

# Secret Digital Image Sharing by various Image Media using NVSS Scheme

Satish.B.N<sup>1</sup> P.Praveen.Kumar<sup>2</sup>

<sup>1</sup>Professor <sup>2</sup>M.Tech. Student (Signal Processing)

<sup>1,2</sup>Department of Electronics and Communication Engineering

<sup>1,2</sup>Citech, Bangalore, Karnataka

**Abstract**— Secure digital image sharing is a new concept of providing security to digital images. Now a day's security is most important issue. So this project gives an idea about the sharing digital image in different medias without affecting its privacy. Conventional visual secret sharing (VSS) technique hides secret images in shares. The images may be either printed on transparencies or are encoded and stored in a digital form. The shares can be appear as noise-like pixels or as meaningful images, but it will cause intuition and increase interception risk during transmission of the shares. Hence, VSS schemes suffer from a transmission risk problem for the secret itself and for the participants who are involved in the VSS scheme. To overcome this problem, we proposed a natural image based VSS scheme (NVSS scheme) that shares secret images via various carrier media to protect the secret and the participants during the transmission phase. The proposed (n, n) - NVSS scheme can share one digital secret image over n-1 arbitrary selected natural images (called natural shares) and one noise-like share. The natural shares can be photos or hand-painted pictures in digital form or in printed form. The noise-like share is generated based on these natural shares and the secret image. The unaltered natural shares are many and harmless, thus greatly reducing the transmission risk problem. We also propose possible ways to hide the noise-like share to reduce the transmission risk problem for the share. The results indicate that the proposed approach is an excellent solution for solving the transmission risk problem for the VSS schemes.

**Key words:** VSS, NVSS, Secure Digital Image Sharing

## I. INTRODUCTION

In day today life data is progressively vital and gets more esteem when imparted to others. Because of networking and communication media, it is utilized to share the essential data like images, audio, pictures effectively. Programmers attempted to get to unapproved data. To tackle this issue certain strategies are utilized so we can give more security in sharing advanced pictures. Today in this innovative period sharing visual secret pictures has turned into an essential issue today. So the visual secret images can be of distinctive sorts, for example, manually written documents, photographs and others. At the point when we need to share these sorts of pictures safely we may get so issues so to illuminate these issues we concoct certain methods to tackle these issues and offer the any sort of the pictures safely with no danger while sharing.

Visual cryptography (VC) is one the technique and is only the isolating or encryption of secret pictures into the n number of shares and these shares are meaningful shares and that image is significant image.

Watermarking is the method of concealing the secret information or the image into another image or

information. That another image is only the transporter image in which we are putting away our secret image or information.

Visual secret sharing scheme (VSS) is a method used to conceal secret images that may be either printed transparencies or are encoded and put away in advanced form. Visual secret sharing strategy was initially persuaded to share secret images in non-PC helped environment. Visual secret sharing is a system used to convey and transmit secret images.

Conventional visual secret sharing is one of the systems in visual secret sharing scheme. In the routine visual secret sharing it is comprise of such a variety of arbitrary and pointless pixels which fulfill security prerequisite for securing secret information.

Natural image based visual secret sharing scheme (NVSS) is a technique that is acquainted with beat the all issues of past routines. NVSS utilizes various media as a transporter.

Conventional visual secret sharing (VSS) schemes hide secret images but it has interception risk during transmission of the shares. Hence, VSS schemes suffer from a transmission risk problem for the secret itself and for the participants who are involved in the VSS scheme and it is not user friendly.

In this paper Section II clearly provides the proposed methods along with frame work of algorithm, basic requirements to designs need for the algorithms. Section III discusses implementation of the algorithm along with flowchart and image features extraction from the model based parameters. Section IV describes the software tool required for the algorithm. Section V gives the simulation results and followed by the conclusion and future work in Section VI, ending with relevant references.

## II. SYSTEM ARCHITECTURE

The System architecture, Fig. 1 shows the block diagram of the In NVSS (Natural picture Based Visual secret sharing scheme), computerized secret picture over n-1 randomly natural pictures and one offer. This methodology extracts features from every normal offer. These unaltered natural shares are enormously diminishing the interception possibility of these shares. The created noise like shares can be covered by utilizing information hiding techniques to build security level during transmission of data. In this system secret image and important shares are taken as input feature extraction calculation and encryption algorithm to acquire uproarious offer are connected. Further more security reason, the noise share are implanted with carrier picture and steganography strategy is applied to get a steno picture. Applying unscrambling and de-steganography, the recouped mystery picture is obtained.

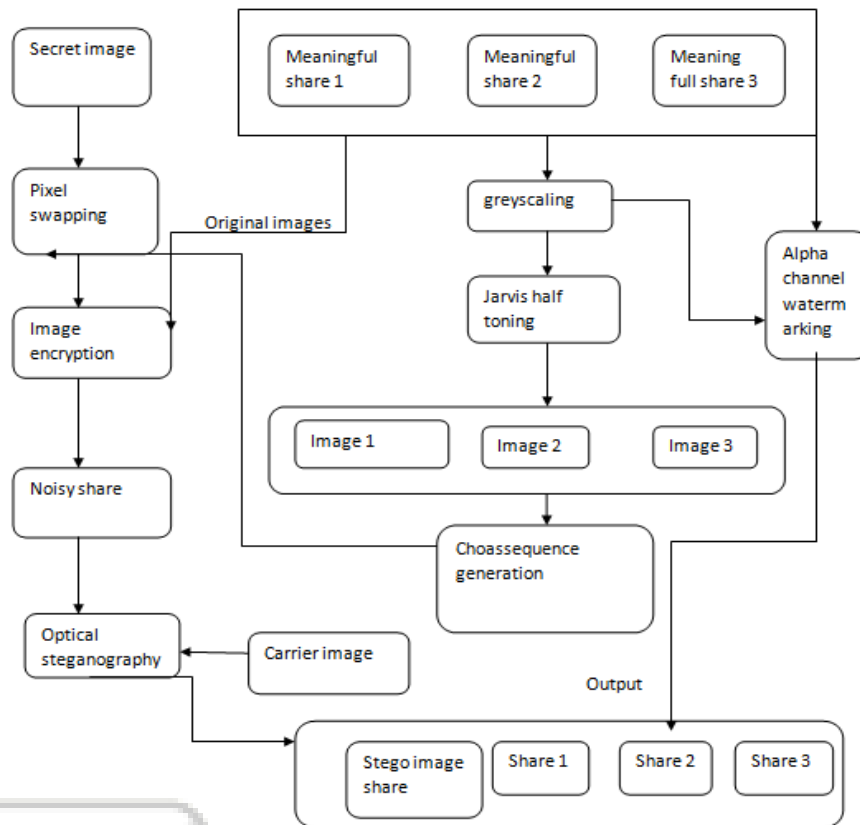


Fig. 1: Block diagram of NVSS scheme using jarvis half toning

Algorithm shows as follows.

#### A. Grey-Scaling

Traverse through entire input image array. Read individual pixel color value (24-bit). Split the color value into individual R, G and B 8 Values

$$B = \text{pix} \& 0\text{ff};$$

$$G = (\text{pix} \gg 8) \& 0\text{ff};$$

$$R = (\text{pix} \gg 16) \& 0\text{ff};$$

Calculate the grey scale component (8-bit) for given R, G and B pixels using a conversion formula.

$$Gs = (r + g + b) / 3;$$

Compose a 24-bit pixel value from 8-bit greyscale value.

Store the new value at same location in output image

#### B. Thresholding

Traverse through entire input image array. Read individual pixel color value (24-bit) and convert it into grey scale. Calculate the binary output pixel value (black or white) based on current threshold. Store the new value at same location in output Image.

#### C. Encryption:

In the encryption phase, the  $n - 1$  feature images ( $F_1, \dots, F_{n-1}$ ) combined with the secret image. Execute the XOR operation to generate one noise like share  $S$  with 24-bit/pixel color depth.

Traverse through the entire input image array. Read individual pixel value. Assume the initial value of the password is zero.

If  $x=y=0$ , then calculate black pixels. If  $x=y=1$ , then calculate white pixels. Add password value into the black and white pixels to obtain first password value.

Generate the password using three images.

### III. SYSTEM MODULES

#### A. Input Image

An image is a two-dimensional picture, which has a comparable appearance to some subject normally a physical article or a man. Picture is a two-dimensional, for example, a photo, and screen show.

#### B. Embedding Procedure

Input: Cover image of size, secret Image bit stream, Output: Steno image. Find the minimum satisfying, and convert into a list of digits with a binary notational system. Solve the discrete optimization problem to find and. In the region defined by, record the coordinate such that, Construct a no repeat random embedding sequence. To embed a secret Image bit stream, two pixels in the cover image are selected according to the embedding sequence, and calculate the modulus distance between and, then replace with. Repeat above step until all the secret Image bit streams are embedded.

#### C. Extract Procedure

To extract the embedded message digits, pixel pairs are scanned in the same order as in the embedding procedure. The embedded secret Image bit streams are the values of extraction function of the scanned pixel pairs.

Input: Steno image, Output: secret Image bit stream.

- 1) Construct the embedding sequence.
- 2) Select two pixels according to the embedding sequence.
- 3) Calculate, the result is the embedded digit.
- 4) Repeat Steps 2 and 3 until all the secret Image bit streams are extracted.
- 5) Finally, the secret Image bits can be obtained by converting the extracted secret Image bit stream.

#### IV. SOFTWARE REQUIREMENTS

Operating System: Windows XP/7, Coding Language: MATLAB. There is no hardware requirement in this project because we are doing this project on software (Simulation) basis only. Therefore we are not mentioned any hardware requirements.

MATLAB is a system for doing numerical calculation. It was initially intended for tackling straight variable based math sort issues utilizing lattices. Its name is gotten from Matrix lab. MATLAB has subsequent to been

extended and now has a few inherent capacities for tackling issues needed for information investigation, sign handling, advancement, and a few different sorts of investigative calculations. Math and computation consists of as follows.

Algorithm development, data acquisition, modelling, simulation and prototyping, Data analysis, exploration and visualization, Scientific and engineering graphics, Application development, including graphical user interface building.

#### V. SIMULATION RESULTS

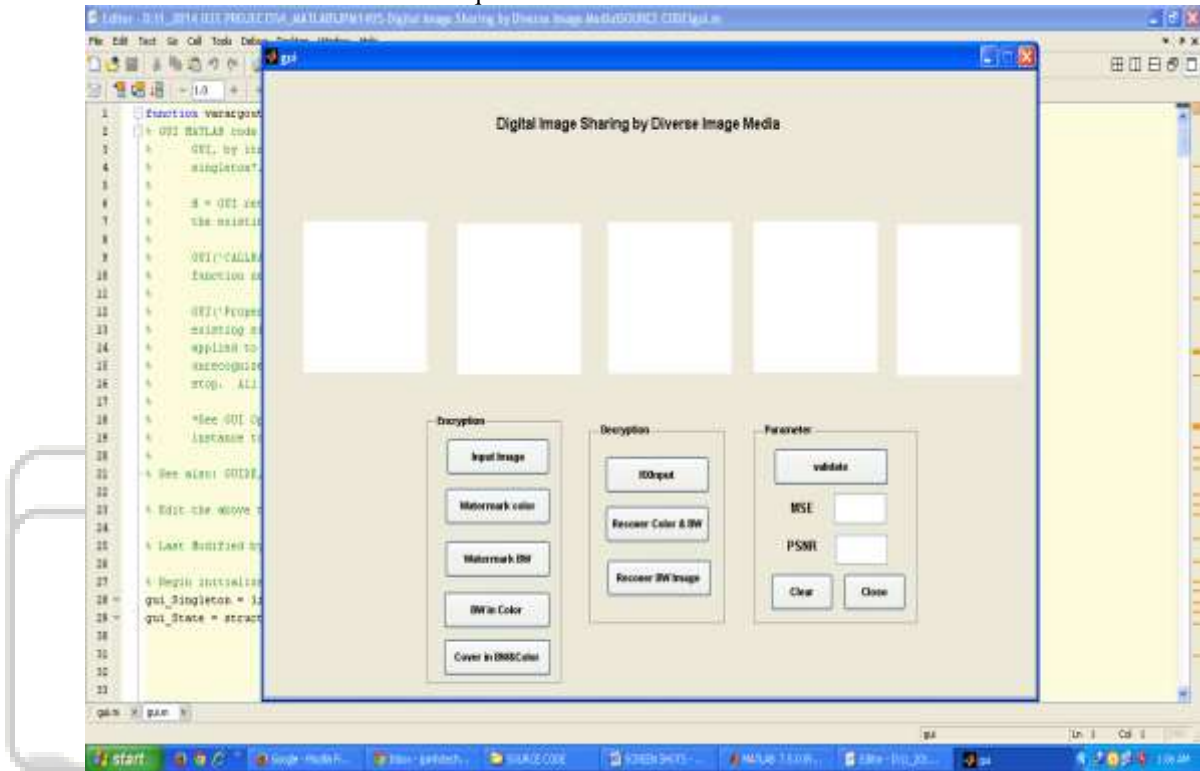


Fig. 2: Output window of the NVSS scheme without inputs and outputs



Fig. 3: An input cover image is taken it is a photo cover image

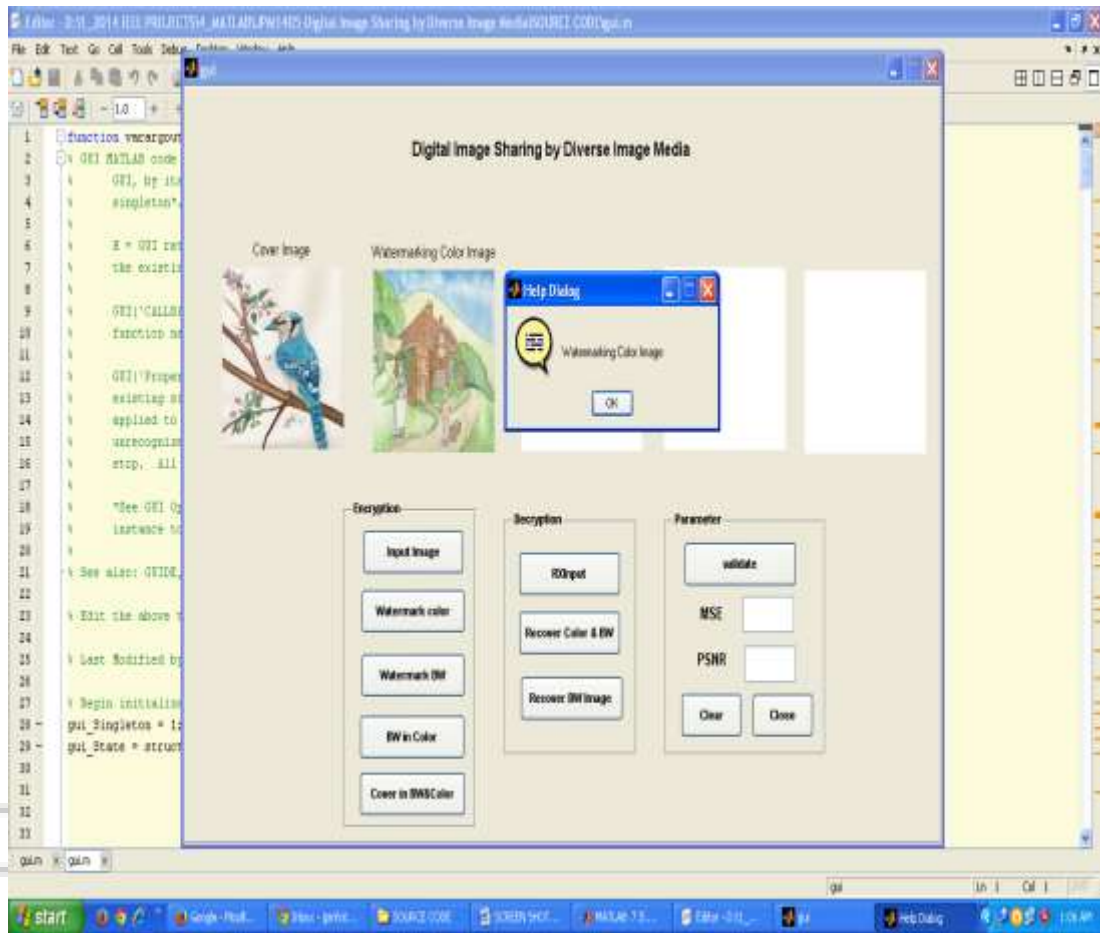


Fig. 4: An input watermarking color image taken at encryption side

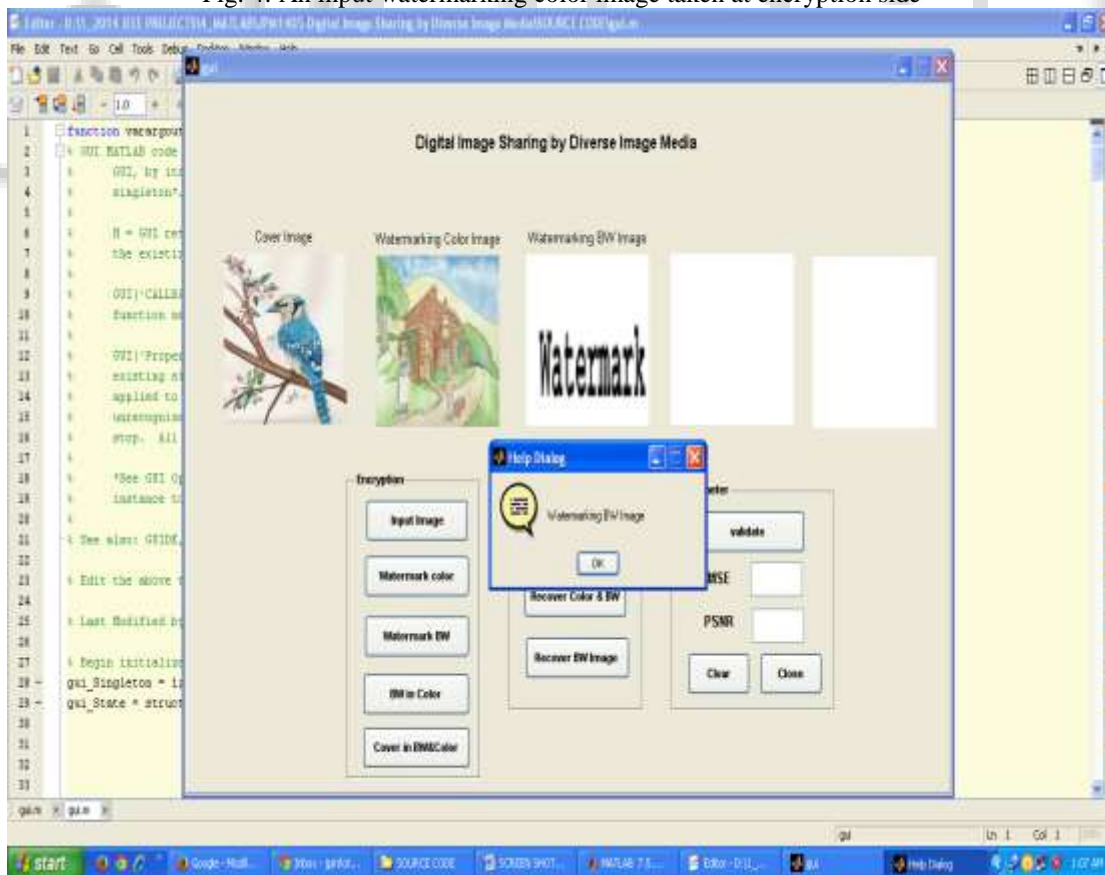


Fig. 5: watermark BW image taken at encryption side

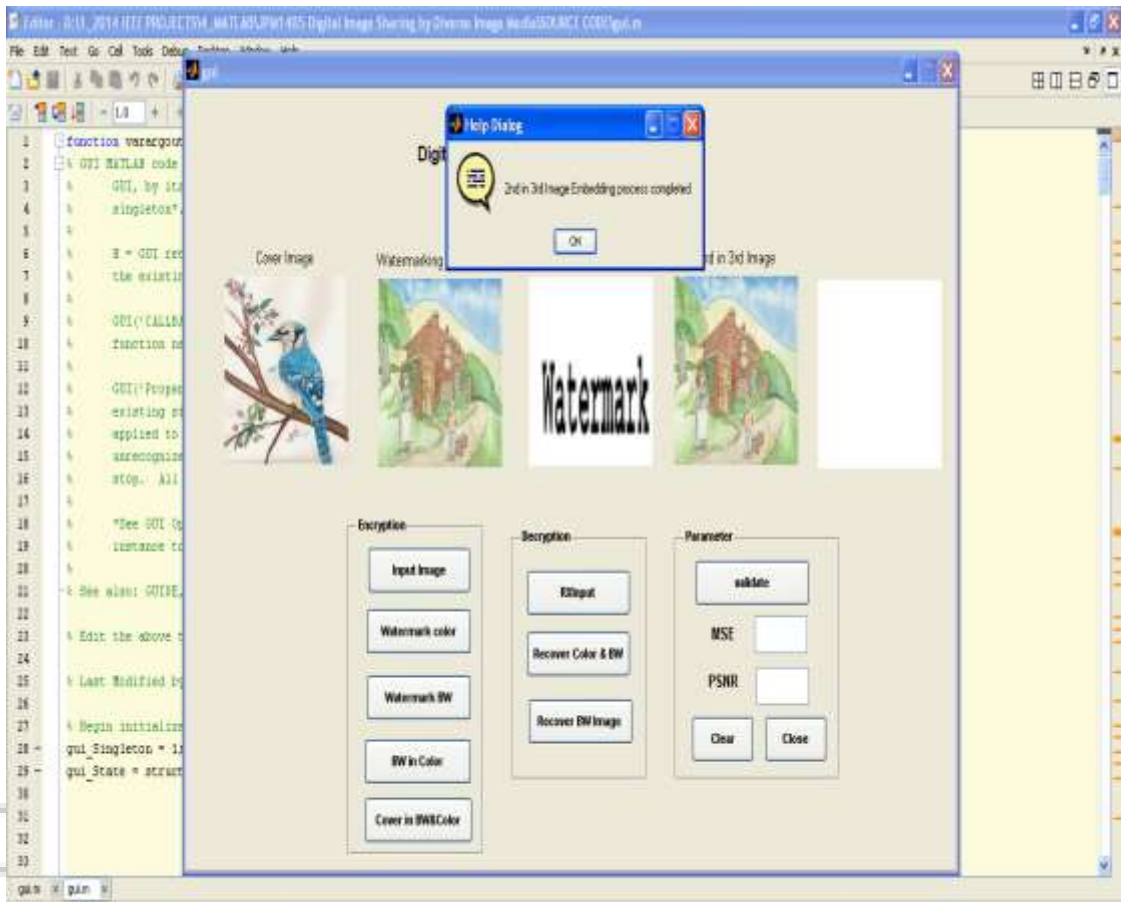


Fig. 6: watermark colour image and watermark BW image are combined to get new image in encryption side



Fig 7 cover image is mixed with fourth image obtained from 2<sup>nd</sup> and 3<sup>rd</sup> image to get new image

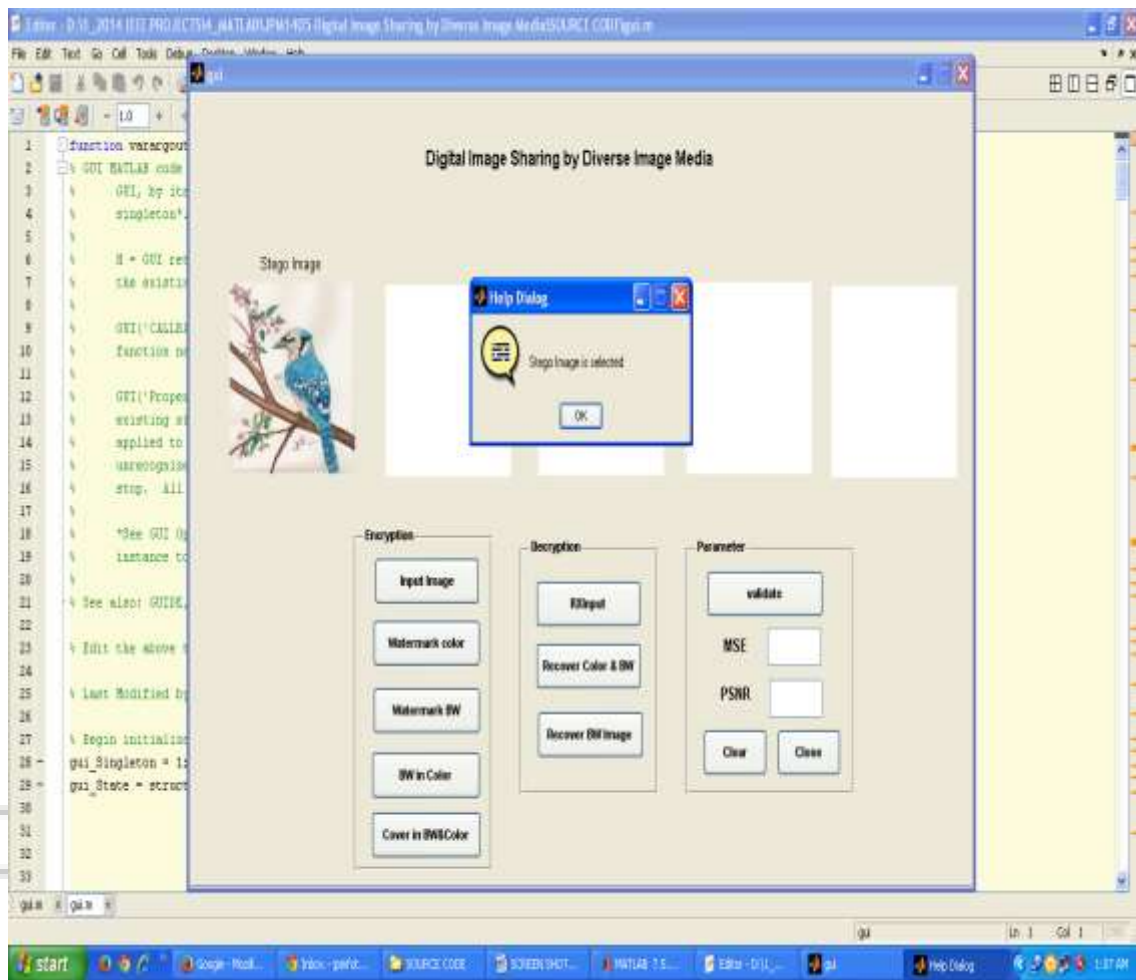


Fig 8 A stego image is formed after sharing all images at the decryption



Fig. 9: From the stego image colour image is recovered



Fig. 10: From stego image watermark image is recovered in decryption process so all the images are shared without any transmission risk

## VI. CONCLUSION

The project proposes a VSS scheme,  $(n, n)$ -NVSS scheme, that can share a digital image using diverse image media. The media that include  $n-1$  randomly chosen images are unaltered in the encryption phase. Therefore, they are totally innocuous. Regardless of the number of participants' increases, the NVSS scheme uses only one noise share for sharing the secret image. Compared with existing VSS schemes, the proposed NVSS scheme can effectively reduce transmission risk and provide the highest level of user friendliness, both for shares and for participants.

This project provides four major contributions. First, this is the first attempt to share images via heterogeneous carriers in a VSS scheme. Second, we successfully introduce hand-printed images for images-sharing schemes. Third, this study proposes a useful concept and method for using unaltered images as shares in a VSS scheme. Fourth, we develop a method to store the noise share as the QR code.

After decryption process has been done. Recovered image will be formed by using comparing the pixels values of secret image and recovered image we can found that there is no pixel expansion or pixel corruption in the recovered image hence there is no change in the secret and recovered image.

There are many attractive questions that future work has to consider. In this project future work is this method is applied for diverse images it can be tried to videos if we want to share videos through different Medias.

## ACKNOWLEDGMENT

The Author Mr. P.Praveen.kumar wants to give a special thanks to Co-author Prof.Satish.M.N, for his valuable guidelines and corrections for editing. Authors are very thankful to CiTech HOD, Principal and Friends.

## REFERENCES

- [1] M. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryptology*, Vol. 950. New York, NY, USA: Springer-Verlag, 1995, pp. 1–12.
- [2] R. Z.Wang, Y. C. Lan, Y. K. Lee, S. Y. Huang, S. J. Shyu, and T. L. Chia, "Incrementing visual cryptography using random grids," *Opt. Commun.*, vol. 283, no. 21, pp. 4242–4249, Nov. 2010.
- [3] P. L. Chiu and K. H. Lee, "A simulated annealing algorithm for general threshold visual cryptography schemes," *IEEE Trans. Inf. ForensicsSecurity*, vol. 6, no. 3, pp. 992–1001, Sep. 2011.
- [4] K. H. Lee and P. L. Chiu, "Image size invariant visual cryptography for general access structures subject to display quality constraints," *IEEETrans. Image Process.*, vol. 22, no. 10, pp. 3830–3841, Oct. 2013.
- [5] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Extended capabilities for visual cryptography," *Theoretical Comput. Sci.*, vol. 250, nos. 1–2, pp. 143–161, Jan. 2001.
- [6] C. N. Yang and T. S. Chen, "Extended visual secret sharing schemes: Improving the shadow image quality," *Int. J. Pattern Recognit. Artif.Intell.*, vol. 21, no. 5, pp. 879–898, Aug. 2007.

- [7] K. H. Lee and P. L. Chiu, "An extended visual cryptography algorithm for general access structures," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 219–229, Feb. 2012.
- [8] Z. Zhou, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography," *IEEE Trans. Image Process.*, vol. 15, no. 8, pp. 2441–2453, Aug. 2006.
- [9] Z. Wang, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography via error diffusion," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 3, pp. 383–396, Sep. 2009.
- [10] I. Kang, G. R. Arce, and H. K. Lee, "Colour extended visual cryptography using error diffusion," *IEEE Trans. Image Process.*, vol. 20, no. 1, pp. 132–145, Jan. 2011.
- [11] F. Liu and C. Wu, "Embedded extended visual cryptography schemes," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 307–322, Jun. 2011.
- [12] T. H. Chen and K. H. Tsao, "User-friendly random-grid-based visual secret sharing," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 21, no. 11, pp. 1693–1703, Nov. 2011.
- [13] T. H. N. Le, C. C. Lin, C. C. Chang, and H. B. Le, "A high quality and small shadow size visual secret sharing scheme based on hybrid strategy for greyscale images," *Digit. Signal Process.*, vol. 21, no. 6, pp. 734–745, Dec. 2011.
- [14] D. S. Tsai, G. Horng, T. H. Chen, and Y. T. Huang, "A novel secret image sharing scheme for true-colour images with size constraint," *Inf.Sci.*, vol. 179, no. 19, pp. 3247–3254, Sep. 2009.

