ISSN:0975-9646

B.Srikanth et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 2432-2437

Secured Bank Authentication using Image Processing and Visual Cryptography

B.Srikanth[1], G.Padmaja[2], Dr. Syed Khasim[3], Dr. P.V.S.Lakshmi[4], A.Haritha[5]

[1]*Assistant Professor, Department of CSE, PSCMRCET, Vijayawada*

[2]*Associate Professor, Department of IT, PSCMRCET, Vijayawada.*

[3]*Associate Professor, Department of ECM, KL University, Guntur.*

[4]*Professor, Department of IT, PVPSIT, Kanuru.*

[5]*Assistant Professor, Department of IT, PVPSIT, Kanuru.*

***Abstract*—Today's banking system has brought core banking for the user's convenience, which is a set of services, where authentication plays main role. But these days, because of tremendous realization and growth in the field of hacking it is not safe to rely on internet to store all the information. So in order to overcome this problem we are proposing an efficient algorithm for secured bank authentication. The algorithm mainly deals with Image Processing and Visual Cryptography. In this paper, signature of the applicant is processed in such a way that, signature is taken as input and is divided into different number of shares depending upon the banks scheme. One share is preserved in the bank database and all other shares are given to the applicant. The applicant need to provide his shares during every transaction and those shares are over lapped with the already existing bank shares and a check for authentication will be done by using correlation technique. If a higher correlation coefficient is achieved, then the authentication is succeeded.**

I. INTRODUCTION

Today, due to rapid growth in the field of hardware, design and technology has improved enduringly. So it is also equally impossible to detect any problem. In such a case, a computer allied with internet cannot be considered to be secured. Now the inquest is how to access application which requires greater security such as internet banking and mobile banking.

In traditional banking procedure there is a threat of forgery during transactions. In online banking, security begins with the authentication process, used to confirm that it is you, and not someone who has stolen your identity. Authentication generally involves one or more basic factors:

- Something the user knows (e.g., password, PIN)
- Something the user has (e.g., ATM card, smart card)
- Something the user is(e.g., biometric characteristic, such as a fingerprint).

Single factor authentication uses one of these methods; multi-factor authentication uses more than one, and thus is considered a stronger fraud deterrent. When you use your ATM, for example, you are utilizing multi-factor authentication. Factor number one is something you have, your ATM card; factor number two is something you know, your PIN. But in any of these methods, key elements like passwords can be hacked and misused. So here we propose a technique to shield the customer information and to defend the possible forgery.

Image Processing is a form of signal processing for which input is an image, such as photograph or video frame; the output of image processing may be either an image or a set of characteristics or parameters related to the image. Most image-processing techniques involve treating the image as a two-dimensional signal and applying standard signal-processing techniques to it. Visual Cryptography is a cryptographic technique for encryption in which input image is divided into some shares and while decrypting some or all the shares are overlapped to avow the original image.

The basic principle of the visual cryptography scheme (VCS) was first introduced by Naor and Shamir. VCS is a kind of secret sharing scheme that focuses on sharing secret images [1]. The idea of the visual cryptography model proposed in is to split a secret image into two random shares (printed on transparencies) which separately reveals no information about the secret image other than the size of the secret image. The secret image can be reconstructed by stacking the two shares. The underlying operation of this scheme is logical operation OR.

II. Related Work

A detailed explanation related to the work done in the area of Visual cryptography is discussed in this section. We call a VCS with random shares as the traditional VCS or simply the VCS [2]. In general, a traditional CS takes a secret image as input, and outputs shares that satisfy two conditions:

1) Any qualified subset of shares can recover the secret image
2) Any forbidden subset of shares cannot obtain any information of the secret image other than the size of the secret image.

As suggested by Borchert [3], a segment-based visual cryptography can be used only to encrypt the messages containing symbols, especially number like bank account number,balance etc. The Visual Cryptography scheme proposed by Wei-Qi Yan et al[4]., can be just applied for printed text or image.

Previously, VC more concentrated on two parameters. They are pixel expansion and contrast. Let us assume that all the customers are honest and will not share their shares with others. Thus, the image shown on the stacking of shares is considered as the real secrete image. But, this may not be true always. So, cheating prevention methodologies are introduced by Yan et al., [5], Horng et al., [6] and Hu et al., [7]. But, it is observed in all these methodologies, there is no facility of authentication testing.

III. Methodology

In all kinds of banking applications, applicant has to sign in application form while opening an account in the bank. This signature is taken as input. Now from the application form, the signature of the applicant is scanned and taken as input. In order to thicken the lighter shades of the image and to increase the intensity of the image, image is pre-processed. In further stage pre-processed image is encrypted into some share depending upon the scheme followed by the bank.

Now we are mainly concentrating on a 2 out of 2 scheme, which means that the input image is divided into two shares in which one share is stored in the bank database, where as another share is given to the applicant.

Apart from the scheme settled above there are some more scheme to be discussed, as follows:

- 2 out of 3: This scheme is useful for a joint account. Here three shares are created out of which 2 shares are given to the applicants and one share will be stored in the bank database. Any one of the applicant can transact by using his share.
- 3 out of 3: This is more secured in case of joint accounts. All the three shares are to be produced to transact. Thus both the applicants need to be present during the transaction.
- Key-Share Scheme: In this scheme as similar to 2 out of 2 scheme, four shares are drawn from two signatures of the applicants and a key share is generated by using one share of both the signatures. Over lapping key share on each of the remaining shares will reveal the two images independently. Thus both the applicants can transact individually.

In all of the above mentioned cases, shares are printed and given to the applicants as likely as in the case of credit/debit cards. During further transactions printed share of the customer is scanned and overlapped on the share that is already present in the bank data base. Resulting image is compared with the original image. Authentication will be succeeded when the correlation coefficient is high.

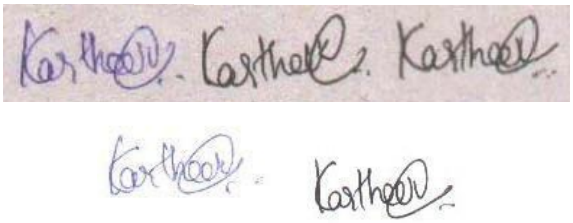


Fig 1-5. Different input Signatures 1-5

A. Pre-Processing:

The scanned image h (a, b) is first converted to grey-scale image and then thresholded. Threshold value is chosen automatically. The image is composed of dark coloured data on a light coloured back ground. Thus there are two different intensity levels that are grouped to form an image. One way to separate the data from the back ground is to set a threshold value T that separates these intensity levels. Then for any pixel (a, b) for which h(a, b)≥T is called a data pixel; or else the point is called a back ground pixel. The threshold image i (a, b) is defined as

$$i(a,b) = \begin{cases} 1 \text{ if } h(a,b) \geq T \\ 0 \text{ if } h(a,b) \leq T \end{cases}$$

Pixels denoted by 1 correspond to data, whereas pixels denoted by 0 correspond to the back ground. This is called global thresholding, where T is a constant. When back ground illumination is even, then there will be a chance of using global thresholding or else, the image is pre-processed before applying global thresholding. This process can be defined as

$$i(a,b) = \begin{cases} 1 \text{ if } h(a,b) \geq T(a,b) \\ 0 \text{ if } h(a,b) \leq T(a,b) \end{cases}$$

T(a, b) is a locally varying threshold function. The formula is given by

$$T(a,b) = f_0(x,y) + T_0$$

The morphological opening of f is the image h_o (a, b) and the result of global threshold applied on h_o is T_o.

Now we will apply morphological erosion on thresholded image which is to shrink the image using a structured element. This is given as

The pre-processed image will be as shown below

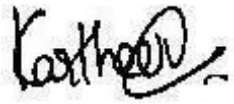


Fig 6. The image Signature 5 after pre-processing

B. Creation of Shares

The image is considered to be the collection of black and white pixels and each pixel is accessed individually. Every pixel will appear in m modified versions, one for each share. Whereas each share is a collection of n black and white sub-pixels that are printed close to each other. The resulting structure can be described by mxn Boolean matrix M = [m_{ij}] where m_{ij} =1 iff the j^{th} sub-pixel in the i^{th} share is black. The following figures show how shares will be created by using 2 out of 2 scheme.

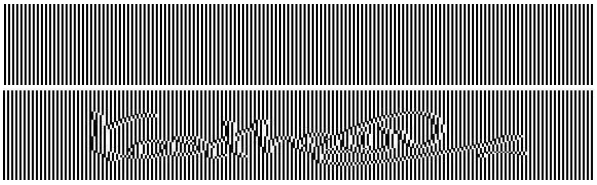


Fig 5-6. Share1 – Share 2

C. Stacking

Stacking is a procedure of decoding the original image by overlapping the shares. Where shares are overlapped together in an aligned order, such that one can see black sub pixels i.e., data pixels represented by the Boolean OR of shares in S. The grey level of this resultant share is proportional to Hamming weight H(V) of the ORed n-vector V. This grey level is interpreted by the visual system of the users as black if H(V) ≥ d and as white if H(V) ≤ d-αn for some fixed threshold 1 ≤ d ≤ and relative difference α>0. The overlapped image would be as shown below

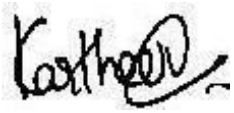


Fig 7. Stacked image signature 5

D. Post-Processing

The overlapped shares results in required image with a randomly distributed redundant information. To avoid this noise we are applying Morphological closing. Closing of an image X by the structured element Y is a dilation followed by erosion, which is represented as

$$A \bullet B = (A \oplus B) \ominus B$$

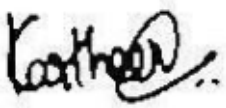


Fig 8. The image signature 5 after post processing

Then filters are used, whose response is based on ranking the pixels contained in the image area encompassed by the filter. The response of filter at any point is then determined by the ranking result. This technique uses Median filter, given as

$$\hat{h}(a, b) = median_{(s,t) \in S_{ab}}\{g(s, t)\}$$

E. Authentication Testing

Whenever two shares are stacked the resulting image is checked for authentication. Whenever two shares of different images are overlapped together then an absurd image will be formed. Thus an attempt to cheat the bank can be overruled. Even though the shares of different signatures are overlapped an image will be formed which will be different from the original image, now the resulting image is compared with the original image. This technique is called correlation, which is used for authentication testing.

Correlation is a technique which is used to compare two sets of values, here images. Here we are using Karl Pearsons correlation technique where correlation coefficient reveals the dependency or independency between the variables. If A and B are two arrays, then the Karl Pearsons correlation coefficient can be computed as

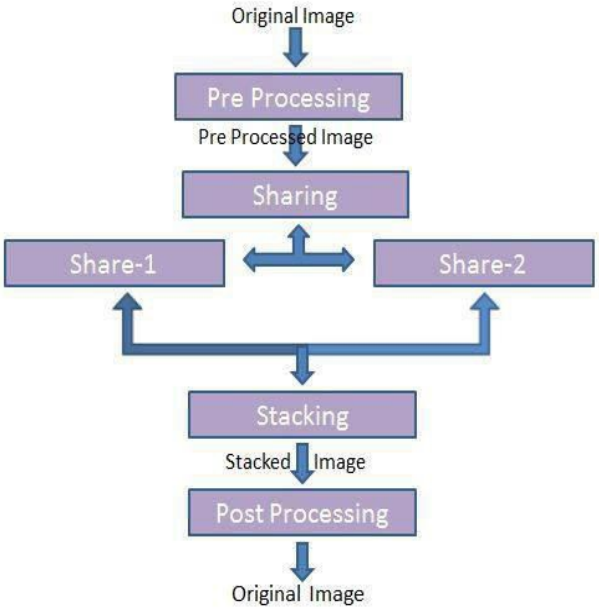
$$\tau_{AB} = \frac{E((A - \mu_A)(B - \mu_B)}{\sigma_A \sigma_B}$$

Where E is the expected value operator, μA ,μB and σA,σB are means and standard deviations of A and B respectively. The value coefficient ρXY may range from -1 to +1. If the correlation coefficient value is -1, then the variables A and B are inversely related. If the value is 0, the variables are independent and if the value is +1 then the

variables are completely related. Thus, the higher degree of positive correlation indicates that the values are very much close to each other. Thus authentication will be succeeded if the correlation coefficient is very nearer to +1. If the correlation coefficient is nearer to 0, then it can be confirmed that the share produced is fake.

IV. ALGORITHM

The algorithm includes four steps. The first step is pre- processing. In this step, the input image is processed so as to remove the noise and to increase the clarity of the image. In the second step, input image is encrypted into shares depending upon alignment of the black and white pixels. The third step is to overlap the shares to reconstruct (decrypt) the original image containing signature. And the last step is to compare the overlapped image with the original image using correlationtechnique.



The main aim of the algorithm is to check the authenticity of the applicant in core banking or internet banking during transact. The pseudo codes for all the steps are given here. For a given image, the first thing is to convert the image to a binary image in order to remove the redundant data and to increase the intensity. In the next step shares are generated depending upon black and white pixels. The black pixel denoted by 1 is a data pixel , where as white pixel denoted by 0 is a back ground pixel. For a 2 out of 2 scheme, the initial Boolean matrices are gives as

$$S_0 = [1100]$$

$$S_1 = [0011]$$

The procedure for creating shares will be discussed here. If a particular pixel is white in the original image, two matrices are put in to two shares respectively. If the data pixel is black then the matrix S_0 is put into both the shares. Thus the single pixel in the original image is filled with a matrix of four pixel values. Thus the resultant share will be four times the size of original image.

Now decryption is done by overlapping the shares. If every 5^{th} pixel in both the shares is a data pixel then the data pixel is black, if not data pixel is white.

In this 2 out of 2 scheme, one share is preserved in the bank data base and the other is printed and given to the customer. During every transaction, applicant should produce his share. This applicant's share will be scanned and overlapped with the share that is already preserved in the bank database. To get the image decryption matrices are used. The resultant image is post processed to remove the noise and is compared with the original image by using correlation technique.

TABLE I
PRE-PROCESSING :THRESHOLDING

```
stack()
begin
for i=1 to rows
   for j=1 to columns
          if share1 && share2 are 1
            setResImg=1
          else
            setResImg=0
          end if
   end for
end for
end
```

The algorithm given in the above table improves the intensity of the image. In the beginning, an arbitrary value is selected for the threshold *T*. So that by using the threshold *T*, we can divide the image into two groups of pixels. One group of pixel values ranges below the threshold *T*and another group of pixels will ranges above the threshold *T*. Now the average grey values are computed and by using these values, new threshold value *T* is found out. This procedure is followed until the threshold value *T*is less than the predefined parameter ε.

TABLE - II

SHARING: CREATION OF SHARES

Step 1: Select an initial threshold value T.
Step 2: Divide the image into two group of pixels G_1 and G_2:
G_1 consisting of with values > T and G_2 consisting of pixel values $\leq T$
Step 3: For the given group of pixels, compute the average grey values μ_1, μ_2
Step 4: Now calculate the new threshold value using the formula

$$T = \frac{1}{2}(\mu_1 + \mu_2)$$

Step 5: Steps 2 to 4 are repeated until the difference in T in Successive iterations is smaller than a predefined Parameter ε

TABLE III

STACKING FOR 2 OUT OF 2 SCHEME

```
Step 1: Define two Boolean matrices S0 and S1
Step 2: Initialize two variables share1 and share2
Step 3:
share()
begin
s0=[1 1 0 0]
s1=[0 0 1 1]
for i=1 to rows
   for j=1 to columns
      for k=1 to 4
            if image(i,j) is 1
              set  share1=s0
              set share2=s0
            else
              set share1=s1
              set share2=s1
            end if
      end for
   end for
end for
end
```

The algorithm in the above Table II is to create shares by using 2 out of 2 scheme. Initially two Boolean matrices are defined for white and black pixels.

Depending upon the value of the pixel in the i^{th} row, 4 pixels are appended as per the matrices for both the shares. Now, we cannot reconstructed the original signature with just any one of the share i.e., we need both the shares to reconstruct the original image.

In Table III, the algorithm discuss about the process of stacking, where two shares of two out of two scheme are overlapped together. This overlapped image is now compared with the original image by using correlation technique. Karl Pearson's Correlation Coefficient is calculated between the original image and resultant image as shown in the Table IV below

TABLE IV

CORRELATION : USING KARL PEARSON'S TECHNIQUE

```
Corr_coeff()
begin
Initialize sumx=0, sumy=0, sumxy=0, sumsx=0, sumsy=0,
length=rowsXcolumns
for i=1 to rows
   for j=1 to columns
            sumx=sumx+x(i,j)
            sumy=sumy+y(i,j)
            sumxy=sumxy+(x(i,j) X y(i,j))
            sumsx=sumsx+(x(i,j))^2
            sumsy=sumsy+(y(i,j))^2
   end for
end for
corrcoeff=((lengthXsumxy)-
(sumxXsumy))/squareroot(((lengthXsumsx)-
(sumx)^2)((lengthXsumsy)-(sumy)^2))
end
```

V. RESULTS

Pre-processing, post-processing, sharing, overlapping and authentication testing using correlation method are implemented using MATLAB 2010. A very high correlation coefficients are observed while relating input images with output images during simulation. This algorithm has been tested on various signatures of different back grounds. The correlation coefficients are listed as given in the Table V

When two shares of different signatures are overlapped, then the output image will be absurd and gives zero correlation coefficient.

TABLE V

Input Images	Correlation Coefficient
Signature 1	0.8748
Signature 2	0.9416
Signature 3	0.9054
Signature 4	0.9232
Signature 5	0.8919

VI. CONCLUSIONS

In this paper we proposed an effective technique to provide greater security in the field of core-banking and internet banking applications. At the beginning, while creating an account the bank, signature of the applicant is taken by scanning his/her signature from the application. Now this scanned image is taken as input and is subjected to pre-processing to remove noise and to increase intensity. This pre-processed image to encrypted into two share by using two out of two scheme. One share is stored in the bank data base, another share is printed and given to the applicant. Applicant had to provide his share during every transaction. During transaction applicants share is

scanned and overlapped with the bank's share, if higher correlation coefficient is obtained, then authentication will be success. If the shares of two signatures are overlapped then the correlation coefficient will be zero thus authentication will be failed. Thus this algorithm strictly prohibits forgery up to greater extent. This algorithm is designed for binary images, but in future this can be extended to colour images. Here signatures are taken as inputs since they are uniquely identified, but according to the user and bank convenience any kind of images can also be used like photograph of the applicant.

REFERENCES

[1] M. Naor and A. Shamir, "Visual Cryptography". *Advances in Cryptography-EUROCRYPT'94*, Lecture Notes in Computer Science 950, 1995, pp. 1-12

[2] "Visual Cryptography Schemes for Secret Image" N. Anusha, P. SubbaRao, *International Journal of Engineering Research & Technology(IJERT)* Vol. 1 Issue 5, July – 2012.

[3] B. Borchert, ."Segment Based Visual Cryptography". WSI Press, Germany,2007.

[4] W-Q Yan, D. Jin and M. S. Kanakanahalli, "Visual Cryptography forPrint and Scan Applications". *IEEE Transactions*, ISCAS-2004, pp.572-575.

[5] H. Yan, Z. Gan and K. Chen, "A Cheater Detectable Visual Cryptography Scheme," *Journal of Shanghai University*, vol. 38, no.1,2004

[6] G. B. Horng, T. G. Chen and D. S. Tsai, "Cheating in Visual Cryptography," *Designs, Codes, Cryptography*, vol.38, no.2, 2006, pp. 219- 236.

[7] C. M. Hu and W. G. Tzeng, .Cheating Prevention in Visual Cryptography,. *IEEE Transaction on Image Processing*, vol. 16, no. 1, Jan- 2007,pp. 36-45.