Passport Authentication System Using Visual Secret Sharing Scheme

Milind K. Wagh, Nilesh R. Jagtap, Sagar S. Jadhav, Pritamsing J. Salunkhe

Abstract- Passport is the most important document while travelling from one country to another. It is the proof of citizenship of the country. Hence, it needs to keep it secure from unauthorized use. Authentication and security of passport and checking integrity of a person on the airport is a challenging task. In order to face this challenge of security and privacy, we propose a method based on Visual Secret Sharing (VSS) for black and white passport number. In our proposed method we have a new approach in VSS with improved contrast. Two shares of a passport number image are formed by applying 2-out-of-2 VSS. Shares generated will contain only black and white pixels, which make it difficult to retrieve any information about the image by viewing only one share. However, when the two shares are overlaid the secret image is retrieved.

Keywords- VSS.

I. INTRODUCTION

Computerized technologies in authentication systems are emerging to help security professionals in handling the security of passport data explosion and increasingly complex security information. Current and future authentication systems require large amounts of information to be collected, stored, processed and managed. The security of these information systems and data is important. In order to deal with the security in passport authentication field in this paper we present a VSS scheme in a better way. Visual Cryptography or Visual Secret Sharing is a field of cryptography in which a secret image is encrypted into n shares such that stacking a sufficient number of shares reveals the secret image. This technique was introduced by the Naor and Shamir in 1994. In VSS the shares generated contains only black and white pixels which make it to difficult to gain any information about the secret image by viewing only one share.

The secret image is revealed only by stacking sufficient number of shares. There are different visual secret sharing schemes, like n-out-of-n and k-out-of-n, we have used n-out-of-n VSS scheme. In n-out-of-n scheme n shares will be generated from the original image and in order to decrypt the secret image all n shares are needed to be stacked.

Following n-out-of-n scheme we have taken n value as 2. In this paper we have used 2-out-of-2 VSS scheme in an optimized way. Our approach can be used in providing security in the passport authentication field.

The number of security issues associated with security for passport authentication is vast however security in this field is concerned mainly on authentication of the citizen's data and systems used in the passport authentication field and also on hiding the confidential images.

In this paper we have used our approach to achieve this security or in other words the scope of our paper is limited to application level concerns such as data integrity, confidentiality, authentication, and access control. This technique can be implemented in the passport authentication for storing and sharing passport number. On each and every airport, scanning of passport is essential process so it won't need to establish additional hardware capabilities. Now-a-days, duplication of passport by some terrorist organizations is the vital issue for many countries. So, this method will help to stop unauthorized person from entering into other country as his/her shares are not authenticated.

This paper is organized as follows. Section II introduces the fundamental principles of VSS, based on which our method is proposed. Section III shows our proposed method for constructing the simplest 2-out-of-2 scheme with modification. The application of our VSS scheme in the medical field can be viewed in section IV. In section V future work related to our method is mentioned. Finally, conclusions are drawn in section VI.

II. VISUAL SECRET SHARING

VSS is a model in which the decryption of the secret image is done by using human visual system without any computational complexity. In VSS the shares are Xeroxed onto transparencies and distributed among participants, one for each participant. No participant knows the share given to another participant. Any t or more participants can visually reveal the secret image by superimposing any t transparencies together. The secret cannot be decoded by any t-1 or fewer participants, even if infinite computational power is available to them [1]. In 2-out-of- 2 VSS scheme, a secret image is encrypted into two shares such that each share has random binary pattern of pixels. In order to decrypt the image, the two shares need to be overlaid.

A. Basic Model

Consider a set X = {1, 2,. . . , n} be a set of elements called participants. By applying set theory concept we have 2X as the collection of all subsets of X.

Let $\Gamma Q \subseteq 2^x$ and $\Gamma F \subseteq 2^x$, where $\Gamma Q \bigcap \Gamma F = \theta$ and $\Gamma Q \bigcup \Gamma F = 2^x$

members of ΓQ are called qualified sets and members of ΓF are called forbidden sets [2]. The pair (ΓQ ,ΓF) is called the access structure of the scheme.

ΓQ can be defined as all minimal qualified sets:

ΓQ ={ A $\in$ ΓQ : $A^|$ $\notin$ ΓQ for all $A^| \subset$ A }

ΓQ can be considered as the closure of ΓQ. ΓQ is

Manuscript received August, 2013.

Milind K. Wagh, Dr. D. Y. Patil Institute of Engineering & Technology, Ambi (Talegaon), India.
Nilesh R. Jagtap, Dr. D. Y. Patil Institute of Engineering & Technology, Ambi (Talegaon), India.
Sagar S. Jadhav P, Dr. D. Y. Patil Institute of Engineering & Technology, Ambi (Talegaon), India.
ritamsing J. Salunkhe, Dr. D. Y. Patil Institute of Engineering & Technology, Ambi (Talegaon), India.

termed a basis, from which a strong access structure can be derived [1]. Considering the image, it will consist of a collection of black and white pixels. Each pixel appears in n shares, one for each transparency or participant. Each share is a collection of m black and white sub-pixels. The overall structure of the scheme can be described by an n x m (No. of shares x No. of sub-pixels) Boolean matrix S = [Sij], where Sij = 1 if and only if the j^{th} subpixel in the i^{th} share is black. Sij = 0 if and only if the j^{th} subpixel in the i^{th} share is white.

Following the above terminology, let $(\Gamma Q, \Gamma F)$ be an access structures on a set of *n* participants. A $(\Gamma Q, \Gamma F, \alpha)$- VCS with the relative difference α and set of thresholds $1 \leq k \leq m$ is realized using the two n x m basis matrices S^0 and S^1 if the following condition holds:

1. If X = { i1, i2, ………ip } ∈ ΓQ , then the "or" V of rows i1, i2, ……ip of S^0satisfies $H(V) \leq k - \alpha.m$, whereas, for S^1 it results that $H(V) \geq k2$. If X = { i1, i2, ………ip } ∈ ΓF , then the two p x m matrices obtained by restricting $S^0$and S^1 to rows i1,i2, ………ip are identical up to a column permutation[2][10].

The first condition is called contrast and the second condition is called security. The collections C0 and C1 are obtained by permuting the columns of the basis matrices S^0 and S^1 in all possible ways [3][4]. The important parameters of the scheme are:

1. *m*, the number of sub pixels in a share. This represents the loss in resolution from the original image to the shared one. The m has to be as small as possible. The m is computed using the equation:

$$m = 2^{n-1} \qquad (1)$$

2. α, the relative difference, it determines how well the original image is recognizable. This represents the loss in contrast. The α to be large as possible. The relative difference α is calculated using the equation:

$$\alpha = | nb- nw | / m \qquad (2)$$

Where nb and nw represents the number of black sub-pixels generated from the black and white pixels in the original image.

3. β, the contrast. The value β is to be as large as possible. The contrast β is computed using the equation:

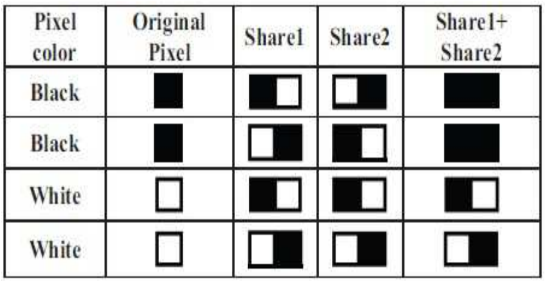
$$\beta = \alpha .m \qquad (3)$$

The minimum contrast that is required to ensure that the black and white areas will be distinguishable if $\beta \geq 1$ [5].

B. Generation of shares

In order to generate the shares in the 2-out-of-2 scheme we have the following mechanism:

TABLE 1. PIXEL PATTERN FOR 2-OUT-OF-2 VSS SCHEME



Pixel color	Original Pixel	Share1	Share2	Share1+ Share2
Black	■	■□	□■	■■
Black	■	□■	■□	■■
White	□	■□	■□	■□
White	□	□■	□■	□■

An original black pixel is converted into two sub pixels for two shares, shown in 1st row. After stacking the two shares we will get a perfect black. Similarly we have other combination for two sub-pixels generated shown in 2nd row. For original white pixel also we have two sub-pixels for each of the two shares, but after stacking the shares we will not get exact white. We have a combination of black and white sub-pixels. This results in the loss of the contrast. Considering the following Fig. 1, we can generate the basis matrix:

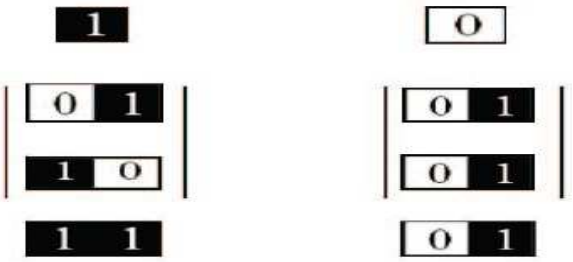


Fig. 1. Basis Matrices Construction.

The basis matrices are given as:

$$S^0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \text{ and } S^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

In general if we have X= {1, 2} as set of number of participants, then for a creating the basis matrices S0 and S1 we have to apply the odd and even cardinality concept of set theory. For S0 we will consider the even cardinality and we will get ES0= {Θ, {1, 2}} and for S1 we have the odd cardinality OS1= {{1}, {2}}. In order to encode the black and white pixels, we have collection matrices which are given as:

C0 = {Matrices obtained by performing permutation on the columns of

$$\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}\}$$

C1= {Matrices obtained by performing permutation on the columns of

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\}$$

So finally we have,

$$C_0 = \{ \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \}$$

$$C_1 = \{ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \}$$

Now to share a white pixel, randomly select one of the matrices in C0, and to share a black pixel, randomly select one of the matrices in C1. The first row of the chosen matrix is used for share S1 and the second for share S2.

C. Stacking of shares

Fig 2(a) Original image

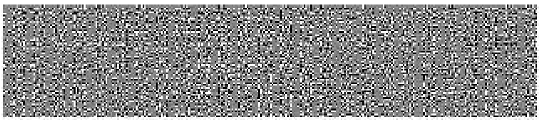


Fig 2(b) Share 1

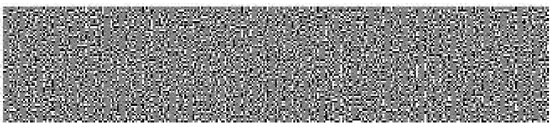


Fig 2(c) Share 2

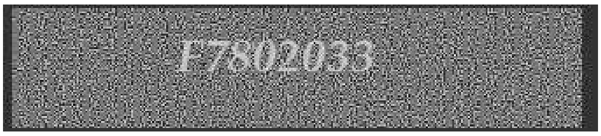


Fig 2(d) Decrypted image

Fig.2 VSS Scheme

Fig. 2 shows the stacking of the shares. Fig 2(a) shows the original image, Fig 2(b) and Fig 2(c) are the shares generated from the original image. Fig 2(d) shows the decrypted image after stacking the two shares. From the Fig 2(d) it can be observed that contrast in the decrypted image is less. In order to improve the contrast an analysis on the relative contrast value is required.

III. PROPOSED METHOD

Based on the analysis on the relative contrast we have the following observation:

TABLE 2. RELATIVE CONTRAST VALUES

Shares n	Sub Pixels $m=2^{n-1}$	Relative Contrast(α)	Contrast $\beta = \alpha.m$
2	2	0.50	1
3	4	0.25	1
4	8	0.125	1
5	16	0.0625	1
6	32	0.03125	1

From the table II we can see that the relative contrast value decreases as the number of sub pixel increases. The following Fig. 3 depicts the same.

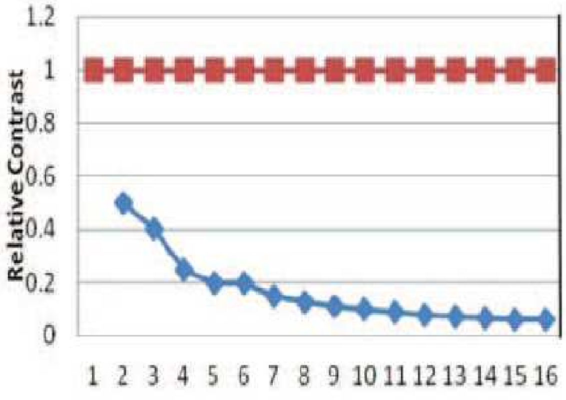


Fig. 3 Relative contrast Vs. Number of sub pixels

Fig. 3

So considering the same 2-out-of-2 VSS in order to increase the relative contrast value, we have used an additional matrix along with the basis matrices. The additional matrix is used to share the white pixels in the reconstructed secret image. The additional matrix can be formed in the following manner:

Let X be the set which is given by

X= {i1, i2 ….in} of n elements.

We define an additional matrix A S^0 with order n x m such that

AS^0 = [ASij] where,

ASij = 0 if and only if $1 \le i \le n$ and j=1, 2.

$$S^0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \quad S^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ and } AS^0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

The collection matrices will be obtained in the following manner:

C0 = {Basis Matrix $\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$ + Additional Matrix $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ }

C1= {Matrices obtained by performing permutation on the columns of $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ }

Now the value of α will be equal to 3/4. This result shows that the relative difference of proposed method is better compare to the existing one. Algorithm : Creation of Shares for 2 out of 2 Scheme (Box I)

```
Step 1: Create two matrices S0 and S1 for
white and black pixels.
Step2: Initialize two variables WHITEPIXEL
and BLACKPIXEL:
Step 3:
 for i = 1 to rows
    for j = 1 to columns
       for k = 0 to 3
           if Img (i; j)==WHITEPIXEL
              set Share1 (i; j + k)=WHITEPIXEL
              set Share2 (i; j + k)=WHITEPIXEL
            else
              set Share1 (i; j + k)=BLACKPIXEL
              set Share2 (i; j + k)=BLACKPIXEL
           end if
        end for
    end for
end for
```

Algorithm : Stacking the Shares for 2 out of 2 Scheme (Box II)

```
Stack()
     begin
       for i = 1 to rows
             for j = 1 to columns
                 for k = 0 to 3
                   if Share1 (i; j + k)==BLACKPIXEL
                   set OutImg (i; j + k)=WHITEPIXEL
                   else
                   set OutImg (i; j + k)=BLACKPIXEL
                   end if
                 end for
             end for
        end for
      end

sdaf
```

Algorithm : Calculate Correlation

Coefficient (Box III)

```
Corr - Coeff()
//Input: The original image X and the resulting image Y .
//Output: The Correlation Coef_cient between X and Y .
begin
Intialize SumX = 0, SumY = 0, SumSqX = 0,
             SumSqY = 0and SumXY = 0
   for i = 1 to rows
     for j = 1 to columns
      set SumX = SumX + X (i; j)
      set SumY = SumY + Y (i; j)
      set SumSqX = SumSqX + X (i; j)2
      set SumSqY = SumSqY + Y (i; j)2
      set SumXY = SumXY + X (i; j) _ Y (i; j)
     end for
    end for
AvgX = SumX=(rows _ cols)
AvgY = SumY=(rows _ cols)
EXY = SumXY=(rows _ cols)
StdX = sqrt(SumSqX=(row _ cols)AvgX2)
StdY = sqrt(SumSqY=(row _ cols)AvgY 2)
Corr = (EXY AvgX _ AvgY )=(StdX _ StdY )

end
```

Algorithm in Box I is to create shares for a given signature image. Initial matrices S0 and S1 are created for white and black pixels. Depending on the value of any pixel in thei^{th}row of image, four pixels in that row are set as per the matrices for both the shares. Now, these two shares cannot individually be used to get the secret image.

Algorithm Stack() in Box II is to overlap two shares to get the secret image. Box III reveals the calculation of Karl Pearson's Correlation Coefficient between the original image and the resulting secret image.

IV. AUTHENTICATION TESTING

After obtaining the passport number, it is tested for the authenticity. If the shares of different passport numbers are stacked, an absurd image is obtained. A possible attempt made to cheat the security may thus be overruled. There is a possibility of producing a share which will result in some number format, but not the actual number. Such an attempt is overruled by comparing the decrypted number with the original number. This algorithm uses the correlation technique for checking the authenticity. Correlation is a method of identifying the degree of relationship between two sets of values. Karl Pearson's correlation coefficient reveals the dependency or independency between the variables. If *X* and *Y* are two arrays, then the Karl Pearson's correlation coefficient between *X* and *Y* is computed using the formula

$$\rho_{XY} = \frac{E(XY) - \mu_X \mu_Y}{\sigma_X \sigma_Y}$$

Here, *E* is the *expected value* operator, µX, µY andσX, σY are means and standard deviations of *X* and *Y* respectively. The value of correlation coefficient PXY may range from -1 to +1. If the value of correlation coefficient is -1, the variables *X* and *Y* are inversely related. If the value is 0, then the variables are independent and if the value is 1, then the variables are completely (or positively or directly) related. Thus, the high degree of positive correlation indicates that the values of variables are very much close to each other. So, if the correlation coefficient between the original image and the output image is nearer to +1, authenticity may be granted. If the correlation coefficient is nearer to zero, one can decide that the share produced by passport holder is fake and can be rejected.

V. APPLICATION

VSS can be mainly applied to Passport Authentication System and security issues associated with other system. First considering the Passport Authentication System, in this exchange of private data among offices is a very common practice. The impetus is to have the complete personal information of a passport holder available in one consistent application rather than over several information systems. It saves storage space in Passport Service Center (PSC) information system. The confidentiality of the passport is very critical and thus it is essential to efficiently hide the data during transmission.

VSS can be used for this purpose. The sensitive information like address, contact no of a V.I.P. person can be put into the Passport Authentication System database server. If in certain circumstances that information is required to be shared with some other authority, then in that case two shares can be generated for the password of that passport number. Both shares need to be sent to the referred authority in different ways like by sending two shares in two different emails. The authority will get to know about the password by stacking the two shares received through different mails. Now using that password authority can access the passport record present in the database of the Passport Authentication System who has sent the password.

The advantage of the above approach is that if an intruder gets an access to any one communication channel, then he will receive only one share from which no information regarding the password can be generated and whatever be the personal data, they are safe in the Passport Authentication database until the password is not known to the intruder. The same approach is also applicable to evaluate the issues of security threats and vulnerabilities that effect security of data.

VI. CONCLUSION

In this paper we explained, VSS with its application in the passport authentication field. In addition, an improved method for generating shares is proposed and proved using examples. The proposed method increases the number of white pixels and thus the contrast of the decrypted image. We can apply this concept in maintaining the security and privacy of passport information and will avoid the fake intruders from getting entered into country without legal documents.

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] A. Shamir, ”How to Share a Secret,” Communication ACM, vol. 22,1979, pp. 612-613.

[3] G. R. Blakley, ”Safeguarding Cryptographic Keys,” Proceedings of AFIPS Conference, vol. 48, 1970, pp. 313-317.

[4] A. Menezes, P. Van Oorschot and S. Vanstone, ”Handbook of Applied Cryptography,” CRC Press, Boca Raton, FL, 1997.

[5] B. Borchert, ”Segment Based Visual Cryptography,” WSI Press, Germany, 2007.

[6] W-Q Yan, D. Jin and M. S. Kanakanahalli, ”Visual Cryptography for Print and Scan Applications,” IEEE Transactions, ISCAS-2004, pp. 572-575.

[7] T. Monoth and A. P. Babu, ”Recursive Visual Cryptography UsingRandom Basis Column Pixel Expansion,” in Proceedings of IEEE International Conference on Information Technology, 2007, pp. 41-43.

[8] H. J. Kim, V. Sachnev, S. J. Choi and S. Xiang, ”An Innocuous Visual Cryptography Scheme,” in Proceedings of IEEE-8th International Workshop on Image Analysis for Multimedia Interactive Services, 2007.

[9] C. Blundo and A. De Santis, ”On the contrast in Visual Cryptography Schemes,” in Journal on Cryptography, vol. 12, 1999, pp. 261-289.

[10] P. A. Eisen and D. R. Stinson, ”Threshold Visual Cryptography with specified Whiteness Levels of Reconstructed Pixels,” Designs, Codes, Cryptography, vol. 25, no. 1, 2002, pp. 15-61.

[11] E. R. Verheul and H. C. A. Van Tilborg, ”Constructions and Properties of k out of n Visual Secret Sharing Schemes,” Designs, Codes, Cryptography, vol. 11, no. 2, 1997, pp. 179-196.

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

[13] G. B. Horng, T. G. Chen and D. S. Tsai, ”Cheating in Visual Cryptography,” Designs, Codes, Cryptography, vol. 38, no. 2, 2006,

1) Jagtap Nilesh Ravindra[redacted].E.(Information Technology) Dr. D. Y. Patil Institute of Engineering & Technology , Ambi , Pune 410506 +918237706275

2) Jadhav Sagar SuryakantB.E.(Information Technology)Dr. D. Y. Patil Institute of Engineering & Technology , Ambi , Pune 410506
Sagar.jadhav417@gmail.com
+918655478198

3) Salunkhe Pritamsing JyotisingB.E.(Information Technology)Dr. D. Y. Patil Institute of Engineering & Technology , Ambi , Pune 410506Pritamsalunkhe4@gmail.com+919890640560

4) Wagh Milind Kailas B.E.(Information Technology)Dr. D. Y. Patil Institute of Engineering & Technology , Ambi , Pune
410506Milindwagh23@gmail.com+919503141387