

# International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: [www.ijirset.com](http://www.ijirset.com)

Vol. 8, Issue 5, May 2019

## High Secure Gray Scale Images Sharing Using Visual Cryptography Secret Sharing Scheme

Abhirami E V<sup>1</sup>, Dr.G Chithra Ganapathi ,ME , ph.D<sup>2</sup>

M.E Scholar, Dept. of CSE, CMS College of Engineering and Technology, Coimbatore, Tamil Nadu, India<sup>1</sup>

Asst. Professor & Head of the Dept, Dept. of CSE, CMS College of Engineering and Technology, Coimbatore,  
Tamil Nadu, India<sup>2</sup>

**ABSTRACT:**In this paper, a (k, n) visual secret sharing scheme using Boolean and shift operations that provides high security to the secret image is designed. An algorithm is proposed to encode the original secret image to generate n share images using simple Boolean XOR and circular shift operations. The secret data cannot be revealed with any k - 1 or less number of share images. The security is provided to the original secret by encrypting this secret with a random image and distinct authentication id used for each share during generation of shares. The size of generated share images is same as that of original image and requires no pixel expansion. The proposed scheme eliminates security issues observed in the related techniques. Experimental results confirm the feasibility and security of the proposed technique. We provide an overview of the emerging Visual Cryptography (VC) techniques used in the secure transfer of the thousands of images collected and stored in medical imagery system. In this paper, we propose a (2,2) improved gray scale visual secret sharing (IGVSS) scheme using dynamic threshold method to reduce the problems of computational complexity and pixel expansion. The proposed IGVSS scheme, to encode the secret information into meaningful shares for producing high quality share images.

**KEYWORDS:** Visual Cryptography, Improved Gray Scale Visual Secret Sharing, Medical Imagery System.

### I. INTRODUCTION

The startling innovations in information and communication technology have brought a massive change in the transmission of data to anywhere in the world making it quite effortless and easy. Various techniques like data encryption, steganography, etc., are proposed by researchers to improve security of the secret image data. But these techniques suffer from a drawback where the secured data is usually placed in the information carrier.

And an intruder has a chance to intercept this information carrier to steal or modify the original data. The secret sharing scheme divides the original data into pieces known as shares. These shares are distributed to individual l participants and then by stacking these pieces, the original data can be recovered. The original image can be reconstructed with the help of human visual system by stacking k or more share images together, while less than k share images does not give any clue about the original secret image. First of all, the contents of the secret image are encrypted by a random image of equal size using Boolean XOR operation and dividing the result by k (threshold number of shares). This is the first level of security which does not give any clue about original image. The shares  $R_i$ , for  $1 \leq i \leq n$ , are generated by circularly right shifting the encrypted image by an authenticated id. The authenticated id is unique for each share whose four most significant bits (MSBs) are the result of performing Boolean XOR operation on four most significant bits and four least significant bits (LSBs) of a random number and the four least significant bits of that random number left unchanged.

In this paper, a (k, n) visual secret sharing scheme using Boolean and shift operations that provides high security to the secret image is designed. An algorithm is proposed to encode the original secret image to generate n share images using simple Boolean XOR and circular shift operations. The secret data cannot be revealed with any k-1 or less number of

# International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: [www.ijirset.com](http://www.ijirset.com)

Vol. 8, Issue 5, May 2019

share images. The security is provided to the original secret by encrypting this secret with a random image and distinct authentication id used for each share during generation of shares.

## II. RELATED WORK

### On The Relation of Random Grid and Deterministic Visual Cryptography

Visual cryptography is a special type of secret sharing. Two models of visual cryptography have been independently studied: 1) deterministic visual cryptography, introduced by Naor and Shamir, and 2) random grid visual cryptography, introduced by Kafri and Keren. In this paper, we show that there is a strict relation between these two models. In particular, we show that to any random grid scheme corresponds a deterministic scheme and vice versa. This allows us to use results known in a model also in the other model. By exploiting the (many) results known in the deterministic model, we are able to improve several schemes and to provide many upper bounds for the random grid model and by exploiting some results known for the random grid model, we are also able to provide new schemes for the deterministic model.

### Enhanced Efficient Half toning Technique Used in Embedded Extended Visual Cryptography Strategy for Effective Processing

Visual cryptography is a fixed technique which allows visual information to be encrypted using an encoding system and decrypted by an automatic operation that doesn't need a terminal. A visual cryptography strategy (VCS) is a method of secret splitting strategy which converts a secret image into  $n$  portions of dual form. VCS is not highly-effective and highly worth, because of the security issues. Due to various disadvantages of VCS, a popular method called extended visual cryptography strategy (EVCS) was developed, where the portion images are constructed to contain expressive cover images, thereby used for biometric security techniques. In this paper, we have proposed the effective dithering halftone technique for time reduction process on generating the halftone image and also for enlightening the visual quality of the secret image.

### An Improved Secret Sharing Using Xor-Based Visual Cryptography

In order to share a secret information among a group of participants, the method of secret sharing is used. The secret sharing method that is used to share or encrypt images is called Visual Cryptography. The main problems that subsist in Visual Cryptography are pixel expansion and poor image quality. Research are being conducted to solve the above mentioned problems. In this research, effective technique of share generation based on XOR-based visual cryptography for General Access Structures is introduced. Perfect restoration of the secret, no pixel expansion and no code book requirement are the advantages that the algorithm is expected to have. The generated shares are then covered in an image using steganography which provides additional security.

### Secure Visual Secret Sharing Scheme For Color Images Using Visual Cryptography And Digital Watermarking

In today's world of digital communication, as technology progresses, there is more and more attention required on image security. Many visual cryptography algorithms have been suggested and digital watermarking in association with visual cryptography is also proposed for more image security. An image watermarking model based on progressive visual cryptography is proposed to decide optimal number of shares. A study on implementation of meaningful shares in combination with visual cryptography scheme for secret images is carried out for implementation of algorithm. A visual cryptography techniques are used to create meaningful shares.

### Enhancement of Security in Visual Cryptography System Using Cover Image Share Embedded Security Algorithm (Cisea)

Visual Cryptography is an encryption technique used to hide visual information in such a way that it can be decrypted by the human visual system, without using any decryption algorithm. There exist various schemes like digital watermarking algorithm etc. In this paper we have proposed a new algorithm to enhance the security in visual cryptography. To achieve this level of security, we have proposed a Cover Image Share Embedded security algorithm (CISEA) to produce the meaningful shares from the secret image. In this algorithm we have applied a new concept for generation of compliment images of a cover image over which the shares of secret image are to be embedded. CISEA provides one more layer of security for the images in communication channel.

## III. METHODOLOGIES

The proposed visual secret sharing technique employs Boolean XOR and circular shifting operations to encode the secret image. First, an algorithm for high secure  $(k, n)$  visual secret sharing scheme for gray scale images is proposed. Then, reconstruction and security properties for proposed method are analyzed. The security is provided by encrypting the secret image with a random image

# International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: [www.ijirset.com](http://www.ijirset.com)

Vol. 8, Issue 5, May 2019

and using distinct authentication id for each share during generation of shares. In this proposed scheme, first of all, the contents of the secret image are encrypted by a random image of equal size using Boolean XOR operation and dividing the result by k (threshold number of shares). This is the first level of security which does not give any clue about original image. The shares  $R_i$ , for  $1 \leq i \leq n$ , are generated by circularly right shifting the encrypted image by an authenticated id.

The authenticated id is unique for each share whose four most significant bits (MSBs) are the result of performing Boolean XOR operation on four most significant bits and four least significant bits (LSBs) of a random number and the four least significant bits of that random number left unchanged. Hence, the proposed scheme provides more security than other schemes proposed earlier. During secret image reconstruction phase, minimum k shares are gathered from participants and circular left shifting of each share by the respective authentication id is applied. Finally, the respective random image, supplied by the sender, is XOR with the result of circularly left shifted combined k shares to recover the original secret image.

Hence the proposed scheme does not require additional memory and bandwidth compared to the visual cryptography based schemes. No codebook design: The proposed scheme does not require any codebook for the encryption process. The proposed scheme extends to multi-user secret sharing environment of (k, n) case also.

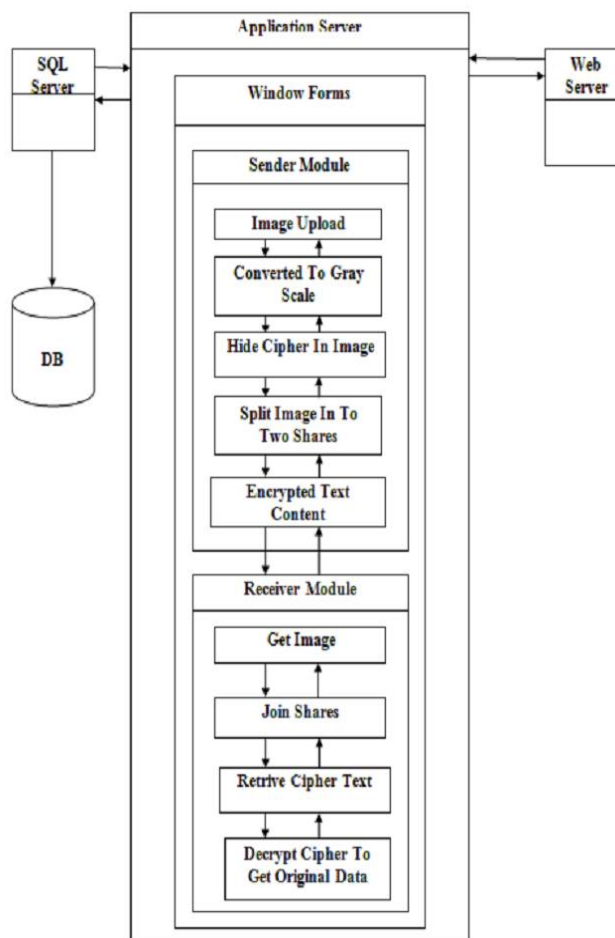


Fig 1 Proposed System Architecture

# International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: [www.ijirset.com](http://www.ijirset.com)

Vol. 8, Issue 5, May 2019

## SENDER

### Image Upload

Sender can upload image to send .The security is provided by encrypting the secret image with a random image and using distinct authentication id for each share during generation of shares. Hence high security is provided to the original secret.

### Convert to gray scale

Uploaded image is converted to gray scale image for encryption the contents of the secret image are encrypted by a random image of equal size using Boolean XOR operation and dividing the result by  $k$  (threshold number of shares). This is the first level of security which does not give any clue about original image.

### Hide cipher in image & Split image into two shares

The original text is wrapped inside the gray scale image the contents of the secret image are encrypted by a random image of equal size using Boolean XOR operation.

### Encrypted text content

The shared content is encrypted using fuzzy algorithm and cipher text is send to receiver

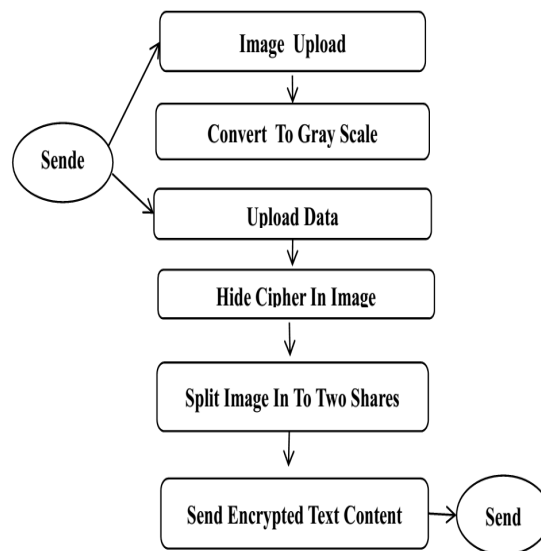


Fig 2 Encryption Management

## RECEIVER

### Upload image & Join shares

Receiver can upload image. The shared contents are joined at the receiver Side

### Retrieve cipher text & Decrypt cipher to get original data

Cipher text is retrieved from joined content by using X. The secret message is decrypted at receiver side. During secret image reconstruction phase, minimum  $k$  shares are gathered from participants and circular left shifting of each share by the respective authentication id is applied.

# International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: [www.ijirset.com](http://www.ijirset.com)

Vol. 8, Issue 5, May 2019

Finally, the respective random image, supplied by the sender, is XORed with the result of circularly left shifted combined k shares to recover the original secret image.

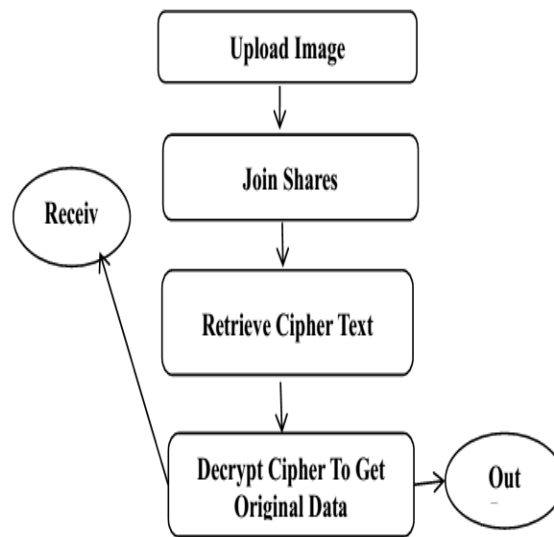


Fig 3 Decryption Management

## IV. RESULTS ANALYSIS

Implementation of the system refers to the final installing of the package in its real environment, to the satisfaction of the indeed users and the operation of the system. It is the process of converting a new or revised system design to operation. It is the key stage in achieving successful new system. The process of putting the developed system in actual use is called system implementation. This includes all those activities that take place to convert from the old system to new system. It must therefore be carefully planned and controlled. Proper guidance should be imparted to the users so that he is comfortable in using the application

# International Journal of Innovative Research in Science, Engineering and Technology

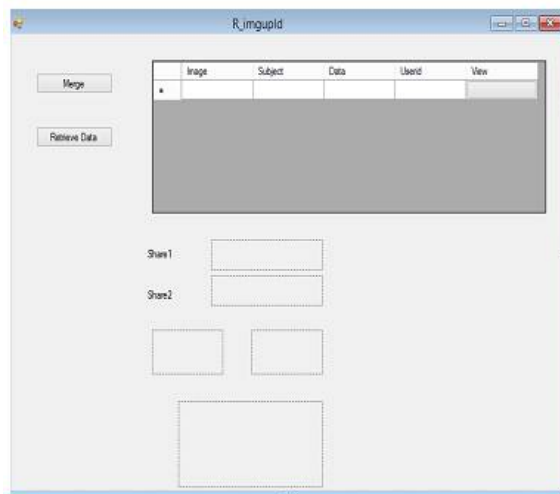
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: [www.ijirset.com](http://www.ijirset.com)

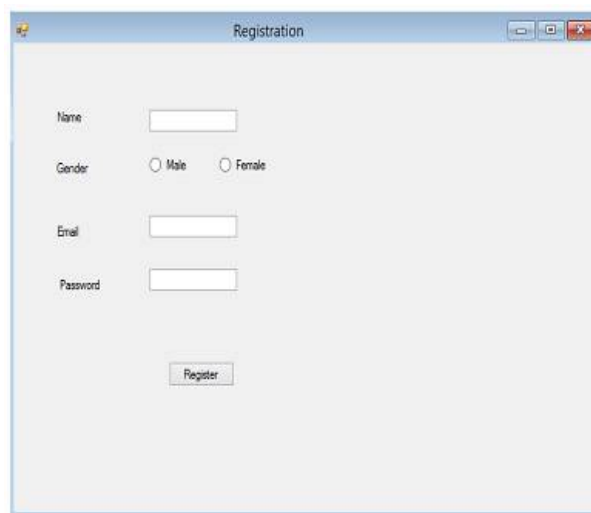
Vol. 8, Issue 5, May 2019

## SCREENSHOT

HOME PAGE



## REISTRATION FORM



The screenshot shows a registration form window titled "Registration". It contains the following fields and controls:

- Name: A text input field.
- Gender: Two radio buttons labeled "Male" and "Female".
- Email: A text input field.
- Password: A text input field.
- Register: A button at the bottom.

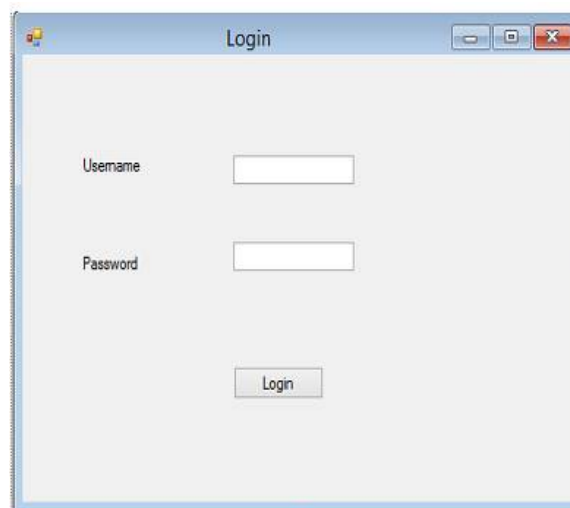
# International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: [www.ijirset.com](http://www.ijirset.com)

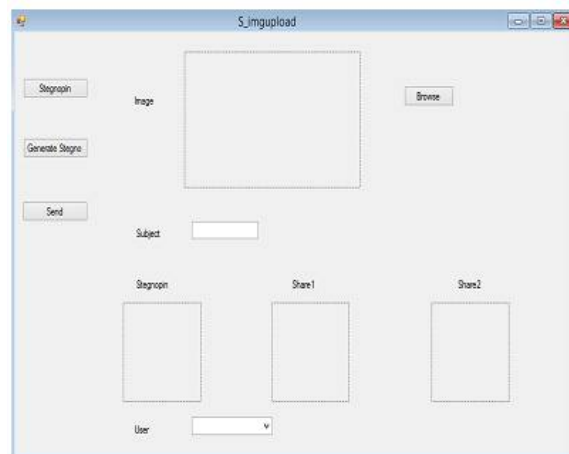
Vol. 8, Issue 5, May 2019

## LOGIN FORM



The screenshot shows a web browser window titled "Login". It contains two input fields: "Username" and "Password". Below these fields is a "Login" button. The window has standard Windows-style window controls (minimize, maximize, close) in the top right corner.

## SHARES GENERATION PAGE



The screenshot shows a web browser window titled "S\_imgupload". It features a "Browse" button next to an "Image" input field. Below the image field is a "Generate Stegno" button. There is also a "Send" button. A "Subject" input field is located below the "Generate Stegno" button. At the bottom, there are three preview boxes labeled "Stegno", "Share1", and "Share2", and a "User" dropdown menu.

## V. CONCLUSION

The visual secret sharing scheme based on Boolean XOR operations is extended by new (k,n) visual secret sharing technique which uses the concept of circular shifting to increase the security of the original secret image to a great extent. The security and recoverability of the proposed scheme is confirmed by experimental results. Hence the proposed technique satisfies the fundamental requirements of security (any  $k-1$  or fewer share images never reconstructs the original image) and recoverability (any  $k$  or more share images reveal the original secret image). And, the proposed scheme has no pixel expansion problem and codebook design in the encoding process in comparison with traditional visual cryptography schemes. This makes the proposed scheme more flexible and

# International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: [www.ijirset.com](http://www.ijirset.com)

Vol. 8, Issue 5, May 2019

adaptable. The proposed technique can be extended further to share color secret images. Also, the research can be further extended to share multiple secret images with high security.

Future Work, The system  $(k, n)$  visual secret sharing scheme using Boolean and shift operations that provides high security to the secret image is designed. An algorithm is proposed to encode the original secret image to generate  $n$  share images using simple Boolean XOR and circular shift operations. The secret data cannot be revealed with any  $k-1$  or less number of share images. The security is provided to the original secret by encrypting this secret with a random image and distinct authentication id used for each share during generation of shares. The shares are sent through different communication channels from sender to receiver so that the probability of getting sufficient shares by the intruder minimizes. But the distorted shares may arise suspicion to the hacker's mind that some secret information is passed. The original image can be encrypted using a key to provide more security to this scheme. The key may be a text or a small image. Steganography can be used by enveloping the secret shares within apparently innocent covers of digital picture. This technique is more effective in providing security from illicit attacks.

## REFERENCES

- [1] Design of High Secure Visual Secret Sharing Scheme for Gray Scale Images
- [2] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual cryptography for general access structures," *Inf. Comput.*, vol. 129, no. 2, pp. 86–106, Sep. 1996.
- [3] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Extended schemes for visual cryptography," *Theoretical Comput. Sci.*, vol. 250, pp. 143–161, Aug. 2001.
- [4] C. Blundo, S. Cimato, and A. De Santis, "Visual cryptography schemes with optimal pixel expansion," *Theoretical Comput. Sci.*, vol. 369, nos. 1–3, pp. 169–182, Dec. 2006.
- [5] Gilat, Amos (2004). MATLAB: An Introduction with Applications 2nd Edition. John Wiley & Sons.
- [6] Quarteroni, Alfio; Fausto Saleri (2006). Scientific Computing with MATLAB and Octave. Springer.
- [7] Bart M. ter Haar Geometry-Driven Diffusion in Computer Vision by Romeny (Ed.), (1994) .
- [8] M. Naor and A. Shamir, "Visual cryptography", in EUROCRYPT'94 Proceedings, Lecture Notes in Computer Science, Springer-Verlag, vol. 950, pp. 1-12, 1995.
- [9] A. Ross and A. A. Othman, "Visual Cryptography for Biometric Privacy", *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 1, pp. 70-81, 2011
- [10] G. Ateniese, C. Blundo, A. De Santis and D. R. Stinson, "Extended Capabilities for Visual Cryptography", *Theoretical Computer Science*, vol. 250, pp. 143-161, 2001.
- [11] Feng Liu and Chuankun Wu, Senior Members, IEEE, "Embedded Extended Visual Cryptography Schemes", *IEEE transactions on information forensics and security*, vol. 6, no. 2, June 2011.
- [12] Enhanced Efficient Halftoning Technique used in Embedded Extended Visual Cryptography Strategy for Effective Processing ,2015 International Conference on Computer Communication and Informatics (ICCCI -2015), Jan. 08 – 10, 2015, Coimbatore, INDIA
- [13] On the Relation of Random Grid and Deterministic Visual Cryptography Roberto De Prisco and Alfredo De Santis. *IEEE Transactions On Information Forensics And Security*, VOL. 9, NO. 4, APRIL 2014
- [14] Shankar Parimi ,A.SaiKrishna,N.Rajesh Kumar,N.R.Raajan "An imperceptible Watermarking Technique for Copyright content using Discrete Cosine Transformation",2015 International Conference on Circuit, Power and Computing Technologies [ICCPCT]
- [15] Olcay Duman and olcay Akay "A New Method of wavelet Domain WaterMark Embedding and Extraction using Fractional Fourier Transform
- [16] Shiji Johny, Anil Antony "Secure Image Transmission Using Visual Cryptography Scheme without Changing the Color of the Image", ICETECH'15 © 2015 IEEE
- [17] Ali Al-Haj, Gheith Abandah, Noor Hussein "Crypto-based algorithms for secured medical image transmission", *IET Inf. Secur.*, 2015, Vol. 9, Iss. 6, pp. 365–373 & The Institution of Engineering and Technology 2015
- [18] Hsinag-Cheh Huang, Jiun Lin, Yuh-Yih Lu "Visual Secret Sharing for Copyright Protection and Authentication of Color Images", 2015 Third International conference on Robot, vision and signal Processing © 2015 IEEE
- [19] Jena Debasish, Jena Sanjay K., "A novel visual cryptography scheme" 978-0-7695-3516-6/08 © 2008 IEEE.
- [20] M. Naor and A. Shamir, "Visual cryptography". *Advances in Cryptology EUROCRYPT*, Lecture Notes in Computer Science