International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 9, September- 2014

Face Detection and Steganography Algorithms for Passport Issuing System

Chirag Hingorani
B.E. Computer Engineering
Vivekanand Education Society's Institute of Technology
Mumbai, India

Reshma Bhatia
B.E. Computer Engineering
Vivekanand Education Society's Institute of Technology
Mumbai, India

Omesh Pathai
B.E. Computer Engineering
Vivekanand Education Society's Institute of Technology
Mumbai, India

TarunMirani
B.E. Computer Engineering
Thadomal Shahani Engineering College
Mumbai, India

***Abstract*—In this digital era, advanced technologies can be explored to deliver efficient and quality services to public. So is required in passport issuing systems. The composition of this paper presents how the security issues in passport delivering systems can be bailed out by using face recognition and Steganography techniques.Face detection is a technology which helps figure out the location of the face in an given image. This ameliorate the biometric authentication in process of passport issuing.Face detection technique is moduled for static single images,its performance can be further improved by annexing steganography technique. Steganography is practice of concealing the secret information within another non-secret data.**

Keywords—face detection; Steganography; biometrics; Principal Component Analysis; Least Significant Bit technique;

I. INTRODUCTION

Biometrics technique have been served as silver bullet under many cases where authentication comes in picture. Biometrics is the termed coined for automated recognition of a human depending upon physiological or behavioral characteristics such as face, fingerprints, palm print, hand and iris. Under the biometrics techniques used, face detection and recognition is commonly used compared with iris recognition, fingerprint recognition etc. The greatest advantage of using these traits for identification are that, they are based on unique features of human being which always persists and cannot be lost of forgotten.

Face detection technique involves tracing out the locations of face in an image. Face recognition systems deal with two realms of identification and verification of data[1]. In identification technique the algorithm identifies an unknown face in an image whereas In verification technique the algorithm confirms the claimed identity of a particular face. Face detection techniques will enhance the passport issuing system as it will first authenticate the concerned user and then allows himfor document verification. Thus providing double check mechanism. Also it will provide its asset in management system.

For futher revamp the passport issuing system, Steganography can be used. It stands for hidding of secret information. Steganography in passport systems can be used to hide the documents of a particular user in his own picture. This can solve many issues related to memory and information systems. The personal details in this way no longer be theft thus maintaining privacy.Composition of this paper presents the face detection and Steganography algorithm to incorporate the same.

II. FACE RECOGNITION

The process in which an image or sequences of images are provided and said to authenticate people in a picture is said to be face recognitionBut it can be done in three ways i.e

- face detection
- feature extraction
- recognize face

Face Detection can be defined as to extract faces from picture.so that system should recognize some region as a face. The next step is Feature Extraction, it fetches various features of faces like eye spacing etc. Then finally Face Recognition will compare the faces and their features with stored database pictures and recognize them.

Feature Extraction and recognition will be needing special algorithm to extract their features and algorithm should make them recognize from stored databases. The simple and efficient algorithm tocalculate features and recognize them is Principal Component Analysis (PCA) .

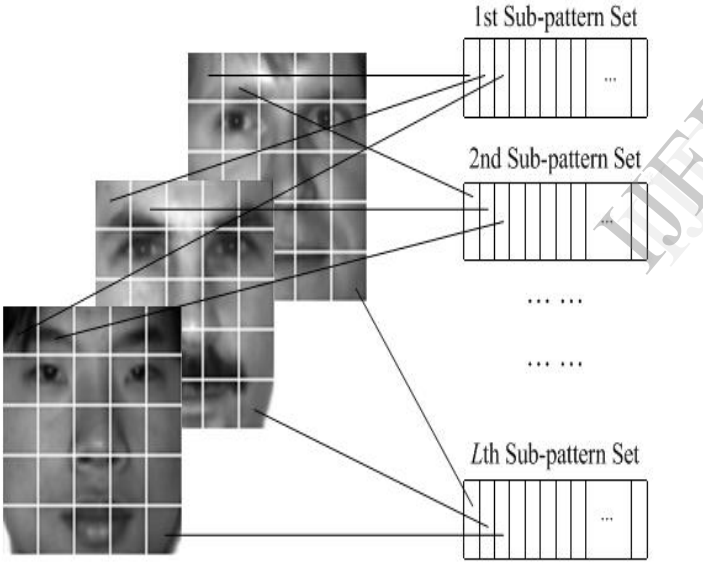
PCA is a popular method which reduces the dimensionality of image and fetches back with variations in image and build compact representation of face image to get it recognized.

Notations:-

- *Eigen faces* - Pca extracts face images and changes into small sub sets of feature face images, they can be said Eigen faces.
- *Training set* – the set of images are trained to recognize faces and then stored in database , suppose the picture on passport is trained using PCA with face detection of that person so that next time when the picture is made to recognize , it should be faster because of training set.
- *Contribution Factor*- it is giving importance to selected features of faces. For e.g eyes are most important factor for human face so Contribution Factor will give the value of eyes as important .
- *Classification decision* – it is final decision in which the features once extracted or training set images are matched with the face detection at run time.

Algorithm can be explained as follows: [2]

Step 1: face images are to be partitioned into sub patterns. Sub patterns are nothing but the feature extracted during training set. Patterns are face features like eye brows less or more, forehead wrinkles.



Step 1: calculate the contribution factor of each sub pattern

- First extract the Eigen faces and put them in for training set so that next time when the authentication process is carried out the face should be recognized.
- In second step , now the person is put in front of camera to detect the face , the face is cropped and being saved in gallery sets (another place to save faces captured during runtime) , minimum 10 images are took and saved in gallery sets.
- For each face detected in the training set, calculatiois being made and all the faces from training set and all faces from gallery sets are being made to match similarities between them to make face detect.

If a face from training set of imagesis correctly determined, and for every image it being +1 (just for count) .
In this way the faces are being recognized .

III. STEGANOGRAPHY

The steganography is art or practice to hide a message, image or file within another image, file or message. The origin of steganography came from Greek word it means to hide something through writing. Steganography is art of science which hides the secret messages into amedium. Steganography takes cryptography a level more by hiding an encoded message using least significant bit (LBS) technique. It hides the messages in such a way that no one except the receiver knows how to expose the secret messageImage steganographydata is encoded and then put, using a special algorithm, data that is part of a particular file format such as a bitmap image.

LSB (Least Significant Bit) technique will replace the least significant bits with the message to be encrypted. We have used the bmp images as it does lossless compression so LBS can be resourcefully while using bmp.it will embed secret message into image.

We will use least significant bit because of following reason. [3]

a. After hiding the message, the intensity of image is change by 1 or 0.

b. Change of intensity is either 0 or 1 because it changesyour last bit .e.g.

00101111 ----> 00101110

The only change is 1 bit so that its intensity should not be affected.

For example, suppose a message is hidden in image (24-bitcolorsi.e.rgb). Suppose the original 3 pixels are: [16]

00101101**1**0001110111011100

10100111**0**11000101 00001100

11010011**1**1010110101100011

Now if we insert ‘T’ in image. Binary equivalent for A is 01010100, it will change 6 bits

00101100**0**0001110111011100

10100111**1**1100010000001101

11010010**0**1010110001100011

In this way, the binary equivalent or secret message ‘T’ is embedded into image(24bit).

Procedure:-[3]

A. Secret message Insertion

1. Take cover image pixels.
2. Take secret message characters
3. Take steganography key characters
4. Take first pixel and any characters from steganography key and keep them at first part of pixel
5. Now take any terminating symbols like 0 to indicate that key has been terminated.
6. Now insert each character of secret message in each of first part of next pixels.
7. Replace each characters of secret message with first part of next pixels.
8. Repeat step 6 and step 7 untill all the characters from secret message are been encoded.

B. Secret message extraction

1. Obtain stenographic image pixels.

2. Now take first pixel and obtain steganography key characters from first part.

3. If the steganography key matches with the key entered by user while insertion then go to next pixels and obtain your secret message characters, follow this until you obtain 0 (terminating symbol) or obtain secret message.

4. If key does not matches with the key entered by user while insertion, then terminate the program.

In this way both the procedures are used to insert as well as extract the secret message.

IV. Encorporating Face Detection And Steganography Techinques In Passport System

Our paper aims at finding out solutions for security issues in passport issuing systems using face detection and Steganography techniques. Following steps explains the entire functioning

Step 1: User can apply for passport online by submitting the necessary details like name,age, contact information along with updated copy of their picture.

Step 2: User will get the appointment date to visit the passport office for verification of documents.

Step 3 : On day verification of the concerned user will be done by authenticating the image sent by the user at the time of online application and the image taken instantly in the passport office.(Image Recognition)

Step 4: After authenticating the user, original documents specifying the user nationality, origin, caste, etc. can be verified.

Step 5: User's official documents will be steganographed with its digital photo and sent for further process. (Steganography)

In this way we ensure that security is maintained. Also it will provide aid to management issues. These records will be stored in database and will be assigned with a identification key concerned to the user. This will help when in future the records are demanded by the concerned user at time of renewal of passport. Moreover this mechanism will ensure that mismatch of information does not take place for e.g. we need to transfer the information of XYX PQR (name surname) then there will never be case that the documents are related to XYZ PQR and picture is of XYZ ABC.

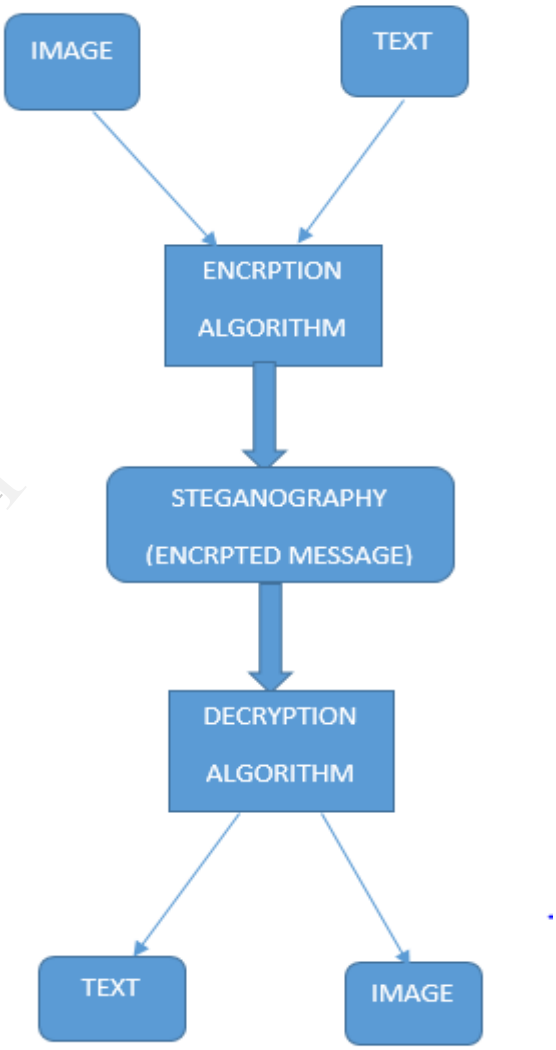


Fig. 2 Block Diagram addressing the working

V. Future Scope

With the emergence of new technology and security systems, steganography has touched all the integral aspects of society. This application can be mainly used by Election commission in order to avoid forgedvoting. Image encrypted with voter's information can be given to all the voters in the form of voting cards,each polling booth will have a decryptor which will recognise the authenticity of the voter.

Its future can be seen in all the government offices where data storage is huge problem, data can be encrypted and kept in the form of images which can be easily decrypted by the officials whenever the data is needed.This will also ensure safety of data from theft and will ensure optimal storage.

VI. CONCLUSION

Our paper presents a system that uses face recognition based on PCA along with Steganography for authentication of users on first place and security of data by encrypting them in images later. In PCA the facial features are being extracted and finally the faces are recognized and the user is authenticated. After PCA, the Steganography method is used so that the documents required for passport are encrypted by steganography techniques. Thus passport office , will have a system which authenticates the users and later stores important and highly confidential information using steganography. Thus solving two major purposes of saving memory and securing data from unauthorized attacks and thefts. Our system can be implemented in various other offices like passport office , which need authentication and security of data, memory management being delivered as a by-product.

REFERENCES

[1] "Face Recognition Systems ", Biometric Face Recognition,Global Security.

[2] Keren Tan, Weiming Chen, Rong Yang, "A PCA-based feature extraction method for face recognition", Dartmouth.

[3] Chandra Mohan & Reddy Sivappagari, " Image/message Steganography using LSB insertion Algorithms for DRM system", Docstoc, March 2013.

[4] Tarun Mirani, Yogesh Motwani, Disha Gurnani , "3-Way Authentication for Virtual Locker", IJERT, September 2014.

.