Data Hiding Using Steganography And Authentication Using Digital Signatures And Facial Recognition

B.B.Gite[1], Divya Choksey[2], Mahesh Jambhulkar[3],Rahul Ramath[4], Yashovardhan Jhamvar[5]

[1](Assistant Professor, Department of Computer Engineering, STES's Sinhgad Academy of Engineering, University of Pune, Pune-48,Maharashtra,India)

[2](Department of Computer Engineering, STES'sSinhgad Academy of Engineering, University of Pune, Pune-48,Maharashtra,India)

[3](Department of Computer Engineering,STES's Sinhgad Academy of Engineering, University of Pune, Pune-48,Maharashtra,India)

[4](Department of Computer Engineering,STES's Sinhgad Academy of Engineering, University of Pune, Pune-48,Maharashtra,India)

[5](Department of Computer Engineering,STES's Sinhgad Academy of Engineering, University of Pune, Pune-48,Maharashtra,India)

ABSTRACT

Steganographyis the art or technique of hiding messages in such a way that no one except the sender and the intended recipient suspects the existence of the message, a form of security through obscurity.

We use this concept wherein text is hidden behind the image and the intended recipient is able to view it. The purpose of the system is covert communication to hide a message from a third party.

In this paper, a technique called digital signature is also included which is added to all the documents sent by the sender to increase the reliability and authenticity of the document. Thus, the proposed system would help to hide the existence of confidential data and would increase the difficulty of detecting the hidden (embedded) data.

We are also including facial recognition which automatically identifies the person by comparing selected facial features from the image and a facial database. Hence when an image is sent with data encrypted in it, the recipient's facial features will be compared with the one in the central database. In this way the receiver is authenticated using facial recognition tool.

Thus this paper gives a brief idea about image steganography that makes use of Least Significant Bit (LSB) algorithm for hiding the data into an image which is implemented through the Microsoft .NET framework.

This system will prove to be helpful in areas where security of data is of utmost importance. It will also be very easy to share and send data to a recipient via a single image file.

Keywords **:**Cryptography, Data Security, Decryption, Digital Signatures, Encryption, Facial Recognition, LSB Algorithm, PCA Algorithm, RSA Algorithm, Steganography.

I. INTRODUCTION

In the current trends of the world, the technologies have advanced so much that most of the individuals prefer using the internet as the primary medium to transfer data from one end to another across the world. There are many possible ways to transmit data using the internet: via e-mails, chats, etc. The data transition is made very simple, fast and accurate using the internet. However, one of the main problems with sending data over the internet is the security threat it poses i.e. the personal or confidential data can be stolen or hacked in many ways. Therefore it becomes very important to take data security into consideration.

Data security basically means protection of data from unauthorised users or hackers and providing high security to prevent data modification. In order to improve the security features in data transfers over the internet, many techniques have been developed, like: Cryptography, Steganography and Digital Signatures.

In this paper we propose a system in which we integrate more than one of the above mentionedtechniques to provide a higher level of data security, whereas the existing systems implement these techniques individually.This proposed system will prove to be helpful in areas where security of data is of utmost importance ranging from college offices to military purposes.

II. CRYPTOGRAPHY

The word cryptography is derived from two Greek words which mean "secret writing". Cryptography is the process of scrambling the original text by rearranging and substituting the original text making it unreadable for others. Cryptography is an effective way to protect the information that is transmitted through the network communication paths [1].

In general, cryptography is transferring data from source to destination by altering it through a secret code. The cryptosystems uses a plaintext as an input and generate a cipher text using encryption algorithm [2].

III. STEGANOGRAPHY

Steganography is the art of hiding and transmitting data through apparently innocuous carriers to conceal the existence of data [3].This technique is performed by different steganographic algorithms like F5, LSB (Least Significant Bit), JSteg etc. and the act of detecting the information hidden through these algorithms is called “Steganalysis”.

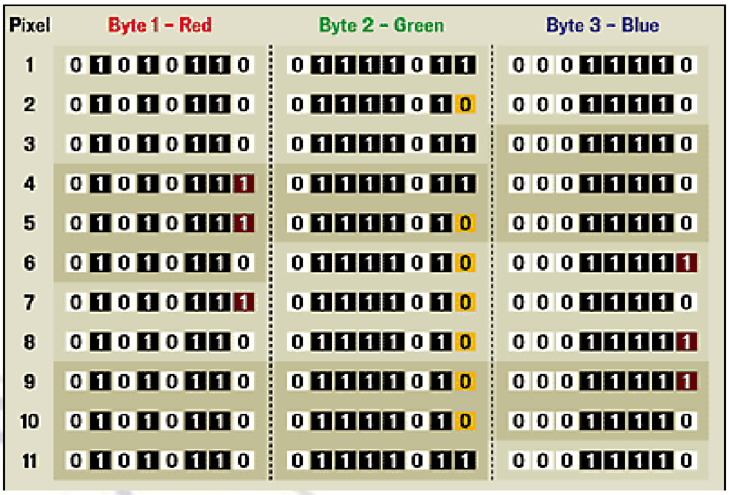
When steganography is applied to an image, the new image is called the “steganographic image”. This steganographic image goes unnoticed as there is almost no difference between the original image and the steganographic image which is visible to the human eye.

Thus steganography is considered as a powerful tool to provide data security.

3.1 LSB algorithm

LSB (Least Significant Bit) is an algorithm to implement steganography. It is the process of adjusting the least significant bitsof thepixels of the carrier image behind which the confidential data is hidden. It is a simple approach for embedding message into the image [4].

The Least Significant Bit insertion varies according to number of bits in an image. For an 8 bit image, the least significant bit i.e., the 8th bit of each byte of the image is changed to the bit of secret message. For 24 bit image, the colors of each component like RGB (red, green and blue) are changed. It has high speed, provides good quality in hiding data, high security and low complexity.



Pixel	Byte 1 - Red	Byte 2 - Green	Byte 3 - Blue
1	0 1 0 1 0 1 1 0	0 1 1 1 1 0 1 1	0 0 0 1 1 1 1 0
2	0 1 0 1 0 1 1 0	0 1 1 1 1 0 1 0	0 0 0 1 1 1 1 0
3	0 1 0 1 0 1 1 0	0 1 1 1 1 0 1 1	0 0 0 1 1 1 1 0
4	0 1 0 1 0 1 1 1	0 1 1 1 1 0 1 1	0 0 0 1 1 1 1 0
5	0 1 0 1 0 1 1 1	0 1 1 1 1 0 1 0	0 0 0 1 1 1 1 0
6	0 1 0 1 0 1 1 0	0 1 1 1 1 0 1 0	0 0 0 1 1 1 1 1
7	0 1 0 1 0 1 1 1	0 1 1 1 1 0 1 0	0 0 0 1 1 1 1 0
8	0 1 0 1 0 1 1 0	0 1 1 1 1 0 1 0	0 0 0 1 1 1 1 1
9	0 1 0 1 0 1 1 0	0 1 1 1 1 0 1 0	0 0 0 1 1 1 1 1
10	0 1 0 1 0 1 1 0	0 1 1 1 1 0 1 0	0 0 0 1 1 1 1 0
11	0 1 0 1 0 1 1 0	0 1 1 1 1 0 1 1	0 0 0 1 1 1 1 0

Fig No.1: Implementation of LSB Algorithm

In the above Figure No. 1, a glimpse of how the LSB Algorithm works is shown; the message to be hidden behind an image is first considered. The next step is to get the ASCII (American Standard Code for Information Interchange) of every character of the message. Since the ASCII will be an 8 bit binary number, we will require 8 Least Significant Bits to store the ASCII of one character.

As every pixel in a standard Bitmap image is made up of 3 colors - Red, Green and Blue, we will get 3 Least Significant Bits of the 3 component colors of each pixel. Therefore roughly 3 pixels are required to store the 8 bits of ASCII of every character.

In the above Figure No.1,the message considered is “Aha!”. The ASCII of the first character A is 65 i.e.01000001 in binary. Hence the first 8 Least Significant Bits of the RGB components of the first 3 pixels are changed according to the binary representation of the ASCII of ‘A’.Similarly the same procedure is incorporated for the rest of the message, using the binary representation of each character’s ASCII value.

IV. Difference Between Steganography And Cryptography

In cryptography the message is not hidden, any unintended receiver can intercept and decrypt the message, if the decryption keys are possessed by him/her.

However in steganography message is hidden and the enemy must discover the medium as the message is hidden behind an image and the image goes unnoticed as a usual, harmless image.

Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

V. DIGITAL SIGNATURE

A digital signature is a scientific pattern which verifies the authenticity of a digital message or document [5]. A valid digital signature makes sure that the message was created by a known sender and the person cannot deny sending it. Hence it guarantees data integrity and non-repudiation of documents and transactions. Digital Signature also assures that the document is not tampered during transmission and no alterations are made to the data once the document has been digitally signed.

Digital signatures use asymmetric cryptography and it mainly consists of three algorithms:

1. Key Generation: Generates the private key and a corresponding public key.
2. Signing: Generates the signature using the message and the private key.
3. Signature Verification: Claims the authenticity of the sender using the message, public key and the signature [6].

5.1RSA Algorithm

RSA is an algorithm for public-key cryptography/digital signatures that is based on the presumed difficulty of factoring large integers, the factoring problem.
The algorithm involves the above 3 steps - key generation, signing/encryption, signature verifying/decryption.

A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with vast knowledge of the prime factors can feasibly decode the message [7].

VI. 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. 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 [8]. 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.

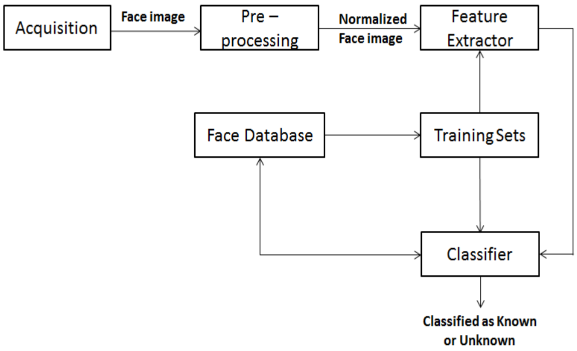


Fig No.2: Facial Recognition Process

- Acquisition- Image acquisition module seeks and thenextracts 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 sothat it is suitable for recognition.
- Preprocessing- The purpose of the preprocessing module is to reduce or eliminate some of thevariations in face due to illumination. It performs normalization and filtering, improves image clarity, adjusts brightness and sets the default image size [9].
- 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 computed with all the signatures in the database. Image is identified as the one which gives least distance with the signature of the image torecognize [10].
- Classifier- The purpose of the classification sub-module is to map the feature space of a test data to adiscrete set of label data that serves as template. It compares the Eigen vectors with those already stored in the database library.
- Training sets- It adjusts the feature extraction parameters to ensure optimization and accuracy.

VII. PREVIOUS WORKS

The literature survey done for the proposed system has immensely helped us to understand the purpose and functionality of the systems presently existing to perform Image Steganography.

Some of the systems presently existing to cater image Steganography are as-

1. QuickStego.
2. FortKnox.

7.1 QuickStego

QuickStego lets you hide text in pictures so that only other users of QuickStego can retrieve and read the hidden secret messages. Once text is hidden in an image the saved picture is still a 'picture', it will load just like any other image and appear as it did before. The image can be saved, emailed, uploaded to the web etc.

QuickStego alters the pixels of the image, encoding the secret text by adding small variations in color to the image. In practice, to the human eye, these small differences do not appear to change the image.

QuickStego does not ENCRYPT the secret text message though it is well hidden in the image.If you require the message to also be encrypted then QuickCrypto, which is a paid product, needs to be purchased. This software is priced at £34.99.

The user needs to go to http://quickcrypto.comand then download the free version of the software. After installing the software, it requires the user to select an image to work on. The user is now supposed to choose whether he/she wants to hide text or get text. The text can also be opened from a text file and the text retrieved from the image can also be saved into a text document.

7.1.1 Advantages

1. QuickStegois comparatively faster than other web based steganographic software providers as it is an offline software based on windows.

7.1.2 Disadvantages

1. The Graphical User Interface of QuickStego makes it difficult for users to understand whether the user is in the hide text mode or the get text mode.
2. It does not require the user to be registered with the software; hence misuse of the software is possible.
3. There is no encryption of the message that is hidden behind a steganographic image.
4. Only Bitmap images can be used to hide data.

7.2 FortKnox

It is also a Windows based application which has been developed to provide image Steganography. This software uses the LSB algorithm for the steganography, the only difference being that instead of changing the values the Least Significant Bit, it changes the values of the two Least Significant Bits.

7.2.1 Advantages

1. A simple Graphical User Interface, which makes it easier for users to understand what are his/her options to execute the task.
2. The data is encrypted before the Steganography is done.

7.2.2 Disadvantages

1. Due to the change of color values of the two Least Significant Bits, the steganographic image looks considerably different from the original image in many cases.
2. The source of the image is not verified in any way to pin point that the image has come from a particular trusted source.
3. Only 24-bit Bitmap images can be used to hide the data.

VIII. PROPOSED SYSTEM

The proposed system aims to provide a high degree of security for the confidential message. It uses MySQLdatabase which is located on a server machine.

The proposed system can be divided into 2 phases, Hiding phase and Extraction phase.

The new users need to register with the system and the existing users can login into the system in order to access the system features.

The new user needs to specify basic personal information like name, email id and a profile picture.

The system also captures additional pictures of the users face, required for facial recognition in the decryption phase.

Once all the input is accepted from the user, the system generates 2 sets of keys for the user using the RSA algorithm.

The first set is called the Data Keys which are used for the encryption and decryption of the message data.Data Keys consists of a Data Public Key and a Data Private Key.

The second set is called the Signature Keys which are used to create the Digital Signature and verify the Digital Signature of the Sender. This set consists of the Signature Public Key and the Signature Private Key.

All these 4 keys are unique for every user.

After successfully logging in the user can view his profile which contains his personal information as well as all his keys which will be used for data encryption, decryption and for creating a digital signature for that particular user. He may also change his password if required.

8.1 Hiding Phase

This process can be explained with the help of thediagram given below.

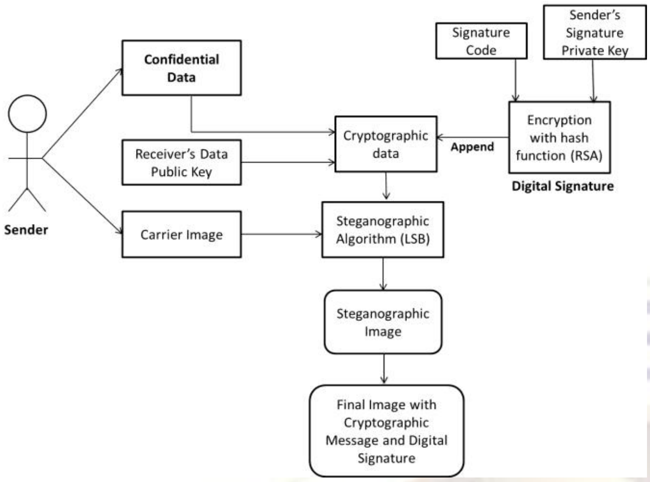

Confidential Data
Receiver's Data Public Key
Carrier Image
Sender
Signature Code
Sender's Signature Private Key
Encryption with hash function (RSA)
Digital Signature
Append
Cryptographic data
Steganographic Algorithm (LSB)
Steganographic Image
Final Image with Cryptographic Message and Digital Signature

Fig No.3: Hiding Process

In the Hiding process the user has to select an image from the storage. This image can be of any of the following file types (.bmp,.jpg,.png)

The secret message can be typed or can be loaded from a text file. The size of the secret message which can be hidden depends on the size of the image selected. The user selects the receiver to whom he wants to send the secret message. Then the encryption process starts. It uses the Data Public Key of the receiver for encryption. Once encryption of the message is done, the message text is scrambled and it will be unscrambled only in the decryption phase.This scrambled data is called the "cryptographic message".

Every user will have a signature code which will be his unique code. The sender's Signature Private Key is now used, and when applied on the signature code of the sender, it will generate a scrambled signature.

This scrambled signature is appended to the cryptographic message and once this is done, the LSB Algorithm is applied to hide the entire cryptographic message along with the Digital Signature behind the carrier image.

The new image created is called the "Steganographic image"; this image can then be sent to the receiver using any transmission method.

8.2 Extraction Phase

This process can be explained with the help of the block diagram given below.

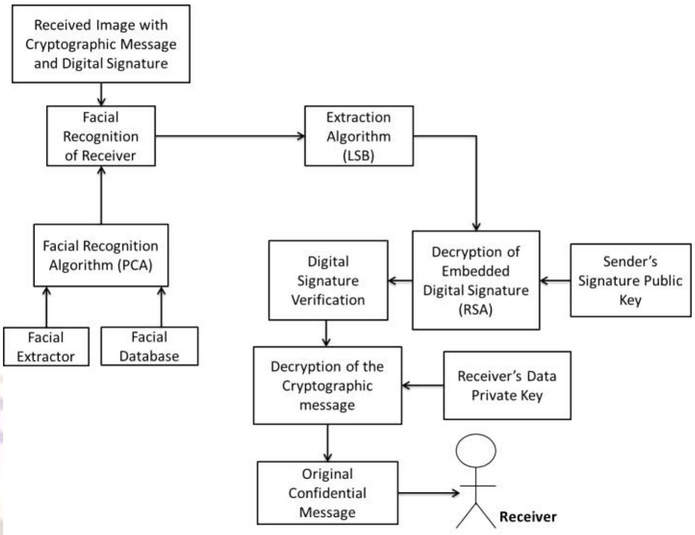

Received Image with Cryptographic Message and Digital Signature
Facial Recognition of Receiver
Extraction Algorithm (LSB)
Facial Recognition Algorithm (PCA)
Facial Extractor
Facial Database
Digital Signature Verification
Decryption of Embedded Digital Signature (RSA)
Sender's Signature Public Key
Decryption of the Cryptographic message
Receiver's Data Private Key
Original Confidential Message
Receiver

Fig No.4: Extraction Process

Once the receiver receives the steganographic image he needs to login to the system. To extract the message from the image the receiver needs to successfully pass the facial recognition wherein the Eigen vectors of the users face are compared with the pre calculated Eigen vectors stored in the database. If the user successfully passes the facial recognition test, the encrypted Digital Signature is extracted from the Steganographic Image.The receiver then chooses the Sender's Signature Public Key to decrypt and verify the digital signature of the sender. Once the digital signature is verified the next step is to extract the cryptographic message from the Steganographic Image. The receiver now uses his/her Data Private Key to decrypt the encrypted, cryptographic message.

Table No 1: Tasks To Be Performed

Steps	Tasks to be Performed
1	Acceptance of input from the new user.
2	Generation of public and private keys of the user.
3	Logging in of an existing user.
4	Selecting an image and the message to hide behind the image.
5	Start of the encryption process and sending the steganographic image to the receiver.
6	Logging in of the receiver.
7	Uploading the received steganographic image.
8	Facial recognition of the receiver.
9	Selection of the public key of thesender.
10	Verification of the sender's digital signature.

11	Decryption of the steganographic image and display of the original message.

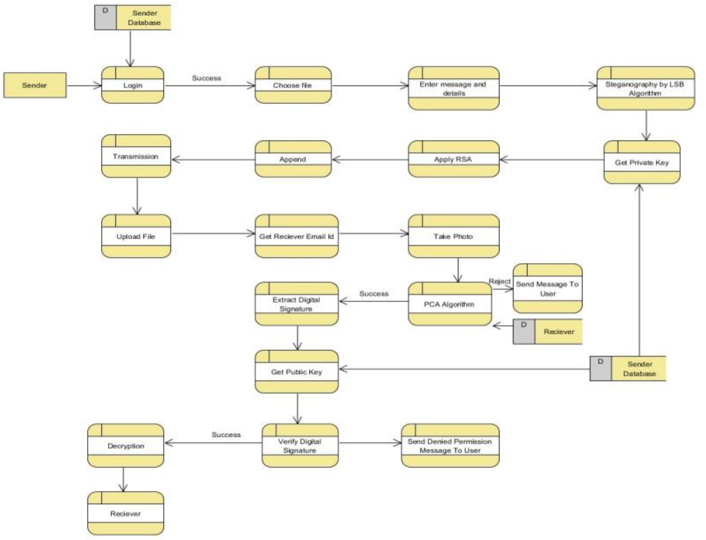


Fig No.5: Data Flow Diagram Level 2

IX. CONCLUSION

All the systems that exist as of today that provide Image Steganography have some flaws and inconsistencies. The systems provide less security in terms of encryption of the message data, the sender of the image is not verified, and the receiver is not authenticated to view the secret data hidden behind the image.

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. This system will provide the users a digital signature that they can embed in the steganographic image to validate the source of the image, facial recognition at the receiver's end will authenticate the receiver of the image and only he/she will be authorized to view the data behind the image.
Encryption of the message data will ensure that even if the image is decrypted using some other tools, the message will not be decrypted and all that will be seen is data that does not make sense.
Our tool uses MySQL as database which will ensure a more robust approach towards security, performance and disaster recovery as compared to other databases such as MS-Access 2007 [11].

X. FUTURE SCOPE

The scope of proposed system can be expanded in the following ways:

1. An image can be hidden behind the carrier image
2. The application can be installed on a number of client machines and the database can be placed on a server machine with a Static IP Address. This will enable the users to use the proposed system on their client machines connected to a central database.
3. Improve the compression ratio of text to image. That is to accommodate more text data in a given image.

REFERENCES

[1] "Introduction to computer security" -Bishop, M., Pearson publications.
[2] "Cryptography and Data Security", Dorothy Elizabeth Rob, Ling Denning, Purdue University.
[3] Neil F. Johnson, ZoranDuric, and Sushil Jajodia, Information Hiding: Steganography and Watermarking - Attacks and Countermeasures, MA, Kluwer Academic Publishers, 2001.
[4] Thesis On Information Security Through Image Steganography Using Least Significant Bit Algorithm by NaniKoduri
[5] S.R. Subramanya and Byung K. Yi: Digital Signatures- 0278-6648/06 2006 IEEE.
[6] .Chaitanya1 and Y.Raja Sree: Design of new security using symmetric and asymmetric cryptography algorithms- World Journal of Science and Technology 2012.
[7] A Method for Obtaining Digital Signatures and Public-Key Cryptosystems R.L. Rivest, A. Shamir, and L. Adleman.
[8] "How Facial Recognition Systems Work": Kevin Bonsor.
[9] T. Chen, W.Yin, X.S. Zhou, D. Comaniciu, T. S.Huang,"Total Variation Models for VariableLighting Face Recognition and UnevenBackground Correction", IEEE Transactions onPattern Analysis and Machine Intelligence, vol.28(9), 2006.
[10] Zhujie, Y.L.Y., 1994. Face recognition withEigen faces. Proc.IEEE Intl. Conf. IndustrialTechnology.
[11] "MySQL Enterprise Edition". MySQL 5.5 Reference Manual, Oracle. 5 February 2013.