.15#how are you. The developed pattern (belongs an arrangement of numbers) is saved in an array-list (lp). New message b= a#b Hash New message=.15#how are youb36g87fgg34ml56bb76q.
7) First chunk from lc and lp are read. So that string saved in lc is viewed and tokenized. The ASCII value for each token lc[i] is changed with the i byte of the lp[i].
8) The product (output) is the image belonging saved data and a hash-key (h) that is applied to retrieve data. Now image=image+ a#b Hash new message hided inside image jpg.

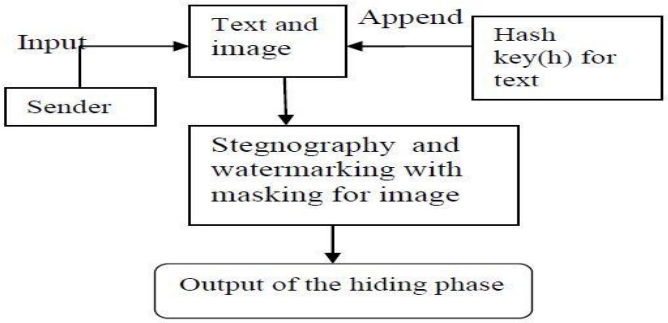

Fig. 3: Hiding Phase Process

B. Extraction Phase:

1) Input the image of any format of file (.jpg, .gif, .bmp or .tiff) that belongs that saved information and the hash-key (h) that was previously used to store data. New message=.15#howare youb36g87fgg34ml56bb76q.
2) The input hash-key (h) is applied with the hash-function (H) to produce sequence of numbers in an array-list (lp) and all produced sequence numbers are the position of the actual pixels in that place data was be stored. Therefore the hash function (H) produces the same pattern of the following random numbers for a hash-key (H) what was produced during the coding time. Scan message b from left to right .we find length a=15 by scanning from left to right.
3) A is the length and new length of message b. Each value of the produced patterns describes the index of a pixel where the data is saved. lp[i] are read where values of the grey color byte are read. Here all the byte belongs an ACSII value of an every character, the viewed ASCII value is changed to a character and each character is written to a text file in the same sequence as

– It is read from the image. How are you? Is the original message.
– -a=a.//after scan right side of #, b is retrieved message.
– Calculation of new hash =h(How are you)// same method during sending the message from sender side, new message
– Of given function by new Hash=b36g87fgg34ml56bb76q
– Now compare if (Hash==new Hash), correct message else message incorrect.
– The result of performed operation is a text file that belongs to the retrieved data from the particular image.

All rights reserved by *www.ijste.org*

VI. CONCLUSION

All the systems that exist as of today that provide Image Steganography have some flaws and inconsistencies. The proposed system aims to overcome the shortcomings of the existing systems which aim at developing a more secure environment to carry out Image Steganography with watermarking.

The presented new approach is worked on perfect hash function. The designed approached system has ability to hide information (text) in an image without reduction the quality of the image up to maximum extent of limit.

This following system specifically used for efficient and secure data hiding in images to make possible large-sized data stenography in image and transmission over internet. With the steganography it is easy to add one more concept watermarking for the proper secure and authorized user from the prevention of attack.

REFERENCES

[1] "Introduction to computer security" - Bishop, M., Pearson publications.
[2] "Cryptography and network security" – Atul Kahate, Tata McGrew.
[3] Thesis on Information Security through Image Steganography Using Least Significant Bit Algorithm by NaniKoduri.
[4] Satya kumari, k. John Singh "A robust and secure steganography approach using hash algorithm", in international journal of latest research in science and technology volume 2, issue 1: page no.573-576, january-february (2013), pp.573 and 574.
[5] Kousik dasgupta, j.k. Mandal and Paramartha Dutta in "hash based least significant bit technique for video steganography(HLSB)" international journal of security, privacy and trust management (ijsptm), vol. 1, no 2, April 2012.pp. 1-4.

All rights reserved by *www.ijste.org*