MEANINGFUL AND UNEXPANDED SHARES FOR VISUAL SECRET SHARING SCHEMES

Mr. V.B.Phadtare
Dr. V.R. Ghorpade
Dr. D.Y. Patil College of Engg. & Tech. Kolhapur

ABSTRACT

In today's internet world it is very essential to secretly share biometric data stored in the central database. There are so many options to secretly share biometric data using cryptographic computation. This work reviews and applies a perfectly secure method to secretly share biometric data, for possible use in biometric authentication and protection based on concept of visual cryptography. The basic concept of proposed approach is to secretly share private image into two meaningful and unexpanded shares (sheets) that are stored in two separate database servers such that decryption can be performed only when both shares are simultaneously available; at the same time, the individual share do not open identity of the private image. Previous research, such as Arun Ross *et al.* in 2011, was using pixel expansion for encryption, which causes the waste of storage space and transmission time. Furthermore, some researcher such as Hou and Quan's research in 2011, producing meaningless shares, which causes visually revealing existence of secret image. In this work, we review visual cryptography scheme and apply them to secretly share biometric data such as fingerprint, face images for the purpose of user authentication. So, using this technique we can secretly share biometric data over internet and only authorized user can decrypt the information.

INDEX TERMS- Meaningful, privacy, secret, sharing, shares, unexpanded, security.

INTRODUCTION

IOMETRIC systems are more consistent and more user friendly. Still there are certain issues particularly the security aspects of both biometric system and biometric data. As template is stored in centralized database, they are vulnerable to eavesdropping and attacks. This has heightened the need to accord privacy to biometric data by adequately protecting the content of the database.

Generally speaking, images, audio, and video files are usually too larger than text files. Therefore, using conventional complicated cryptographic technique to encrypt/decrypt such information seems to be rather wasting processing time. In order to preserve privacy of biometric data, the best way is to store transformed biometric template instead of the original template in the database.

In this work use of visual cryptography is explored to preserve privacy of biometric data by decomposing the original image into two images in such a way that the secret image can be revealed only when both images are simultaneously available. The basic scheme is referred as (*k, n*) VCS. For given binary image *T*, it is encrypted in *n* images, such that

$$T = S_{h1} \oplus S_{h2} \oplus S_{h3} \oplus \cdots \oplus S_{hk} \qquad (1)$$

Where $\oplus$ is a Boolean operation, S_{hi} , $h_i \in 1,2,\ldots\ldots k$ is an image which appears as white noise, $k \leq n$, and n is the number of noisy images.

In the case of (2, 2) VCS, each pixel *p* in the original image is encrypted into two sub pixels called shares. Fig 1 denotes shares of black pixel and a white pixel. Each pixel *p* from a secret binary image is encoded into *m* black and white sub pixel in each share. If *p* is white (black) pixel, one of the rows is selected randomly with equal probability, replacing *p*. Thus single share gives no clue about original value of *p.* When two shares are superimposed together, we will get the original value of pixel *p.* Therefore reconstructed image will be twice of the width of the original image and there will be a 50% loss in contrast. However the original image will become visible.

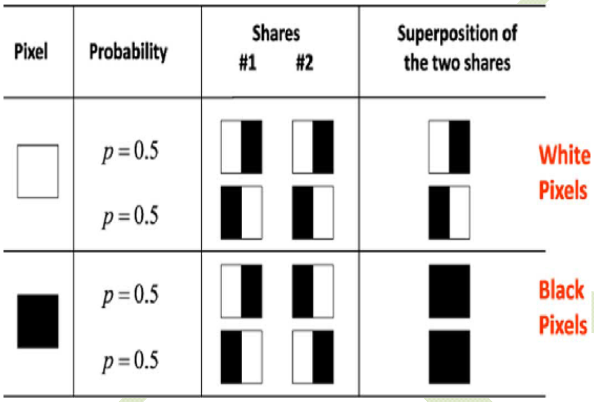


Fig. 1: Illustration of (2, 2) VCS.

RELATED WORK

Naor and Shamir [1] introduced the visual cryptography scheme (VCS) as a simple and secure way to allow the secret sharing of images without any cryptographic computation. In their approach, the secret was partitioned into *n* shares, and each participant would receive only one share. Once any *k* or more shares stacked together, the secret image will be visible without help of the computer. That is to say that secret image will be invisible if the number of stacked shares is less than *k*. This is termed as (*k*, *n*) - threshold mechanism.

In 2011, Hou and Quan [3] proposed a method of progressive VCS to share secret image with *n* participants by encrypting secret image into *n* meaningless shares. The secret image can be recovered gradually by superimposing more and more share, the detail of hidden information can be revealed progressively. However, producing meaningless shares can pique the interest of an eavesdropper by suggesting existence of secret data.

Ross *et al.* in 2011 [2] explored the use of VCS to produce meaningful shares but with pixel expansion. VCS with pixel expansion would cause a problem of wasting storage space and transmission time. Hou *et al.* [4] in 2003 used halftoned technique to simulate gray scale of an image, thus solved the problems of Naor and Shamir's [1] method which could only be applied to black and white images. Shyu [10] used random grid and halftone technique to produce shares.

Visual cryptography for general access structures

In (k,n) Basic model any 'k' shares will decode the secret image which reduces security level. To overcome this issue the basic model is extended to general access structures by G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson [7],where an access structure is a specification of all qualified and forbidden subsets of 'n' shares . Any subset of 'k' or more qualified shares can decrypt the secret image but no information can be obtained by stacking lesser number of qualified shares or by stacking disqualified shares. Construction of k out of n threshold visual cryptography scheme for general access structure is better with respect to pixel expansion than [6].

Visual cryptography for gray level Images

Previous efforts in visual cryptography were restricted to binary images which is insufficient in real time applications. Chang-ChouLin, Wen-HsiangTsai [8] proposed visual cryptography for gray level images by dithering techniques. Instead of using gray sub pixels directly to constructed shares, a dithering technique is used to convert gray level images into approximate binary images. Then existing visual cryptography schemes for binary images are applied to accomplish the work of creating shares. The effect of this scheme is still satisfactory in the aspects of increase in relative size and decoded image quality, even when the number of gray levels in the original image still reaches 256.

Recursive Threshold visual cryptography

The (k,n) visual cryptography explained in section I needs 'k' shares to reconstruct the secret image. Each share consists at most [1/k] bits of secrets. This approach suffers from inefficiency in terms of number of bits of secret conveyed per bit of shares. Recursive threshold visual cryptography proposed by Abhishek Parakh and Subhash Kak [9] eliminates this problem by hiding of smaller secrets in shares of larger secrets with secret sizes doubling at every step. When Recursive threshold visual cryptography is used in network application, network load is reduced.

Extended visual cryptography for natural images

All of the VC methods suffer from a severe limitation, which hinders the objectives of VC. The limitation lies in the fact that all shares are inherently random patterns carrying no visual information, raising the suspicion of data encryption. Mizuho NAKAJIMA and Yasushi YAMAGUCHI [10] proposed Extended visual cryptography for natural images constructs meaningful binary images as shares. This will reduce the cryptanalysts to suspect secrets from an individual shares. While the previous researches basically handle only binary images, [10] establishes the extended visual cryptography scheme suitable for natural images.

Halftone Visual Cryptography

The meaningful shares generated in Extended visual cryptography proposed by Mizuho NAKAJIMA and Yasushi YAMAGUCHI [10] was of poor quality which again increases the suspicion of data encryption. Zhi Zhou, Gonzalo R. Arce, and Giovanni Di Crescenzo proposed halftone visual cryptography which increases the quality of the meaningful shares. In halftone visual cryptography a secret binary pixel 'P' is encoded into an array of Q1 x Q2 ('m' in basic model) sub pixels, referred to as halftone cell, in each of the 'n' shares. By using halftone cells with an appropriate size, visually pleasing halftone shares can be obtained. Also maintains contrast and security.

Visual cryptography for color images

The researches in visual cryptography leads to the degradation in the quality of the decoded binary images, which makes it unsuitable for protection of color image .F. Liu,C.K. Wu X.J. Lin proposed a new approach on visual cryptography for colored images. They proposed three approaches as follows: 1. The first approach to realize color VCS is to print the colors in the secret image on the shares directly similar to basic model. It uses larger pixel expansion which reduces the quality of the decoded color image.

2. The second approach converts a color image into black and white images on the three color channels (red, green, blue or equivalently cyan, magenta, yellow), respectively, and then apply the black and white

VCS to each of the color channels. This results in decrease of pixel expansion but reduces the quality of the image due to halftone process.

3. The third approach utilizes the binary representation of the color of a pixel and encrypts the secret image at the bit-level. This results in better quality but requires devices for decryption.

Progressive visual cryptography

In traditional Color Visual Cryptography, loss of contrast makes VCS practical only when quality is not an issue, which is quite rare. The application of digital halftoning techniques results in some downgrading of the original image quality due to its inherently lossy nature and it is not possible to recover the original image from its halftone version. Duo Jin Wei-Qi Ya n,Mohan S, Kankanhalli[6] proposed a new encoding method that enables us to transform gray-scale and color images into monochrome ones without loss of any information. Incorporating this new encoding scheme into visual cryptography technique allows perfect recovery of the secret grayscale or color image.

Regional incrementing Visual Cryptography

VC schemes mentioned above usually process the content of an image as a single secret i.e all of the pixels in the secret image are shared using a single encoding rule. This type of sharing policy reveals either the entire image or nothing, and hence limits the secrets in an image to have the same secrecy property. Ran-Zan Wang [7] proposed Region Incrementing Visual cryptography for sharing visual secrets in multiple secrecy level in a single image. The 'n' level RIVC scheme, an image S is designated to multiple regions associated with secret levels, and encoded to shares with the following features: (a) Each share cannot obtain any of the secrets in S, (b) Any t(2<t<n+1) shares can be used to reveal (t-1) levels of secrets (c) the number and locations of not-yet revealed secrets are unknown to users, (d) all secrets in S can be disclosed when all of the (n+1) shares are available,

Segment based visual cryptography

The VC Methods mentioned above is based on pixels in the input image. The disadvantage of pixel based visual cryptography is loss in contrast of the reconstructed image which is directly proportional to pixel expansion 'm'. A New approach proposed by Bernd Borchert [8] was based on segments which takes pixels as the smallest unit to be encrypted .The advantage of segment based over pixel is that it may be easier for the human eye to recognize the symbols, The messages consists of numbers can be encoded by segment based visual cryptography using seven segment display.

NEED OF WORK

1. Handling secret sharing of Biometric data:

The existing implementation uses cryptography and data hiding to protect biometric data. So these methods require complicated decryption and decomposition computations. The current implementation stores secret data on single server. Handling break-ins to server are very hard to detect when the attacker simply steals certain information without modifying the store data.

2. Handling pixel expansion factor used in VCS:

The existing VCS implementation uses pixel expansion factor *m*, increasing the pixel expansion factor *m* leads to an increase in the storage requirement for the sheets.

3. Handling meaningless shares used in VCS:

The existing VCS implementation uses meaningless shares to encrypt secret image. Using meaningless shares may result in visually revealing the existence of secret image. It can pique the interest of an eavesdropper by suggesting the existence of secret data.

VISUAL CRYPTOGRAPHY SCHEME

Visual cryptography scheme (VCS) is a simple and secure way to allow secret sharing of images over internet without any cryptographic computation [1]. VCS preserves the privacy of biometric data by decomposing the original image into *n* images in such a way that the original image can be revealed only when *k* or more images are simultaneously available and individual image do not reveal any information about original image.

a) Visual cryptography for gray level images:

Previous efforts in visual cryptography were restricted to binary images which is inefficient in real time applications. Chang ChouLin *et al.* [6] proposed VCS for gray level images using dithering techniques. Dithering technique is used to convert gray level images into approximate binary images. Then existing VCS for binary images are applied to perform encryption/decryption.

b) Recursive Threshold visual cryptography:

The (*k, n*) visual cryptography needs '*k*' shares to reconstruct the secret image. Each share consists at most [*1/k*] bits of secrets. This approach suffers from inefficiency in terms of number of bits of secret conveyed per bit of shares. Recursive threshold VCS eliminates this problem by hiding of smaller secrets in shares of larger secrets.

c) Halftone Visual Cryptography

The meaningful shares generated in extended visual cryptography proposed by Nakjima and Yamaguchi [7] was of poor quality which again increases the suspicion of data encryption. Halftone visual cryptography increases the quality of the meaningful shares.

PROPOSE SCHEME

The proposed visual cryptography scheme works in two phases. Fig. 2 shows block diagram of proposed visual cryptography scheme. During the enrollment phase, private biometric data is sent to visual cryptography server. Once the visual cryptography server receives it, the private biometric data is decomposed into two images and original private biometric data is discarded. The decomposed components are then transmitted and stored in two different database servers such that individual server do not reveal any identity of secret biometric data. During the authentication phase, to authenticate claimed identity, the visual cryptography server sends a request to each server and the corresponding sheets are transmitted to it. The private image is reconstructed by superimposing received sheets thereby avoiding any complicated decryption and decoding computations.

The proposed system consists of following works,

1) To secure private face image, Iris and Fingerprint images
2) To share biometric data securely without cryptographic computation
3) To implement visual cryptography scheme with minimum pixel expansion factor *m.*

4) To implement such VCS that uses meaningful shares.

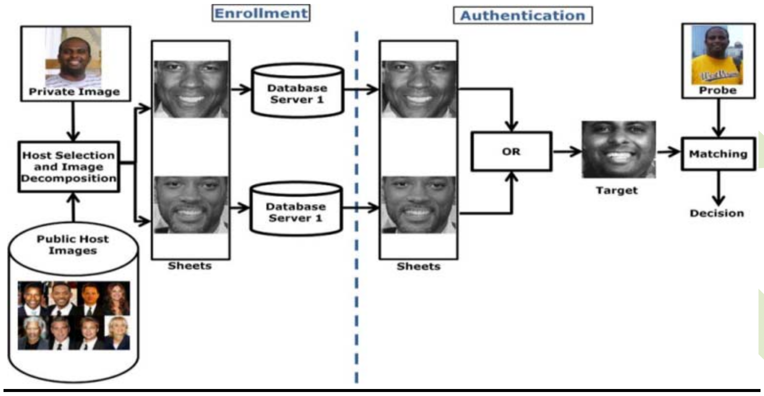


Fig. 2 Proposed approach for de-identifying and storing a private image.

The proposed system will be designed and implemented in the following modules,

1. Digital Halftoning and Error diffusion:

Digital halftoning is a technique for transforming a digital gray-scale image to an array of banary values represented as dots in the printing process. In this module private image is transformed into array of binary values and quantization error of pixel is distributed to neighboring pixel which have not yet been processed.

Error diffusion is type of halftoning technique in which the quantization error of pixel is distributed to neighboring pixels which have not yet been processed. Fig. 3 shows a binary error diffusion diagram where *f(m, n)* reprents the pixel at (*m, n*) position of the input image, *d(m, n)* is the sum of input pixel value and the diffused errors, *g*(*m, n*) is the output quantized pixel value, *h(k,l)* is error filter, *e(m, n)* is the difference between *d(m, n)* and *g(m, n)*. Finaly we compute
d(*m, n*) as

$$d(m, n) = f(m, n) - \sum_{k,\,l} h(k, l)e(m-k, n-l) \qquad (2)$$

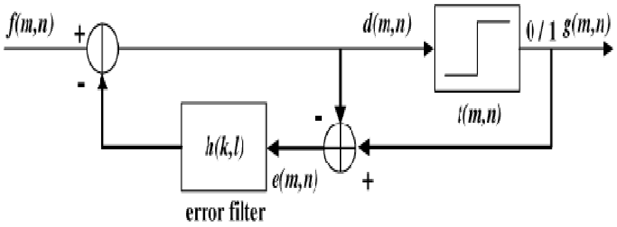


Fig. 3 Error diffusion block diagram

The filter used for error difusion is widely used filter proposed by Floyd and Steinberg

$$h(k, l) = \frac{1}{16} \times \left/ \begin{matrix} & \blacksquare & 7 \\ 3 & 5 & 1 \end{matrix} \right/ \qquad (3)$$

where ■ is thecurrent processing pixel.

2. Selection of Host images (Sheets):

This module selects host images that are most likely to be compatible with the private image based on appearance and geometry. Therefore this module characterizes shape and texture of the face using active appearance model (AAM) [2]. AAM is used to determine the similarity between the private image and host image.

3. Secret Encryption:

To perform encryption of secret image requires input in digital halftoned format and error must be diffused to neighboring pixel. During encryption phase secret image is encrypted into randomly selected two host images and operational matrix is generated which is stored in the secret VCSDB database. Also randomly selected host images are transmitted to two different servers. After encryption of private image one enrollment number is generated this is used to reconstruct private image.

The generated two host images and the operational matrix generated during encryption process are stored on two different servers. So that individual server does not reveal any information about original image.

During Encryption process two compatible host images *hm and hn* are selected randmly. Initialy assign *hm* and *hn* to S^1 and S^2 respectively. To share white pixel *(i, j),* value of pixel (*i, j*) of share S^1 is assigned to value of pixel (*i, j*) of share S^2. By the same time to share black pixel (*i, j*), complement value of pixel (*i, j*) of share S^2 is assignd to value of pixel (*i, j*) of share S^1. Detail algorithm is explained below.

Algorithm for Encryption-

Input: a W X H halftone secret image P where p (i, j) ϵ P

Output: 2 shares S^1 and S^2 of size W X H and operational matrix opr [W][H].

Process:

1. Accept secret image from user.
2. Perform scaling and digital half toning on accepted secret image.
3. Apply following algorithm to encrypt secret image.
   3.1) Select two host images *hm & hn*, ($m \neq n$ and *m, n* Є 1,2…,N) from public host database *h.*
   3.2) for each pixel p(*i, j*)

```
        if pixel $p(i, j) = 0$ AND $S^1(i, j) = = S^2(i, j)$,
            opr(i,j)=XOR;
        else
            opr(i,j)=XNOR;
        If pixel $p(i, j) = 1$ AND $S^1(i, j) = = S^2(i, j)$,
            opr(i,j)=XNOR;
        else
            opr(i,j)=XOR;
```

4. Retrieve previous enrolment number from database and calculate new enrolment number to encrypt current secret image using formula-
   Enrolment no= max (0, retrieved enrolment no) + 1.
5. Now store operational array opr, host1 *hm* and host2 *hn* on different server along with enrolment number.
6. End.

Fig.4. shows example of secret encryption. Each pixel from a secret binary image is encoded into black/white pixels in each share *h1, h2* and operation of array Opr. If *p* is a white (black) pixel, one of the four rows is selected randomly with equal probability, replacing *p*. Regardless of the value of the pixel *p*, it is replaced by a set of host pixel and operation array. Thus, the individual column gives no clue as to the original value of *p*. When pixels of *h1* and *h2* originating from pixel *p* are superimposed and performing operation specified by opr array gives original pixel p. After observing example shown in fig. 4 we can easily say that original pixel can be retrieved only when all the three things (h1, h2, opr) are simultaneously available. The probability of getting original image from operational matrix is 0.5 which can be improved by adding more operation instead of two operations.

p(i, j)	h1(i, j)	h2(i, j)	Opr(i, j)
0	0	0	XOR
	0	1	XNOR
	1	0	XNOR
	1	1	XOR
1	0	0	XNOR
	0	1	XOR
	1	0	XOR
	1	1	XNOR

Fig 4: Example of Encryption process

4. Secret Reconstruction:

This module reconstructs the original image from two Shares by superimposing two sheets and performing binary operations specified by opr matrix on each pixel. The final image is obtained by the reconstruction process that performs XOR/XNOR operation to retain the original image size.

Algorithm for Encryption-

Input: 2 shares S^1 and S^2 of size W X H and operational matrix opr[W][H].

Output: a W X H halftone secret image P

Process:

1. Accept enrollment number from user.
2. Send request to different server to obtain share S^1, S^2 and operational matrix along with enrollment number.
3. Apply following algorithm to obtain secret image.

```
3.1) for each pixel p(i, j)
        if opr(i,j)=XOR
        if $S^1(i, j)= =S^2(i, j)$
        p(i, j) =0;
        else
    p(i, j) =1;
    else
if $S^1$(i, j)= =$S^2$(i, j)
    p(i, j) =1;
        else
    p(i, j) =0;
```

Retrieve previous enrolment number from database and calculate new enrolment number to encrypt current secret image using formula-
Enrolment no= max (0, retrieved enrolment no) + 1.

4. Now store operational array opr, host *hm* and host2 *hn* on different server along with enrolment number.

5. End.

ANALYSIS PARAMETER

The analysis will be done with help of following parameters,

***1.* Pixel expansion factor:**

The number of pixel used in each share to encrypt a pixel of secret image. This parameter is helpful l to determine size require to encrypt secret image.

***2.* Equal error rate (EER):**

a. False rejection rate (FRR):

is the measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an authorized user. A system's FRR typically is stated as the ratio of the number of false rejections divided by the number of identification attempts.

b. Th*e* false acceptance rate *(FAR):*

is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. A system's FAR typically is stated as the ratio of the number of false acceptances divided by the number of identification attempts.

c. Equal error rate (EER):

A biometric security system predetermines the threshold values for its false acceptance rate and its false rejection rate, and when the rates are equal, the common value is referred to as *the* equal error rate. The value indicates that the proportion of false acceptances is equal to the proportion of false rejections. The lower the equal error rate value, the higher the accuracy of the biometric system.

Thus above parameter will be useful to analyze the better performance of the proposed system from existing system.

EXPERIMENTAL RESULTS & ANALYSIS:

Enrollment Phase (Encryption):

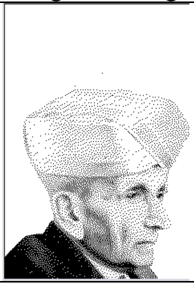
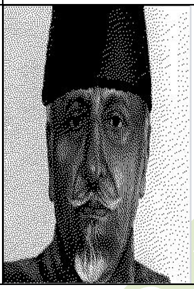
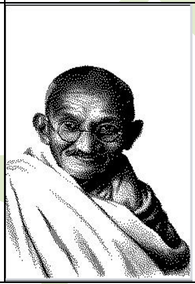
Original Image	Generated Sheet 1	Generated Sheet 2
		

Fig 4: Experiment on Enrollment Phase

After comparison of original image and generated sheets, it has been observed that original image and generated sheets are different. Generated shares do not reveal any identity of original image. Also during encryption process pixel expansion factor *m* is 1, so problem of wastes of storage space and transmission time is easily solved.

Authentication Phase (Decryption):

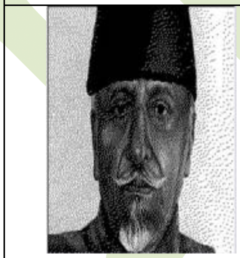
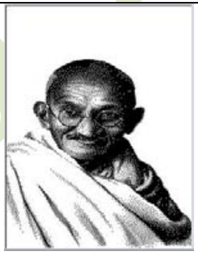
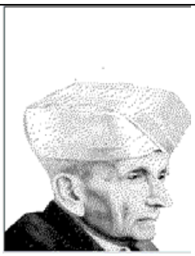
Secret Share 1	Secret Share 2	Reconstructed Image
		

Fig 5: Experiment on Authentication Phase

During authentication phase secret image is reconstructed from generated secret shares. After performing experiment it has been observed that reconstructed image and original image is same.

REFERENCES

[1] Arun Ross and Asem Othman, "*Visual Cryptography for Biometric Privacy", IEEE Transactions on Information and Security, March, 2011.*

[2] P.S. Revenkar, Anisa Anjum and W.Z. Gandhare, "*Secure Iris Authentication Using Visual Cryptography", International Journal of Computer Science and Information Security (IJCSIS), 2010.*

[3] Young-Chang Hou and Zen-Yu Quan, *"Progressive Visual Cryptography with Unexpanded Shares", IEEE Transaction on Circuit and System for Video Technology, November, 2011.*

[4] O.Kafri and E.Keren, "*Encryption of pictures and shapes by random grids", Optics Letters,Vol.12,No.6,pp.377-379,1987*

[5] Mr. V.B. Phadtare and Dr. V.R. Ghorpade, "*Visual Cryptography for Biometric Privacy with meaningful and unexpanded shares", International Journal of Multidisciplinary Educational Research (IJMER), ISSN NO- 2277-7881, Vol.- 3, Issue-3(9), pp. 115-118, March 2014.*

[6] Naor, M., and Shamir, A. (1995), *Visual cryptography, in ''Advances in Cryptology Eurocrypt '94'' (A. De Santis, Ed.), Lecture Notes in Computer Science, Vol. 950, pp. 1 12, Springer-Verlag, Berlin.*

[7] G.Ateniese,C.Blundo,A.DeSantis,D.R.S tinson, *Visual cryptography for general access structures, Proc.ICALP96,Springer,Berlin,1996, pp.416-428.*

[8] Chang-Chou Lin , Wen-Hsiang Tsai, *Visual cryptography for gray-level images by dithering techniques [Pattern Recognition Letters, v.24 n.1-3.*

[9] Abhishek Parakh, Subhash Kak: *A Recursive Threshold Visual Cryptography Scheme CoRR abs/0902.2487: (2009).*

[10] Nakajima, M. and Yamaguchi, Y., *Extended visual cryptography for natural images. Journal of WSCG. v10 i2. 303-310.*

[11] Jin, D., Yan, W. and Kankanhalli, M.S., *Progressive color visual cryptography. J. Electron. Imaging. v14 i3.*

[12] Wang, R.Z.[Ran-Zan], *Region Incrementing Visual Cryptography, SPLetters(16), No. 8, August 2009, pp. 659-662.*

[13] Bernd Borchert, Klaus Reinhardt: Abh or- und *manipulation ssichere Verschl usselung f ur Online Accounts. Patent application DE-10- 2007-018802.3, 2007*
.

[14] HU Chih-Ming, TZENG Wen-Guey, "*Cheating prevention in visual cryptography", IEEE transactions on image processing ISSN 1057-7149,2007, vol. 16, no1, pp. 36-45.*

[15] M. Nakajima and Y. Yamaguchi, **"***Extended visual cryptography for natural images," J.wscg, vol. 10, no. 2, pp. 303-310, 2002*