Electronic Medical Report Security Using Visual Secret Sharing Scheme

Rajendra Basavegowda
PES College of Engineering
Mandya- 571401 ,Karnataka, India
rajendraab@hotmail.com

Sheshadri Seenappa
PES College of Engineering
Mandya- 571401 ,Karnataka, India
hssheshadri@hotmail.com

***Abstract*- Privacy and security is an important concern in the medical field. Authentication and security of medical data, storing and sharing medical images secretly 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 medical images. In our proposed method we have a new approach in VSS with improved contrast. Two shares of a medical 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. This technique can be implemented in the medical field for storing and sharing Electronic Medical Report (EMR) and also images of X-ray, MRI scan; CT scan and Ultrasound scan in a secure way.**

Keywords – Electronic Medical Report (EMR), Medical image, Visual Secret sharing VSS, Shares.

I. INTRODUCTION

Computerized technologies in medical systems are emerging to help health care professionals in handling the difficult problems of patient data explosion and increasingly complex diagnostic information. Current and future health care systems require large amounts of information to be collected, stored, processed and managed. The security of these medical information systems and data is important. In order to deal with the security in medical 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 medical field. The number of security issues associated with security for medical applications is vast however security in the medical field is concerned mainly on authentication of the medical data and systems used in the medical field and also on hiding the confidential medical 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 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 2^X as the collection of all subsets of X.

978-0-7695-4994-1/13 $26.00 © 2013 IEEE
DOI 10.1109/UKSim.2013.123

Let $\Gamma_Q \subseteq 2^X$ and $\Gamma_F \subseteq 2^X$, where $\Gamma_Q \cap \Gamma_F = \theta$ and $\Gamma_Q \cup \Gamma_F = 2^X$,

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

Γ_O can be defined as all minimal qualified sets:

$\Gamma_O = \{A \in \Gamma_Q : A^{|} \notin \Gamma_Q \text{ for all } A^{|} \subset A\}$

Γ_Q can be considered as the closure of Γ_O. Γ_O is 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 $S = [s_{ij}]$, where

$s_{ij} = 1$ if and only if the j^{th} subpixel in the i^{th} share is black.

$s_{ij} = 0$ if and only if the j^{th} subpixel in the i^{th} share is white.

Following the above terminology, let (Γ_Q, Γ_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 $1 \le k \le m$ is realized using the two n x m basis matrices S^0 and S^1 if the following condition holds:

1. If $X = \{ i_1, i_2, \ldots\ldots i_p \} \in \Gamma_Q$, then the "or" V of rows $i_1, i_2, \ldots\ldots i_p$ of S^0 satisfies $H(V) \le k - \alpha.m$, whereas, for S^1 it results that $H(V) \ge k$.2. If $X = \{ i_1, i_2, \ldots\ldots i_p \} \in \Gamma_F$, then the two p x m matrices obtained by restricting S^0 and S^1 to rows $i_1, i_2, \ldots\ldots i_p$ are identical up to a column permutation[2][10].

The first condition is called contrast and the second condition is called security. The collections C_0 and C_1 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:

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

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:

$$\alpha = | n_b - n_w | / m \quad (2)$$

where n_b and n_w 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:

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

The minimum contrast that is required to ensure that the black and white areas will be distinguishable if $\beta \ge 1$ [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. Similarlily 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:

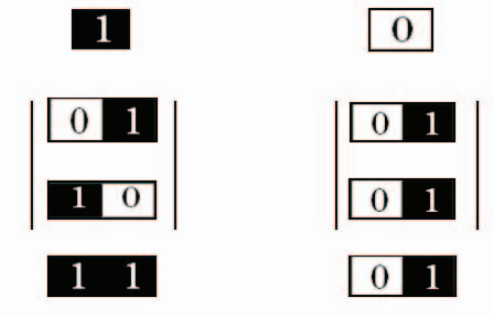

Fig. 1. Basis Matrices Construction.

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 S^0 and S^1 we have to apply the odd and even cardinality concept of set theory. For S^0 we will consider the even cardinality and we will get E_{S0}= {Θ, {1, 2}} and for S^1 we have the odd cardinality O_{S1}= {{1}, {2}}. In order to encode the black and white pixels, we have collection matrices which are given as:

C_0 = {Matrices obtained by performing permutation on the columns of $\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$}

C_1= {Matrices obtained by performing permutation on the columns of $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ }

So finally we have,

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

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

Now to share a white pixel, randomly select one of the matrices in C_0, and to share a black pixel, randomly select one of the matrices in C_1**.** The first row of the chosen matrix is used for share S1 and the second for share S_2.

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 β = α.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 subpixel increases. The following Fig. 3 depicts the same.

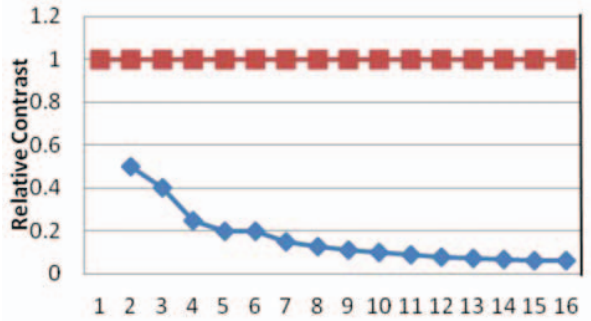

Fig. 3 Relative contrast Vs. Number of sub pixels

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= $\{i_1, i_2 \ldots . i_n\}$ of n elements.

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

$AS^0 = [As_{ij}]$ where,

$As_{ij} = 0$ if and only if $1 \leq i \leq n$ and j=1, 2.

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

A. Algorithm for Encryption Process

```
Algorithm: Encryption Algorithm
Input: Black and White Image
Output: Two shares
read (InputImage)
share1=Zeros (rows, (2*columns))
share2=Zeros (rows, (2*columns))
// Black Pixel processing
  [x y] = find (InputImage == 1)
  len = length(x)
  for i=1 to len
     do
        a=x(i)
        b=y(i)
        T=column_permutation(S1)
        share1((a),(2*b-1):(2*b))=T(1,1:2)
        share2((a),(2*b-1):(2*b))=T(2,1:2)
  end for
// White pixel Processing
[x y] = find (InputImage == 1)
 len = length(x)
  for i=1 to len
     do
        a=x(i)
        b=y(i)
        T=column_permutation(S0)
        T1= [ T,AS0]
        Set share1((a),(2*b-1):(2*b))=T1(1,1:2)
        Set share2((a),(2*b-1):(2*b))=T1(2,1:2)
  end for
end
```

B. Algorithm for Decryption Process

```
Algorithm: Decryption
Input: Two shares share1, share2
Output: Decrypted Image share12
 for i = 1 to rows
    for j = 1 to columns
      Set T1 (1, 1:2) = share1 (i, 2*(j-1):2*j)
     Set T2 (1, 1:2) = share2 (i, 2*(j-1):2*j)
     Share12=bitxor (T1, T2)
   end for
 end for
display(Share12)
end
```

C. Stacking of the shares:

Fig 4(a) Secret Image

Fig 4(b) Share 1

Fig 4(c) Share 2

Fig 4(d) Decrypted Image

Fig.4 Improved VSS Scheme

Fig. 4 shows the stacking of the shares. Fig 4(a) shows the original image, Fig 4(b) and Fig 4(c) are the shares generated from the original image. Fig 4(d) shows the decrypted image with better contrast. With this better contrast we can apply our approach in various fields for achieving the security objectives.

IV. APPLICATION IN THE MEDICAL FIELD

A. Authentication

VSS can be mainly applied to Electronic Medical Report and security issues associated with medical devices & systems. First considering the Electronic Medical Report, in medical field exchange of medical data among hospitals is a very common practice. The impetus is to have the complete medical information of a

patient available in one consistent application rather than over several information systems. It saves storage space in hospital information system. The confidentiality of the medical reports is very critical and thus it is essential to efficiently hide the data during transmission [6]. VSS can be used for this purpose. The medical information like Electronic Medical Report of a person can be put into the hospital database server. If in certain circumstances that information is required to be shared with some other hospital, then in that case two shares can be generated for the password of that medical information. Both shares need to be sent to the referred hospital in different ways like by sending two shares in two different emails. The authority of the referred hospital will get to know about the password by stacking the two shares received through different mails. Now using that password hospital authority can access the EMR present in the database of the hospital who has sent the password. The following Fig. 5 depicts the same:

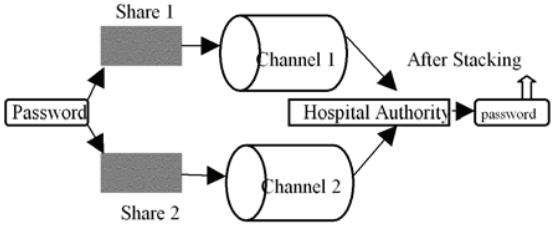

Fig. 5 Sharing the password over network

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 medical data like Ultrasound Images, MRI scan images, Electronic Medical Report etc they are safe in the hospital 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 medical devices. This approach can be used in the safe delivery of medical devices from manufacturer to hospital authority. The medical devices should be password protected and one share can be sent to the hospital through the email and other alongwith the machine. Similarly,it can also be applied in the hospitals for protecting the medical devices from unauthorized person.

B. Image Hiding

The concept of VSS can also be applied in hiding the medical images. The Fig. 6 shows the hiding of an ultrasound image using VSS. Shares are generated from the original ultrasound image and after stacking the shares we have decrypted image shown in Fig. 6(d).

Our approach is useful in hiding the medical images of MRI scan, Ultrasound scan etc from which useful information can be gained or the images which can be tampered by any unauthorized person. Our approach also provides a mechanism in which the integrity and confidentiality of the medical images will be in the hands of authorized persons.

Fig 6(a) Ultrasound image

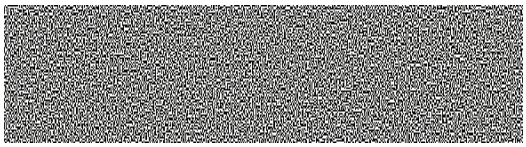

Fig 6(b) Share 1

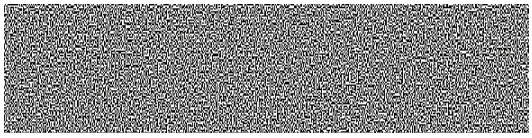

Fig 6(c) Share 2

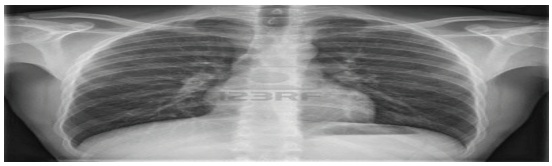

Fig 6(d) Decrypted ultrasound image

Fig. 6 VSS in Medical Field

VI. CONCLUSION

In this paper we explained VSS with its application in the medical 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 Electronic Medical Report, medical devices and medical images.

REFERENCES

[1] Zhi Zhou, Member, IEEE, Gonzalo R. Arce, Fellow, IEEE, and Giovanni Di Crescenzov Halftone Visual

Cryptography, IEEE Transactions On Image Processing, Vol. 15, No. 8, August 2006.
[2] Carlo Blundo ,University of Salerno , Alfredo De Santis and Douglas R Stinson,University of Nebraska-Lincon, On the contrast in visual cryptography scheme, September 1996.
[3] D.Stinson, Visual cryptography and threshold schemes, Potentials, IEEE, 1999, Vol. 18 Issue: 1, pp. 13 -16.
[4] Carlo Blundo, Alfredo De Santis, Moni Naor, Visual cryptography for grey level image,. Information Processing, 2000, Letters, 75, pp. 255-259.
[5] Thomas Monoth and Babu Anto P,Achieving Optimal Contrast in Visual Cryptography Schemes without Pixel Expansion, International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009.
[6] K. A. Navas, S. Archana Thampy, and M. Sasikumar EPR Hiding in Medical Images for Telemedicine, International Journal of Biological and Life Sciences 3:1 2007 .
[7] M. Naor & A. Shamir, Visual Cryptography, Proc.Advances in Cryptology EUROCRYPT '94, LNCS, Springer-Verlag, 1995, pp. 1-12.
[8] A. Shamir, How to Share a Secret, Communications of the ACM, 22(1979) 612-613.
[9] E. Verheul and H. V. Tilborg, Constructions and properties of k out of n visual secret sharing schemes, Designs, Codes and Cryptography, 1997,11(2): pp.179–196.
[10] A B Rajendra and H S Sheshadri,A Study On Visual Secret Sharing Schemes Using Biometric Authentication Techniques,AJCST,Vol 1,2012,pp. 157-162