Secure Face-Recognition using Encrypted image Between Client and Server

Akhil Kumar Singh, Dr.Harsh K.Verma, and Vaibhaw Dixit

ABSTRACT—This paper includes two different parts, first one encrypt an image at the client side and the next part is used for the recognition purpose, which results that the claimed identity is authorized or not. In this paper we are presenting an approach to the detection and identification of human faces for the purpose of secure authentication between a client and a server and describe a working, near real-time face recognition system which tracks a subject's head and then recognizes the person by comparing characteristics of the face to those of known individuals. Here our approach treats face recognition as a two-dimensional recognition problem, and we are using Principal component analysis(PCA) for the image recognition and compression purpose. Face images are projected onto a feature space ("face space") that best encodes the variation among known face images. The face space is defined by the "eigen-faces", which are the eigen vectors of the set of faces. The block based transformation technique with Blowfish algorithm makes PCA algorithm more secure for face recognition and for very strong authentication between client and server communication.

Index Terms— Block based transformation, Client-Sever Communication, Eigen-faces, PCA.

1 INTRODUCTION

The face is our primary focus in social intercourse, playing a very important role in identifying identity and emotion of human being.Although the ability to infer intelligence or character from facial appearance is suspect, the ability to recognize faces is remarkable.

As we mentioned in this paper we are going collaborate two aspects , first one is the image security and after that face recognition.

1.1 Image Transformation and Encryption

Encryption techniques are used to secure information over open network. Different data has their different features, therefore different encryption techniques are used to protect confidential information, specially for the authentication purpose. Most of the available encryption techniques are used for only text data and these techniques does not suits for multimedia data such as images or videos. Therefore in this paper we are using block based transformation technique based on the combination of transformation algorithm and an encryption and decryption algorithm called Blowfish algorithm.

In most of the images, the values of the neighboring pixels are strongly correlated it means the value of any given pixel can be predicted from the values of its neighbours ;S. P. Nana'vati., P. K. Panigrahi, c. Ratael, Gonzales, AL. Vitali, A. Borneo [1],[2],[3]. In this paper our main idea is to reduce the correlation between neighbourer pixels and to increase the antropy between them.For this purpose we propose a block based transformation algorithm that divides the image into a number of blocks and then shuffles their positions before it passes them to the Blowfish encryption algorithm.

By using the correlation and entropy as a measure of security, this process results in a lower correlation and a higher entropy value when compared to using the Blowfish algorithm alone, and thus improving the security level of the encrypted images.

There are two main keys to increase the entropy; the variable secret key for the transformation process, which is used to build the secret transformation table with a variable number of blocks(In case if the key is changed, another seed will be generated, and then a different secret transformation table is obtained) and the variable secret key for the Blowfish algorithm, which is used to encrypt the transformed image.

1.2 Face Recognition

After secure transmission of image of human face from the client-side, server is responsible for the recognition of face, that is authorized or not. In this case we are using PCA algorithm which provide more accuracy checking for the human face images. The main reason behind using PCA is it can provide prediction, redundancy control feature, feature extraction, data compression etc.

2 BACKGROUND

Encryption is the process which is used to transform an information into a secure form. With the huge growth of computer networks and the latest advances in digital technologies, a huge amount of

- *Akhil Kumar Singh with the National Institute of Technology, Jalandhar, Jalandhar, 144011. E-mail: akhils070@gmail.com.*
- *Dr. Harsh K Verma, Head, Department of Computer Science and Engineering,NIT jalandhar, E-mail: vermah@nitj.ac.in*
- *Vaibhaw Dixit with the National Institute of Technology, Jalandhar, Jalandhar, 144011. E-mail: vaibhaw.dixit@gmail.com.*

digital data is being exchanged over various types of networks. For the security of confidential and private data we have used different security mechanism , but those mechanisms are not perfectaly suits for multimedia data; H. El-din. H. Ahmed, H. M. Kalash, and O. S. Farag Allah [4].

Image encryption techniques try to convert an image to another one that is hard to understand, there is no single encryption algorithm satisfies the different image types; Li. Shujun, X. Zheng [5]. There are two major groups of image encryption algorithms: (i) non-chaos selective methods and (ii) Chaos-based selective or non-selective methods. Some of the algorithms are scalable and have different modes ranging from degradation to strong encryption; S.S. Maniccam, N.G. Bourbakis[6]. Mitra A[7] have proposed a random combinational image encryption approach with bit, pixel and block permutations. Zhi-Hong Guan[8] have presented a new image encryption scheme, in which shuffling the positions and changing the grey values of image pixels are combined to confuse the relationship between the cipher image and the plain image.

Sinha A. and Singh K.[9] proposed an image encryption by using Fractional Fourier Transform (FRFT) and JigSaw Transform (JST) in image bit planes. Shujun Li[10] have pointed out that all permutation-only image ciphers were insecure against known/chosen-plaintext attacks.

Maniccam S.S. and Bourbakis N G.[6] proposed image and video encryption using SCAN patterns. The image encryption is performed by SCAN-based permutation of pixels and a substitution rule which together form an iterated product cipher.

The algorithm which is proposed by us ,divides the image into random number of blocks with predefined maximum and minimum number of pixels, resulting in a stronger encryption and a decreased correlation.

3 PROCEDURE

The whole process contains the image encryption at client-end and face recognition at server-end which is described in Fig 1,Fig 2,Fig 3.

3.1 Transformation and Encryption of Image

First of all we need to transform an image using block based transformation. In this our main focus should be to increase the number of blocks ,so that after shuffeling those blocks the correla

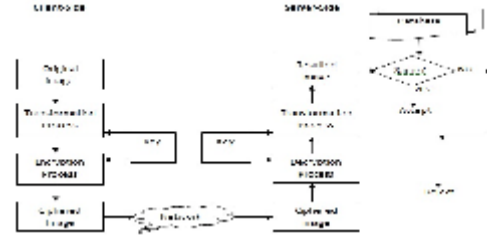

Fig 1: whole process

tion between neighbor pixel will be minimum. In this paper we have used following algorithm for block based encryption with a slightly change in it. We have added a large prime number into a portion (HorizontalNoBlocks * VerticalNoBlocks) to increase the number of blocks.

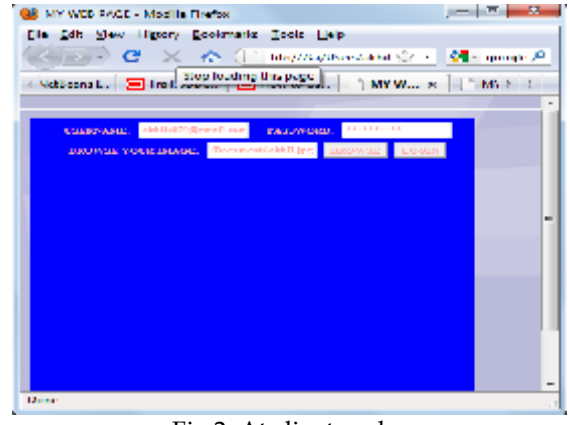

Fig 2: At client-end

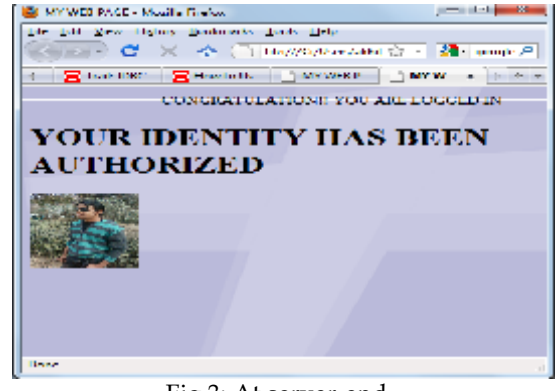

Fig 3: At server-end

Algorithm Create_Transformation_Table

1: Load Image
2: Input key
3: Get ImageWidth and ImageHeight
4:
4.1: LowerHorizontalNoBlocks
=Int(ImageWidth /10)
4.2: LowerVerticalNoBlocks
= Int(ImageHeight /10)
5: Randomize ()
6:

6.1: HorizontalNoBlocks
=RandomNumbertween (LowerHorizontal-NoBlocks and ImageWidth)
6.2: VerticalNoBlocks
= RandomNumberbetween (LowerVertical-NoBlocks and ImageHeight)
7: NoBlocks = (HorizontalNoBlocks * Verti-calNoBlocks) + large prime number
8: Seed = | Hash value (Key) |
9: HashValue1
= |Hash value (first half of the Key)|
HashValue2
= |Hash value (second half of the Key)|
10: Randomize using seed
11: If HashValue1 > HashValue2 Then
SEEDALTERNATE = 1 Else
SEEDALTERNATE = 2 End If
12: I = 0 Number-of-seed-changes (N) = 1
13: While I < NoBlocks
R = RandomNum between (zero and NoBlocks -1)
If R is not selected Then
Assign location R to the block I
I +=1
Else If SEEDALTERNATE = 1 Then
seed = seed + (HashValue1 Mod I) +1
SEEDALTERNATE = 2 Else
seed = seed + (HashValue2 Mod I) + 1
SEEDALTERNATE = 1
Randomize (seed)
End If Else
Number-of-seed-changes += 1
If Number-of-seed-changes > 1000,000 then
For K = 0 to NoBlocks -1
If K not selected then
Assign location K to Block I
I=I+1
End if
Next K
End if
End if
End While
END Create_Transformation_Table

Input: BMP image file, a string Key
Output: Transformation table

Algorithm Perform_Transformation
1: For I = 0 to NoBlocks -1
1.1: Get the new location of block I from the transformation table
1.2: Set block I in its new location
END Perform_Transformation

Input: Original Image (BMP image file) and Transformation table
Output: Transformed Image.

Correlation and entropy are computed for each case according to "(1)" and "(2)".

$$r=\frac{n\sum(xy)-\sum x\sum y}{\sqrt{\left[n\sum(x^2)-(\sum x)^2\right]}} \quad (1)$$

Where
r: correlation value
n: the number of pairs of data
∑(xy): sum of the products of paired data
∑*x*: sum of *x* data
∑*y*: sum of *y* data
∑*x*: sum of squared *x* data

Entropy defined as follows M. Sonka, V. Hlavac., R. Boyle , and D. Feldman [17],[18].

$$H_e=-\sum_{k=0}^{G-1}p(k)\log_2 p(k) \quad (2)$$

Where:
H: entropy.
G: gray value of input image (0... 255).
P(k): is the probability of the occurrence of symbol *k*.

3.2 Face Recognition using PCA

A 2-D image can be represented as 1-D vector by concatenating each column or each row into a long thin vector. Now let's suppose that we have V vectors of size N(= (RowsofI-mage*ColumnofImage) + large Prime Number) representing a set of sampled images. P_j's represents the pixel values.

$$x_i=[p_1p_2\ldots..p_N]^T,\quad i=1,2,3\ldots\ldots..,V \quad (3)$$

The mean centered images can be obtained by subtracting the mean image from each image vector.Let's suppose that m represents the mean image.

$$m=\frac{1}{V}\left(\sum_{i=1}^{V}x_i\right) \quad (4)$$

Let m_c represents the mean centered image, then mc can be defined as-

$$m_c=(x_i-m) \quad (5)$$

We set our goal as we need to find a set of e_i's which has the largest possible projection onto each of the m_c's value. We need to find a set of V orthogonal vectors e_i for which the quantity

$$\lambda_i = \frac{1}{V}\sum_{n=1}^{V}\left(e_i^T w_n\right)^2 \quad (6)$$

is maximized with the orthonormality constraints-

$$e_l^T e_k = \lambda_{lk} \quad (7)$$

e_i's and λ_i's can be obtained from eigenvectors and eigenvalues of the covariance matrix

$$C = WW^T \quad (8)$$

Where W is a matrix composed of the column vectors w_i placed side by side. The size of C is $N \times N$. In linear algebra vectors ei and scalar λi can be obtained by solving the eigenvectors and eigenvalues of VxV matrix W^TW.Let d_i and μ_i be eigenvector and eigenvalue of W^TW respectively,

$$W^T W d_i = \mu_i d_i \quad (9)$$

By multiplying W to both sides

$$WW^T(Wd_i) = \mu_i(Wd_i) \quad (10)$$

Which means that the first V_i-1 eigenvectors ei and eigenvalues λ_i of WW^T are given by Wd_i and μ_i respectively. Wd_i needs to be normalized in order to be equal to e_i. Since we can only sum up a finite number of image vectors,V, the rank of covariance matrix can't exceed V-1.

A facial image can be projected on V' dimension by computing

$$\Omega=[v_1\ v_2 \ldots . v_{M'}]^T \quad (11)$$

Where $v_i=e_i^Tw_i$. v_i is the i^{th} coordinate of the facial image in the new space, which came to be the principal component. e_i is also known as eigenimages or eigenfaces. The simplest method to determine which face class provide the best description of input image, is to calculate the euclidean distance as-

$$\epsilon_k = \| \Omega - \Omega_k \| \quad (12)$$

Where Ω_k is the vector describing the k^{th} face class. Minimum value of Euclidean distance shows that Ω belongs Ω_k.

4 Experiments and Results

In this paper we maintain our database as training database and test database.

Training Database

Fig 4: Training database

Test database

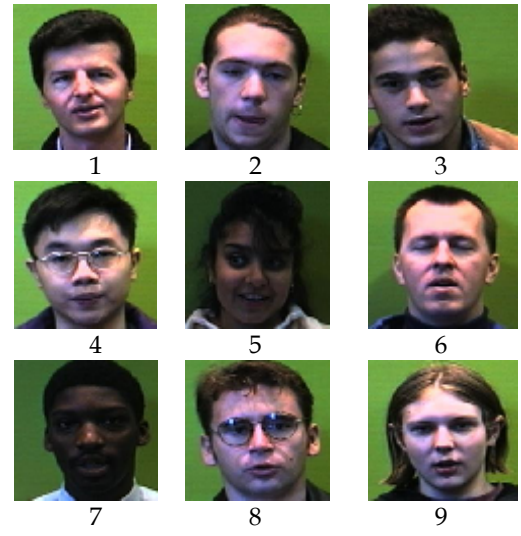

Fig 5: Test Database

When we check our result for test data 1 it gives an output as shown below:

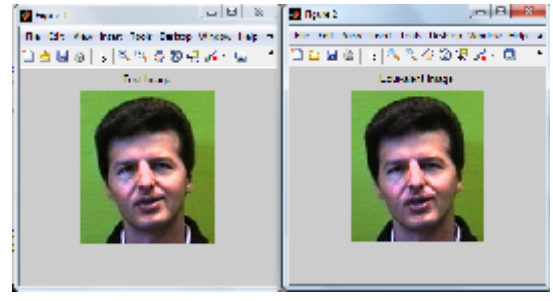

Fig 6: result output

But when we check our result for test data 9 it

gives an output as shown below:

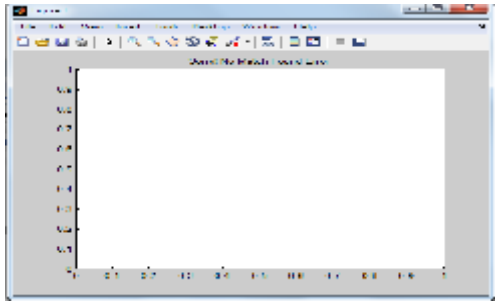

Fig 7: Result output

In this way we can say that there is a secure face-recognition between client and server.

5 Conclusion and Future Work

In this work Blowfish and PCA algorithms have been improved by adding block based transformation capability. The abovealgoritms and results showed that the correlation was decreased when the proposed algorithm was applied to them before the Blowfish algorithm. When compared to many commonly used algorithms, the proposed algorithm resulted in the best performance; the lowest correlation and the highest entropy. The PCA algorithm compares the closest faces and gives the best result on the basis of eigenfaces.

Overall we can conclude that the above work will be beneficial in todays era for information security(text as well as multimedia data) over a huge and complex network.

In future we can apply special shuffling rule over block of images so that an intruder can't understand the correlation between neighbor's pixels. This enhancement may provide an extra security features in future.

.

6 Acknowledgment

The present work would not have been possible without the co-ordination and help of Dr, Harsh K Verma. I unreservedly acknowledge the deep gratitude to my project guide for his persistent intellectual guidance. I also thanks to Mr. Vaibhaw Dixit for his ideas and interesting discussions regarding this work.Finally I would like to thanks our college management which support us financially.

7 References

[1] S. P. Nana'vati., P. K. panigrahi. "Wavelets:applications to image compression- I,". *joined of the scientific and engineering computing*, vol. 9, no. 3, 2004, pp. 4- 10.

[2] c. Ratael, gonzales, e. Richard, and woods, "Digital image processing," 2nd ed, Prentice hall, 2002.)

[3] AL. Vitali, A. Borneo, M. Fumagalli and R. Rinaldo, "Video over IP using standard-compatible multiple description coding," *Journal of Zhejiang University-Science A*, vol. 7, no. 5 ,2006, pp. 668- 676.

[4] H. El-din. H. Ahmed, H. M. Kalash, and O. S. Farag Allah, "Encryption quality analysis of the RC5 block cipher algorithm for digital images," Menoufia *University, Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menouf-32952, Egypt*, 2006.

[5] Li. Shujun, X. Zheng "Cryptanalysis of a chaotic image encryption method," Inst. of Image Process. Xi'an Jiaotong Univ., Shaanxi, This paper appears in: Circuits and Systems, ISCAS 2002. IEEE International Symposium on Publication Date: 2002, Vol. 2, 2002, page(s):708,711.

[6] S.S. Maniccam, N.G. Bourbakis, "Image and video encryption using SCAN patterns," *Journal of Pattern Recognition Society*, vol. 37, no. 4, pp.725– 737, 2004.

[7] A. Mitra, , Y V. Subba Rao, and S. R. M. Prasnna, "A new image encryption approach using combinational permutation techniques," *Journal of computer Science*, vol. 1, no. 1, p.127, 2006, Available: http://www.enformatika.org

[8] G. Zhi-Hong, H. Fangjun, and G.Wenjie, "Chaos-based image encryption algorithm," *Department of Electrical and computer Engineering*, University of Waterloo, ON N2L 3G1, Canada. Published by: *Elsevier*, 2005, pp. 153-157.

[9] A. Sinha, K. Singh, "Image encryption by using fractional Fourier transform and Jigsaw transform in image bit planes," Source: *optical engineering, spie-int society optical engineering*, vol. 44, no. 5 , 2005, pp.15-18.

[10] Li. Shujun, Li. Chengqing, C. Guanrong, *Fellow., IEEE.*, Dan Zhang., and Nikolaos,G., Bourbakis *Fellow., IEEE*. "A general cryptanalysis of permutation-only multimedia encryption algorithms," 2004, http://eprint.iacr. Org/2004/374.pdf

[11] A. Sinha, K. Singh, "A technique for image encryption using digital signature," Source: *Optics Communications*, vol.218, no. 4, 2003, pp.229-234.http://www.elsevier.com/

[12] Jui-Cheng Yen, Jiun-In Guo, "A new chaotic image encryption algorithm",Department of Electronics Engineering National Lien-Ho College of Technology and Commerce, Miaoli, Taiwan, Republic of China, *E-mail:* jcyen@mail.lctc.edu.tw

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

[14] K. I. Diamantaras and S. Y. Kung, "Principal Component Neural Networks: Theory and Applications", John Wiley & Sons,Inc., 1996.

[15] S.C. Chen, Y.L. Zhu, D.Q. Zhang, J.Y. Yang, Feature extraction approaches based on matrix pattern: MatPCA and MatFLDA, Pattern Recognition Letters 26(8) (2005) 1157-1167.

[16] D. Q. Zhang, S.C. Chen, J. Liu, Representing image matrices: Eigenimages vs. Eigenvectors, In: Proceedings of the 2nd International Symposium on Neural Networks (ISNN'05), Chongqing, China, LNCS 3497 (2005) 659-664.

[17] M. Sonka, V. Hlavac. and R. Boyle, "Digital image processing," in: image Processing, Analysis, and Machine Vision, 1998, 2nd ed. *http://www.pws.com*

[18] D. Feldman, "A brief introduction to: information theory, excess entropy and computational mechanics," college of the atlantic 105 eden street, bar harbor, me 04609, 2002, http://hornacek.coa.edu/

Akhil Kumar Singh received B.Tech Degree from Institute of Technology and Management,Gida Gorakhpur,pursuing M.tech from National Institute of technology jalandhar in 2009 and 2011 respectively, current research interests are biometric security area and Databases .

Dr.Harsh K Verma has completed his Ph.D(Numerical Computing) from Punjab Technical University Jalandhar Punjab (INDIA). Head of Dept,Computer Science and Engineering, NIT Jalandhar, Area of interest are Numerical Computing, Information Security and Computer Networks.
He has published various research papers in international/national journals and conferences. Presentely he is also the head examination controller of NIT jalandhar.He has attended various international and national workshops, training schools and other technical activitivies during his academic career.

Vaibhaw Dixit received B.Tech degree from Maharana Pratap Engineering College Kanpur,Uttar Pradesh, pursuing Mtech from National Institute of Technology Jalandhar, Punjab in 2008 and 2011 respectively.Current research interests are information security,wireless security and data mining.