# Statistical Analysis towards Image Recognition

Samir Kumar Bandyopadhyay
*Department of Computer Science and Engineering,*
*University of Calcutta, Kolkata, India*
*skb1@vsnl.com*

Poulami Das
*Computer Science and Engineering Department,*
*Heritage Institute of Technology, Kolkata, India*
*dippoulami@yahoo.com*

Debnath Bhattacharyya
*Computer Science and Engineering Department,*
*Heritage Institute of Technology, Kolkata, India*
*debnathb@gmail.com*

### *Abstract*

*In this paper we propose a new Handwritten Signature Authentication Scheme. The scheme consists of two main Rule Set Algorithms and one Authentication Algorithm. The Algorithms are based on extensive statistical analysis, Mean Variance and Theory of Estimation. This is an extension work of Handwritten Signature Identification. This scheme supports the application environment and we strongly believe that "User Authentication" could be a solid platform for future research and study.*

## 1. Introduction

Various good techniques of secure transmission of data are proposed and already taken into practice. Data Hiding is the process of secretly embedding information inside a data source without changing its perceptual quality. Digital watermarking is the process of conveying information by imperceptibly embedding it into the digital media. Steganography (covered writing) the process of secretly embedding information into a data source in such a way its very existence is concealed. Extraction and Authentication of Data also equally important for security purpose. The researchers have proposed numerous authentication schemes, out of these Biometric authentications are used widely. Biologically inspired approaches have got better popularity in research.

## 2. Earlier works

Numerous approaches have been proposed for Handwritten Signature Identification, Recognition and Authentication systems. Besides all, one approach that has shown great promise is the use of Artificial Neural Network in the Handwritten Signature Identification. An Artificial Neural Network is trained to identify patterns among different supplied handwriting samples. Handwritten signature samples are considered input for the artificial neural network model and typically weights also supplied for recognition [3].

According to Berend-Jan van der Zwaag, the used method in Neural Network is, various characters are taught to the network in a supervised manner. A character is presented to the system and is assigned a particular label. Several variant patterns of the same character are taught to the network under the same label. Hence the network learns various possible variations of a single pattern and becomes adaptive in nature [5].

Debnath Bhattacharyya, Samir Kumar Bandyopadhyay and Deepsikha Chaudhury, 2007, proposed a scheme where the Standard Deviation for each byte of the Training Image Files (sample signatures) is computed and then each corresponding byte of Test Signature is compared to check whether it falls within the range of (Mean ± Standard Deviation ). If 70% cases match, then the Test Signature is accepted [4].

F. Bartolini, A. Tefas, M. Barni and I. Pitas discussed the problem of authenticating video surveillance image. After an introduction motivating the need for a watermarking-based authentication of VS (video surveillance) sequences, a brief survey of the main watermarking-based authentication techniques is presented and the requirements that an authentication algorithm should satisfy for VS applications are discussed. A novel algorithm which is suitable for VS visual data authentication have proposed [6].

Rehab H. Alwan, Fadhil J. Kadhim, and Ahmad T. Al-Taani, 2005, have explained a method with three main steps. First, the edge of the image is detected using Sobel mask filters. Second, the least significant bit LSB of each pixel is used. Finally, a gray level connectivity is applied using a fuzzy approach and the ASCII code is used for information hiding. The prior bit of the LSB represents the edged image after gray level connectivity, and the remaining six bits represent the original image with very little difference in contrast. The given method embeds three images in one image and includes, as a special case of data embedding, information hiding, identifying and authenticating text embedded within digital images [7].

Yusuk Lim, Changsheng Xu and David Dagan Feng, 2001, described the web-based authentication system consists of two parts: one is a watermark embedding system and the other is authentication system. In case of watermark embedding system, it is installed in the server as application software that any authorized user, who has access to server, can generate watermarked image. The distribution can use any kind of network transmission such as FTP, e-mail etc. Once image is distributed to externally, client can access to authentication web page to get verification of image [8].

Min Wu and Bede Liu, June, 2003, proposed a new method to embed data in binary images, including scanned text, figures, and signatures. The method manipulates “flippable” pixels to enforce specific blockbased relationship in order to embed a significant amount of data without causing noticeable artifacts. Shuffling is applied before embedding to equalize the uneven embedding capacity from region to region. The hidden data can be extracted without using the original image, and can also be accurately extracted after high quality printing and scanning with the help of a few registration marks [9].

Debnath Bhattacharyya, Samir Kumar Bandyopadhyay and Poulami Das, 2007, have conducted [10] an extensive survey of the existing graphical password schemes and proposed an alternate scheme. Entire work have divided into three phases- a. sampling of users passwords, processing and storage; b. security on transmission; and c. Recognition and authentication.

## 3. Our work

Mainly, in this paper, we have focused on Authentication of Handwritten Signature.

Prior to discuss ‘Authentication of Handwritten Signature’, it is important to get some idea of ‘Data Hiding and Extraction of Handwritten Signature’; our earlier work.

Before Embedding process, in Figure-1, processing of the image is must. Firstly, Draw the Signature on a device by pen or by mouse on the screen panel. This drawn image is captured and put into the processes of extracting Region Of Interest (ROI), scaled (the ROI) into a specific size and thinned into single pixel format [1].

Law of Independent Assortment is used to watermarking the processed Handwritten Signature; double lined protection is provided during transmission of Handwritten Signature over network [2].

For Handwritten Signature Identification and Authentication - a forward propagation technique is used to authenticate of input image out of the available training images [3].

Here we are providing another alternative of Authentication Technique as follow:

Variance is the average of the squared differences from the Mean. Work out the Mean. Now, for each number subtract the Mean and then square the result (the squared difference). Then work out the average of those squared differences.

$$\text{Variation: } V = (1/N) \sum_{i=1}^{N} (P\text{-mean})^2 \quad \text{-------------(i),}$$

in equation (i), P is the pixel value, N is number of images and Count is the number of elements.

$$\text{Mean Variance: } M = (1/S) \sum_{i=1}^{S} V^2 \quad \text{-----------------(ii),}$$

where V is the locational value of ‘2D Variance Array’. Count is number of array elements.

To calculate the Threshold, take each difference, square it, and then average the result. Prior to start, we have converted the Bi-Color images into 2D corresponding arrays, where elements of the array are the pixel values of Bi-Color images, taken as ‘0’ for white and ‘1’ for black..

### 3.1. Authentication Rule Set Algorithm1 (ARSA1)

```
Input : N-Training Image(s)
Output : Mean Variance
Function ARSA1 ( N-Training Images )
{
    Declare an Array with N number of elements, B[N].
    Declare an Array with N number of elements, M.
    Declare ‘2D Variance Array’ of size Training Image(s).
    Read values pixel by pixel from same location of Images and store to the elements of
    B Array.
    Compute Variance of the elements of B Array.

    Store the Variance in the Corresponding location of ‘2D Variance Array’
    (2DVA).
    Continue Steps-2 to Step-4 until end of Training Image(s).
    Compute, Mean Variances of 2DVA, i.e., M.
```

```
        Return M
    }
```

Analysis of ARSA1 Algorithm:

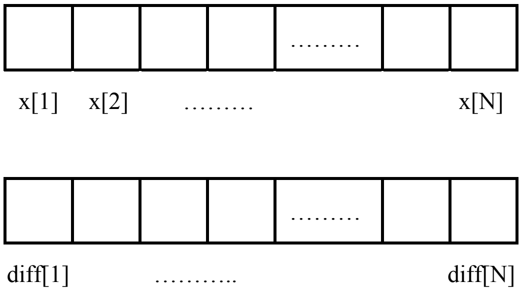
Training Images are equal in size and monochrome. Read the first pixel value from the N number of Training images and each time store into the corresponding array location, here it is taken as B[N] array in Figure-2. Compute the variance of B array and store the computed value into the first location of 2-Dimensional Variance Array, 2DVA. The size of this 2-Dimensional Variance Array is equivalent to the size of any one Training image. In this way the 2-Dimensional Variance Array will be enriched with the computed variance value from the next corresponding pixel values of the corresponding Training images. At end, when all the cells of 2-Dimensional Variance Array will be filled, then the Mean Variance, M, is computed from the 2-Dimensional Variance Array.

### 3.2. Authentication Rule Set Algorithm2 (ARSA2)

```
    Input : N-Training Image(s)
    Output : Estimated Range
    Function ARSA2 ( N-Training Images )
    {
        Declare Arrays each with N number of elements,
        ‘x[N]’ and ‘diff[N]’
        Declare variables G, G1, G2, D, Threshold
        G1 = ARSA1 ( N Training Images )
        for(i = 1; i <= N; i++)
        do
            x[i] = ARSA1 ( N Training Images + Training Image1 )
            diff[i] = x[i] – G1
        end for
        Calculate Mean of  the elements of ‘x’ array and store to G2
        G = G2 – G1
        D = [ Maximum Value of ‘diff’ array ] – G
        Set ER (Estimated Range),  G2 ± (Maximum(G, D)).
    }
```

Analysis of ARSA2 Algorithm:

Consider the following two arrays (‘x’ and ‘diff’) used in our ARSA2 algorithm-



G1 = mean variance of N Training Images, i.e., the output returned by ARSA1 Algorithm. x[i] = mean variance of "N Training Images + **i**th. Training Image (from the N number of training Images)", i.e., mean variance of N+1 Training Images. All images from same problem domain.

Every time, store the difference of "mean variance of N+1 Training Images, x[i]" and "mean variance of N Training Images, $G_1$". That is, $G_1 – x[i]$ to diff[i].

Calculate Mean of N number of elements of 'x' array, that is, $G_2$.

Now compute, $G = G_1 – G_2$.

Now, find max. value from 'diff' array, and that is taken as, D.

Again find the Maximum of G and D, and that is taken as Estimated Range (ER), which is ±(G or D) with $G_2$, keeping in the middle of the range.

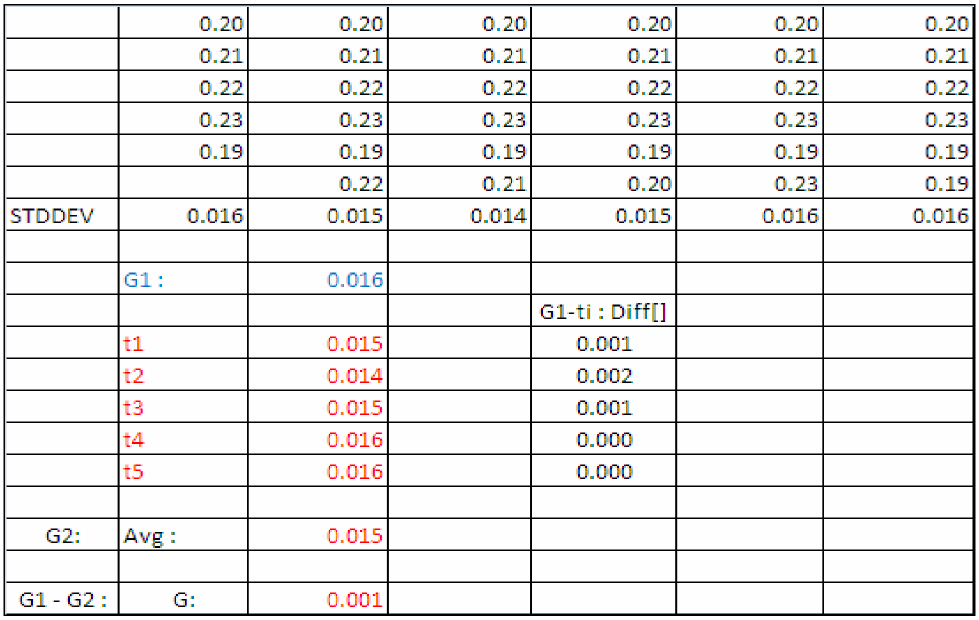
### 3.3. Handwritten Signature Authentication Algorithm (HSAA)

```
Input : N-Training Images, Test Image
Output : Estimated Range
Function HSAA ( N-Training Images, Test Image )
{
    Declare y
    y = ARSA1 ( N Training Images + Test Image )
    Call ARSA2 (N-Training Images) and set Estimated Range,
        ER, [$G_2 \pm$ (G or D)]
    If y falls within the Range ER
    Then
        Test Image Authentic
    Else
        Test Image Not Authentic
    End If
}
```

Analysis of HSAA Algorithm:

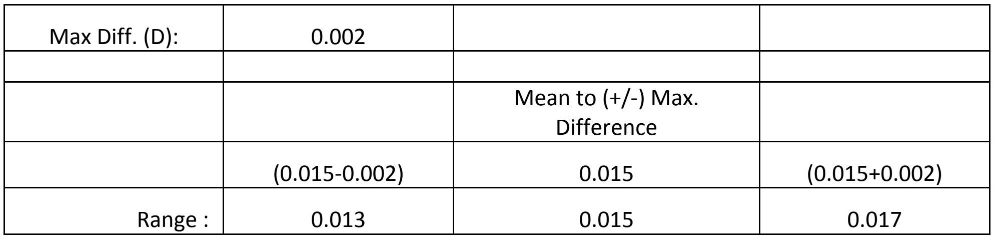
Consider Table 1, here in our example, we have taken five numbers of training images from same domain, standard deviation is calculated accordingly for those five images, that is $G_1$, 0.016. Then after, keeping these five images we have taken one extra image from those five, so, six images are considered and standard deviations are calculated five times each with the six images, those values are 0.015, 0.014, 0.015, 0.016, 0.016. Average is $G_2$, 0.015. Thus, G is, 0.001. Then the calculation of G1-diff[i], stated in our algorithm, values are 0.001, 0.002, 0.001, 0.000, 0.000. Here maximum is D, 0.002. Thus this D, 0.002 is taken for range, consider Table 2.

Table 1



| | | | | | | |
|---|---|---|---|---|---|---|
| | 0.20 | 0.20 | 0.20 | 0.20 | 0.20 | 0.20 |
| | 0.21 | 0.21 | 0.21 | 0.21 | 0.21 | 0.21 |
| | 0.22 | 0.22 | 0.22 | 0.22 | 0.22 | 0.22 |
| | 0.23 | 0.23 | 0.23 | 0.23 | 0.23 | 0.23 |
| | 0.19 | 0.19 | 0.19 | 0.19 | 0.19 | 0.19 |
| | | 0.22 | 0.21 | 0.20 | 0.23 | 0.19 |
| STDDEV | 0.016 | 0.015 | 0.014 | 0.015 | 0.016 | 0.016 |
| | | | | | | |
| | G1 : | 0.016 | | | | |
| | | | | G1-ti : Diff[] | | |
| | t1 | 0.015 | | 0.001 | | |
| | t2 | 0.014 | | 0.002 | | |
| | t3 | 0.015 | | 0.001 | | |
| | t4 | 0.016 | | 0.000 | | |
| | t5 | 0.016 | | 0.000 | | |
| | | | | | | |
| G2: | Avg : | 0.015 | | | | |
| | | | | | | |
| G1 - G2 : | G: | 0.001 | | | | |

Table 2



| | | | |
|---|---|---|---|
| Max Diff. (D): | 0.002 | | |
| | | | |
| | | Mean to (+/-) Max. Difference | |
| | (0.015-0.002) | 0.015 | (0.015+0.002) |
| Range : | 0.013 | 0.015 | 0.017 |

For the setting of rules in a specific problem space, the execution of the algorithms may be single time, the complexity can be calculated as for example, ‘N’ training images are stored with size ‘S’. Here, in this problem space number of images and sizes of all the images are identical and fixed.

Store pixel values of each of training images to corresponding 2D Array, for which time complexity is, S x N, near about, $N^2$. For each round of Authentication, the Authentication Rule Set Algorithm1 (ARSA1) will be reading the identical locational pixel values from N images, the time complexity for reading the identical locational value from N images with size S, is again S x N = $N^2$, so, $N^2 + N^2 = 2N^2$, then calculate and stores into another 2D Array. Time complexity to store the calculated values in another 2D array is N. So, another N time is necessary to calculate the mean variance, i.e., N+N=2N. Thus, the time complexity is 2N(N+1).

For Authentication Rule Set Algorithm2 (ARSA2), the same time complexity can be calculated, because, every Test Image, (N+1) times it calls the Authentication Rule Set Algorithm1 (ARSA1). So,

$$
\begin{aligned}
&2(2N(N+1)) \text{ x } (N+1) \\
&= 4N(N+1) \text{ x } (N+1) \\
&= 4N \text{ x } (N+1)^2 \\
&= 4N + 8N^2 + 4N^3 \\
&= N^3 \text{ (around),}
\end{aligned}
$$

in large problem space. Bit slowly, but the algorithms give output in polynomial time. This is very common, because, algorithms have to handle large sets of image data.

## 4. Result

Estimation is done depending on 100 various training signatures, which are already captured, processed [1] and stored in the storage area at the target where extraction and authentication of the test image has to be done. This work is our extension work [4], and here we are especially worked on authentication. Various test results with discussions are stated in the Figure-3 and Figure-4.

In case of Test Image authentication, 2D Variance Array (2DVA) is generated by replacing the (N+1)th. Image as an incoming Test Image, stated in Figure-4. From the 2D Variance Array mean is calculated and then checked with already generated Estimated range, if satisfied then incoming Test Image is recognized and authenticated.

## 5. Conclusion

This is an extension work of Handwritten Signature Recognition that we have started a year back. Various Watermarking and Data Hiding techniques we have already proposed and published in different International Journals and Conference Proceedings.

Prior to these we have worked on Morphological Image Processing focused on Handwritten Signature Scaling, Thinning and extraction of area of interest (Handwritten Signature Area within an Image). Thus a series of work just going to be completed with this proposed new and novel Authentication Scheme.

This authentication scheme is based on extensive Statistical Analysis, Theory of Estimation and Mean Variance. Various test results are positively backing this scheme. One such instance we have shown in the Figure-3 and Figure-4.

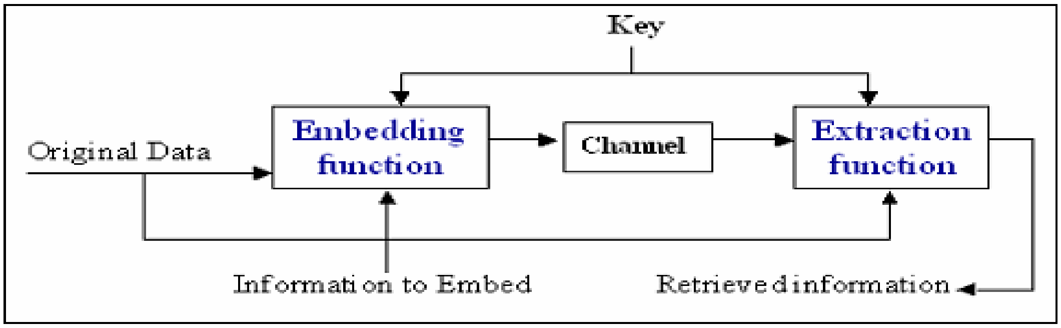
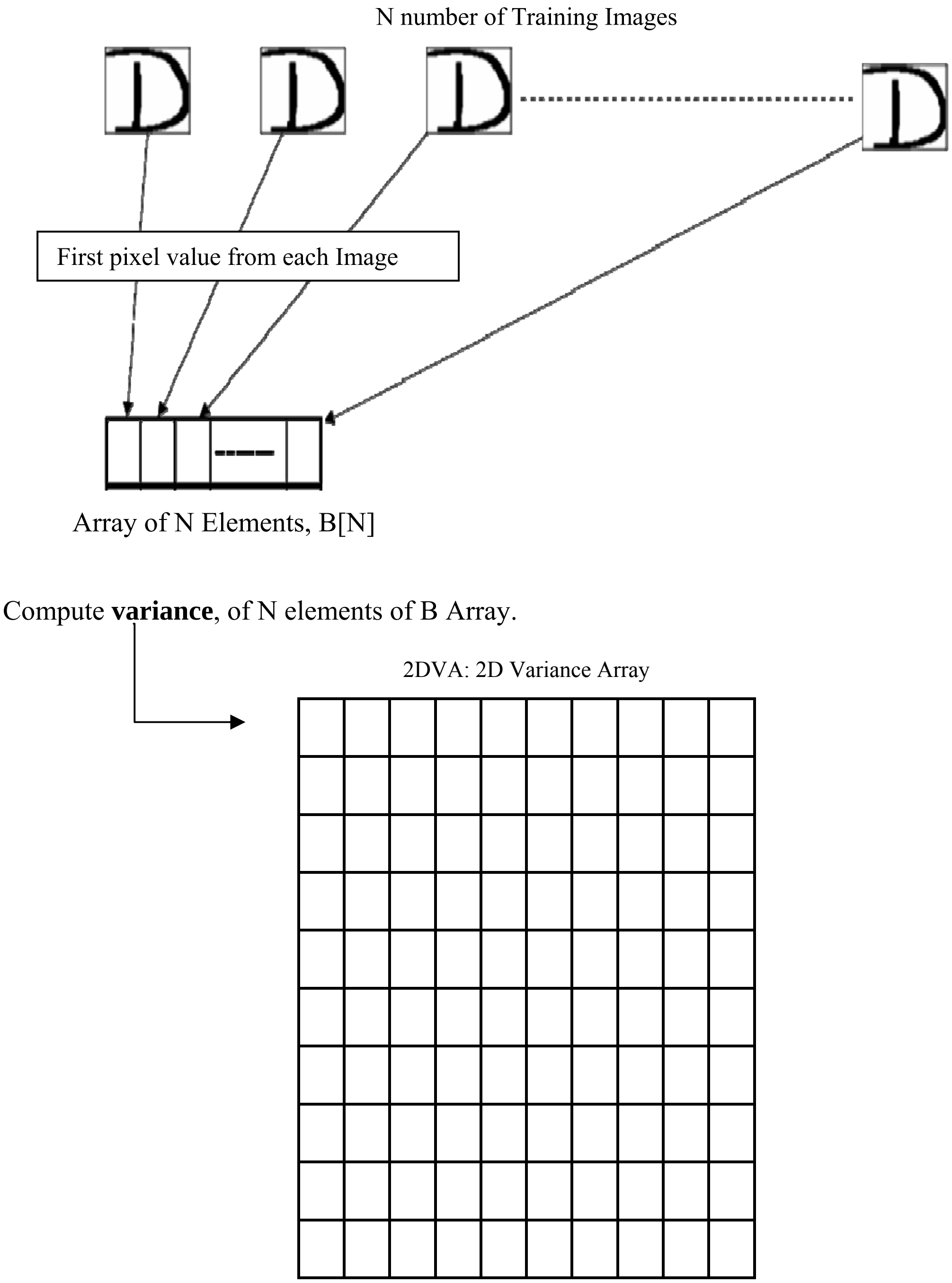


Figure 1


N number of Training Images
First pixel value from each Image
Array of N Elements, B[N]
Compute **variance**, of N elements of B Array.
2DVA: 2D Variance Array

Array, 2DVA[n, m], where, n = width of any training image
and m = height of that training image.

Compute, Mean Variances of 2DVA, i.e., **M**.

Figure 2

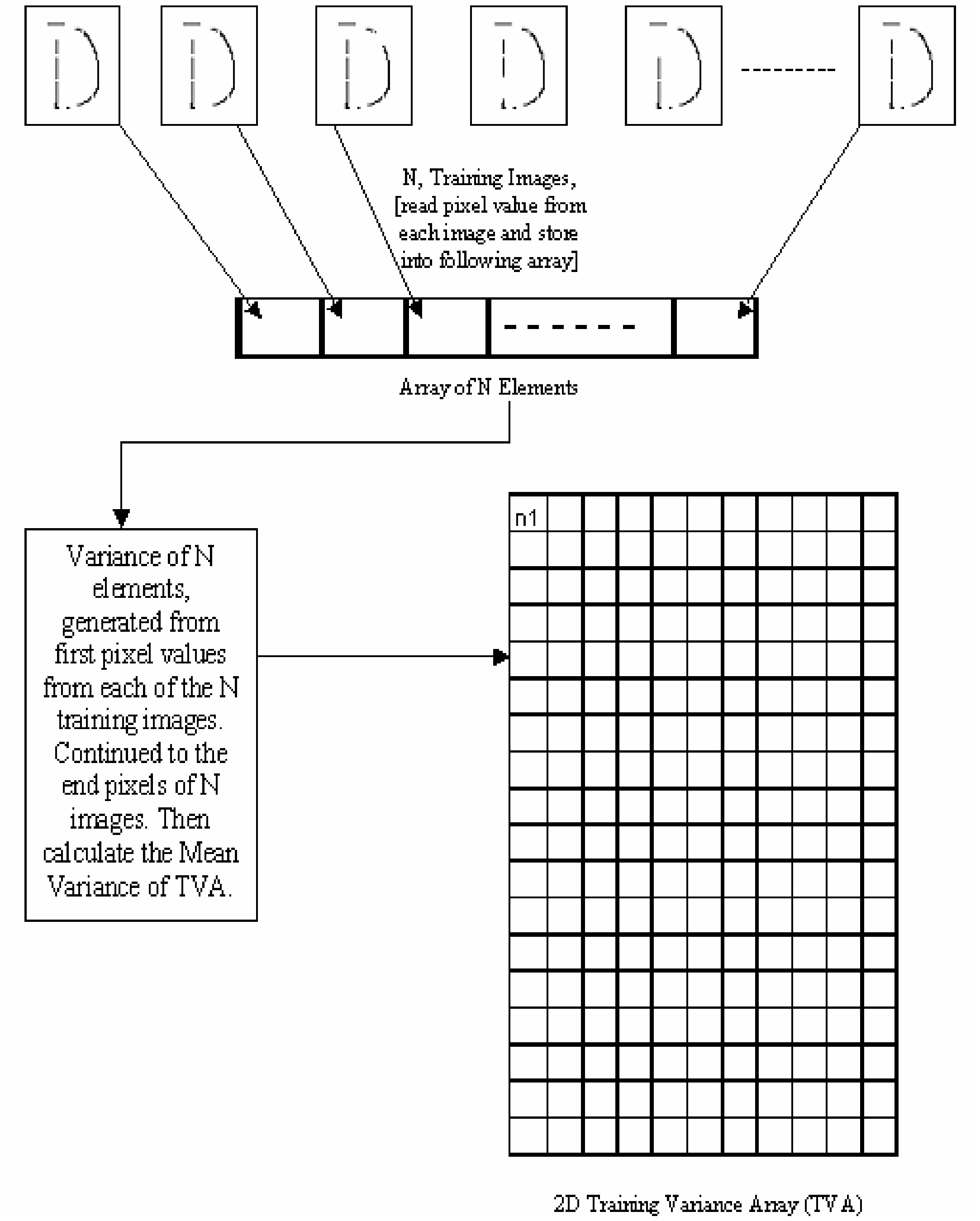
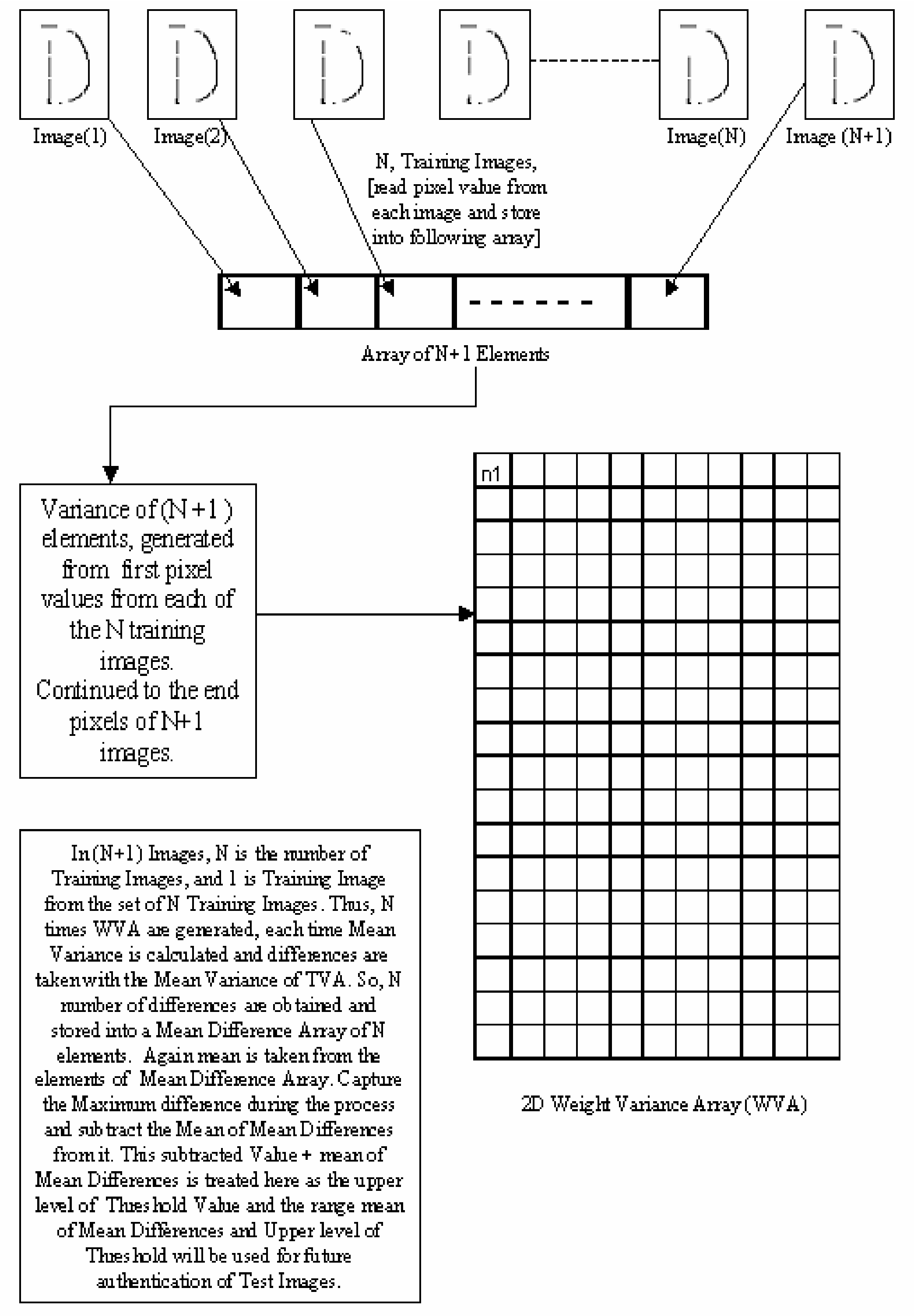

N, Training Images,
[read pixel value from
each image and store
into following array]
Array of N Elements
Variance of N elements, generated from first pixel values from each of the N training images. Continued to the end pixels of N images. Then calculate the Mean Variance of TVA.
n1
2D Training Variance Array (TVA)

Figure 3

We have started our work a year back with the images displayed in Figure-3 and Figure-4. This new scheme also strongly applicable to authenticate a whole Handwritten word as well as a full Handwritten Signature.


Image(1)
Image(2)
Image(N)
Image (N+1)
N, Training Images,
[read pixel value from each image and store into following array]
------
Array of N+1 Elements
n1
2D Weight Variance Array (WVA)

Variance of (N+1) elements, generated from first pixel values from each of the N training images. Continued to the end pixels of N+1 images.

In (N+1) Images, N is the number of Training Images, and 1 is Training Image from the set of N Training Images. Thus, N times WVA are generated, each time Mean Variance is calculated and differences are taken with the Mean Variance of TVA. So, N number of differences are obtained and stored into a Mean Difference Array of N elements. Again mean is taken from the elements of Mean Difference Array. Capture the Maximum difference during the process and subtract the Mean of Mean Differences from it. This subtracted Value + mean of Mean Differences is treated here as the upper level of Threshold Value and the range mean of Mean Differences and Upper level of Threshold will be used for future authentication of Test Images.

Figure 4

Table 3

| **Mean Variance of N Training Images** | **Mean Variance of N Training Images + Single Test Image** | **Mean Variance Difference** |
|---|---|---|
| 3.7489177489177448 | 3.806057224025974 | 0.05713947510822964 |
| 3.7489177489177448 | 3.798447646103896 | 0.04952989718615131 |
| 3.7489177489177448 | 3.777873602092352 | 0.02895585317460731 |
| 3.7489177489177448 | 3.764909136002887 | 0.01599138708514164 |
| 3.7489177489177448 | 3.757440476190476 | 0.00852272727273132 |
| 3.7489177489177448 | 3.770123106060606 | 0.02120535714286165 |
| 3.7489177489177448 | 3.738416531385282 | 0.01050121753246314 |
| 3.7489177489177448 | 3.735316332972583 | 0.01360141594516154 |
| 3.7489177489177448 | 3.591016188672438 | 0.15790156024530627 |
| 3.7489177489177448 | 3.704596185064935 | 0.04432156385280953 |
| 3.7489177489177448 | 3.691208964646465 | 0.05770878427127993 |
| 3.7489177489177448 | 3.806057224025974 | 0.05713947510822964 |
| 3.7489177489177448 | 3.777873602092352 | 0.02895585317460731 |
| 3.7489177489177448 | 3.750112734487734 | 0.00119498556998971 |
| 3.7489177489177448 | 3.806057224025974 | 0.05713947510822964 |
| 3.7489177489177448 | 3.591016188672438 | 0.15670154985569983 |
|  | Mean of Mean Variances of N Training Images + Single Test Image | Maximum Mean Variance Difference |
|  | 0.040653935185187 | 0.15790156024530627 |

According to the Table 3, in another test (with little change in the approach), following estimated range has been calculated.

(0.15790156024530627-0.040653935185187) + 0.040653935185187
= 0.12 + 0.040653935185187.

Estimated Range, ER: 0.040653935185187 to [0.040653935185187+0.12].

## 6. References

[1] Samir Kumar Bandyopadhyay, Debnath Bhattacharyya and Poulami Das, Handwritten Signature Verification System using Morphological Image Analysis", *CATA-2007* International Conference, Honolulu, Hawaii, USA, March 28-30, 2007, pp. 112-117.

[2] Samir Kumar Bandyopadhyay, Debnath Bhattacharyya and Poulami Das, "Handwritten Signature Extraction from Watermarked Images using Genetic Crossover", *MUE'07 IEEE CS Conference*, Seoul, Korea, April 27-30, 2007, pp. 987-991.

[3] Samir Kumar Bandyopadhyay, Debnath Bhattacharyya and Poulami Das, "A Flexible ANN System for Handwritten Signature Identification", IMECS '07, Volume II, March 21 - 23, 2007, Hong Kong, pp. 1883-1887.

[4] Debnath Bhattacharyya, Samir Kumar Bandyopadhyay and Deepsikha Chaudhury, "Handwritten Signature Authentication Scheme using Integrated Statistical Analysis of Bi-Color Images", *IEEE ICCSA 2007 Conference*, Kuala Lumpur, Malaysia, August 26-29, 2007, pp. 72-77.

[5] Berend-Jan van der Zwaag, Handwritten Digit Recognition : A Neural Network Demo, Euregio Computational Intelligence Center , Dept. of Electrical Engineering, University of Twente, Enschede, the Netherlands.

[6] F. Bartolini, A. Tefas, M. Barni and I. Pitas, "Image Authentication Techniques for Surveillance Applications", IEEE Proceedings, Vol. 89, No. 10, October 2001.

[7] Rehab H. Alwan, Fadhil J. Kadhim, and Ahmad T. Al-Taani, "Data Embedding Based on Better Use of Bits in Image Pixels", International Journal of Signal Processing Vol 2, No. 2, 2005.

[8] Yusuk Lim, Changsheng Xu and David Dagan Feng, "Web based Image Authentication Using Invisible Fragile Watermark", 2001, Pan-Sydney Area Workshop on Visual Information Processing (VIP2001), Sydney, Australia.
[9] Min Wu, Member, IEEE, and Bede Liu, Fellow, IEEE, "Data Hiding in Binary Image for Authentication and Annotation", IEEE Trans. Image Processing, vol. 12, pp. 696–705, June 2003.
[10] Samir Kumar Bandyopadhyay, Debnath Bhattacharyya and Poulami Das, "User Authentication by Secured Graphical Password Implementation", APSITT-2008, April 22-24, 2008, Bandos Island, Maldives.

## Authors

**Prof. Samir Kumar Bandyopadhyay**, B.E., M.Tech., Ph. D (Computer Science & Engineering), C.Engg., D.Engg., FIE, FIETE, currently, Professor of Computer Science & Engineering and visiting Faculty Dept. of Comp. Sc., Southern Illinois University, USA, MIT, California Institute of Technology, etc. His research interests include Bio-medical Engg, Mobile Computing, Pattern Recognition, Graph Theory, Software Engg.,etc. He has 25 Years of experience at the Post graduate and under-graduate Teaching & Research experience in the University of Calcutta. He has already got several Academic Distinctions in Degree level/Recognition/Awards from various prestigious Institutes and Organizations. He has published 300 Research papers in International & Indian Journals and 5 leading text books for Computer Science and Engineering. He has visited USA, Finland, Sri Lanka.

**Poulami Das**, M.Tech in Computer Science and Engineering from the University of Calcutta. She is working as a Lecturer with the Computer Science and Engineering Department at Heritage Institute of Technology, Kolkata. Her research interests include Bio-Informatics, Image Processing and Pattern Recognition. She has more than 3 Years of experience in the line of Teaching. She is working towards his research, since, middle of 2006 under the guidance of Prof. Samir Kumar Bandyopadhyay. She has published seventeen Research Papers in International Journals and Conferences and one Text Book for Computer Science.

**Debnath Bhattacharyya**, M.Tech in Computer Science and Engineering from West Bengal University of Technology, Kolkata. He is working as a Lecturer with the Computer Science and Engineering Department at Heritage Institute of Technology, Kolkata. He was an Education Officer in Computer Society of India, Kolkata for 10 years. His research interests include Bio-Informatics, Image Processing and Pattern Recognition. He has 13 Years of experience in the line of Teaching and Projects. He is working towards his research, since, middle of 2006 under the guidance of Prof. Samir Kumar Bandyopadhyay. He has published twenty one Research Papers in International Journals and Conferences and one Text Book for Computer Science.