I. J. Computer Network and Information Security, **2017, 5, 38-43**
Published Online May 2017 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2017.05.05

A Method for Verifiable Secret Image Sharing

Priya Venny
PG Student, Computer Engineering, DYPIET (Pimpri), Pune, India
E-mail: priyavenny@gmail.com

Dr. Jyoti Rao
Associate Prof., Computer Engineering, DYPIET (Pimpri), Pune, India
E-mail: jyoti.aswale@gmail.com

Abstract—Secret Image Sharing using Verifiable method has become an important field in cryptography in today’s world. Security is of main concern and verifiability has become a demand of this era in order to avoid cheating prevention and a new scheme of secret image sharing scheme for identification of the presence of cheater is has been analyzed and described. A method for ensuring integrity of secret image prior to its recovery is proposed. An secret image and verification image are used to create shares by ARGB to CMYK conversions which are sent via cover image for transmission. The shares created are meaningful therefore this method is able of identifying whether cheater exists or not in order to preserve the integrity of the image.

Index Terms—Cheating Prevention, Secret Sharing, Visual Cryptography, Verification Image, Secret Image, RGB, CMYK, LSB.

I. INTRODUCTION

Cryptography is a technique of altering messages to make them secure and unaffected to attacks and Visual Cryptographic (VC) technique is a technique of converting plaintext into ciphertext. Shares are the encrypted form of a secret image so that the SI is regained by stacking enough number of shares and the shares are given to various users. Few properties of VC are pixel expansion, security and contrast.[2]

The use of internet has increased and secrets are transferred using internet. A secret is a thing which is kept from the knowledge of many except the people who are intended to know. Secret sharing defines a method by which each participant is allocated a piece of the secret. This portion of the secret is known as a share. The secret recreation can be done only when ample shares are joined together. As the shares are distinct no facts about the secret can be gained. The shares are not of any use when they are separated.

The efficient method of Visual secret sharing (VSS) for hiding secret image in a very secure way and this is done by dividing the image as shares i.e. the secret image is divided and encrypts them in order to provide protection. In this system everyone can see it is very easily by the human visual system. The key concept behind the original (VSS) scheme is the encoding of a secret image into meaningless n share images. In this non-computer environment the scheme of (VSS) is a scheme that is used for sending the image securely [2].

The secret image is split into a number of share images and the secret image can be regenerated by predefined assembly of share images known as secret image sharing. There are two basic objects – Sender and Receiver. Sender is an object which deals the task of share creation and allots these shares to various dispersed receivers. Receivers receive the share images from sender and take part in secret reconstruction process. If any one of the object behaves like a cheater and tries to hamper the shares then the secret recovery is hampered. So, there is requirement for Verifiable Secret Image Sharing. [7]

A numeric illustration of 2Dimage is known as digital image. Reliant on the image resolution is fixed or not but that might be of vector or raster type. The term "digital image" usually refers to a raster image or bit mapped images.

$$\begin{bmatrix} P_{0,0}(a,R,G,B) & P_{0,1}(a,R,G,B) & \cdots & P_{0,n-1}(a,R,G,B) \\ P_{1,0}(a,R,G,B) & P_{1,1}(a,R,G,B) & \ldots & P_{1,n-1}(a,R,G,B) \\ P_{2,0}(a,R,G,B) & P_{2,1}(a,R,G,B) & \ldots & P_{2,n-1}(a,R,G,B) \\ \vdots & \vdots & \vdots & \vdots \\ P_{n-1,0}(a,R,G,B) & P_{n-1,1}(a,R,G,B) & \ldots & P_{n-1,n-1}(a,R,G,B) \end{bmatrix}$$

The above matrix represents the Bits Representation of Image in the form of matrix.

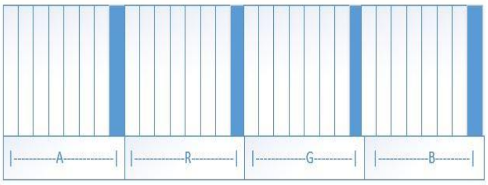


Fig.1. RGB Representation of Image

A digital image is defined for the purposes of this document as a raster based, 2-dimensional, rectangular array of static data elements called pixels, intended for display on a computer monitor or for transformation into another format, such as a printed page. To a computer, an image is an array of numbers that represent light intensities at various points, or pixels. These pixels make up the image's raster data. Digital images are typically stored in 32-, 24- or8-bit per pixel files. In 8-bit color images, (such as GIF files), each pixel is represented as a single byte. A typical 32 bit picture of width=n pixels and height = m pixels can be represented by an m x n matrix of pixels as shown in above matrix.[9]

The three 8 bit parts - red-R, blue-B and green-G - constitute24 bits which means that a pixel should have 24 bits. 32 bit refers to the image having an "alpha channel". An alpha channel is like an extra color, although instead of displaying it as a color, it is rendered translucently (see-through) with the background as shown in (Fig.1).[9]

A specific organization of colors is color space. In grouping with physical device outlining, it allows for mimicking illustrations of color both in analog and digital illustrations. A color space might be random with specific colors allocated to a set of physical color strips and corresponding allotted names or numbers.

A. RGB Color Space

The constitutions of colors are commonly described by the additive and subtractive models shown in (Fig.2). Additive color mixing model is used for RGB as it describes what kind of light requires to be emitted to produce a given color. RGBA is RGB with an additional channel, alpha, to indicate transparency. Required colors are being found by mixing a number of RGB components in the additive system where the primaries are Red, Green, and Blue (RGB). The quantity of red (green or blue) in the compound light can be controlled by adjusting the intensity of red (green or blue) component. The brightness increases by mixing more and more colored lights and the white color is the result of mixing all the components of the red, green and blue with equal intensity,. The monitor of a computer is a perfect example of the additive model. [4]

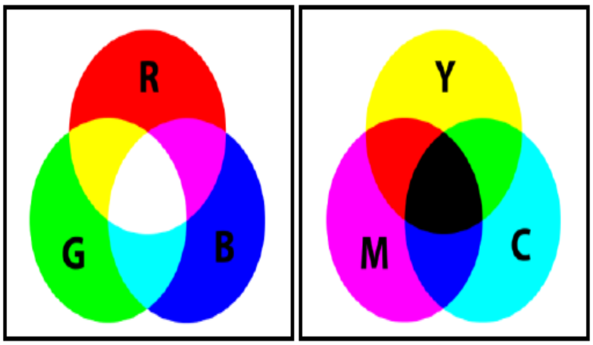


Fig.2. Additive and Subtractive Model

B. CMYK Color Space

CMYK uses subtractive color mixing used as it tells what type of colors are needed to be used so the light reflected from the substrate and via the inks creates a given color. In the subtractive model color is signified by using the mixtures of colored lights redirected from the surface of an object. Therefore the mixing of Cyan (C) with Magenta (M) and Yellow (Y) pigments huge range of colors can be produced. The intensity of the light decreases the more pigment we provide and therefore the darkened is the light. So, it is called the subtractive model. The three primitive colors of pigment are C, M, and Y and other colors cannot compose them. The color printer is an example of the application of the subtractive model. [4]

II. Related Works

In 1979 Blakley [1] and Shamir [2] were the first to propose the thought of secret sharing through a scheme known as (t,n) threshold scheme. i.e. out of n shares the t shares are necessary to recreate the secret. The (t, n) Visual Cryptographic technique in which an image is divided into various n shares was first proposed by Naor and Shamir and in this scheme the secret image was retrieved by stacking minimum t shares amid the n share images and stacking of less than t shares failed the decode to be effective. [3].

An alternative form of secret sharing is visual secret sharing and the decoding depends only on the human vision system and therefore it is quite efficient. Cheating is VSS is a highlighted issue in this system. A lot of work is being done for cheating activities and schemes like cheating prevention visual secret sharing (CPVSS) have been introduced. Analysis of the research challenges involved in CPVSS has been done. Some of the well-known cheating activities have been seen and then the cheating activities are categorized into meaningful cheating, non-meaningful cheating, and meaningful deterministic cheating. New schemes which are better than the previous schemes with respect to some of the security requirements have been defined. [6]

A group of participants who are qualified can recover the secret message. But the original scheme can easily be corrupted by malicious participant. To verify the presence of cheaters based on digital watermarking an extension of VCs has been proposed. Without any additional cryptographic computation and other information every user can verify the validity of shares of other users only by watermark extraction operation. Therefore we get enhanced security. [7]

Today, attention is more towards protecting sensitive data transmitting across network. In now we to require use of color images as the cover image and large amount of data is to be hidden in image. In this method confusion and diffusion methods uses chaotic encryption to secure cover image which encodes a few of the bits in image. In this method use of Reverse Data Hiding using saving room in advance approach original cover can be losslessly regenerated after extraction of inserted data. [9]

Table 1. Abbreviations and Description

Symbol	Description
VI	Verification Image
SI	Secret Image
R1, R2, R3 and Rn	Shares of SI
S1 and S2	Shares of VI
LSB	Least Significant Bit

This (Table 1) shows the various abbreviations used to describe this system.

III. Proposed System

In VC cheaters may provide a Fake Share (FS) so that they can cheat the other users. The encryption of a secret image into transparent shares so that sufficient number of shares when stacked together reveals the secret image and this technique is called as Visual Cryptography (VC). Cheating Prevention is an important part of VC. [9] To detect the presence of the cheater our proposed scheme of using verification image helps.

A. Senders Side Architecture

Visual secret sharing scheme is a part of visual cryptography and the use of verification image and cover image helps in increasing the security and integrity of the verifiable scheme.[6] The Shares of VI and SI are created by converting RGB to CMYK. Created shares are further steganographed.

The shares are created by converting RGB to CMYK which is done by using the following formula. The R,G,B values are divided by 255 to change the range from 0..255 to 0..1:

$$R' = R/255 \tag{1}$$

$$G' = G/255 \tag{2}$$

$$B' = B/255 \tag{3}$$

The black key (K) color is calculated from the red (R'), green (G') and blue (B') colors:

$$K= 1-\max(R', G', B') \tag{4}$$

The cyan color (C) is calculated from the red (R') and black (K) colors:

$$C= (1-R'-K) / (1-K) \tag{5}$$

The magenta color (M) is calculated from the green (G') and black (K) colors:

$$M = (1-G'-K) / (1-K) \tag{6}$$

The yellow color (Y) is calculated from the blue (B') and black (K) colors:

$$Y= (1-B'-K) / (1-K) \tag{7}$$

In this scheme after the shares are created the one of the share of the verification image is embedded with the shares of the secret image by Least Significant Bit (LSB) and new set of shares are created. The rest of the verification share is kept for the regeneration process at the end. This is done in order to increase the security of the Secret Sharing Scheme.

At the senders side (Fig.3) the proposed system would work as shown in the figure below.

The secret sharing scheme is further enhanced by this system as the system generated cover images are created for transmission. The use of cover image is to hide the existence of the secret image is order to divert the attention of the intruders. The cover Images are formed in such a way in that the cover image doesl not attract the attention of the cheaters. The produced shares are meaningful therefore the existence of the secret is hidden. This method is simple and fulfills the basic needs of cheating prevention.

The other share of the verification image is sent to the receiver’s end by creating system generated the cover image. This will help is securing the transmission of the share as the attacker may try to access it in search of the secret image.[5]

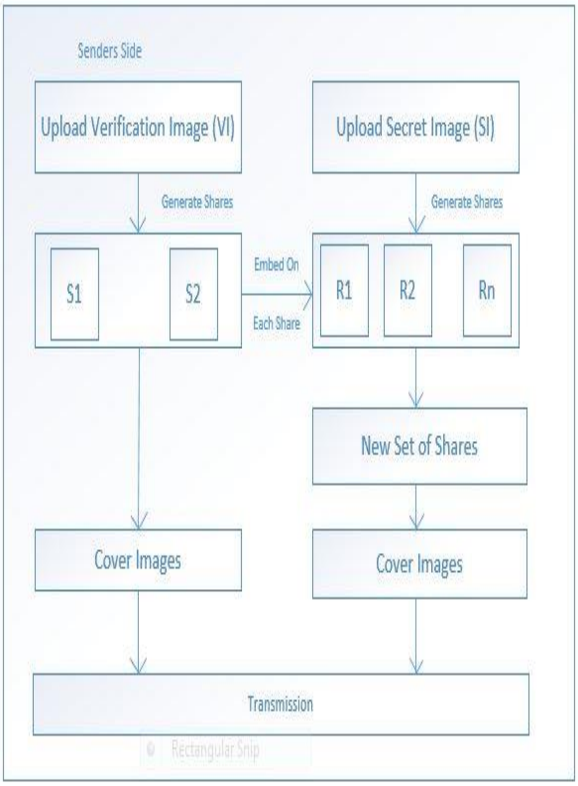


Fig.3. Architecture of Senders Side

B. Receivers Side Architecture

The reverse process (Fig.4) is done and after the cover images is received at the receivers end. The decomposition process starts. The cover image is decomposed the set of shares are received which were the combination of the shares of secret image and a share of verification image. These are further decomposed to separate the share of verification image and secret image. The verification image shares S1 and S2 is combined with its other share by XORing them and if the verification image is got and not distorted then it is proved that cheaters are not present. Similarly secret image is retrieved by combining the shares. The reconstruction of the original secret image is done by

XORing the shares R1, R2, R3 and R4 in order to retrieve the Secret image. [5]

The recovered shares are again recreated by again doing CMYK to ARGB conversion. To do the following conversion the below formula is used. The R, G, B values are given in the range of 0..255.

The red (R) color is calculated from the cyan (C) and black (K) colors:

$$R= 255 \times (1-C) \times (1-K) \tag{8}$$

The green color (G) is calculated from the magenta (M) and black (K) colors:

$$G = 255 \times (1-M) \times (1-K) \tag{9}$$

The blue color (B) is calculated from the yellow (Y) and black (K) colors:

$$B= 255 \times (1-Y) \times (1-K) \tag{10}$$

The shares are given to the participants and during the retrieval phase, the verification image is recovered first then the secret image is recovered. Any distortion in the shares is noticed and if any distortion is seen then the presence of the cheater is found out. If the shares are not distorted then the integrity of the shares is well-preserved. Then the secret image is retrieved. The use of verification image helps secure the secret images integrity.

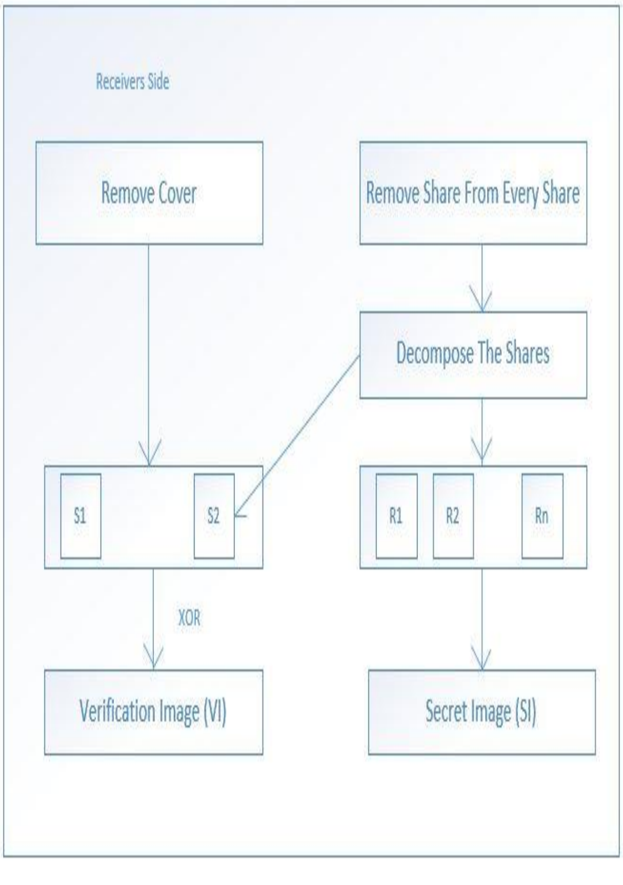


Fig.4. Architecture of Receivers Side

C. Algorithm

Algorithm-1 Share Construction and Steganography

Original secret image (SI)
Verification image (VI)

Output:
N number of Cover images formed for transmission.

Begin

1. Upload VI and SI
2. Apply ARGB to CMYK conversion for Share Creation.
3. Two shares S1and S2 of VI are created.
4. Multiple shares R1, R2, R3,… Rn of SI are formed.
5. Apply LSB Steganography on S2 and shares of SI to form new set of shares.
6. System generated cover images are formed for transmission.

End

Algorithm-2 Revealing algorithm

Input: N number of Cover images formed for transmission.

Output:
Original secret image (SI)
Verification image (VI)

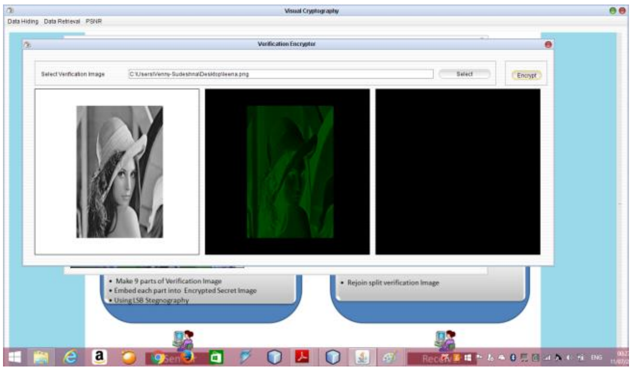
Begin

1. Cover Images are removed and stego shares are retrieved.
2. Stego shares are further decomposed to separate the VI share S2 and R1, R2, R3,… Rn.
3. The Shares S1 and S2 are XORed to obtain VI.
4. The quality of the VI image is checked to detect the presence of cheater.
5. If quality of original VI is equal Recovered VI then cheater is not present.
6. SI is obtained by XORing R1, R2, R3,… Rn.

End

IV. Results

To depict this method, we can use a set of images as shown in figures below. The set images used contains binary images: Leena, Joker, Peppers, Lady. In the example given below (Fig.5) Joker is our secret image and (Fig.6) Leena is taken as the verification image which is used to verify the reconstructed secret images.


Visual Cryptography
Data Hiding Data Retrieval PSNR
Verification Encryptor
Select Verification Image
Select
Encrypt
Make 9 parts of Verification Image
Embed each part into Encrypted Secret Image
Using LSB Stegnography
Rejoin split verification image

Select Verification Image: C:\Users\Venny-Sudeshna\Desktop\leena.png

Fig.5. Verification Image Upload and Share Creation

The (Fig.5) Shows the upload and then creation of the shares of the Verification Image using ARGB to CMYK conversion and similarly in (Fig.6) depicts the upload of Secret Image and its share creation.

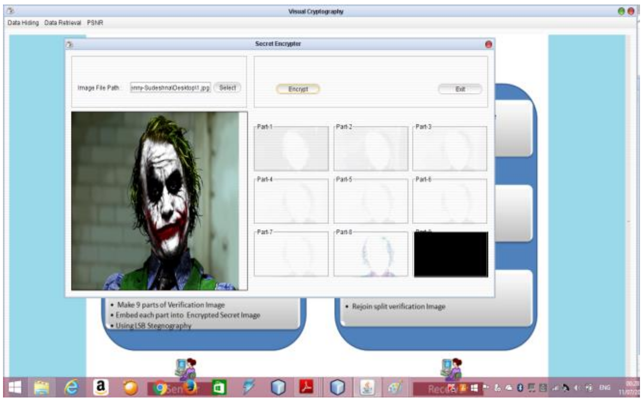

Visual Cryptography
Data Hiding Data Retrieval PSNR
Secret Encryptor
Image File Path
Select
Encrypt
Exit
Part-1
Part-2
Part-3
Part-4
Part-5
Part-6
Part-7
Part-8
Make 9 parts of Verification Image
Embed each part into Encrypted Secret Image
Using LSB Stegnography
Rejoin split verification image

Image File Path: enny-Sudeshna\Desktop\1.jpg

Fig.6. Secret Image Upload and Share Creation

The following (Fig-7) given below shows the process of Steganography performed using LSB technique.

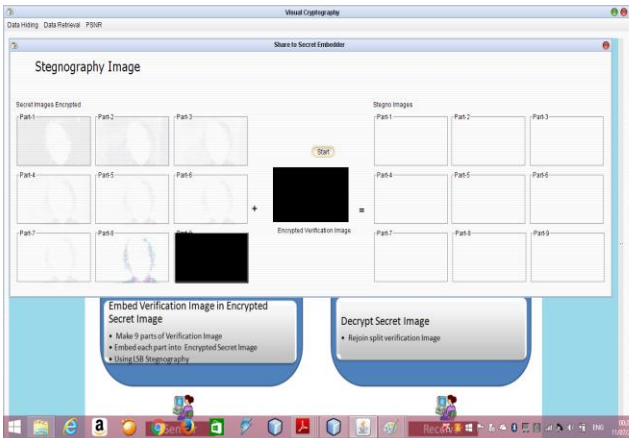
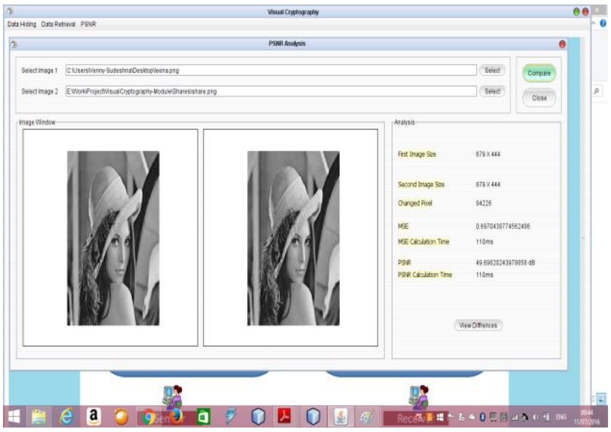


Fig.7. Steganography

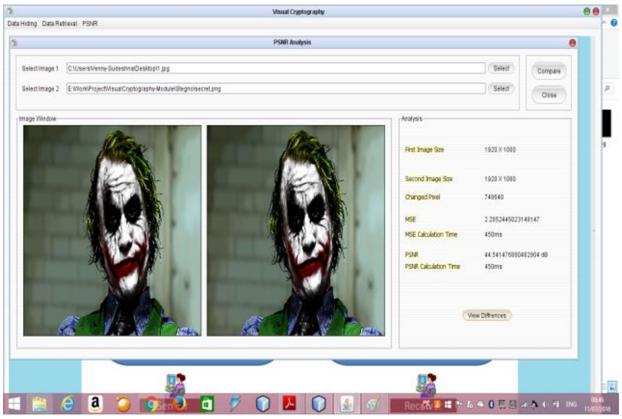
In the end we will extract and recover and check the PSNR and MSE value of the verification image as shown in (Fig.8) and if it is retrieved finely then secret image is retrieved and it has been shown in (Fig.9).



Select Image 1: C:\Users\Venny-Sudeshna\Desktop\leena.png
Select Image 2: E:\Work\Project\VisualCryptography-Module\Shares\share.png

First Image Size 679 X 444
Second Image Size 679 X 444
Changed Pixel 84226
MSE 0.6970438774562486
MSE Calculation Time 110ms
PSNR 49.69820243978858 dB
PSNR Calculation Time 110ms

Fig.8. Verification Image Retrieval



Select Image 1: C:\Users\Venny-Sudeshna\Desktop\1.jpg
Select Image 2: E:\Work\Project\VisualCryptography-Module\Stegno\secret.png

First Image Size 1920 X 1080
Second Image Size 1920 X 1080
Changed Pixel 748640
MSE 2.2852445023148147
MSE Calculation Time 450ms
PSNR 44.541476980492904 dB
PSNR Calculation Time 450ms

Fig.9. Secret Image Retrieval

Accuracy of the images retrieved is checked using parameters like MSE and PSNR. MSE is mean squared error of an estimator measures the average of the squares of the errors or deviations, that is, the difference between the estimator and what is estimated. PSNR is most commonly used to measure the quality of reconstruction of the image. The signal in this case is the original data, and the noise is the error introduced during process.

$$\text{MSE}=\frac{1}{n}\sum_{i=1}^{n}(Q_i' - Q_i)^2 \qquad (11)$$

$$\text{PSNR}= 10\ log_{10}\frac{255^2}{MSE} \qquad (12)$$

The Mean squared error should be less. The lesser it is the more accurate is the recovered image. Similarly the peak signal to noise ratio should be more, the more it is then the noise is less. This system overall maintains the quality of the images taken as shown in the graph.

The (Fig.10) shows the MSE and PSNR values of the various images like Leen, joker, auto, cars used during the time of running the system and it shows that the system maintains the accuracy.

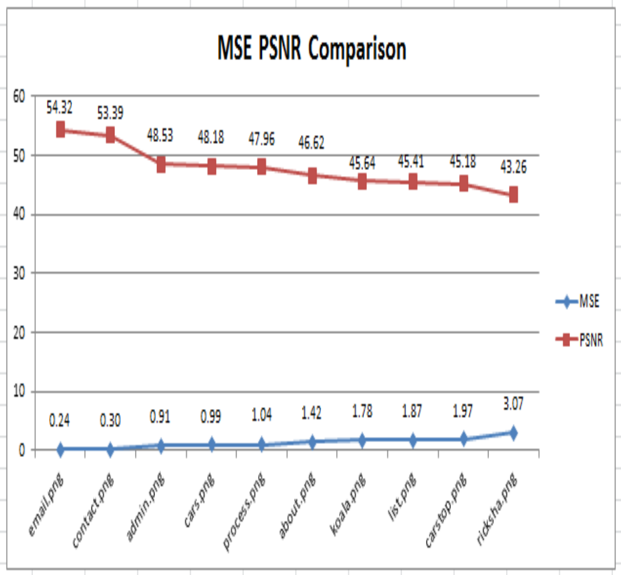


Fig.10. MSE and PSNR Analysis

V. Conclusion

Highly sensitive and highly information can be stored using Secret sharing schemes as they are ideal. A method for verifiable secret sharing helps in identifying the presence of the cheater in the system. The method fulfills the basic features of secret sharing scheme. Shares are combined and reconstructed to retrieve the verification image and secret image. The regenerated images are checked and it should be under a reasonable possibility of error as that confirms that no cheater is present in the system. The proposed method can identify the cheater is there or not and hence can be an ideal method of cheating prevention.

References

[1] M. Naor and A. Shamir, Visual cryptography, Lecture Notes Computer Science, vol. 50, pp. 1-12, 1995.

[2] Mary, G. Germine, and M. Mary Shanthi Rani. "A Study on Secret Image Hiding in Diverse Color Spaces."

[3] Chen, Yu-Chi, Du-Shiau Tsai, and Gwoboa Horng. "Visual secret sharing with cheating prevention revisited." *Digital Signal Processing* 23.5 (2013): 1496-1504.

[4] Tan, Xiaoqing, and Qiong Zhang. "A Kind of Verifiable Visual Cryptography Scheme." *Emerging Intelligent Data and Web Technologies (EIDWT), 2013 Fourth International Conference on*. IEEE, 2013.

[5] Rao, Jyoti, and Priya Venny. "A new approach of Secret Image Sharing using Verifiable scheme." *Computing, Communication and Automation (ICCCA), 2016 International Conference on*. IEEE, 2016.

[6] Rose, A. Angel, and Sabu M. Thampi. "A Secure Verifiable Scheme for Secret Image Sharing." *Procedia Computer Science* 58 (2015): 140-150.

[7] Jana, Biswabandhu, et al. "Cheating prevention in Visual Cryptographic Schemes using message embedding: A hardware based practical approach."*Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference on*. IEEE, 2014.

[8] Besteena, K. J., and Philumon Joseph. "Reversible data hiding in selectively encrypted RGB images by reserving room in advance." *Computational Systems and Communications (ICCSC), 2014 First International Conference on*. IEEE, 2014.

[9] Jana, Biswabandhu, et al. "Cheating prevention in Visual Cryptographic Schemes using message embedding: A hardware based practical approach."*Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference on*. IEEE, 2014.

[10] https://www.scribd.com/doc/54600936/Steganography-Report.

[11] Vijayalakshmi, V., G. Zayaraz, and V. Nagaraj. "A modulo based LSB steganography method." Control, Automation, Communication and Energy Conservation, 2009. INCACEC 2009. 2009 International Conference on. IEEE, 2009.

Authors' Profiles

Priya Venny was born in Pune Maharashtra on 18th August 1992 is currently pursuing Master of Engineering. in Computer Engineering from Dr. D. Y. Patil Institute of Engineering Technology Pimpri, Pune, Savitribai Phule Pune University, Maharashtra, India. She has completed her B.E Information Technology Engineering Degree in 2014 from Sagar Institute of Research and Technology, Bhopal, Rajeev Gandhi Prodyogiki Vishwavidlaya, Madhya Pradesh, India.

Jyoti Rao She has completed Phd in Computer Engineering from JJT University Rajasthan in 2016, Masters of Computer Engineering from D. Y. Patil College of Engineering, Pune in 2008 and Bachelors of Computer Engineering from D. Y. Patil College of Engineering, Pune in 2001.

She is working as Associate professor in Dr. D.Y. Patil Institute of Engineering and Technology, Pimpri college under Savitribai Phule Pune University. She has published fifteen papers. Her area of research is Information Security.

How to cite this paper: Priya Venny, Jyoti Rao,"A Method for Verifiable Secret Image Sharing", International Journal of Computer Network and Information Security(IJCNIS), Vol.9, No.5, pp. 38-43, 2017.DOI: 10.5815/ijcnis.2017.05.05