

A Robust Three-Way Authentication System using Modified Random Grid based Reversible Style Visual Cryptography

B. Padhmavathi
Department of Information
Technology
Meenakshi College of
Engineering ,Chennai - 078
Tamil Nadu, India

P. Nirmal Kumar
Department of Electronics &
Communication
College of Engineering,
Guindy, Anna University
Chennai - 25,Tamil Nadu

M. A. Dorai
Rangaswamy
Department of Computer
Science & Engineering
AVIT ,Vinayaka Mission
University, Chennai,
Tamil Nadu, India

ABSTRACT

The growing possibilities of modern communications require a special means of confidential and intellectual property protection against unauthorized access and use. Cryptography provides important tools for the protection of information and they are used in many aspects of computer security. This paper makes use of encrypted secret sharing to increase the security level of hidden data and to provide Mutual Authentication of the users. The visual cryptography scheme is a perfect secure method that encrypts a secret image by breaking it into shadow images. A distinctive property of visual cryptography scheme is that one can visually, without computation, decode the secret by superimposing shadow images. The property of visual secret sharing in reversible style provides more security. This method not only can fast decode without causing pixel expansion but also increase the secret-hiding ratio. Random-Grid Algorithm is used to create secret shares without pixel expansion. This paper extends the capabilities of the Visual Cryptography as a mere secret sharing technique to a Novel Mutual Authentication provider. If one stacks two transparencies (shares) together straightforwardly, a secret image will appear. Stacking two transparencies after reversing one of the transparencies, another secret image will unveil. An attempt is made to provide two transparency three-way mutual authentication by using Visual cryptography in the reversible style.

General Terms

Visual Cryptography, Secret Shares, Mutual Authentication, Encryption, Secure Communication, Secret-hiding Ratio et.al

Keywords

Visual Cryptography in Reversible style, Pixel Expansion, Random Grid Algorithm, Secret transparencies, Share Stacking.

1. INTRODUCTION

Cryptography includes a set of techniques to achieve confidentiality (amongst others) when transmitting or storing data. Traditional cryptographic schemes require end users to employ complex operations for encryption as well as decryption. An alternative to encrypt messages is visual cryptography, where the decryption is completely performed by the human visual system. This approach seems to be a very promising and user-friendly technique for security issues. However, Visual Cryptography is used to hide and carry secret information confidentially. But the technique could be extended to provide Mutual Authentication among the true users of a real time application.

In the visual secret sharing scheme [1], an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any $n-1$ shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear. But this scheme had several drawbacks like pixel expansion in shares, memory loss due to this, error in transmission etc., It was possible to create fake shares to generate fake images and thus causing Cheating attacks [2],[3] Very complicated and time consuming procedures were needed to prevent cheating attacks [4],[5],[6].

Therefore, Reversible visual cryptography scheme came into existence. Here there are two secret images; one secret image appears by stacking two shares and the other second secret image appears by stacking two shares after reversing one of them. Because there are two secret images, it is more difficult to create a fake share. However, there is a pixel expansion step in all of the methods. To avoid this another visual secret sharing approach without pixel expansion method, namely Random-grid method is used in this paper. This method neither needs an extra code book nor pixel expansion for generating shares.[7],[8].

In this paper, a non-expansion visual secret sharing method with reversible property is proposed to provide Three party Mutual Authentication. The properties of the proposed method include security, confidentiality, fast secret decoding and small share size. This idea of the proposed method can also be extended to various applications of complex visual cryptography.











2. RELATED WORK

2.1 Visual Cryptography

All material Security has become an inseparable issue as information technology is ruling the world. Cryptography is the study of mathematically related techniques to achieve Information Security in terms of confidentiality, data security, entity authentication and data origin authentication. However, it is not the only means of providing information security. Visual cryptography is a new technique which provides information security which uses simple algorithm unlike the complex, computationally intensive algorithms of traditional cryptography. This technique allows Visual information (pictures, text, etc) to be encrypted in such a way that their decryption can be performed by the human visual system, without any complex cryptographic algorithms. This

technique encrypts a secret image into shares such that stacking a sufficient number of shares reveals the secret image. Shares are usually presented in transparencies.[1]

Table 1: (2,2) Visual Cryptography Shares

PIXEL	PROBABILITY	SHARES	
		#1	#2
WHITE 	P = 0.5		
	P = 0.5		
BLACK 	P = 0.5		
	P = 0.5		

In the (2, 2) visual cryptography scheme each secret image is divided into two shares such that no information can be reconstructed from any single share. Each share is printed on a transparency. The decryption process is performed by stacking the two shares and the secret image can be visualized by naked eye without any complex cryptographic computations.

In the above basic Visual cryptography scheme each pixel ‘p’ of the secret image is encrypted into a pair of sub pixels in each of the two shares. If ‘p’ is white, one of the two columns under the white pixel in is selected. If p is black, one of the two columns under the black pixel is selected. In each case, the selection is performed randomly such that each column has 50% probability to be chosen. Then, the first two pairs of sub pixels in the selected column are assigned to share 1 and share 2, respectively. Since, in each share, p is encrypted into a black–white or white–black pair of sub pixels, an individual share gives no clue about the secret image. By stacking the two shares, if ‘p’ is white it always outputs one black and one white sub pixel, irrespective of which column of the sub pixel pairs is chosen during encryption. If ‘p’ is black, it outputs two black sub pixels

Basically, visual cryptography is the process of encoding a secret into several meaningless shares and later decoding the secret by superimposing all or some of the shares without any computation involved

2.2 Security issues of Visual Cryptography

Visual cryptography has been adopted to support some practical applications, such as image authentication, visual authentication, image hiding, and digital watermarking. Unfortunately, in many applications, visual cryptography has been shown to suffer from the "cheating problem"[4],[5] in which the disclosed secret image may be altered by malicious insiders who are called "cheaters."

While ubiquitous computing has been well developed, it has recently occurred to people in both academia and industry that research could benefit more from computational visual

cryptography by introducing light-weight computation costs in the decoding phase. In this paper, a simple scheme is proposed to conquer the cheating problem by facilitating the capability of share authentication.

It is worthwhile to note that the proposed scheme can identify for certain whether cheating attacks have occurred or not, while other schemes that have the same objective frequently provide a vague answer. In addition, the proposed scheme effectively addresses the two main problems of visual cryptography, i.e., the inconvenience of meaningless share management and the challenge of achieving difficult alignment.

2.3 Visual Cryptography in Reversible style

In order to hide the secrecy in visual cryptography we go for expansion and increasing of the number of shares, but this affects the resolution. Therefore an optimum number of shares are required to hide the secrecy. At the same time security is also an important issue. The quality of the original image or text to encrypt decreases immensely while decryption, as the loss of resolution is inevitable. Hence research in Visual cryptography is towards maintaining the contrast at the same time maintaining the security. To overcome the disadvantages and security issues of visual cryptography, Reversible Visual Cryptography scheme is used. In this scheme,

1. The increase of file size due to pixel expansion is avoided because of the Random Grid Algorithm used to create shares..
2. Each participant verifies the shares of other participants. This is somewhat necessary because each participant is a potential cheater. Thus cheating or Fake shares problem is eliminated.
3. The verification image of each participant is different and confidential. It spreads over the whole region of the share, so it is necessary for avoiding the attacks.
4. The contrast of the secret image in the stacking of shares is reduced significantly.
5. A mutual authentication is provided and is applicable for any visual cryptography scheme.

3. PROPOSED SYSTEM

Please use Reversible style system proposed a novel reversible visual secret sharing method. In this system two transparencies are created from two secret images. Without any computing, if we stack two transparencies directly, a secret image will appear. Stacking two transparencies after reversing one of transparencies, another secret image will unveil. This system focuses on multi-secret images wherein visual cryptography system uses only one image. Also in reversible style size of the pixels is not expanded.

The proposed system aims to modify the existing system by providing mutual authentication. We implement this using the concept of reversible cryptography. We are providing mutual authentication in this system in which the secret image is shared and gets authenticated on server, sender and receiver side.

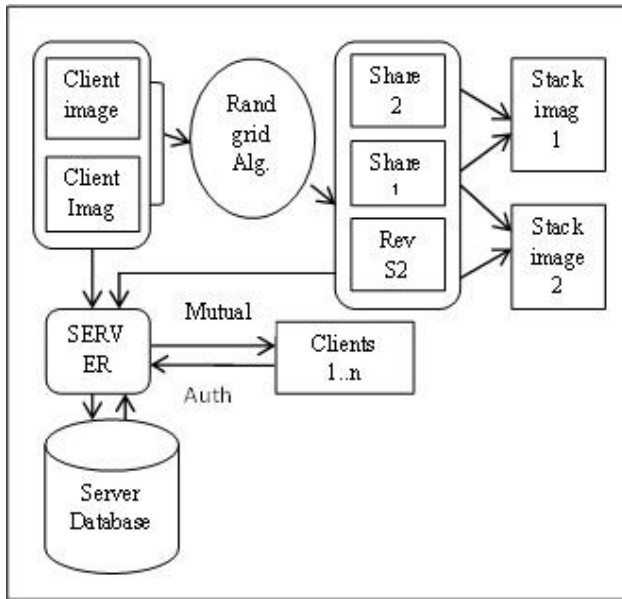


Fig. 1: Proposed Overall Architecture

The system designed in our proposed project is mainly to provide mutual authentication and transferring data in secure manner. For implementing this we have used reversible visual cryptography as basic concept. Two images are sent as input to the server. The images should be halftone and $n*n$ pixels. If they are not of required type then they will be converted to that form by halftone generation algorithm. These images taken as input are converted to two shares using random grid algorithm. One share is generated randomly and the other share is generated comparing the first share and input images. All the input images, shares and stacked result are saved in the server. The server will give one share to one client and the reversed share to other client. When the client sends this share to server they will get authenticated and their remaining share is send back to them. In this way server authenticates the client individually.

The client will stack the share sent by the server and checks whether he gets his image and then send his share to the other client. The second client stacks the share sent by the first client along with the share sent by the server and gets the stacked image sent by the first client and thus he authenticates. Hence mutual authentication is provided.

The proposed system implements the three way authentication in the following three modules.

3.1 Shares creation by Random Grid method

Visual cryptography is to encrypt a secret image into two shares (transparencies) such that any qualified subset of the shares can recover the secret “visually.” The conventional definition requires that the revealed secret images are always darker than the backgrounds.

In this module, 512 X 512 pixels Halftone images are taken as input images. If the images are colored and are of different sizes, they are converted to the halftone images of required size i.e., 512 X 512.

By using the Random Grid Algorithm of Wang et al.,[7],the shares are created. For every two images passed as input, three shares would be created. They are denoted a Share 1, Share 2 and Reversed Share 2. The algorithm first generates

empty upper and lower grids of the shares $S1U, S2U, S1L, S2L$ and then fills them with 0s and 1s by comparing each pixel with that of the input secret images. There is no pixel expansion involved and the size of the shares would be same as that of the input images. The following algorithm By Wang et.al of [7] generates the shares.

Algorithm:

Input : Original images $I1$ and $I2$, both are halftone images and the image size is 512 by 512 pixels

Output: Shares $S1, S2$ and Reversed $S2$

Step. 1 Assign the pixel values of $S1U$ randomly.

Step. 2 Assign the pixel value of $S2U$.

if $I1U[x][y] = \text{white}$ then $S2U[x][y] = S1U[x][y]$.

else $S2U[x][y] = \text{complement of } S1U[x][y]$.

end if

Step 3. Reverse $S2U$, that is $Temp[x][y] = S2U [512-x][y]$.

Step 4. Assign the pixel value of $S1L$.

if $I2L[x][y] = \text{white}$, then $S1L[x][y] = TempU[x][y]$.

else, $S1L [x][y] = \text{complement of } temp[x][y]$.

end if

Step 5. Assign the pixel value of $S2L$,

if $I1L[x][y] = \text{white}$ then $S2L[x][y] = S1L[x][y]$.

else, $S2L[x][y] = \text{complement of } S1L[x][y]$. end if

Step 6. Reverse $S2L$, that is $TempL[x][y] = S2L [512-x][y]$.

3.2 Secret Images Generation by Stacking:

The secret images are obtained as a result of bit by bit comparison of the shares and then applying BitXOR operation. The corresponding upper and lower grids of the shares $S1$ and $S2$ are stacked together to generate the first image. The stacking begins by comparing the pixels of two shares in row and column wise. If the pixels from each share are of same color, then a white pixel is generated in the resultant first secret image. If the pixels are complement to each other, then a black pixel is generated. This logical comparison is equivalent to bitwise XOR operation. Thus the shares $S1$ and $S2$ are stacked one upon the other and Secret image 1 of client 1 is revealed.

To generate the second secret image, share $S2$ is reversed to get $RevS2$. The share $S2U$ and $S2L$ is reversed from left to right, row wise and the reversed pixels are stored in temporary array. This step is described in the Random Grid share generation algorithm. By stacking this reversed share $RevS2$ with share $S1$, Secret image 2 of client 2 is revealed. The stacking operation involves the bitwise XOR operation as explained earlier.

Experimental results show the secret shares generated and the resultant client images revealed.

3.3 Three Party Mutual Authentication:

In the proposed system, the two clients are provided with a User-id and they register themselves with the server by submitting this User Id and their Secret Images. The server saves their Secret image along with their User-ids in its database. As a part of the registration, the server applies the Random Grid algorithm to generate secret shares S1,S2 and Reversed Share RevS2. It also distributes Shares S2 to client 1 and RevS2 to Client 2 retaining the Share S1 in its database against the client id. As explained in the previous modules, the stacking of the shares in their front view would reveal the Client 1's image and stacking the shares after reversing the second share would reveal client 2's image.

Whenever the clients wish to exchange some secret information, Mutual authentication phase begins. This phase establishes authentication between sender and server first and later between receiver and server. And finally ,this is followed by sender and receiver authentication. Thus a three party mutual authentication process takes place in three stages. The following algorithm gives the detailed conversations among the server, sender and receiver during the authentication process.

(i) Sender – Server Authentication :-

1. Sender : Sends his UserId, Share S2 to Server
2. Server : Stacks Share S2 with share S1 from its database and Checks for Secret Image1 of Sender(Client 1).
3. Server : If Stack Image matches with the Sender (Client 1) image against his User Id, it returns Share S1 with an Authentication success Message to Sender(Client 1).
4. Sender : Stacks its Share S2 with the received Share S1 and checks for his own Secret Image 1.

(ii) Receiver – Server Authentication :-

5. Receiver : Sends his UserId, Reverse Share RevS2 to Server.
6. Server : Stacks Reverse Share RevS2 with share S1 from its database and Checks for Secret Image2 of Receiver(Client 2).
7. Server : If Stack Image matches with the Receiver (Client 2) image against his User Id, it returns Share S1 with an Authentication success Message to Receiver(Client 2).
8. Receiver : Stacks its Share RevS2 with the received Share S1 and checks for his own Secret Image 2.

(iii) Sender –Receiver Authentication :-

9. Sender : Sends Share S2 and its UserId with a copy of the Authentication Message.
10. Receiver : Stacks Received Share S2 with S1 which is received from the Server.
11. Receiver : Checks the stacked image and identifies the authenticated sender(client 1).
12. Receiver : As an acknowledgement, it sends its personal sharre RevS2 along with the Authentication message from the server to the sender.(client 1)
13. Sender : Stacks the received RevS2 with S1 which is received from the Server.

14. Sender : Checks the stacked image and identifies the authenticated receiver.

Thus a Three-Party Mutual Authentication is established.

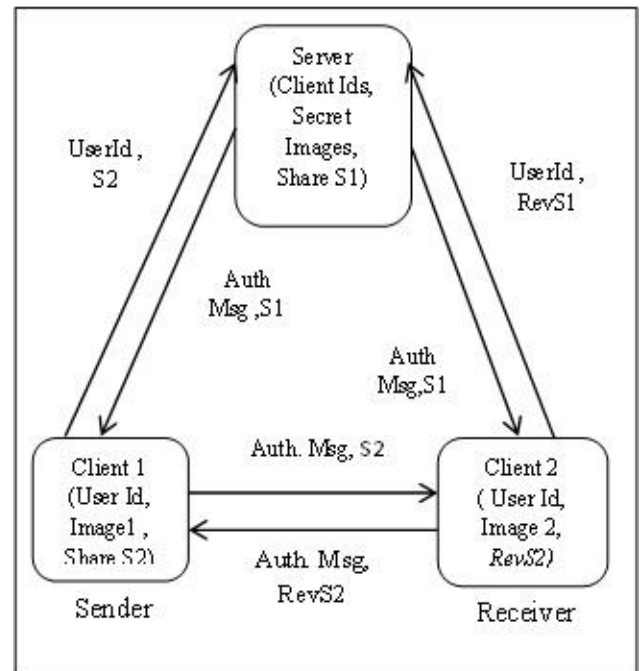


Fig 2 : Three-Party Mutual Authentication

4. EXPERIMENTAL RESULTS

For simulation we have used MATLAB 7.0 tool and tested with images of different sizes. The proposed scheme achieves effective share creation and stacking of shares. The three party mutual authentication was also tested by simulating a scenario of secret message exchange between sender and receiver. Fig. 5 depicts the results obtained on experimentation of the entire proposed Visual Cryptography scheme in reversible style. The clients photographs are taken to be their secret images. Figure 5(a) and 5(b) are the original photographs after conversion to grey scale and then applying halftoning. Figure 5(c) and 5(d) are the two shares created by the application of the Random Grid method. Figure 5(e) is the stack result of 5(c) and 5(d). This is client 1 (sender) image. Figure 5(f) is the stack result obtained after reversing (overturning) 5(d) and stacking with 5(c). This is client 2 (receiver) image. The results of mutual authentication is as shown in figure 6. This snapshot was taken when server authenticates client 1 (sender).

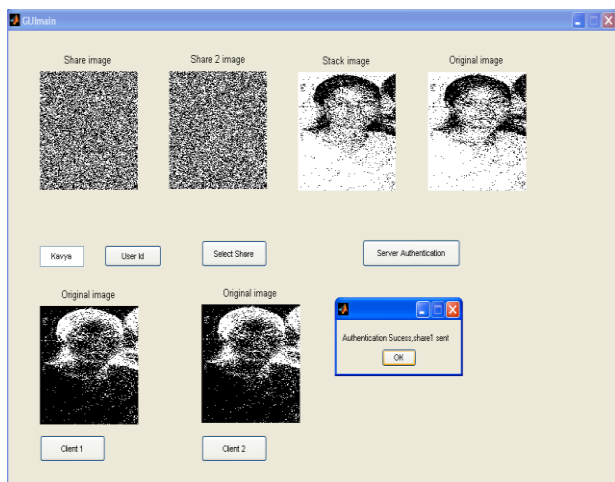


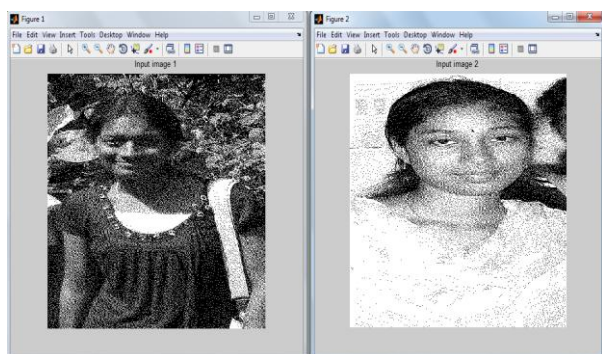
Fig2 : Experimental result showing Server Authentication of Sender (Client 1)

5. CONCLUSION

In normal visual cryptography we have pixel expansion as drawback and extra codebook is needed for stacking. Moreover they don't provide any authentication. To overcome these disadvantages we have proposed the Mutual Authentication scheme in proposed system. This system can send more than one secret images, so that multi secret sharing is enabled. In order to overcome the pixel expansion, we have used a Random grid algorithm for shares creation. In normal reversible visual cryptography after stacking the second image will not be got fully. But in the proposed system both the images are got fully as the same size as original images. In this paper we have used the concept of reversible visual cryptography for providing mutual authentication. Further this mutual authentication can be applied to many numbers of clients. By using this concept they can send many secret messages attached with the shares in a secured manner.

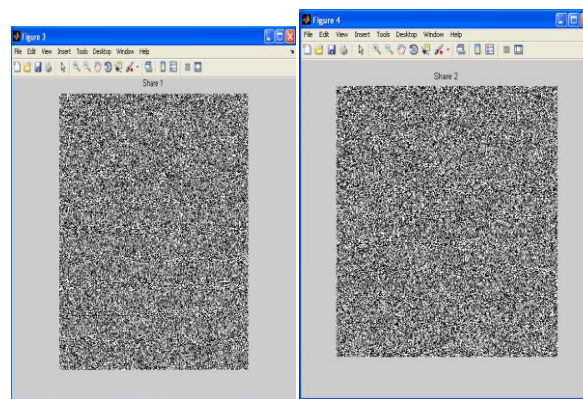
The client's photographs are considered as secret images. During shares creation, each client is provided with an UserId and one of the secret share. The clients send their share to server to receive the other share and then exchange the received shares for mutual authentication. This helps in creating a secure channel for secret message exchange between the clients.

A comparison between the existing and the proposed system with respect to key parameters is depicted in Table 2.



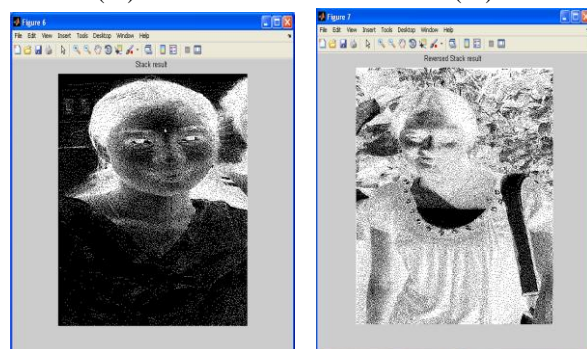
(a)

(b)



(c)

(d)



(e)

(f)

Fig 3 : (a) and (b) are client secret images, (c) and (D) are secret shares S1 and s2, (e) and (f) are stacked results

Table 2 : Comparative performance

Features for comparison	Existing System	Proposed System
Pixel Expansion	Yes	No
Extra Code Book	Yes	No
Number of Secret Images	One	Two
Secret Image Format	Only Half Tone	Any
Authentication	One Way	Mutual

6. 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] H.Yan, Z. Gan, and K. Chen, "A cheater detectable visual cryptography scheme," (in Chinese) J. Shanghai Jiaotong Univ., vol. 38, no.1, 2004.
- [3] G.-B. Horng, T.-G. Chen, and D.-S. Tsai, "Cheating in visual cryptography," Designs, Codes, Cryptog., vol. 38, no. 2, pp. 219–236, 2006.

- [4] M.A.Dorairangaswamy, "A Novel Invisible and Blind Watermarking Scheme for Copyright Protection of Digital Images," *International Journal of Computer Science and Network Security (IJCSNS)*, Vol. 9 , No. 4, pp. 71-78, 2009.
- [5] A.Dorairangaswamy,B.Padhmavathi,'An Effective Blind Watermarking Scheme for Protecting Rightful Ownership of Digital Images, Proceedings IEEE Conference. TENCN 2009,Vol 1.
- [6] B.Padhmavathi,M.A.Dorairangaswamy,P.Nirmal Kumar, 'A Robust Blind & Invisible Watermarking Scheme for Share Authentication in Visual Cryptography to prevent Cheating Attacks',Proc Intl Conf ICISA 2010 Chennai,India.
- [7] Wen-Pinn Fang,"Non-expansion Visual Secret Sharing in Reversible Style", *IJCSNS*, VOL.9 No.2, February 2009
- [8] Wen-Pinn Fang, "Visual Cryptography in reversible style,"IEEE Proceeding on the Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing(IHMSP2007), Kaohsiung, Taiwan, R.O.C, 2007, 11, 26~2007, 11, 28.
- [9] Wen-Pinn Fang and Ja-Chen Lin, "Visual Cryptography with Extra Ability of Hiding Confidential Data" *Journal of Electronic Imaging*, 15, 2006, 4.
- [10] O. Kafri and E. Keren, "Encryption of pictures and shapes by random grids," *Optics Letters*, Vol. 12, No. 6, pp. 377 - 379, 1987.
- [11] S. J. Shyu, "Image encryption by random grids," *Pattern Recognition*, Vol. 40, Issue 3, pp. 1014 - 1031, 2007.
- [12] Shamir, Visual cryptanalysis, Proceedings of the Eurocrypt 98, Espoo, 1998, pp.201-210.
- [13] M. Naor, A. Shamir, Improving the contrast via the cover base, in M.Lomas (Ed.), *Visual Cryptography II*, presented at Security in Communication Networks, Amale, Italy, Sept.1996.