Face recognition along with DWT based steganography for net banking

[1]Priyanka P. Nalawade, [2]Prof. S.R.Khot
Dept. of Electronics and Telecommunication Engineering, DYPCET, Kolhapur.

Abstract- Face recognition technique now a days is emerging as the most significant and challenging aspects in terms of security for identification of images in various fields like banking, police records, biometric etc. other than an individual's thumb and documented identification proofs. Till date for efficient net banking to be initiated, one has to provide the appropriate user name and password for purpose of authentication. This paper introduces a more reliable authentication of an individual by providing Face Image along with User Name and Password to the system. In this an individual's face is identified by biometric authentication support with which, only a person whose account is, can access it. However while transferring this sensitive data of user image, from client machine to bank server it has to be protected from hackers and intruders from manhandling it, hence it is transferred using covert communication called Wavelet Decomposition based steganography.

Key words: DWT (Discrete Wavelet Transformation),
E-GV-LBP (Effective Gabor Volume Linear Binary Pattern), CMI (Conditional Mutual Information)

I. INTRODUCTION

Recently, with the awareness of businessmen and consumers and the development of computer technologies, the potential use of laptop/ computer devices in financial applications such as banking and stock trading has seen a rapid increase. However, the security challenges being faced are diverse and increasing in number because of huge amount of money flowing across the internet. There have been several attempts in the field to protect users from several attacks but due to many security flaws these schemes are not suitable for real-life implementation. In this paper we focus on Net Banking and provide a scheme based on one-factor biometric authentications for a user i.e. face. In this paper to secure the sensitive data steganography is used.

II.BLOCK DIAGRAM OF THE SYSTEM:

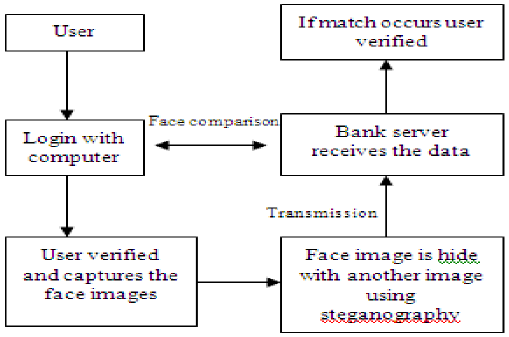
User
If match occurs user verified
Face comparison
Login with computer
Bank server receives the data
Transmission
User verified and captures the face images
Face image is hide with another image using steganography

Figure 1: Block diagram of the System

First of all user has to register with banks with different credentials. If valid user is verified then user face is captured. Apply the steganography to secure the face image and secured face image is sent to the bank server. Bank server uncovers the face image and compares it with the face database. If matching is occurred between received image and database image then and then only user logged into the account.

III. REGISTRATION MODULE

First all user credentials are stored like user name, password, security answer, and number of biometric templates of face. And after that the username is generated. At the time of login, the username is entered and its validity is checked. Then the biometric authentication gets start by capturing the face images. Following is the list of sequences.

1. Accepts the user credentials.
2. Capture the face image and store in individual's folder.
3. Apply E-GV-LBP to generate face variances.
4. Store variances in respective database and complete the registration.

IV. BIOMETRIC AUTHENTICATION MODULE

If the working of registration module is successfully done by giving positive acknowledgment then for login user has to enter username and password. If the provided username and password is valid then and only then the user face is captured to perform biometric authentication. After capturing the face the preprocessing is done to send it to steganography module. The output of steganography module is an extracted face image. Feature matching process is carried out on extracted face image. Following is the list of user actions and system responses.

1. Accepts user's credentials.
2. Capture the face image. Apply steganography to embed and extract image.
3. Apply effective Gabor volume-linear binary pattern (E-GV-LBP) to generate face variances.
4. Apply conditional mutual information-linear discriminant analysis (CMI- LDA) to perform match.

V.STEGANOGRAPHY

Discrete Wavelet transform (DWT) is a mathematical tool used for hierarchically decomposing an image[1]. It is useful for processing of non-stationary signals. The transform is based on small waves, called wavelets, of varying frequency. The DWT splits the signal into high and low frequency parts. The high frequency part contains information about the edge components, while the low frequency part is split again into high and low frequency parts. The high frequency components are usually used for steganography since the human eye is less sensitive to changes in edges [2]. In two dimensional applications, for each level of decomposition, we first perform the DWT in the vertical direction, followed by the DWT in the horizontal direction. After the first level of decomposition, there are 4 sub-bands: LL1, LH1, HL1, and HH1. For each successive level of decomposition, the LL sub band of the previous level is used as the input. To perform second level decomposition, the DWT is applied to LL1 band which decomposes the LL1 band into the four sub- bands LL2, LH2, HL2, and HH2. To perform third level decomposition, the DWT is applied to LL2 band which decompose this band into the four sub-bands – LL3, LH3, HL3, HH3. This results in 10 sub-bands per component. LH1, HL1, and HH1 contain the highest frequency bands present in the image tile, while LL3 contains the lowest frequency band[3]. The three-level DWT decomposition is shown Fig.

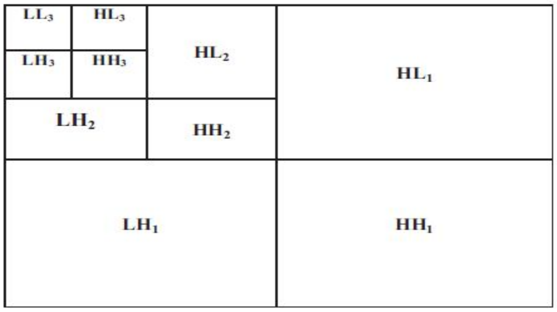

Figure 2:3-level discrete wavelet decomposition

A. *Steganography embedding:*

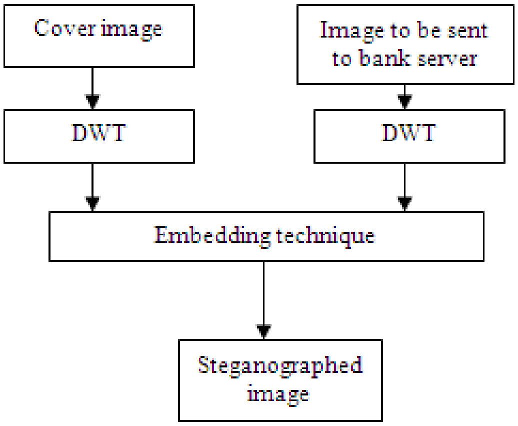

Figure 3: Steganography embedding technique

In this process the gray scale cover image is taken and 2-D, 3-level DWT (Discrete Wavelet Transform) is applied to the image which decomposes image into low frequency and high frequency components. In the same manner 2-D, 3-level DWT is also applied to the face image which is to be embedded in the cover image. The technique used here for inserting the face image is alpha blending [3], [4]. In this technique the decomposed components of the cover image and the face image are multiplied by a scaling factor and are added. According to the formula of the alpha blending the steganographed image is given by

$$WMI = k * (LL3) + q * (WM3)$$

Where,
WMI = low frequency component of steganographed image.
LL3 = low frequency component of the cover image obtained by 3-level DWT.
WM3 = low frequency component of face image.
k, q = Scaling factors for the cover image and face image respectively.

After embedding the cover image with face image, 3-level Inverse discrete wavelet transform is applied on steganographed image to generate the final secure steganographed image.

B. *Steganography extraction:*

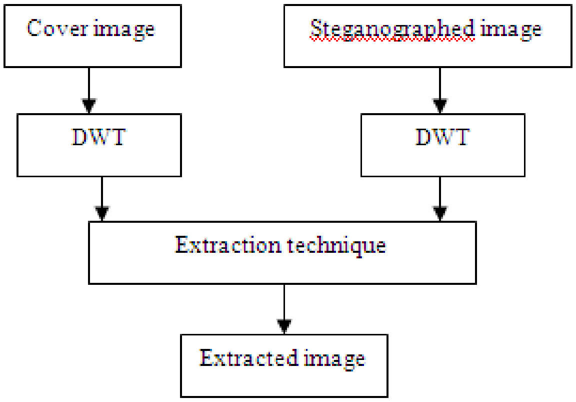

Figure 4:Steganography extraction technique

In this process 3-level DWT is applied to steganographed image and cover image which decomposed the image in subbands. After that the face image is recovered from the steganographed image by using the formula of the alpha blending extraction [4]. According to the formula of the alpha blending the recovered image is given by

$$RW = (WMI - k * LL3) \quad (2)$$

Where,
RW= Low frequency approximation of Extracted image.
LL3= Low frequency approximation of the cover image.
WMI= Low frequency approximation of steganographed image.

After extraction process, 3-level Inverse discrete wavelet transform is applied to the face image coefficient to generate the final extracted face image [5]. Figure shows the

Steganography extraction process.

VI. FACE REPRESENTATION

This module represents the face using Gabor techniques.

A. Gabor filters:

Uncovered image is given as input to Gabor kernel where Gabor faces are generated as a output and it is given to E-GV-LBP to produce face representation as E-GV-LBP.

B. Gabor faces :

Gabor filters, which exhibit desirable characteristics of spatial locality and orientation selectively are localized in the space and frequency domains, have been successfully used in face recognition[6].

C. EGV-LBP:

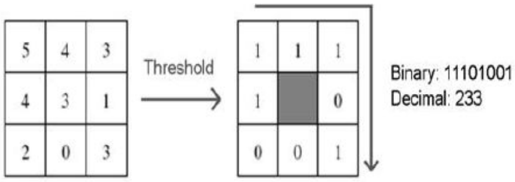

Figure 5: Basic LBP operator

A local binary pattern LBP is introduced as a powerful local descriptor for micro features of images. The basic LBP operator labels the pixels of an image by thresholding the 3*3 neighborhood of each pixel with the centre value and considering the result as a binary number (LBP codes). In LBP 8 values around the centre pixel are calculated. Around values which are less than the centre value are marked as 0. And the around values greater than centre value are marked as 1.Then the binary pattern is decided and the decimal value is calculated. Here the decimal value is always less than or equal to 256. To represent face to be compared with database images the GV-LBP (E-GV-LBP) is developed[7] which encodes the information in spatial, frequency and orientation domains simultaneously and reduces the computational cost.

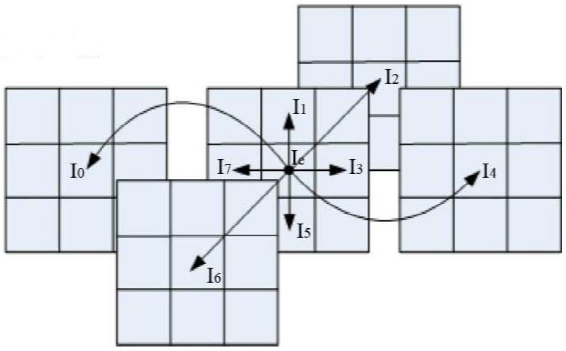

Figure 6: Formulation of E-GV-LBP

For the central point IC, I0, I4 are the orientation neighboring pixels.I2 and I6 are the scale neighboring ones I1, I3, I5, I7 are the neighboring pixels in spatial domains Like in LBP, all the values of these pixels surrounded are compared to the value of the central pixel, threshold into 0 or 1 and transformed into a value between 0 and 255 to form the E-GVLBP value [7]. In E- GV-LBP the neighboring changes in spatial space and during different types of Gabor faces can be encoded moreover to reduce computational complexity this descriptor was developed that describes the neighboring changes according to the central point in spatial, scale, orientation domain. Following figure demonstrates the E-GVLBP codes based upon 40 Gabor magnitudes and phase faces for an input face image. The histogram features are then computed based upon the E-GV-LBP codes.

VII. FACE RECOGNITION

This module compares the features of test and database (Trained) image for that CMI based features selection method is used and variance is calculated by LDA to find the difference between the two images

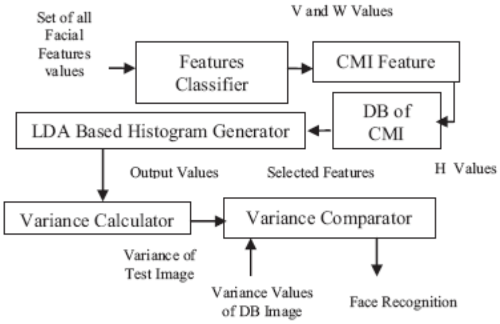

Figure 7: face recognition and comparator

A. CMI based feature selection:

This module compares the features of test and database (trained) image for that CMI based features selection method is used and variance is calculated by LDA to find the difference between the two images Face recognition process has 2 important phases 'CMI based features selection' and 'LDA Histogram generator and variance comparator' CMI based features selection CMI is conditional Mutual Information.

B. LDA based variance comparator:

In this part, conduct LDA on the selected features to learn the most discriminant subspace for classification[6]. The essential idea of LDA is to disperse samples from different classes and meanwhile gather the samples from the same class. Given the training samples z={z1,z2,zn} the between class scatter matrix Sb and within class scatter matrix Sw are calculated. LDA aims to find the projective directions *W* which maximize the ratio of between class scatter matrix to within class scatter. In classification phase, after projecting the original data onto discriminant subspace, cosine distance is utilized to measure the dissimilarity of two samples in subspace.

VIII.CONCLUSION:

This system is exclusively designed as desktop application. It demonstrates the proper functioning of steganography and face recognition algorithms. Besides it requires less database as compared to existing methods, which speeds up the process of authentication. The steganography is effectively implemented by DWT method using alpha blending technique. This reduces both the program and time complexity giving a flawless and tamperproof data hiding technique while passing through an unsecured channel. The new E-GV-LBP technique over seeds the traditional approach of face recognition. Gabor techniques are used for finely capturing expressions and illuminations. Finally Linear Discriminant Analysis is done for variance comparison using CMI based method to get the final output. This project gives tool for secured net banking solution with one factor biometric authentication.

IX.REFERENCEs

[1] X. Xia, C. Boncelet, and G. Arce, A Multiresolution "Watermark for Digital Images Processing". IEEE, Vol 1, PP 548-551, October 1997.
[2] D. Kundur and D. Hatzinakos, "Digital Watermarking using Multiresolution Wavelet Decomposition", Acoustic, Speech, Signal Processing IEEE, Vol 5. PP 2969-2972,1998.
[3] Akhil Pratap Shing, Agya Mishra, "Wavelet Based Watermarking on Digital Image", Indian Journal of computer Science and Engineering, 2011.
[4] Image Watermarking Using 3-Level discrete Wavelet Transform (DWT) Nikita Kashyap Shankaracharya Technical Campus, Bhilai, India I.J.Modern Education and Computer Science, 2012, Vol 3, PP 50-56 April 2012.
[5] Prabakaran, G. "A modified secure digital image steganography based on DWT Computing", Electronics and Electrical Technologies (ICCEET), 2012 International Conference March 2012.
[6] Zhen Lei, Shengcai Liao, Matti Pietikainen, Face Recognition by Exploring Information Jointly in Space, Scale and Orientation IEEE, Vol. 20,. JANUARY 2011.
[7]Ahonen, T.; Hadid, A.; Pietikainen, M. , "Face Description with Local Binary Patterns:Application to Face Recognition" IEEE vol 28, 2006