ORIGINAL RESEARCH PAPER

Volume-8 | Issue-7 | July - 2019 | PRINT ISSN No. 2277 - 8179

INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH

SECURE COMMUNICATION THROUGH STEGANOGRAPHY WITH FACIAL RECOGNITION FOR AUTHORIZATION

Engineering

Pragati Manchanda Student of Bachelor of Engineering, Maharashtra Institute of Technology College of Engineering, Pune

Raghav Pande Student of Bachelor of Engineering, Maharashtra Institute of Technology College of Engineering, Pune

Utkarsh Tyagi Student of Bachelor of Engineering, Maharashtra Institute of Technology College of Engineering, Pune

Priyanka Daware Student of Bachelor of Engineering, Maharashtra Institute of Technology College of Engineering, Pune

Prof Bharati Dixit* Guide, Associate Professor of Computer Engineering, Maharashtra Institute of Technology College of Engineering, Pune *Corresponding Author

ABSTRACT

The data is increasing to a great extent and it is really essential that the security of the data is also taken into consideration. For this purpose, we can make use of cryptography, watermarking and steganography techniques. Steganography is the method in which the message goes undetected so the risk of it being attacked is reduced. Further this paper discusses in detail the various steganography methods and techniques along with face detection and recognition to make it more secure. It also proposes a model which combines steganography and facial recognition. In our proposed algorithm, we have tried to implement Steganography by hiding data in the LSB of the pixels along with face recognition as the pass key for logging into the steganography application. For face recognition various tools like OpenCV, MATLAB and algorithms like LBPH, Eigenfaces, Fischer faces etc. are discussed.

KEYWORDS

Steganography, Spatial Domain, Pixel Intensity, LSB modification, 24-bit Bitmap Image, Haar Cascades, Eigen values, Face Detection, Face Recognition

INTRODUCTION

Information Security is basically securing information so that it is not lost in the communication network and it is not unethically used. This is further divided into three parts:

1. Watermarking is used to verify the authenticity of the owners and indicates the copy rights of particular documents. Watermarking is mainly used in government documents, currency notes, stamp papers, passports etc.
2. Cryptography is generally hiding the information or encrypting it into a form which is not understandable by any other person viewing it.
3. Steganography is basically hiding the fact that communication is taking place.[1]

Steganography is classified into 3 categories,

Pure steganography where there is no stego key and no other party is aware of the communication.

Secret key steganography where the stego key is exchanged prior to communication.

Public key steganography where a public key and a private key is used for secure communication.[2]

This paper presented after referring various IEEE papers and journals presents us with a bitmap image steganography technique which is made more secure by using facial recognition. Thus, only the authorized user can access the software and it could be used where important data is to be exchanged.

LITERATURE SURVEY

Face Detection involves capturing the face and removing the background and focusing on the face followed by feature extraction which includes extracting regions like eyes, nose etc. The final step is face recognition in which the image is matched with the detected image and the face of the person is identified.

Figure 1: A generic face recognition system [3]

There are various tools like MATLAB and OpenCV. OpenCV has a good speed because it uses C/C++ library functions which directly converts into machine language code. Also, it is easily portable and the cost of OpenCV is comparatively less.

Abhishek, Sholaki and Shama[4] proposed an image steganography technique using 24-bit bitmap images. The filtering technique they used is based on finding out the pixel which occurs the most in the bitmap image. The filtering function only checks the first 7 bits of each of red, green and blue components. Data is hidden in the last bit of the red, green and blue components of only those pixels which have the same value as the maximum-occurring pixel. Saleh, Hedieh[5] propose a new method based on AIS algorithm and the least significant bits substitution. The proposed method firstly finds a region of a host image that is similar to the host image and then embed a small part of a message in it to hold the ratio of the number of message bits to the number of host image bits and tunes the parameters of AIS algorithm.

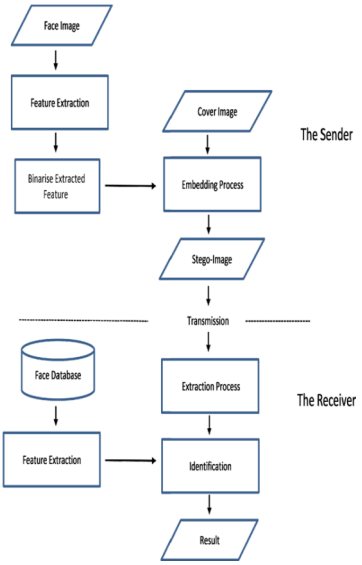

Figure 2: General framework of system [6]

Rasber, Sabah and Harim[6] proposed a high invisibility face biometric data transfer technique which decomposes a face image into multiple frequency bands using wavelet transform. Each sub-band in the wavelet domain is divided into non-overlapping blocks. Then, local binary pattern histograms (LBPHs) are extracted from each block in each subband using only 4 neighbours to extract LBP code. Then, all of the LBPHs are concatenated into a single feature histogram to effectively represent the face image. Finally, the extracted face features are embedded in an image using one of the robust steganography techniques in order for them to be ready for transmission.

RESEARCH GAP

By referring various papers we have identified the research gap and for making the system more secure we could combine steganography and facial recognition together which could be used as a part of various military or espionage applications, Passport Issuing Systems for saving the details of the person who is applying for passport, Election commission in order to avoid forged voting and in government offices where data storage is huge problem data can be encoded and kept and used whenever needed. Thus, there is a need of a generic system to carry out communication securely. This paper guides us regarding development of such a system and the various methods and algorithms available for it.

IMPLEMENTATION OVERVIEW

The admin adds faces of the user into the application. The face is stored in the file structure. The sender and receiver can login into the application using face recognition as an authentication mechanism.
The systems module designs at different phases are:

I. Encryption Module Phase

First, the sender authenticates himself by face recognition. If the sender's face is identified, he is given entry to a form where the sender selects the image and the file to be encrypted. If the file size exceeds then the image size it shows an error. Then the sender clicks on the encrypt button. It asks for the path where to save the encrypted image. Then encryption is done using bitmap steganography least significant bit method and the image is stored in bmp format on the computer itself. The user can then send the encrypted image via internet or any other medium. The bitmap steganography stores the data in the LSB of the image and as a result noise is not observed in image.

ii. Decryption Module Phase

The receiver first authenticates himself by face recognition. After logging in, the receiver selects the bitmap image received from the sender. The receiver also selects the location where he wishes to save the encrypted file. Then by clicking on decrypt button the image is decrypted and the file is saved at the mentioned path. Same least significant bit method is used for decryption.

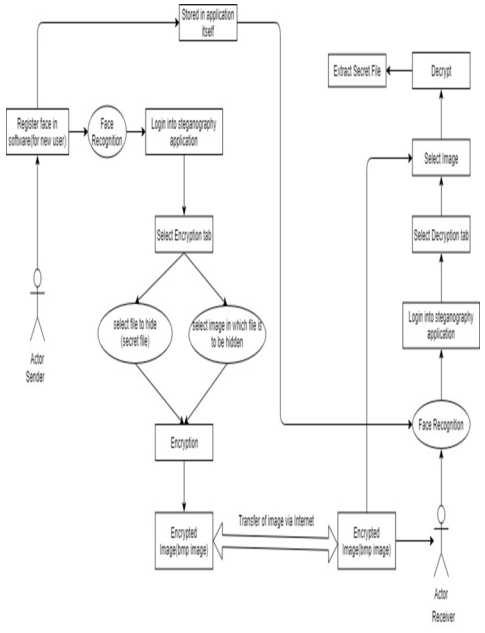

Figure 3: Data flow of proposed system

METHODOLOGIES

Types of Steganography

1) **Text Steganography** uses tabs, white spaces, special characters to hide the message.
2) **Image Steganography** uses image as cover object for hiding text, text files or any other image inside it.

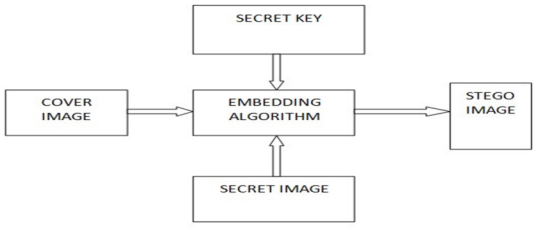

Figure 4: Block Diagram of Image Steganography [7]

3) **Audio Steganography** uses digital audio formats such as WAVE, MIDI, AVI, MPEG etc. for hiding information inside it.
4) **Video Steganography** uses a combination of pictures for hiding information. The video is converted into frames and in one of the frames the secret information is embedded. Video formats like MPEG, AVI or other are supported.

Steganographic Techniques:

Spatial Domain Methods

In these methods the pixel intensities are varied to hide the information.

1) LSB: In LSB technique some pixels of image are replaced with pixels of data. There is less chance that image is degraded but image manipulations can be done.
2) Pixel Value Differencing: Two consecutive pixels from smooth or edge area are selected for embedding the data.
3) BPC: Binary Pattern Complexity measures the noise factor in image and replaces it with binary pattern from the secret data.

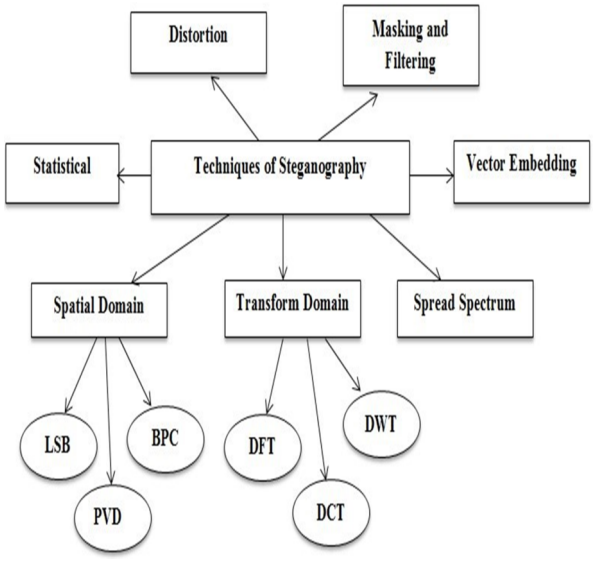

Figure 5: Techniques of Steganography [8]

Transform Domain Steganography: This technique is used for images that are not affected by compression, image processing and cropping. They are classified as Discrete Fourier Transformation (DFT), Discrete Cosine Transformation (DCT) and Discrete Wavelet Transformation (DWT).

Vector Embedding: It embeds audio data into pixels of frames in video.

Spread spectrum: The hidden data is spread over a frequency bandwidth and the data cannot be removed without destroying the cover.

Statistical Technique: Here cover is divided into blocks and then one message bit is embedded in each block.

Distortion Techniques: The data is hidden by distorting the signal and a secret key is also used for encoding and decoding.

Masking and Filtering: Watermarks are used for hiding data in the more significant part of the image.

REQUIREMENTS FOR STEGANOGRAPHIC SYSTEMS

- Message requirements (Maximum message size)
- Container requirements

1) Type of container: Text, Image, Sound, Video could be used for hiding data.
2) Supported file formats: Hide and extract messages from JPG, PNG or any other image types.

- **Stegocontainer requirements**

1) Imperceptibility: Shows how much the container has changed as compared to original container. This is reflected in the form of noises, errors or changes in colour.
2) Fidelity: This is basically the difference in quality between the original and embedded container which the users can notice.
3) Stegocontainer size: It is the minimum and maximum size of the stegocontainer.
4) Embedding efficiency: It is the probability of whether the hidden message could be extracted.

- **Algorithm requirements**

1) Capacity: Number of bits to be hidden, the space complexity.
2) Speed: How efficient is the algorithm, the time complexity.

- **Security requirements**

1) Resistance against steganalysis: Resistant enough for unethically decrypting the message by using steganography.
2) Robustness: It tells the resistance of the message to various transformations (like compression) of the stegocontainer.
3) Resistance against attacks: The resistance of the system to various attacks like geometric, cryptographic attacks.
4) Type of keys: Steganographic key which specifies the steps for hiding message and cryptographic key which encrypts the message.[9]

FACE DETECTION METHODS:

1.Knowledge-Based: - Based on building a set of rules.

2.Feature-Based: - Locate faces by extracting structural features of the face.

3.Template Matching: - Pre-defined face templates are used to detect the faces.

4.Appearance-Based: - It discovers the relevant characteristics of face images and is used in feature extraction. These methods are included:

4.1. Eigenface-Based: - Based on Principal Component Analysis.

4.2. Distribution-Based: - PCA and Fisher's Discriminant along with a trained classifier is used for representing facial patterns.

4.3. Neural-Networks: - Used for face detection, face recognition, emotion detection

4.4. Support Vector Machine: - Based on concept of decision planes that define decision boundary.

4.5. Sparse Network of Winnows: - Sparse network of two linear units representing face patterns and non-face patterns.

4.6. Naive Bayes Classifiers: - It tells the probability of the face to be present in the picture. Also, it helps in telling position of the face.

4.7. Hidden Markov Model: - Used with other techniques to build face detection algorithms.

4.8. Inductive Learning: - Uses algorithms like Quinlan's C4.5 or Mitchell's FIND-S to detect faces.[10]

HAAR CASCADES:

The classifier is first trained with face and non-face images and features are extracted by subtracting sum of pixels under the white rectangle from sum of pixels under the black rectangle.

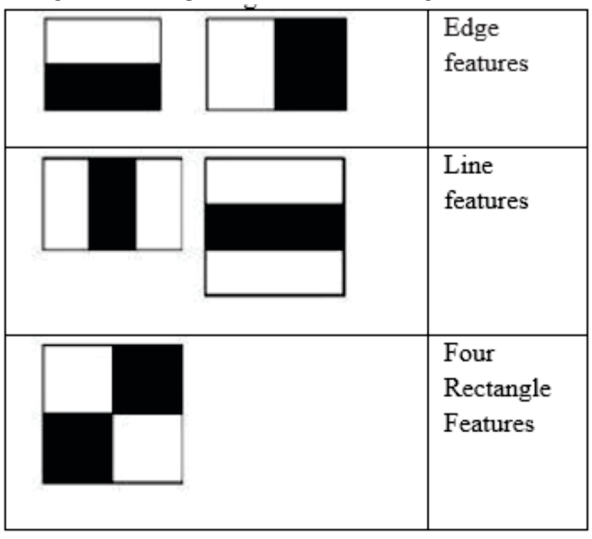

Figure 6: Haar cascades Features [11]

A 24x24 window can give us about 160000 features but most of them are irrelevant and the best features could be selected by **Adaboost**. So, the features get reduced from 160000+ features to 6000 features. Also Cascade of Classifiers is applied in which instead of applying 6000 features on window, features are grouped into different stages. If it fails first stage reject it else apply second stage and continue further. This is working of Viola-Jones face detection algorithm.

FACE RECOGNITION:

The face recognition systems can operate basically in two modes:

- **Verification or authentication of a facial image**
- **Identification or facial recognition**

There are different types of face recognition algorithms, for example:

- Eigenfaces (1991): Eigenfaces is a method that is useful for face recognition and detection by determining the variance of faces in a collection of face images and use those variances to encode and decode a face in a machine learning way without the full information reducing computation and space complexity.
- Principal Component Analysis (PCA): The main goal of PCA is dimensionality reduction. The idea behind it is to linearly project original data onto a lower dimensional subspace offering the principal components (eigenvectors) maximum variance of the projected data and/or minimum distortion error from the projection.
- Local Binary Patterns Histograms (LBPH) (1996): Algorithm is trained using facial images and then a window of 3*3 pixels is applied and a 3*3 matrix is obtained in which the central value is the threshold and neighbour's values are set to 1 if it is equal or higher than threshold else 0. Finally, all binary values are combined and a new decimal value is obtained and is set as the central value of matrix.

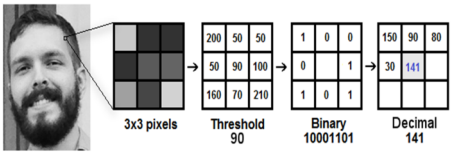

Figure 7: LBPH matrix computation [12]

We can extract the histogram of each region and then concatenate each histogram to create a new and bigger histogram.

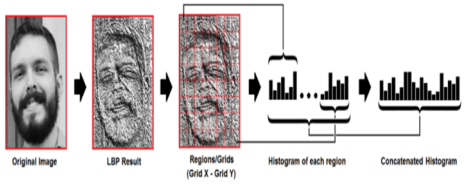

Figure 8: LBPH concatenated system [12]

- Fisher faces (1997): The objective is generating a space with minimum intra-class dispersion and maximum inter-class dispersion, finding vectors providing the best classes for separation, as well as trying to maximize the difference between the classes and minimize the number of classes.
- Scale Invariant Feature Transform (SIFT) (1999): Scale Invariant Feature Transform (SIFT) is an algorithm employed in machine vision to extract specific features of images for applications such as matching various view of an object or scene (and identifying objects.
- Speed Up Robust Features (SURF) (2006): Speed-up robust features (SURF) uses detector to locate the interest points in the image, and the descriptor to describe the features of the interest points and constructs the feature vectors of the interest points.

PERFORMANCE METRICS

There are various performance metrics which can be used to calculate the quality of cover image after applying steganography. Some of the metrics which is calculated for the proposed system is given below:[7]

A. MSE (Mean Square Error): Lower the value of MSE better the quality of the image.

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(X_{ij} - Y_{ij})^2$$

where M and N are the number of rows and columns of the cover image (X_{ij}) and stego-image (Y_{ij}) respectively.

B. PSNR (Peak Signal to Noise Ratio): Higher the value, higher is the quality of the image.

$$PSNR = \frac{10log255^2}{MSE}$$

C. BER (Bit Error Rate):

$$BER = \frac{1}{PSNR}$$

CONCLUSIONS

As information is hidden in an image it would be very difficult for an attacker to guess that communication is taking place between two parties and face recognition for authorization makes it more secure. Thus, various types, techniques and requirements of steganography along with various face detection and recognition methods have been studied. The research gap is identified and a system is proposed which combines steganography and facial recognition together. Thus, the goal of developing a powerful security equipment is fulfilled.

REFERENCES:

[1] B.Chitradevi, N.Thinaharan, M.Vasanthi, "Data Hiding Using Least Significant Bit Steganography in Digital Images", S. Vignesh and A. Philip Arokiadoss (ed.), Statistical Approaches on Multidisciplinary Research, Volume I, January 2017, Doi: 10.5281/zenodo.262996

[2] C.P. Sumathi, T.Santanam and G.Umamaheswari," A Study of Various Steganographic Techniques Used for Information Hiding", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, December 2013

[3] Kruti Goyal, Kartikey Agarwal and Rishi Kumar," Face Detection and Tracking Using OpenCV ", International Conference on Electronics, Communication and Aerospace Technology ICECA 2017

[4] Abhisek Saha, Sholanki Halder, Shama Kollya, "Image Steganography Using 24-Bit Bitmap Images", Proceedings of 14th International Conference on Computer and Infonnation Technology (ICCIT 2011) 22-24 December, 2011, Dhaka, Bangladesh

[5] Saleh Delbarpour, Hedieh Sajedi,"Image Steganography with Artificial Immune System", 2017 Artificial Intelligence and Robotics (IRANOPEN)

[6] Rasber D. Rashid, Sabah A. Jassim and Harin Sellahewa "Covert Exchange of Face Biometric Data using Steganography", 2013 5th Computer Science and Electronic Engineering Conference(CEEC) University of Essex, UK

[7] Vaishali P, Pradyumna Bhat," Transform Domain Techniques for Image Steganography", INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING, National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015), Vol. 3, Special Issue 1, April 2015, DOI: 10.17148/IJIREEICE

[8] Harpreet Kaur and Jyoti Rani," A Survey on different techniques of steganography", MATEC Web of Conferences 57:02003 January 2016, DOI: 10.1051/ matecconf/ 20165702003

[9] Davids Gribermans, Andrejs Jersovs, Pavels Rusakovs, "Development of Requirements Specification for Steganographic Systems", Department of Applied Computer Science, Riga Technical University, Latvia, December 2016, vol. 20, pp. 40–48, doi: 10.1515/acss-2016-0014

[10] Shaily pandey and Sandeep Sharma," Review: Face Detection and Recognition Techniques", International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014

[11] https://docs.opencv.org/3.4/db/d28/tutorial_cascade_classifier.html

[12] https://towardsdatascience.com/face-recognition-how-lbph-works-90ec258c3d6b