A SECURED TEMPLATE BASED FACE RECOGNITION TECHNIQUE

Minakshi Gogoi[1], RupKumar Deka[2], Deepjyoti Mazumdar[3], Rupam Das[4], Manasjyoti Barman[5]

Department of Computer Science and Engineering, GIMT, Azara, Guwahati-17, Assam [1]m_gogoi@tezu.ernet.in
[2](rup.deka,deep.cse2008,m9954508820,mjbarman)@gmail.com

ABSTRACT

Recently face recognition is attracting much attention in the society of network multimedia information access. The face recognition has been a challenging scientific problem that provides a powerful incentive for processing large volume of data automatically for authenticating people. Independent Component Analysis (ICA) is a method in which the goal is to find a linear representation of non-Gaussian data, so that the components are statistically independent, or as independent as possible. Such a representation captures the essential structure of the data in many applications, including feature extraction and signal separation. A biometric template that stores the extracted biometric features as a database is a rising concern about the security and privacy of the biometric data itself. The protection of face template is also to be considered as an issue in deploying a practical biometric system. In this paper we propose a face template protection scheme based on our cryptosystem approach.

KEYWORDS

Independent Component Analysis, Face template, Cryptography

1. INTRODUCTION

In the ever changing world of global data communications, inexpensive internet connections, and fast-paced software development, security is becoming more and more of an issue. Security is now a basic requirement because global computing is inherently insecure. Many applications find confidential information from their users. So there are many situations where we have to verify the individuals as an authentic user by some electronic device or by some knowledge based security such as passwords etc. Both the techniques have disadvantages. They can be computerized or may be forgotten or lost. So these types of security methods don't provide sufficient security in many critical applications. Biometrics is a way to overcome these issues. Biometrics signals are more secure, but they also need to be protected. Biometric template protection is one of the most important issues in deploying a practical biometric system. To tackle this problem, many algorithms, that do not store the template in its original form, instead, a transformed version of the original template is stored in recent years. Biometric like face in the form of still photos, video feed from camera etc are nowadays used in many security based applications. Many researches have been done on this field for decades. In this paper we tried to explain how a face-recognition technology works along with an added security for the templates used in the system.

Natarajan Meghanathan, et al. (Eds): SIPM, FCST, ITCA, WSE, ACSIT, CS & IT 06, pp. 153–166, 2012.
 DOI : 10.5121/csit.2012.2316

The organization of the paper is as follows: Section 2 describes the related face feature extraction works and biometric template protection techniques. In section 3, we discuss about the Independent Component Analysis as a face feature extraction technique and Cryptographic approach of face template security. In section 4, we have given our methods. The performance of the proposed method is demonstrated in section 5, followed by our concluding remarks in section 6.

2. RELATED WORKS

There are many methods proposed for facial feature extraction. The major human face recognition techniques that apply mostly to frontal faces are eigen feature, neural network, dynamic link architecture, hidden Markov model, geometrical feature matching etc.

.

2.1. Face Feature Extraction Method

- PRINCIPAL COMPONENT ANALYSIS (PCA) [2]: Principal component analysis (PCA) is a mathematical procedure that uses an orthogonal transformation to convert a set of observations of possibly correlated variables into a set of values of uncorrelated variables called principal components. The number of principal components is less than or equal to the number of original variables. This transformation is defined in such a way that the first principal component has as high a variance as possible and each succeeding component in turn has the highest variance possible under the constraint that it be orthogonal to (uncorrelated with) the preceding components.

- INDEPENDENT COMPONENT ANALYSIS (ICA) [3]: Independent Component Analysis (ICA) is similar to PCA except that the distribution of the components is designed to be non-Gaussian. Maximizing non-Gaussianity promotes statistical independence. The ICA separates the high-order moments of the input in addition to the second-order moments utilized in PCA. Both the architectures lead to a similar performance. The obtained basis vectors are based on Fast Fixed-Point Algorithm for the ICA factorial code representation. There is no special order imposed on the ICA basis vectors.

- DISCRETE COSINE TRANSFORMS (DCT) [4]: A discrete cosine transform (DCT) expresses a sequence of finitely many data points in terms of a sum of cosine functions oscillating at different frequencies. Like any Fourier-related transform, discrete cosine transforms (DCTs) express a function or a signal in terms of a sum of sinusoids with different frequencies and amplitudes. Like the Discrete Fourier transforms (DFT), a DCT operates on a function at a finite number of discrete data points. DCTs are important to numerous applications in science and engineering, from lossy compression of audio (e.g. MP3) and images (e.g. JPEG), to spectral methods for the numerical solution of partial differential equations.

- GABOR WAVELET [4]: In image processing, a Gabor filter, named after Dennis Gabor, is a linear filter used for edge detection. Frequency and orientation representations of Gabor filters are similar to those of the human visual system, and they have been found to be particularly appropriate for texture representation and discrimination. In the spatial domain, a 2D Gabor filter is a Gaussian kernel function modulated by a sinusoidal plane wave. The Gabor filters are self-similar: all filters can be generated from one mother wavelet by dilation and rotation.

- FACE GLOH SIGNATURE [4]: GLOH features are an extension to the descriptors used in the scale invariant feature transform (SIFT). Like SIFT the GLOH descriptor is a 3D histogram of gradient location and orientation, where location is quantized into a log-polar location grid and the gradient angle is quantized into eight orientations. Each orientation plane represents the gradient magnitude corresponding to a given orientation. To obtain illumination invariance, the

descriptor is normalized by the square root of the sum of squared components. Face-GLOH signatures are invariant w.r.t. scale, translation and rotation and therefore do not require properly aligned images. The resulting dimensionality of the vector is also low as compared to other commonly used local features such as Gabor, Local Binary Pattern Histogram 'LBP' etc. and therefore learning based methods can also benefit from it.

- WALSH HADAMARD TRANSFORMS (WHT) [5]: The Hadamard transform (also known as the Walsh–Hadamard transform, Hadamard–Rademacher–Walsh transform, Walsh transform, or Walsh–Fourier transform) is an example of a generalized class of Fourier transforms. It performs an orthogonal, symmetric, involutional, linear operation on 2m real numbers (or complex numbers, although the Hadamard matrices themselves are purely real).

- HIDDEN MARKOV MODEL (HMM) BASED APPROACH [6]: HMMs are used to model human faces for identication purposes. Faces can be intuitively divided into regions such as the mouth, eyes, nose, etc., and these regions can be associated with the states of an HMM. The identication performance of a top-bottom HMM compares favourably with some of the well-known algorithms, for example eigenfaces. For face images of fixed size there are 3 HMM parameters which affect the performance of the model:

  - the number of HMM states (N),
  - the height of the sampling window (L)
  - The amount of overlap (M).

Table 1. Different feature extraction techniques used in face recognition

Facial feature extraction technique	**Short description**
Discrete Cosine Transform (DCT)	Zahid Riaz. et. al.[4] have expressed a sequence of finite set of many data points in terms of a sum of cosine functions oscillating at different frequencies.
Gabor Wavelet	Zahid Riaz, et. al.[4] expressed a Gabor filter, named after Dennis Gabor, is a linear filter used for edge detection.
Principal Component Analysis (PCA)	Kyungnam Kim. et. al.[2] developed a mathematical procedure that uses an orthogonal transformation to convert a set of observations of possibly correlated variables into a set of values of uncorrelated variables called principal components.
Hidden Markov Model (HMM) Based Approach	Monson H.Hayes III et. at.[6] created HMMs that are used to model human faces for identication purposes. Faces can be intuitively divided into regions such as the mouth, eyes, nose, etc., and the regions can be associated with the states of HMM
Independent Component Analysis (ICA)	Hyvärinen et al. [3] found a computational method for separating a multivariate signal into additive subcomponents supposing the mutual statistical independence of the non-Gaussian source signals. It is a special case of blind source separation.
Face GLOH signature	Zahid Riaz et. al.[4] developed a features that are an extension to the descriptors used in the scale invariant feature transform (SIFT).
Walsh Hadamard Transform (WHT)	M.Hassan et. al [5] performed an orthogonal, symmetric, involutional, linear operation on real numbers or complex numbers .

2.2. Biometric Template Security

A biometric template protection algorithm should satisfy the three basic requirements [16]: security, discriminability and cancelability. That means it should be compositionality hard to reconstruct the original biometric template from the transformed biometric template. The discriminability of the original biometric template should not be degraded after the transformation. Cancelability means the algorithm should be able to generate many transformed template from the original as per requirement and the different transformed template for different applications.

Biometric template security algorithms have been categorized into two main approaches [17]: (i) the biometric cryptosystem approach and (ii) the transformed-based approach. The basic idea behind both the approaches is that instead of storing the original template, the transformed/encrypted template is stored.

2.2.1. Biometric cryptosystem approach [18]:

A critical issue in biometric systems is protecting the template of a user which is typically stored in a database or a smart card. The fuzzy vault construct [19] is a biometric cryptosystem that secures both the secret key and the biometric template by binding them within a cryptographic framework and hence its security level is high. Here the error-correcting coding techniques are employed to handle intraclass variations which may not be strong enough to handle large intraclass variations such as face images captured under different illuminations and poses. Hence the error-correcting coding techniques require input in certain format like binary strings [20] or integer vectors with limited range [21], and it is hard to represent every biometric template in this desired format.

2. 2. 2. Transform-based approach:

In the transform-based approach, a transformed template is generated using a “one-way” transform and the matching is performed in the transformed domain to avoid exposure of the original biometric template. Template transformation techniques modify the template with a user specific key such that it is difficult to recover the original template from the transformed template. While authentication, similar transformation is applied to the biometric query and matching is performed in the transformed domain. The template security is to be guaranteed as the key is to be stored in the system along with the transformed template. Hence the transformation function needs to be non-invertible. Bio-Hashing [49] and cancelable biometrics [42] are few of the transform-based approach. The transform-based approach has a good revocability property, but the drawback of this approach is the trade-off between performance and security of the transformed template.

3. BACKGROUND OF THE WORK

3.1. Feature Extraction and Distance Measuring Techniques

3.1.1. Independent Component Analysis:

Independent component analysis (ICA) is a computational method for separating a multivariate signal into additive subcomponents supposing the mutual statistical independence of the non-Gaussian source signals. A simple application of ICA is the "cocktail party problem”, where the underlying speech signals are separated from a sample data consisting of people talking simultaneously in a room. An important note to consider is that if N sources are present, at least N

observations (e.g. microphones) are needed to get the original signals. ICA finds the independent components (aka factors, latent variables or sources) by maximizing the statistical independence of the estimated components. Typical algorithms for ICA use centering, whitening (usually with the eigen-value decomposition), and dimensionality reduction as pre-processing steps in order to simplify and reduce the complexity of the problem for the actual iterative algorithm. Whitening and dimension reduction can be achieved with principal component analysis or singular value decomposition. Whitening ensures that all dimensions are treated equally a priori before the algorithm is run. Algorithms for ICA include INFOMAX, FASTICA, AND JADE, but there are many others also. In general, ICA cannot identify the actual number of source signals, a uniquely correct ordering of the source signals, nor the proper scaling (including sign) of the source signals.

FastICA[3]

Typical algorithms for ICA use centering, whitening (usually with the eigen-value decomposition), and dimensionality reduction as pre-processing steps in order to simplify and reduce the complexity of the problem for the actual iterative algorithm. Whitening and dimension reduction can be achieved with principal component analysis or singular value decomposition. Whitening ensures that all dimensions are treated equally a priori before the algorithm is run.

FastICA is an efficient and popular algorithm for independent component analysis invented by Aapo Hyvärinen at Helsinki University of Technology. The algorithm is based on a fixed-point iteration scheme maximizing non-Gaussianity as a measure of statistical independence. It can be also derived as an approximative Newton iteration.

The basic form of the FastICA algorithm is as follows:

A. Randomize the initial weight vector $\mathbf{w}$

B. Let $\mathbf{w}^+ \leftarrow E\{\mathbf{x}g(\mathbf{w}^T\mathbf{x})\} - E\{g'(\mathbf{w}^T\mathbf{x})\}\mathbf{w}$

C. Let $\mathbf{w} \leftarrow \mathbf{w}^+ / \|\mathbf{w}^+\|$

D. If not converged, go back to 2

3.1.2. Euclidean Distance

In mathematics the Euclidean distance or Euclidean metric is the ordinary distance between two points that one would measure with a ruler and is given by the Pythagorean formula

If U=(x1, y1) and V=(x2, y2) are two points on the plane, their Euclidean distance (E) is calculated by

$$E=\sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$$

In our process we replaced the co-ordinate points with the pixel values of the images i.e. we calculated the distances between all the pixels of an image. We repeated the whole procedure for all the images of our database .Now for a single individual we have calculated a value called threshold values which is taken as the mean of all the Euclidean Distances for a single individual.

3.2. Template security

Cryptographic approach:

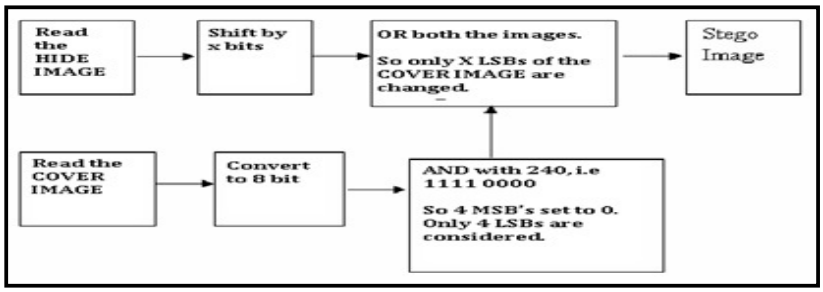

Fig. 1. Block diagram of LSB Steganography

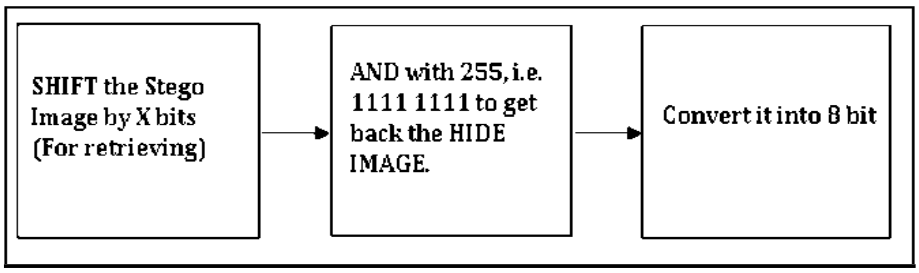

Fig. 2. Block diagram for extracting the hidden image

4. METHODS/ALGORITHMS USED

This paper presents a new framework for the secured face template. The block diagram of the proposed method is shown in **Fig 3**.

4.1. System design

The proposed SecureFace algorithm attempts give an secured face template based on dynamic threshold using CrypFace and KeyGen algorithms.

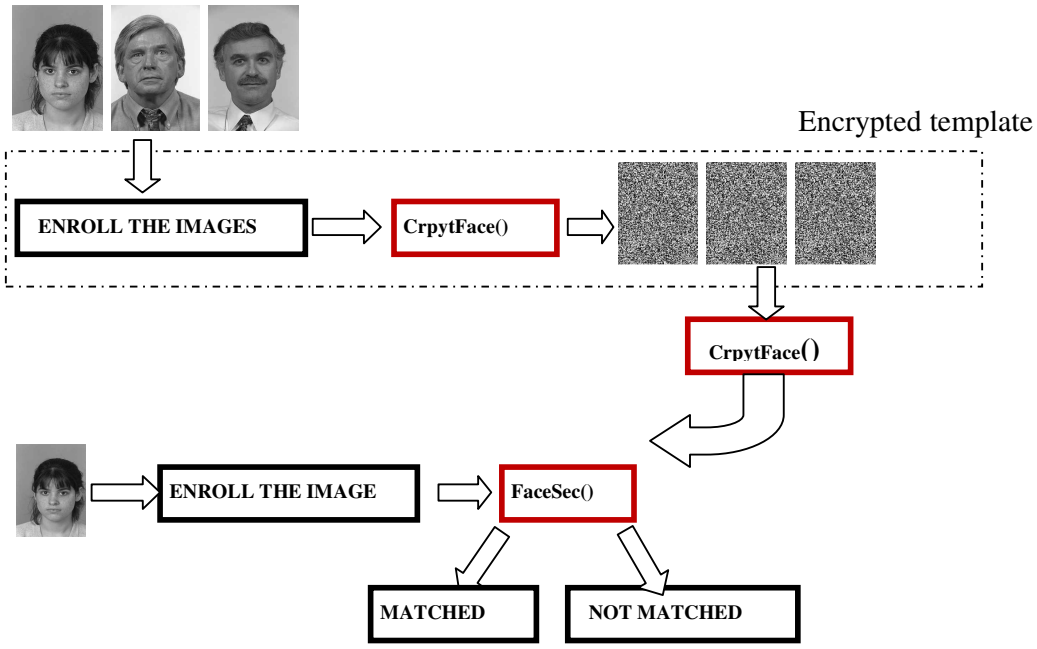

Fig. 3. A secured face recognition design

SecureFace: An Overview

Algorithm SecureFace():
Input: Images
Output: Match/ Not matched
Steps:

1: *Enrol the Train images.*
2: *Secure the images using CryptFace( ) to create the template.*
3: *Enrol the Test images.*
4: *Decrypt the templates.*
5: *Calculate the ICA values of Test image and templates.*
6: *Compute the Euclidean Distances among ICA values of Test image and templates.*
7: *Create the threshold profile using the Euclidean Distances among the ICA values of the templates.*
8: *Based on the threshold profile the Test image is accepted or rejected.*

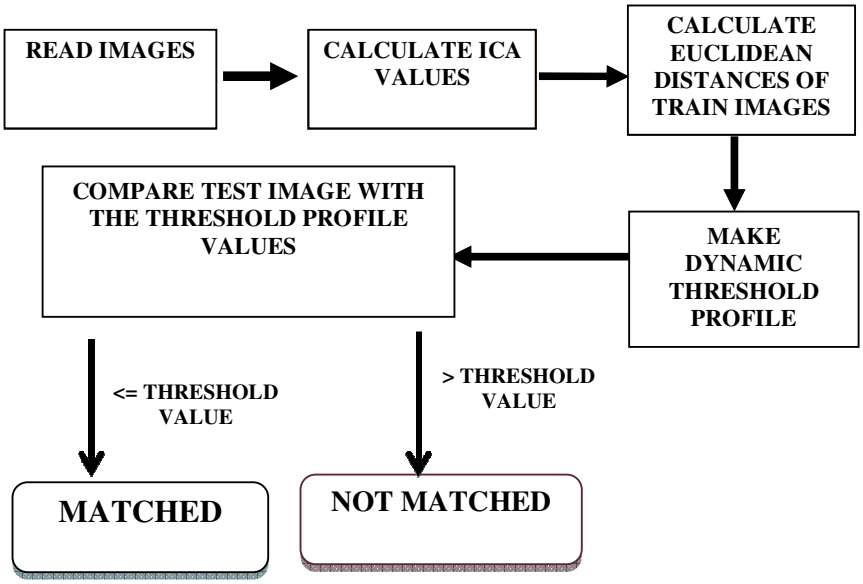

Fig.4.Dynamic threshold based face recognition.

4.3. CryptFace: An Overview

The algorithm CryptFace would use KeyGen algorithm to generate a symmetric key. This function is used to ENCRYPT or DECRYPT the input image, taking the Image matrix and the Key matrix as arguments

Algorithm CryptFace(Img_Inp,Key **):**
Input: Input image, Img_Inp and Key matrix, key
Output: The processed image **Pro_Img_Out**
Steps:

1. *Store the size of the Img_Inp into an array of size (n x m) x d.*
   n = number of rows.
   m = number of columns.
   d = dimensions

   For ***i*** *=1 to m,*
   *p = (i-1)*n.*
   Fkey (i)=Key [(1 + p), ((1+p) +1), ((1+p) +2) ...p + n]
   End
2. *Store the value of n and m in two new variables length and breadth.*
3. *For i =1:d*
   Img=size(Img_Inp)
   For j=1 : length
   For k=1:breadth
   Pro_img_Out(j,k)=bitxor (Img(j, k), Fkey(j,k))
   End
   End
   End
4. *Exit.*

4.4. KeyGen:

This function is used to generate the KEY, taking size of the input image as the input. The output obtained is a matrix of size (no. of rows x no. of columns) x 1.

INPUT: Total elements of the matrix (i.e. n x m)
OUTPUT: A matrix, **key** of size (n x m) x 1.

Steps:

1. *n=n x 8*
2. *A=zeros(size(nx1))*
3. *B and C* **= 0.**
4. *For I =2: n*
   C = 1 - 2BxB
   If C > 0
   *A(i – 1)=**1***
   B=C
   End
5. *Key=zeroes (n/8 x 1).*
6. *For j= 1: n/8*
   For k=1: 8,
   *Key (j) = Key (j) + A (k*j)*2^{k-1}.*
   End
   End
7. *Exit.*

5. Performance Evaluation:

(a) ***Environment used:*** The experiment was carried out on a workstation with Intel Dual-Core processor (1.86 GHz) with 1 GB of RAM .We used Matlab 7.2 (R2006a) version in windows (64-bits) platform for the performance evaluation.

(b) ***Datasets used:*** In this work we have used a standard database known as FERET IMAGE DATABASE. FERET database is a standard dataset used for facial recognition system evaluation. The dataset includes 2413 till facial images representing 856 individuals. In this work we have worked with 100 individual with 10 images each.

(c) ***Experimental Results and analysis:*** From the experimental results obtained based on the 100x10 images from FERET datasets , we have drawn the FAR-FRR curves as in fig. 6 and also the recognition curves as in as in **Fig. 7.**

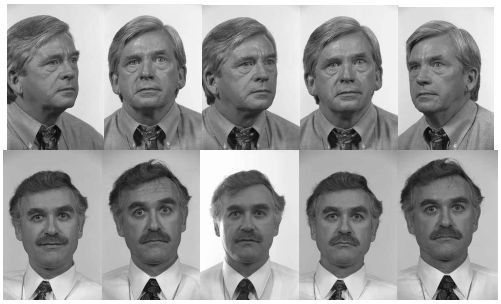

Fig. 5: Some images (faces) we have used in our project.

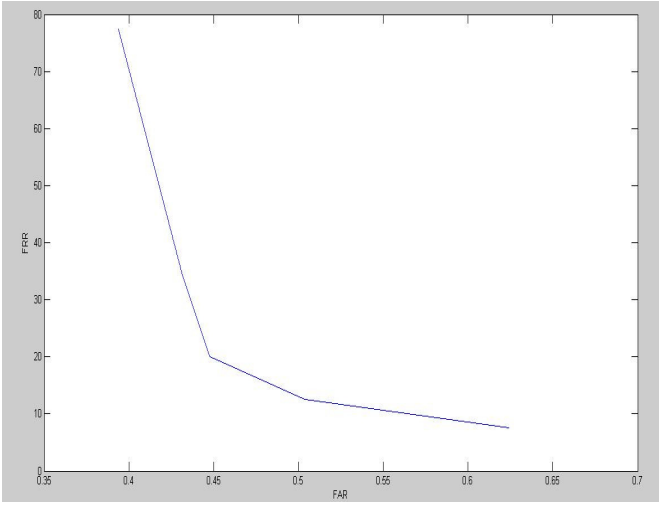

Fig.6. FAR-FRR curves depicting dynamic threshold based face recognition

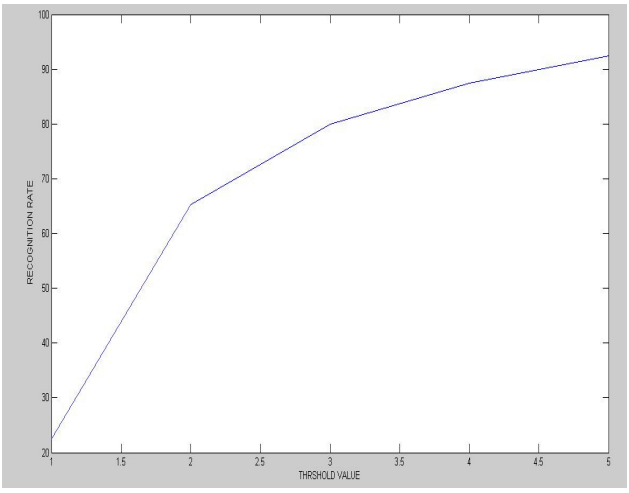

Fig.7. Recognition curve depicting dynamic threshold based face recognition

Table 2. Table for different FAR-FRR values obtained at different dynamic thresholds

METHOD USED	TEST IMAGES	TRAIN IMAGES	FAR	FRR
INDEPENDENT COMPONENT ANALYSIS	4x100	6x100	0.3937	77.416
			0.4312	34.729
			0.4478	20
			0.5036	12.472
			0.6244	7.600

6. Conclusions

With the use of the new technique we were able to:

- Increase the detection rate to a higher extent.
- Our Security Algorithm is much more secured than the LSB insertion method

Fig. 8. Snapshots of the Graphical User Interface showing various results

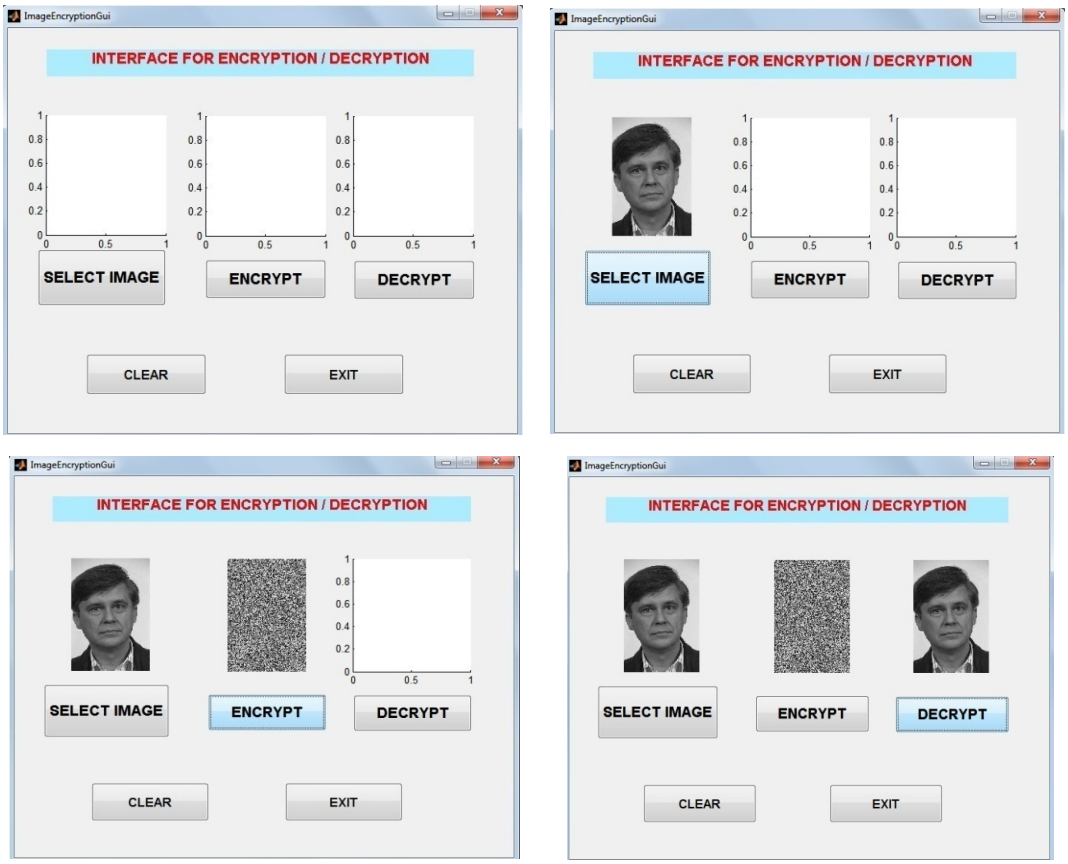

Fig. 9. Different snapshot of the Graphical User Interface for the Encrption/Decreption Process

REFERENCES

[1] M.A. Turk and A.P. Pentland, "Face Recognition Using Eigen faces", IEEE Conf. on Computer Vision and Pattern Recognition, pp. 586-591, 1991.

[2] M.S. Bartlett, J.R. Movellan, and T.J. Sejnowski, "Face recognition by independent component analysis," IEEE Trans. Neural Networks, Vol. 13, no. 6, pp. 1450–1464, 2002.

[3] Erik hjelmas, "Biometric systems: A face recognition approach ", www.researchindex.org, 2000.

[4] Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, Silman, J., "Steganography and Steganalysis: An Overview", SANS Institute, 2001 Jamil, T., "Steganography: The art of hiding information is plain sight", IEEE Potentials, 18:01, 1999.

[5] R. Chandramouli, Nasir Memon, "Analysis of LSB Based Image Steganography Techniques" Proc. IEEE ICIP pp 1019-1022, 2001.

[6] J.Fridrich, M.Goljan and R.Du, "Reliable detection of LSB steganography in color and grayscale images" proc. ACM workshop multimedia security, Ottava,ON Canada ,Oct 5, 2001,pp27-30.

[7] Digital Image Processing using MATLAB by Gonzale Woods.

[8] M.Hasssan "Walsh-Hadamard Transform for Facial Feature Extraction in Face Recognition" World Acedemy of Science and Technology.

[9] Neural Networks, 13(4-5):411–430, 2000.

[10] H.K.Ekenel,Dept of Electrical and Elecctronic Engineering,Bogazici University,Turkey "Feature Selection in the Independent Component Subspace For Face Recognition."

[11] Jian Yang, David Zhang, Jing-yu Yang, "Is ICA Significantly Better than PCA for Face Recognition?" Proceedings of the Tenth IEEE International Conference on Computer Vision (ICCV'05) 1550- 5499/05

[12] Fundamentals of Digital Image Processing: A Practical Approach with Examples in Matlab by Chris Solomon, Toby Breckon.

[13] Kyungnam Kim Dept of Computer Science –University of MaryLand "Face Recognition using Principle Component Analysis"

[14] Zahid Riaz Institute of Informatik,Technical University of Munich,Germany "Sarfraz "Feature Exctraction and Representation for Face Recognititon"

[15] Monson H.Hayes III, "Face Detection and Recognition using Hidden Markov Models" , Geogia Institiue of Technology, Atlanta

[16] Yi C. Feng, Pong C. Yuen, Anil K. Jain, "A Hybrid Approach for Generating Secure and Discriminating Face Template"

[17] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," EURASIP J. Adv. Signal Process. 2008 .

[18] Yi C. Feng, Pong C. Yuen and A. K. Jain, "A Hybrid Approach for Generating Secure and Discriminating Face Template", IEEE Transactions on Information Forensics and Security, Vol. 5, No. 1, march 2010

[19] A. Juels and M. Sudan, "A fuzzy vault scheme," in IEEE Int. Symp.Information Theory, 2002, p. 408.

[20] Teoh, A.B.J., Toh, K.A., Yip,W.K. "2N Discretisation of BioPhasor in Cancellable Biometrics" In: Proc. Second Intl. Conf. on Biometrics, pp. 435–444. Seoul, South Korea (2007)

Authors

Ms. Minakshi Gogoi is working as an Asst. Professor, Department of IT, GIMT, Azara, Guwahati-17. She is pursuing her Ph.D. degree from the Department of Computer Science and Engineering, Tezpur University and her research areas include Bio-metrics authentication and security, Data Mining and Image processing.

Rupkumar Deka is a student of Department of CSE, GIMT, Azara, Guwahati-17. He is pursuing the Bachelor of Engineering in Computer Science and Engineering under Gauhati University. His research interests are in biometric authentication, biometric Security etc.

Deepjyoti Mazumdar is a student of Department of CSE, GIMT, Azara, Guwahati-17. He is pursuing the Bachelor of Engineering in Computer Science and Engineering under Gauhati University. His research interests are in biometric authentication , biometric Security etc.

Manasjyoti Barman is a student of Department of CSE, GIMT, Azara, Guwahati-17. He is pursuing the Bachelor of Engineering in Computer Science and Engineering under Gauhati University. His research interests are in Biometric Security , Network security etc

Rupam Das is a student of Department of CSE, GIMT, Azara, Guwahati-17. He is pursuing the Bachelor of Engineering in Computer Science and Engineering under Gauhati University His research interests are in Biometric authentication , Network Security etc.