ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 2, Issue 3, March 2013

A NEW LEVEL OF IMAGE PROCESSING TECHNIQUE USING CRYPTOGRAPHY AND STEGANOGRAPHY

S.Dhanalakshmi[#1] , Dr.T.Ravichandran[*2]

[#] *Department of Computer Science & Engineering, SNS College of Technology, Coimbatore-641 035, India* [1]

* *Department of Computer Science & Engineering, Hindusthan Institute of Technology, Coimbatore-641 042, India* 2

Abstract

The cryptography is the art and science of encrypting the image in such a way that no-one apart from the sender and intended recipient even realizes the original image, a form of security through obscurity. By contrast, cryptography obscures the original image, but it does not conceal the fact that it is not the actual image. RSA is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption, and was one of the first great advances in public key cryptography. To deal with this issue RSA cryptography can be used to secure Biometric Template. Cryptography and steganography provides great means for helping such security needs as well as extra layer of authentication. Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files. Then the image processing is hiding the information in images.

Index Terms: **Image Processing, Cryptography, Steganography.**

1. INTRODUCTION

Image processing is a technique to perform an algorithmic strategy to signaling an image in multidimensional systematic way. Cryptography is the technology to encrypt or decrypt any kind of digital signal or data for ensuring more securing way to transmit or receive data over any security based applications. Steganography is the more conservative technology to hide any secret information within an image. The given data is embedded into an image to hide its data. Visual Cryptography is the art of work made from formal cryptography scheme by dividing any text based information into N subsequent image frames. The main objective of our project is to use this both technology for a new level of image processing technique to ensure its most convincing level of encrypt and decrypt data using both Visual Cryptography Schemes and Steganography[2]. Cryptography and steganography are well known and widely used techniques that manipulate information (messages) in order to cipher or hide their existence. These techniques have many applications in their Computer science and other related fields: they are used to protect e-mail messages, credit card information and etc.

1.1 Image Processing

It generally refers to processing of a two-dimensional picture by a digital computer. A digital image is a representation of a two-dimensional image as a finite set of digital values, called picture elements or pixels. Pixel values typically represent gray levels, colours, heights, opacities etc [18].

Then the image processing focuses on two major tasks

- Improvement of pictorial information for human interpretation
- Processing of image data for storage, transmission and representation for autonomous machine perception.

Where image processing ends and fields such as image analysis and computer vision start. Visual cryptography is One of the techniques used to encrypt the images by dividing the original image into transparencies. The transparencies can be sent to the intended person, and at the other end the transparencies received person can decrypt the transparencies using our tool, thus gets the original image. Our proposed Visual cryptography provides the demonstration to the users to show how encryption and decryption can be done to the images. In this technology, the end user identifies an image, which is not the correct image. That is, while transmitting the image the sender will encrypt the image using our application here sender gets the two or more transparencies of the same image. Our application provides an option to the end user of encryption. The end user can divide the original image into number of different images. Using our application we can send encrypted images that are in the format of GIF and PNG. The encrypted transparencies can be saved in the machine and can be sent to the intended person by other means (source).

1.2 Image Stenography

Steganography is the art and science of invisible communication. This is the hiding information in other information, thus hiding the existence of the communicated information. Steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" defining it as "covered writing". In image steganography the information is hidden exclusively in images[4]. Extremely difficult to detect, a normal cover message was sent over an insecure channel with one of the periods on the paper containing hidden information. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels.

1.3 Visual Cryptography Schemes

Visual cryptography scheme is a cryptographic technique which allows visual information (e.g. printed text, handwritten notes, and picture) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. There are various measures on which performance of visual cryptography scheme depends, such as pixel expansion, contrast, security, accuracy, computational complexity, share generated is meaningful or meaningless, type of secret images(either binary or color) and number of secret images(either single or multiple) encrypted by the scheme. Intent of this paper is on study and performance analysis of the visual cryptography schemes on the basis of pixel expansion, number of secret images, image format and type of shares generated [20]. The source coding is used to compress data and match it with the band-width of communication channel. However, the obtained data are sensitive to the communication noise and not protected against unauthorized use. To overcome these disadvantages the next two stages are to be used[16]. To protect data against unauthorized access the encryption is accomplished. The encryption stage is performed separately from source coding.

1.4 Embedded Extended Visual Cryptography Schemes

EVCS can also be treated as a technique of steganography. One scenario of the applications of EVCS is to avoid the custom inspections, because the shares of EVCS are meaningful images, hence there are fewer chances for the shares to be suspected and detected [15]. The advantage of Steganography, over cryptography alone, is that messages do not attract attention to themselves. Plainly visible encrypted messages no matter how unbreakable will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties. Then the system is proposed with cryptography and steganography. Steganography means concealed writing, in the digital world steganography consists in hiding data inside data, it is mostly used to hide

code inside pictures or sound files but any kind of data can be hidden and any kind of file can be used as a carrier file. Another use for steganography is digital watermarking. Steganographic software is commonly used in conjunction with encryption; the message is encrypted before hiding it to add an extra layer of security, if the hidden data is ever found it would still be protected by a password.

2. RELATED WORK

Visual Cryptographic scheme Cryptography is the art of sending and receiving encrypted messages that can be decrypted only by the sender or the receiver. Encryption and decryption are accomplished by using mathematical algorithms in such a way that no one but the intended recipient can decrypt and read the message. Then the advantage of Proposed System In our proposing system we ensure multi level of security using both Cryptography and Steganography techniques. The given input data can be divided into N a subsequent layer that is based on an algorithm namely half toning, which divides the pixels of each layer into subsequent matrix format, to ensure the obscured visual frames. Thus by adding our proposed new level Stereography with this system we ensure more reliable and secure way of prevent our information.

3. PROPOSED SCHEMA FOR ENCRPTED AND DECRYPTED IMAGE

In this schema we follow the different models with encrypted and decrypted text/image.

(i) Endorsement - It is processed for proving one's identity. This module ensures that the individual who claims to be, and says about the access rights of the individual. This module acts as an interface with system by the end user, so that the end user is allowed to manipulate the system efficiently. It is used to check that the user is valid or not. Username and password entered by the user are validated. On success the authorized users are allowed to carry out further actions [10]. Invalid users are restricted. The user inputs the data/text which is to be encrypted. Fig.1. shows the authentication process.

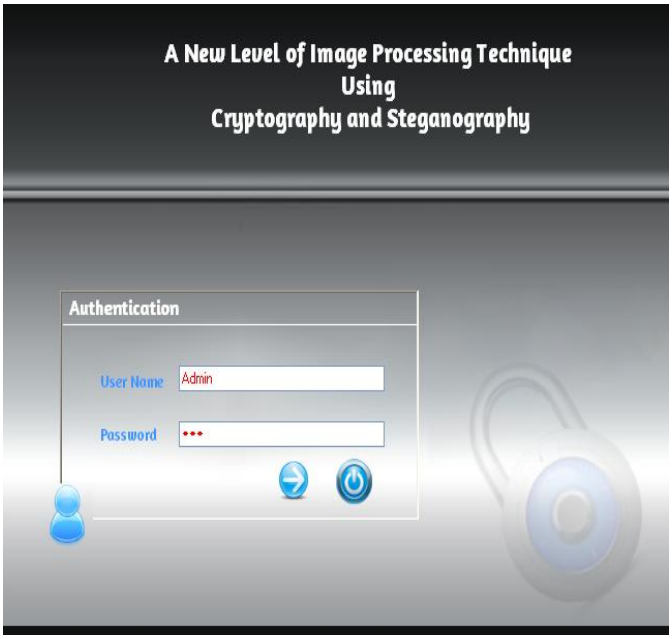


Fig.1. Authentication Process

(ii) Obscured Code/Data – In the obscured code or data is used to hide information into the image none can view the information or file. This system works base on the half toning Technique by Using Dithering Matrix [12].

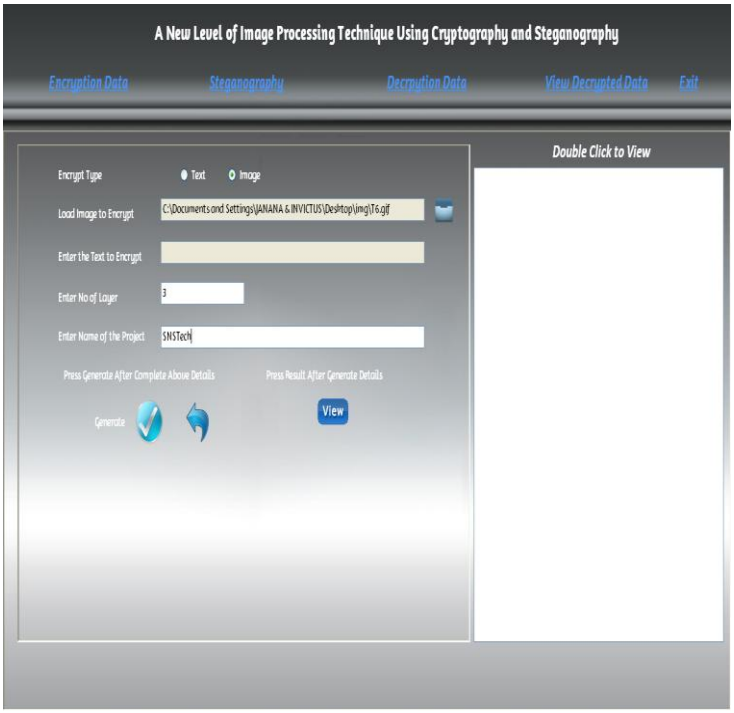


Fig.2. Encrypted Text/Image

The half toning process is to map the gray-scale pixels from the original image into the patterns with certain percentage of black pixels. The text or data is gathered from the client and the input information is encrypted into N layers based on the client or end users requirement and the N layers reside in a designated file path. Fig.2. shows the encryption text or encryption image. It is the first level which provides secure for the data or code. In this module if the code is encrypted the users cannot get the information about the secret image other than the size of the secret image**.**

(iii) Concealed Image - In this concealed image the encrypted data with N layers are covered with the image and forms as a Bitmap image file. This module deals with any type of information file and image files and the path where the user wants to save Image and extruded file. If the file is concealed, anyone who views the image will have no idea that the image contains hidden information with it, so the person will not attempt to decrypt the information. For this process the second algorithm (i.e.) the embedding process is carried over to the original encrypted image.

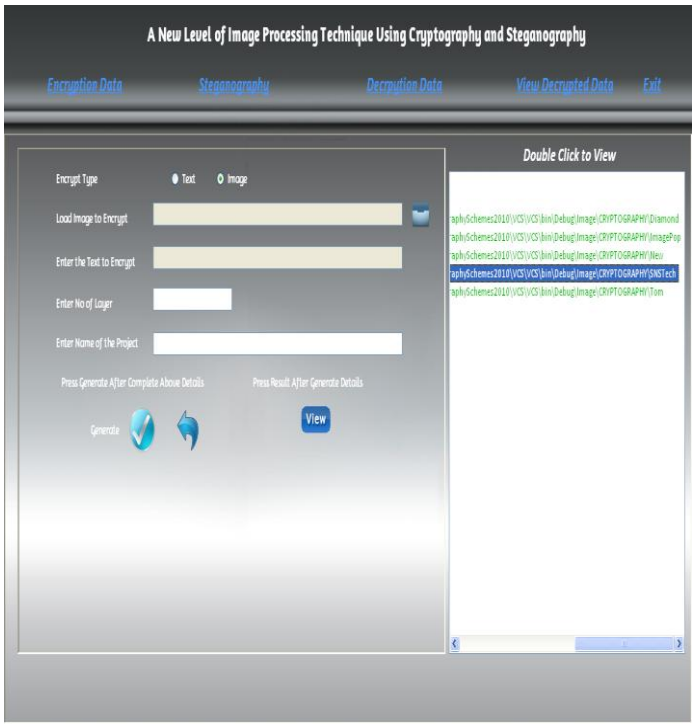


Fig.3. Monitoring Layers

The covering shares are generated which contains images and messages/text will be hidden besides the image. At this stage the file will be a bitmap file [13] [14]. Fig.3.shows the monitoring the layers.

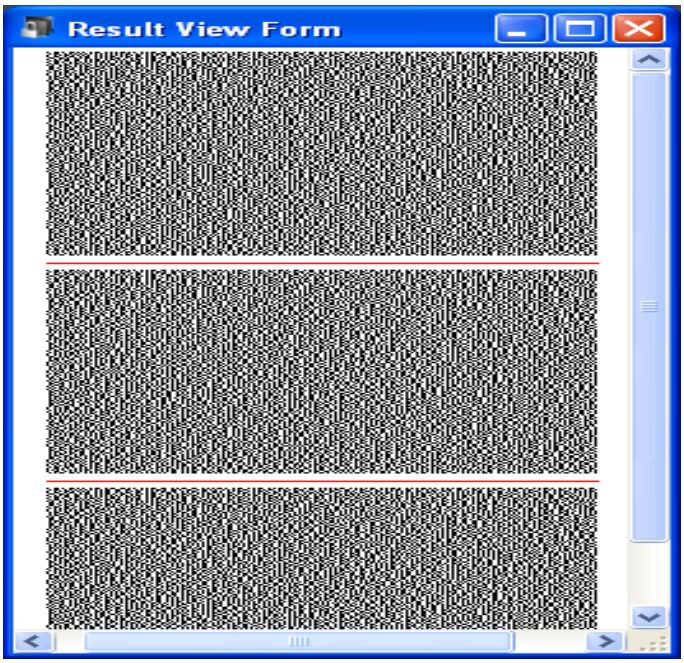


Fig.4. Result view

The image file resides at the same designated file path. This is the second level which provides secure for both messages and communicating parties. Fig.4. shows the result view form of the monitoring layers.

(*iv) Uncover Hidden Data* - This module is used to get the hidden information in an image file (i.e.). The process of converting cipher data form back into its original data. It takes the image file as output file, and sends two file at destination folder, one is the same image file and another is the message file which has been hidden with it. The final output text or data is viewed and is stored in the same file path. Fig.5. shows the steganography of the form. Then the output text or data is stored in the same path and it's monitoring the layers then the layers to view the result of the form.

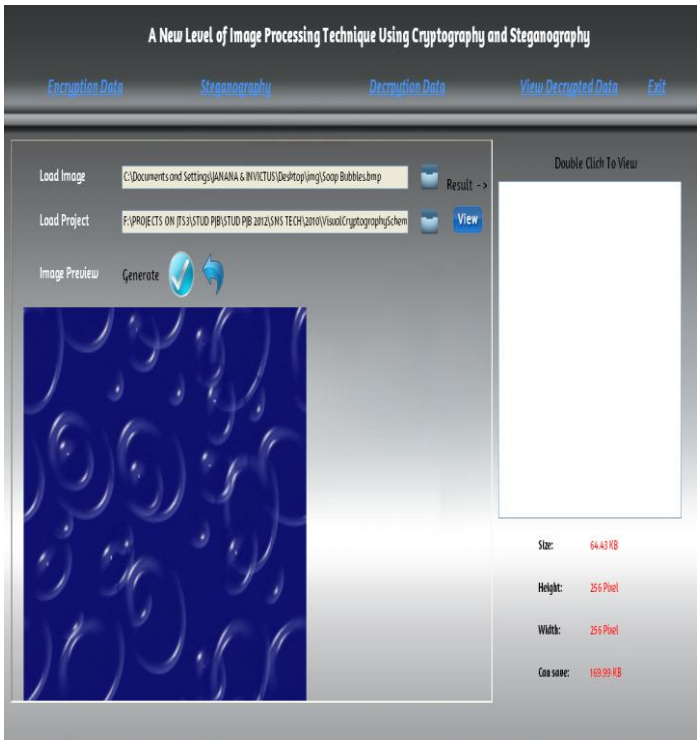
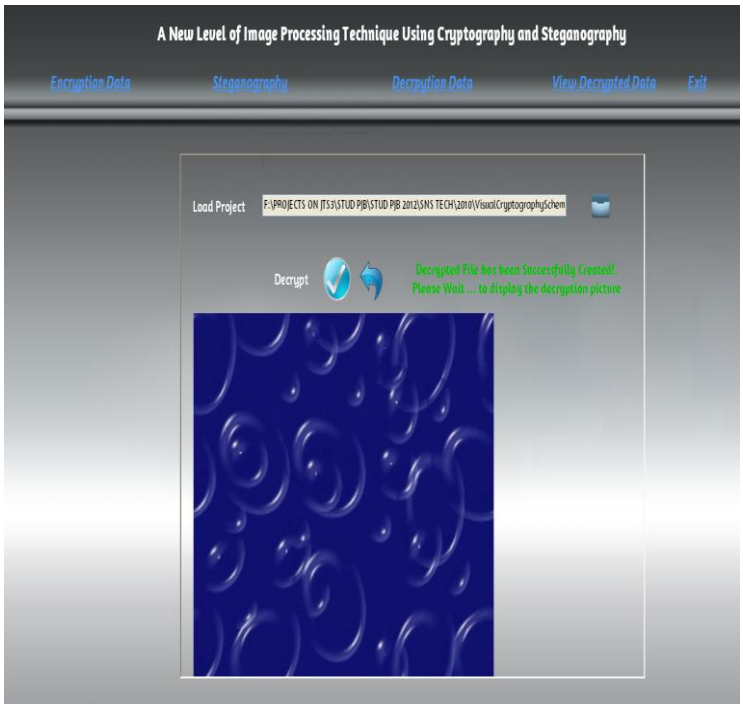
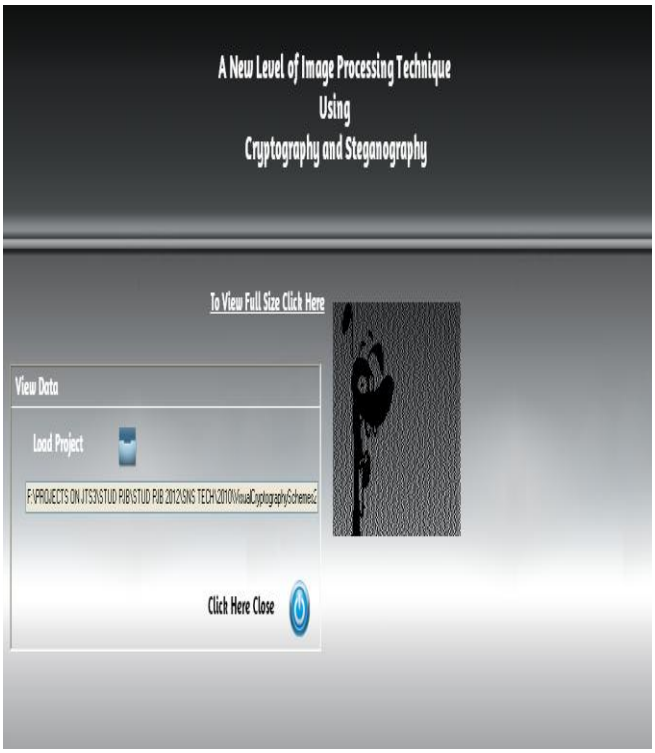


Fig.5. Steganography Form

Then the steganography of the form will appear and it's next retrieve the file and perform decryption and its save the decrypted text/image stored in same file/path. Fig 6. Shows the decrypted image.



(a)



(b)

Fig.6. (a-b) Decrypted Text/Image

3.1 Overall design Process

The design process is performed by the input design and output design. Then the input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.

- Methods for preparing input validations and steps to follow when error occur.

Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. Fig.7. shows the block diagram of design process. The goal of designing input is to make data entry easier and to be free from errors.

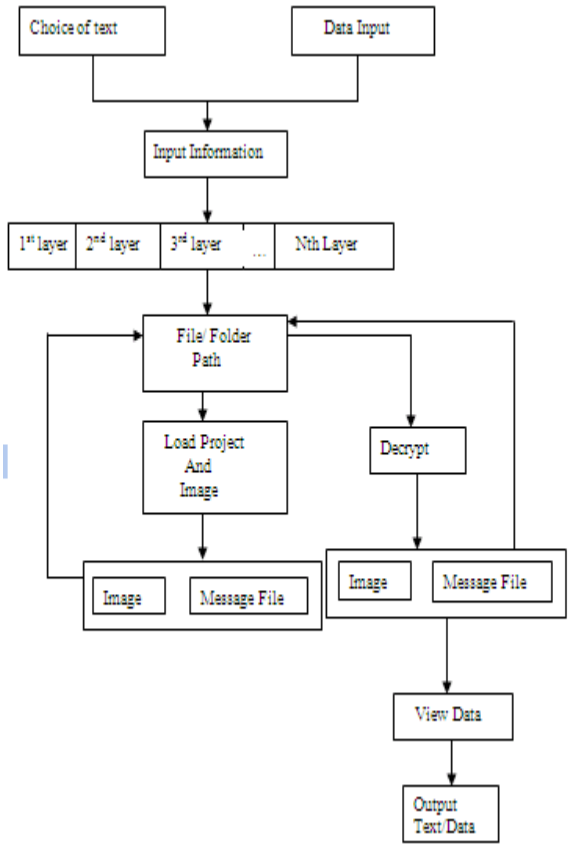


Fig.7. design proces diagram

The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities. When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow. Then the output Design a quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

- Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
- Select methods for presenting information.
- Create document, report or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives. This objectives to follow the convey information about past activities, current status or projections, Future, Signal important events, opportunities, problems, or warnings, Trigger and confirm an action.

4. CONCLUSION

The shares of the proposed scheme are meaningful images, and the stacking of a qualified subset of shares will recover the secret image visually. The project show two methods to generate the covering shares and proved the optimality on the black ratio of the threshold covering subsets. The proposed system improves the visual quality of the share images. Furthermore, the construction is flexible in the sense that there exist two trade-offs between the share pixel expansion and the visual quality of the shares and between

the secret image pixel expansion and the visual quality of the shares. In this future enhancement then this Project propose a future method to reduce the black ratio, which will enhance the visual quality of the shares. This project has been shown to be an important area of research with many implications and beneficial uses. There are still many potential areas for future projects to look into. Other areas of research that would be appropriate include steganography in auto files and Video files, the history of steganography and steganalysis and its use by government agencies to monitor Internet. There are more practical areas that if researched could lead to other software implementations like the one created for this project.

5. REFERENCES

[1] Ateniese .G, Blundo .C, De Santis .A, and Stinson .D.R (1996), "Visual cryptography for general access structures," Inf. Computed., vol. 129, pp. 86–106,.

[2] Blakely .G.R (1979), "Safeguarding cryptographic keys," in Proc. National Computer Conf., vol. 48, pp. 313–317.

[3] Blundo .C, De Bonis .A, and De Santis .A (2001), "Improved schemes For visual cryptography," Designs, Codes and Cryptography, vol. 24, pp. 255–278.

[4] C. Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, and M. Miller, "Rotation, scale, and translation resilient public watermarking for images," *IEEE Trans. Image Process.*, vol. 10, no. 5, pp. 767-782, May 2001.

[5] Chen .T.H and Tsai .D.S. (2006), "Owner-customer right protection mechanism using a watermarking scheme and a watermarking protocol," Pattern Recognition., vol. 39, pp. 1530–1541.

[6] Eisner .P.A Stinson and D.R (2002), "Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels," Designs, Codes and Cryptography, vol. 25, pp. 15–61.

[7] Limb J.O (1969), "Design of dither waveforms for quantized visual signals," Bell Syst. Technol. J., vol. 48, no. 7, pp. 2555–2582.

[8] Luo .H, Yu .F.X, Pan .J.S, and Lu .Z.M (2008), "Robust and progressive color image visual secret sharing cooperated with data hiding," in Proc. 2008 Eighth Int. Conf. Intelligent Systems Design and Applications, vol. 3, pp. 431–436.

[9] Macpherson (2002) "Grey Level Visual Cryptography For General Access Structures," Master Thesis, University of Waterloo,Waterloo,On,Canada

[10] Nair .M and Shamir .A (1995), "Visual cryptography," in Proc. EUROCRYPT' 94, Berlin, Germany, vol. 950, pp. 1–12, Springer-Verlag , LNCS.

[11] Naor .M and Pinkas .B (1997), "Visual authentication and identification," in Proc. CRYPTO'97, vol. 1294, pp. 322–336, Springer-Vela LNCS.

[12] Nakajima .M and Yamaguchi .Y (2002), "Extended visual cryptography for natural images," in Proc. WSCG Conference pp. 303–412.

[13] Prakash .N.K and Govindaraju .S (2007), "Visual secret sharing schemes for color images using half toning," in Proc. Int. Conf. Computational Intelligence and Multimedia Applications, vol. 3, pp. 174–178.

[14] Shamir .A (1979), "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613.

[15] Shyu .S.J, Huang .S.Y, Lee .Y.K, Wang .R.Z, and Chen .K (2007), "Sharing multiple secrets in visual cryptography," Pattern Recognition., vol. 40, no. 12, pp. 3633–3651.

[16] Simmons G. J, Jackson W, and Martin K (1991)."The geometry of shared secret schemes", Bull. ICA,pp 71-88.

[17] Tsai .D.C, Chenc.T and Horng.G (2008)"On Generating Meaningful Shares In Visual Secret Sharing Scheme".Imag.Sci.J.,vol.56,pp.49-55.

[18] Tuyls .P, Kevenaar .T, Shriven .G.J, Staring .T, and Van Dijk .M (2004), "Security displays enabling secure communications," in Proc. First Int. Conf. Pervasive Computing, Bopp. ard Germany, Springer-Verlag Berlin LNCS, vol. 2802, pp. 271–284.

[19] Wang.Z.M and Arce .G.R, (2006) "Halftone visual cryptography through error diffusion," in IEEE Int. Conf. Image Processing, pp. 109–112.

[20] Wang Z. M and Arce G. R and Di Crescenzo G (2006) "Halftone visual cryptography via direct binary search," in proc.EUSIPCO, 06, Florence, Italy.

[21] Wang.D.S, Yi.F, and Li.X.B,"On general construction for extended visual cryptography schemes," Pattern Recognit.,vol.42,pp.3071-3082.