A Lossless data compression algorithm for Secret Image Sharing

V.S.Nikhita Dabbiru[1], Mr. CH. Kodanda Ramu[2], Mr.Y.Ramesh Kumar [3]

PG Scholar, Dept of C.S.E.,Avanthi College of Enginerring,Visakhapatnam,India[1]

Assistant Professor, Dept of C.S.E.,Avanthi College of Enginerring,Visakhapatnam,India[2]

Professor, Dept of C.S.E.,Avanthi College of Enginerring,Visakhapatnam,India[3]

Abstract: Information is increasingly important in our daily life. Information gets more value when shared with others. Due to advances in technologies related to networking and communication, it is possible to share the information like audio, video and image easily. It may give rise to security related issues. Attackers may try to access unauthorized data and misuse it. To solve this problem certain techniques are required. Techniques to provide security, while sharing information are termed as Secret sharing schemes. When it comes to visual information like image and video, it is termed as Visual secret sharing scheme. Visual cryptography (VC) is a technique used for protecting image-based secrets. The basic concept of visual cryptography scheme is, to split secret image into some shares, which separately reveals no knowledge about the secret information. Shares are then distributed to participants. By stacking these shares directly, secret information can be revealed and visually recognized. All shares are necessary to combine to reveal the secret image. The best part is secret image is revealed by overlaying the shares without any complex computation involved. Starting from the basic model, many visual cryptographic techniques have been evolved day by day.

An extended visual cryptography scheme (EVCS) is a kind of VCS which consists of meaningful shares (compared to the random shares of traditional VCS). In this paper, I propose a construction of EVCS which is realized by embedding random shares into meaningful covering shares, and it is called embedded EVCS. Experimental results compare some of the well-known EVCSs proposed in recent years systematically, and show that the proposed embedded EVCS has competitive visual quality compared with many of the well-known EVCSs in the literature. In addition, it has many specific advantages against these well-known EVCSs, respectively. In this paper I propose, an invisible watermarking technique is proposed, to embed multiple binary watermarks into digital medical images based on the concept of Visual Cryptography (VC). The proposed scheme embeds the watermarks without modifying the original host image.

Keywords: Information security, Secret sharing scheme, Visual Cryptography, Data hiding
.

I. INTRODUCTION

Cryptography is a technique where the plain text is converted into cipher text on sender side and this process is known as encryption and the cipher text is converted into plain text on receiver side which is known as decryption process. In order to protect the data Visual Cryptography is a technique which was invented by Moni Naor and Adi Shamir in 1994 which allows visual information like pictures, text, data to be encrypted in such a way that decryption becomes a very easy operation that does not require any type of computation or computer. Visual Cryptography Scheme (VCS) is a kind of secret sharing scheme which allows the encryption of a secret image into n shares that are distributed to n participants. The most important property of visual cryptography scheme is that, the decryption of the secret images requires neither the knowledge of cryptography nor complex computation. The decoder is a human visual system and we can easily recover the secret by using the eyes of human being without the help of any computing devices. VCS is a kind of secret sharing scheme that focuses on sharing secret images. For e.g. as given in the figure given below, shares (a) and share (b) are distributed to two participants secretly, and each participant cannot get any information about the secret image, but after overlaying these shares (a) and (b), the secret image can be observed visually by the participants.

EXTENDED VISUAL CRYPTOGRAPHY (EVCS)

Extended Visual Cryptography is a type of Visual Cryptography which is capable of generating meaningful shares and which reconstructs the image by stacking some meaningful images together. Generally the Extended Visual Cryptography Scheme (EVCS) takes a secret image and n original shares images as input and output n shares which satisfy three conditions as follows:

a)   Any qualified subset of shares can recover the secret image.

b) Any forbidden subset of shares cannot obtain any information of the secret image other than the size of the secret image
c) All the shares are meaningful images

II. EXISTING SYSTEM

Visual Cryptographyis 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.

Limitations:

❖ The existing system does not provide a friendly environment to encrypt or decrypt the data (images).
❖ The existing system supports with only one type of image format only. For example, if it is .jpg, then it supports only that same kind of image format only.

II. PROPOSED SYSTEM

Visual cryptography is one of the techniques used to encrypt the images by dividing the original image into transparencies which can be sent to the intended person, and at the other end the person who receives the transparencies can decrypt the transparencies using the tool, thus can get the original image. The 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 it using our application and gets two or more transparencies of the same image. 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].

This application provides a friendly environment to deal with images. Generally cryptography tools support only one kind of image format. This application supports .gif and .png (portable network graphics) formatted images and our application has been developed using swing and applet technologies, thus providing a friendly environment to users. In this paper an invisible watermarking technique is proposed, to embed multiple binary watermarks into digital medical images based on the concept of Visual Cryptography (VC). The proposed scheme embeds the watermarks without modifying the original host image.

III. EXPERIMENTAL RESULTS
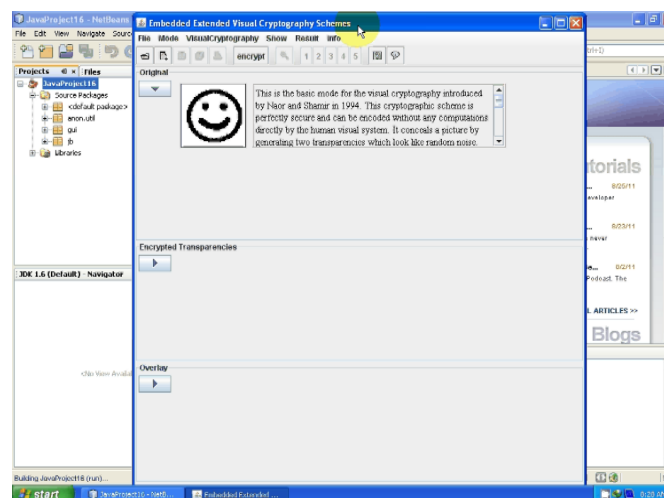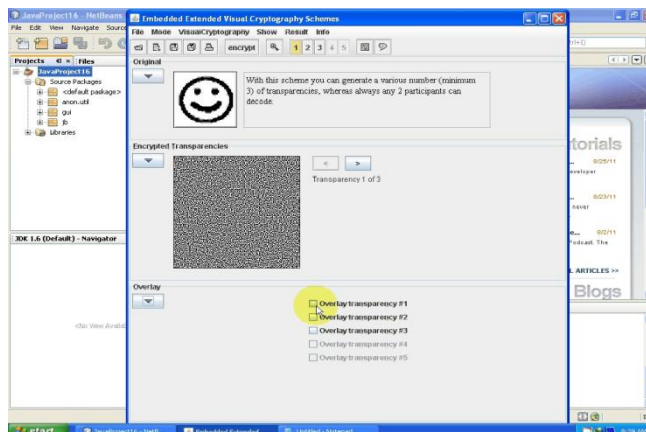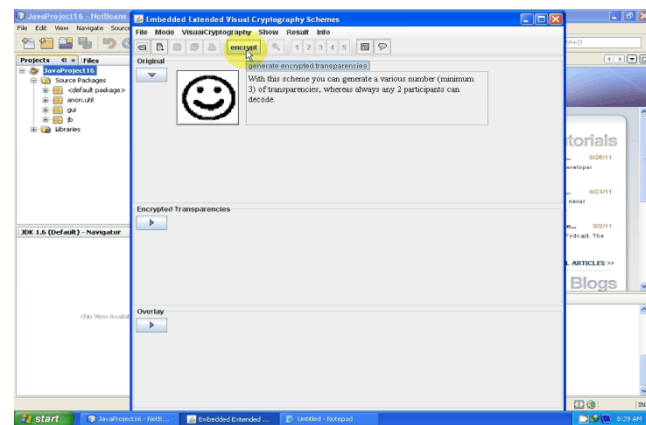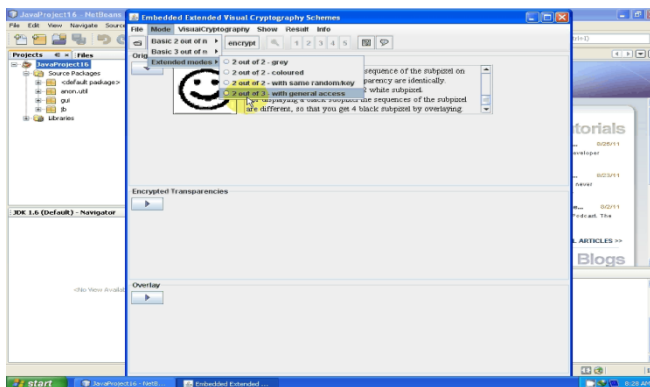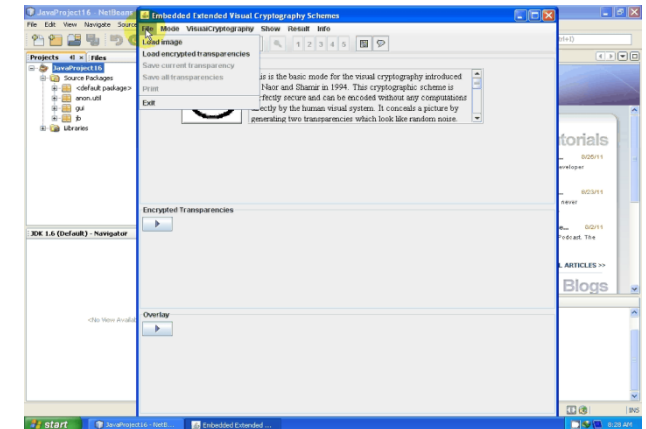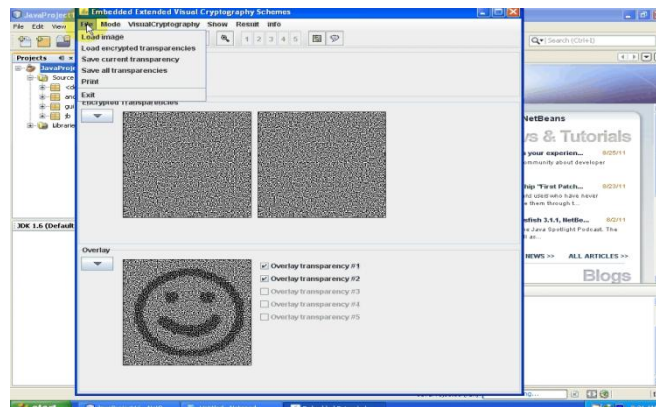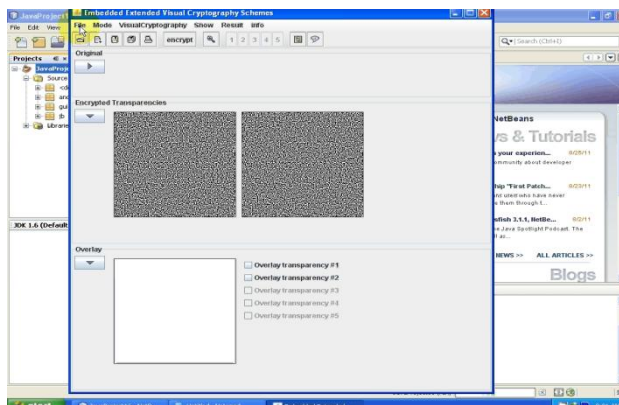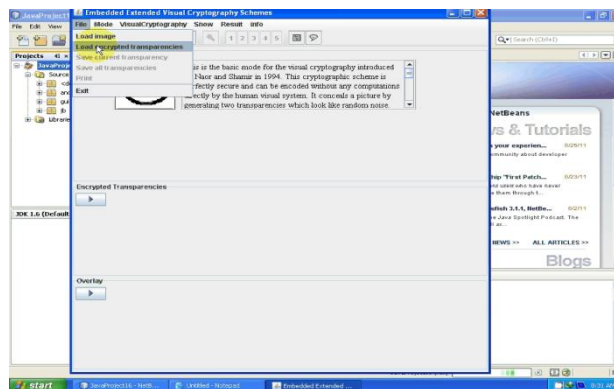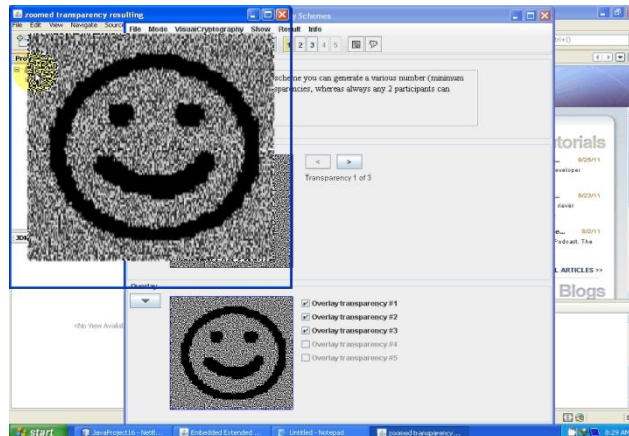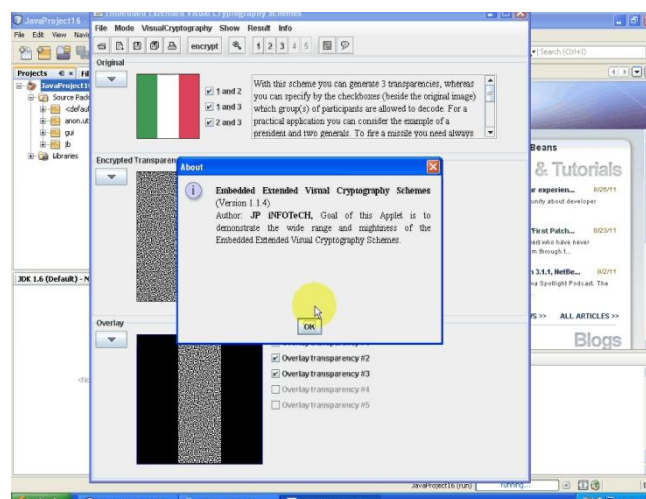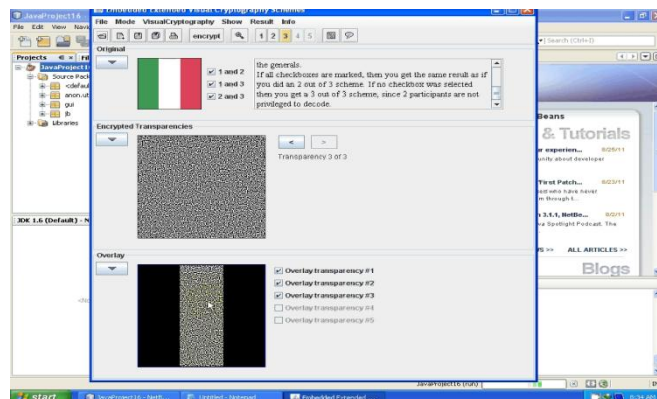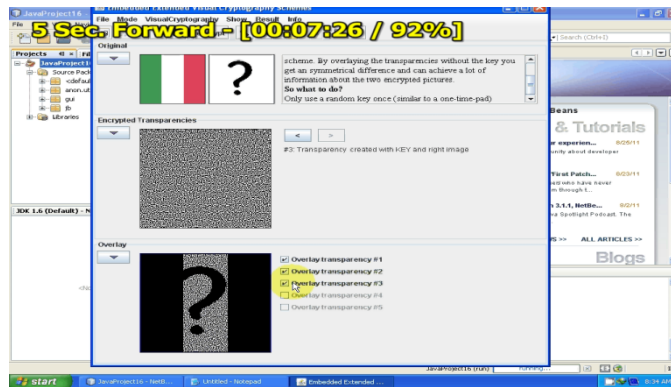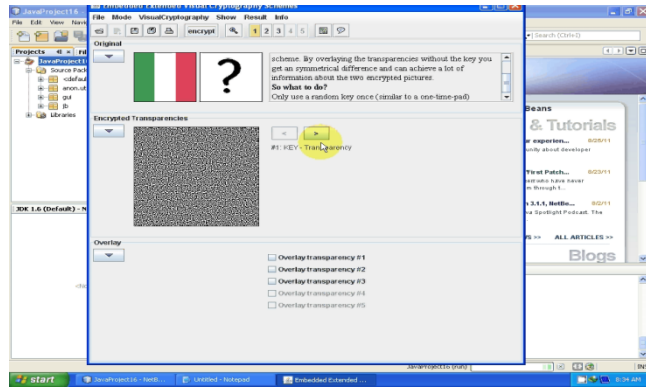
V.CONCLUSION

Providing security to the digital information shared in day to day life is an important issue in real life. Since the origin of Visual cryptography, various extensions have been developed to improve the things, ranging from (2, 2), (k, n) to progressive visual cryptography models, black and white to color images and random dot like shares to meaningful shares. Many researches carried out on these extensions, still there is much scope to do research in progressive visual cryptography, Region Incrementing Visual Cryptography, Segment based Visual Cryptography Scheme and overcome the common limitations of these techniques like large pixel expansion and lower contrast.

REFERENCES

[1] A. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.
[2] G. R. Blakley, "Safeguarding cryptographic keys," in Proc. National Computer Conf., 1979, vol. 48, pp. 313–317.
[3] M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT' 94, Berlin, Germany, 1995, vol. 950, pp. 1–12, Springer-Verlag, LNCS.
[4] M. Naor and B. Pinkas, "Visual authentication and identification," in Proc. CRYPTO'97, 1997, vol. 1294, pp. 322–336, Springer-Verlag LNCS.
[5] T. H. Chen and D. S. Tsai, "Owner-customer right protection mechanism using a watermarking scheme and a watermarking protocol," Pattern Recognit., vol. 39, pp. 1530–1541, 2006.
[6] P. Tuyls, T. Kevenaar, G. J. Schrijen, T. Staring, and M. Van Dijk, "Security displays enabling secure communications," in Proc. First Int. Conf. Pervasive Computing, Boppard Germany, Springer-Verlag Berlin LNCS, 2004, vol. 2802, pp. 271–284.
[7] C. Blundo, A. De Bonis, and A. De Santis, "Improved schemes for visual cryptography," Designs, Codes and Cryptography, vol. 24, pp. 255–278, 2001.
[8] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual cryptography for general access structures," Inf. Computat., vol. 129, pp. 86–106, 1996.
[9] N. K. Prakash and S. Govindaraju, "Visual secret sharing schemes for color images using halftoning," in Proc. Int. Conf. Computational Intelligence and Multimedia Applications (ICCIMA 2007), 2007, vol. 3, pp. 174–178.
[10] H. Luo, F.X.Yu, J. S. Pan, and Z. M. Lu, "Robust and progressive color image visual secret sharing cooperated with data hiding," in Proc. 2008 Eighth Int. Conf. Intelligent Systems Design and Applications, 2008, vol. 3, pp. 431–436.

BIOGRAPHIES

V.S.Nikhita Dabbiru is a PG scholar in computer science and engineering Department, Avanthi College Of Engineering Bhogapuram, Visakhapatnam, India. She received his Bachelor degree in 2013. Her research interests are image Processing, computer Networks, Algorithms. Etc....

Mr. CH. Kodanda Ramu is a Assistant Professor in computer science and engineering Department, Avanthi Institute Of Engineering & Technology, Bhogapuram, Visakhapatnam, India. His research interests are image processing, Computer Networks, Data Mining

Mr.Y.Ramesh Kumar is a Professor in computer science and engineering Department, Avanthi Institute Of Engineering & Technology, Bhogapuram, Visakhapatnam, India. His research interests are image processing, Computer Networks, Data