Gray Visual Cryptography Algorithm for Secret Sharing

Ahmed Mohamed Ragab¹; Mahmoud El Khouly²
¹Faculty of Sciences, Helwan University, Egypt
²Faculty of Computer and Information Sciences, Helwan University, Egypt
¹dr_ahmedragab9@yahoo.com; ²sanagibo2@yahoo.com
DOI: 10.47760/IJCSMC.2020.v09i07.001

Abstract— Visual cryptography technique is a secret sharing scheme used to encode secret visual information, in such a way that decoding process can be performed by a human visual system without any devices or complex computations to reveal the original secret. In this paper, we proposed a visual cryptography scheme for embedding gray secret image into two meaningful shares, and analyzed the relationship between the secret image and the meaningful shares, focusing our attention on improving the visual quality of the revealed secret by measuring the closeness or the differences in similarity between the secret image and the meaningful covers. Experimental results and case studies show that using covers that are less different from secret helps in obtaining a relatively good visual quality reconstructed secret image than using any covers.

Keywords— Secret sharing, cryptography, encoding, extended visual cryptography scheme, meaningful shares, image quality measurements.

I. INTRODUCTION

In spite of, internet is considered as the most popular communication medium but it is also considered as an insecure environment. Intruders and hackers can intercept data transmission to create data security problem.

As the advent of electronic applications increases, providing the security for information in an open network environment is required [1].

To overcome this problem, users need to secure the transmitting data over the internet or other media. There are many secure communication methods for transmitting data over the internet, such as:

- Steganography, which is one of the methods for hiding secret data in a cover medium such as a digital image, a video, or an audio file [2].
- Encryption transforms secret information into an encrypted form, which looks like a random message, Transformation procedure is called encryption process and the result is called cipher text. A computational device is required to perform decryption of the cipher text [2].
- Visual Cryptography (VC) is another method for achieving data security. VCS was first introduced by Naor and Shamir [2].

VC is a method in which cipher text can be decoded directly by the human visual system.

One of the new cryptographic techniques is Visual Cryptography (VC) based on secret sharing developed by Naor and Shamir, which provides more data confidentiality while it requires less computation power only [3].
Visual cryptography is a new type of cryptographic scheme, which can decode images without any cryptographic computation [4]. As the name suggests, visual cryptography is related to the human visual system [4].

Visual cryptography scheme (VCS) as a simple and secure way to allow the secret sharing of images without any cryptographic computation. In their approach, the secret was partitioned into n shares, and each participant would receive only one share. Once any k or more shares stacked together, the secret image will be visible without help of the computer. That is to say that secret image will be invisible if the number of stacked shares is less than k.

In VCS, a secret image is encoded into transparencies, and the content of each transparency is noise-like so that the secret information cannot be retrieved from any one transparency via human visual observation or signal analysis techniques.

Visual cryptography scheme (VCS) is a simple and secure way to allow secret sharing of images over internet without any cryptographic computation. VCS preserves the privacy of biometric data by decomposing the original image into n images in such a way that the original image can be revealed only when k or more images are simultaneously available and individual image do not reveal any information about original image.

II. RELATED WORK

A. Visual Cryptography Scheme

Visual Cryptography scheme was first introduced by Naor and Shamir [2]. Visual Cryptography (VC) is a method for achieving data security.

Visual cryptography is a kind of cryptography that can be decoded directly by the human visual system without any special calculation for decryption [5]. A distinctive property of VCS is that one can visually decode the secret image by superimposing shares without computation [6].

Every original pixel is subdivided into a collection of m black and white sub-pixels in each share, and the shadow images are printed on transparencies and can be easily reconstructed by the human visual system without computations [7].

once the secret image is encoded into n shares and these shares are distributed to participants, then to reveal the image's information and retrieve the secret we need to stack all n shares together or at least k shares, this is called a (k,n)-VCS which means k out of n shares could retrieve the secret but stacking k-1 or less shares does not retrieve the secret. Security is satisfied if each share reveals no information of the original image.

An example of (k,n)-VCS is (2,2)-VCS. The simplest sharing scheme splits a message between two people [8], shown in Fig.1, secret image (a) is encoded into two shares (b) and (c) then these shares are distributed to participants.

Each participant cannot reveal any information about the secret image, but after stacking shares (b) and (c) pixel by pixel, the secret image can be retrieved and observed visually by human visual system of the participants.

![Fig.1: An example of (2,2)-VCS](image)

Each pixel in the secret image is represented after stacking two blocks, the first block from share 1, and the second from share 2, at the same position.

Each block contains 2x2 pixels, half white pixels and the rest are black pixels, after stacking the two blocks, the secret pixel can be revealed and displayed.

For each black secret pixel, randomly choose a block from share 1 that is complementary to a block in share 2 at the same position, otherwise for each white secret pixel, the two blocks from share1 and share2 are the same as listed in Table 1.
TABLE 1
STACKING RESULTS OF (2,2)-VCS

| White pixel | stack 1 block | stack 2 block |
|-------------|---------------|---------------|
|             |               |               |
| Black pixel |               |               |
|             |               |               |

There is a loss of contrast in the reconstructed secret image; this is due to the fact that white pixels, as observed in Table 1, look grey.

There are many applications of VCS such as hiding or sharing secret image, identification, watermarking, authentication, transmitting passwords, and secure printing industry … etc.

Visual Cryptography is the technique that is used for securing data especially image-based secrets such as credit card information, personal health information, military maps and personally identifiable information and commercial identification data [9].

B. Meaningful and Meaningless Shares

In the traditional VCS, shares are appearing meaningless because those shares are carrying no visual information which may attract intruders or hackers. To secure the transmission process of secret data, the shares should be meaningful which means that the secret image is embedded into cover images that look normal to intruders, and then the secret data will be transmitted secretly without paying the intruder's attention.

It is concerned that the meaningless shares always cause suspicion of others, thus leading to the risks during the data transmission [10].

Meaningful shares are more required than meaningless shares in visual secret sharing because they do not attract intruder's attention, since the meaningful shares are in fact normal images hiding secret data, thus the intruders and hackers will not pay attention to these shares which means more security for transmitting the secret data.

The idea of generating shares with meaningful contents can achieve a more secure system for secret sharing courses [10].

The term Extended Visual cryptography scheme (EVCS) means replacing the meaningless shares used in traditional VCS with meaningful shares and stacking of a qualified subset of shares will recover or retrieve the secret image visually.

Extended visual cryptography scheme (EVCS) is a Visual cryptography scheme that uses meaningful shares to avoid attracting intruder's attention.

EVCS takes a secret image and share images as inputs, and outputs shares that satisfy the following three conditions [11]:
(1) Any qualified subset of shares can recover the secret image.
(2) Any forbidden subset of shares can't obtain any information of the secret image
(3) All the shares are meaningful images.

Fig.2 displays an example of EVCS, secret image (a) is encoded into two meaningful shares (b) and (c) then these shares are stacked and the secret image is retrieved.

Fig.2: An example of EVCS
C. Visual cryptography for gray-level images

Chang-Chou Lin, Wen Hsiang Tsai proposed visual cryptography for gray level images. In this scheme a dithering technique is used to convert gray level image into approximate binary image [12].

III. PROPOSED EVCS ALGORITHM FOR GRAY SECRET IMAGE

Algorithm: Embedding gray secret image into meaningful covering images.
Input: gray secret image and meaningful covering images.
Output: embedded shares and stacked shares to reveal secret image.
Steps:
1. Input the secret gray image.
2. Halftone the secret image.
3. Input meaningful images.
4. Halftone the meaningful images.
5. Divide the secret image into two shares images.
6. Divide the two shares images into blocks of 2x2 pixels.
7. Choose a block from share 1 and another block from share 2 at the same position to represent a secret pixel.
8. For each black secret pixel, randomly choose a block from share 1 that is complementary to a block in share 2 at the same position as listed in Table 1.
9. For each white secret pixel, the two blocks from share 1 and share 2 are the same as listed in Table 1.
10. Embed the chosen secret pixel into the embedding positions chosen in step 7.
11. Stacking the shares and the secret can be displayed.

| White secret pixel | Share1 block | Share2 block | Two blocks are the same | Stacking results |
|--------------------|--------------|--------------|------------------------|-----------------|
|                     |              |              |                        |                 |

| Black secret pixel | Share1 block | Share2 block | Two blocks are complementary to each other | Stacking results |
|--------------------|--------------|--------------|-------------------------------------------|-----------------|
|                    |              |              |                                           |                 |

Fig. 3: Shows secret pixel representations

The result of the process of embedding secret image into covering shares and stacked the shares to reveal the secret is shown in Fig. 3 secret image (a), two covering shares (b), secret image embedded into shares (c) then these shares are stacked and the secret image is revealed.

Fig. 4: Shows result of the proposed algorithm

As shown in Fig. 4, embedded shares and reconstructed secret image have bad visual quality. For embedded shares bad visual quality may attract Intruders and hackers who can intercept data transmission to create data security problem. For reconstructed secret image bad visual quality means loss of important information. Next section will discuss how to improve the visual quality of both embedded shares and revealed secret image.
IV. IMPROVING VISUAL QUALITY OF THE RECONSTRUCTED SECRET IMAGE

Since the quality of the reconstructed or restored secret image is important, in this section we examine the relationship between the secret image and the cover images in order to find out the factors that affect in the visual quality of the reconstructed secret image and improving the visual quality of both embedded shares and revealed secret image.

We used a well-known objective numerical measurements for measuring the visual quality of covering shares and secret image, such as Mean Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Average Difference (AD) and Structural Similarity (SSIM).

These numerical measurements are measure the closeness of two images or the differences in similarity between them.

There are many measures that are used to measure the closeness between two images by exploiting the differences in the distributions of pixel values.

In our work, we need to measure the closeness between the secret image and the cover shares and after reconstructing the secret we need to measure the closeness between the secret and reconstructing images.

MSE, PSNR, and SSIM are some useful and most commonly used objective image quality measures [13], also they defined mathematically the image quality measurement.

MSE, PSNR, AD and SSIM are used as Image Quality Metrics in comparing similarity between two images, the original image and the reconstructed image.

MSE and its variants such as PSNR are commonly used as objective IQM [14], these numerical measurements are measure the closeness of two images or the differences in similarity between them.

MSE and PSNR are the two most common full-reference measures for objective assessment of the image quality [15].

The simplest and most widely used pixel wise error based measures are Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) [16].

MSE and PSNR are the two most common full-reference measures for objective assessment of the image quality [15].

A. Mean Square Error (MSE):

MSE averages the squared pixels intensity of the original image and the reconstructed image. The lower the value of MSE, the lower the error [17]. The large value of MSE means that image is poor quality [18].

MSE [19] is calculated for (m x n) image is given as follows:

$$MSE = \frac{1}{mn} \sum_{i=1}^{m} \sum_{j=1}^{n} (x(i,j) - Y(i,j))^2$$

Where, $x$ is a pixel of the reference image and $Y$ is the equivalent pixel of compared image.

B. Peak Signal to Noise Ratio (PSNR):

PSNR is used in decibels as a quality measurement between the original and reconstructed image. Higher the PSNR value means better the quality of reconstructed image.

As mentioned before PSNR is based on the pixel difference between two images, which means that PSNR measures an estimate of quality of reconstructed image compared with original image.

PSNR is often used to compare image quality in compression schemes [19], PSNR is calculated using MSE as follows:

$$PSNR = 10 \log_{10} \left( \frac{M^2}{MSE} \right)$$

PSNR is used as a quality measurement between the original and a compressed image. The higher the PSNR, the better the quality of the compressed or reconstructed image [17]. PSNR, Higher is better [20].

The PSNR value approaches infinity as the MSE approaches zero; this shows that a higher PSNR value provides a higher image quality [21].
C. Average Difference (AD):
AD is simply the average of difference between the reference image and test image [13]. It is calculated as follows:

\[ AD = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} (x(i,j) - Y(i,j)) \]

D. Structural Similarity (SSIM):
SSIM is used to compare the structural similarity between the original and the reconstructed images. SSIM [19] is calculated as follows:

\[ SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{\left(\mu_x^2 + \mu_y^2 + c_1\right)\left(\sigma_x^2 + \sigma_y^2 + c_2\right)} \]

Where, \( x \) and \( y \) are the reference and the test images respectively. \( \mu_x, \mu_y \) are the image averages and \( \sigma_x^2, \sigma_y^2 \) are the respective variances.

SSIM seems to reflect the structural changes in the images much better than MSE.
SSIM is based upon separated comparisons of local luminance, contrast and structure between an original and a distorted image [22]. SSIM mimics quite well the perceived quality of an image by a human observer [23].

SSIM values are between 0 and 1, value 1 indicates perfect structural similarity, and value 0 indicates no structural similarity.

V. CASE STUDY NO.1
In our experiments fifty images of size 512×512 pixels are used as the cover images as shown in Fig.5, these images are known as standard test images in the field of image processing. Three images of size 256×256 pixels are used as secret images as shown in Fig.6. In our experiment we try to find the relationship between cover shares and secret image in order to get a clear picture of the visual quality of the reconstructed secret image.

Fig.5 : 50 standard test images as cover images
VI. EXPERIMENTAL RESULTS AND ANALYSIS OF CASE STUDY NO.1

First we choose randomly any 2 cover images from the collection to hide cameraman secret image and the result of hiding and restoring secret image is shown in Fig.7. secret image (a) is encoded into two camouflage cover images (b) the encoded meaningful shares (c) then these shares are distributed to participants and then the shares are stacked to restore the secret image (d).

![Secret images](image1)

![Secret images](image2)

![Secret images](image3)

![Secret images](image4)

**Fig.6**: Secret images

![Visual cryptography scheme using any cover images](image5)

**Fig.7**: Visual cryptography scheme using any cover images

To improve the visual quality of the reconstructed secret image, we choose cover images that are related to the secret image i.e. by measuring the difference between the cover images and secret image. To measure the difference between two images we use MSE, PSNR and AD and the values are as listed in table 2.

| Cover No. | MSE | PSNR | AD | Cover No. | MSE | PSNR | AD | Cover No. | MSE | PSNR | AD | Cover No. | MSE | PSNR | AD |
|----------|-----|------|----|----------|-----|------|----|----------|-----|------|----|----------|-----|------|----|
| 1        | 125 | 27   | 34 | 11       | 181 | 26   | 65 | 21       | 174 | 26   | 41 | 31       | 177 | 26   | 52 |
| 2        | 32  | 33   | 7  | 12       | 137 | 27   | 34 | 22       | 183 | 26   | 55 | 32       | 150 | 26   | 32 |
| 3        | 57  | 31   | 17 | 13       | 163 | 26   | 51 | 23       | 181 | 26   | 64 | 33       | 129 | 27   | 34 |
| 4        | 161 | 26   | 56 | 14       | 186 | 25   | 47 | 24       | 161 | 26   | 56 | 34       | 178 | 26   | 52 |
| 5        | 61  | 30   | 13 | 15       | 169 | 26   | 41 | 25       | 178 | 26   | 65 | 35       | 129 | 27   | 23 |
| 6        | 183 | 26   | 45 | 16       | 173 | 26   | 56 | 26       | 149 | 26   | 59 | 36       | 122 | 27   | 34 |
| 7        | 169 | 26   | 54 | 17       | 173 | 26   | 53 | 27       | 164 | 26   | 49 | 37       | 145 | 27   | 39 |
| 8        | 138 | 27   | 41 | 18       | 183 | 26   | 57 | 28       | 167 | 26   | 58 | 38       | 166 | 26   | 55 |
| 9        | 166 | 26   | 62 | 19       | 179 | 26   | 49 | 29       | 135 | 27   | 32 | 39       | 110 | 28   | 26 |
| 10       | 169 | 26   | 65 | 20       | 180 | 26   | 65 | 30       | 178 | 26   | 61 | 40       | 163 | 28   | 32 |

According to numerical measurements values listed in Table 2, we choose the two covers that have the least differences with the secret image, relatively close in similarity, as displayed in Fig.8, and also we choose the two cover that have the most differences with the secret image as displayed in Fig.9.
MSE = 32
PSNR = 33
AD = 7

MSE = 57
PSNR = 31
AD = 17

Fig. 8: Two cover images with lowest difference with the secret image

MSE = 185
PSNR = 25
AD = 59

MSE = 186
PSNR = 25
AD = 47

Fig. 9: Two cover images with highest difference with the secret image

The result of embedding secret image into the least differences shares and reconstructing the secret are shown in Fig. 10.

Fig. 10: Embedding secret image into the least differences shares

The result of embedding secret image into the most differences shares and reconstructing the secret are shown in Fig. 11.

Fig. 11: Embedding secret image into the most differences shares
According to results appeared in Figures 7, 10 and 11, reconstructed secret images have good visual quality when we using shares that are similar to secret image as we summarized the results in Fig. 10. (a) Reconstructed secret image using any two shares, (b) reconstructed secret image using two shares with highest differences from original secret image (c) reconstructed secret image using two shares with lowest differences from original secret image.

![Fig. 10: Comparison of reconstructed secret image using different shares](image)

By doing more experiments using different secret images, the results are displayed in Fig. 12, (a) Reconstructed secret images using shares with lowest differences with original secrets and (b) Reconstructed secrets using shares with highest differences with original secrets.

![Fig. 12: Experimental results of improving visual quality for the reconstructed image](image)

We used SSIM to indicate that the reconstructed secret by using shares with lowest differences with the original secret is much better than the reconstructed secret by using shares with highest differences with the original secret, since SSIM is Structural Similarity Based.

In this section, we checked the validity of the proposed scheme in order to embed secret image into two meaningful cover shares and then reconstruct the secret.

Since each secret pixel is represented by a block of 2x2 pixels at cover shares, this means that the reconstructed secret image will be expanded in size; hence the contrast of the cover shares is reduced as a result of embedding secret pixels.

Since by stacking the shares will reveal the secret, then it is important to improve the visual quality of the meaningful shares, we choose shares that are more similar, in structure and color distribution, to the secret by using the numerical measurements as mentioned before. By choosing suitable shares, the visual quality of the generated shares are increased and these share will look natural shares which gives us the advantage of avoiding attacks of hackers and intruders.

As a result of improving the visual quality of the shares, the visual quality of the reconstructed secret also increased.
VII. CASE STUDY NO.2

In our experiments 9084 images of size 512×512 pixels are used as the cover images as shown in Fig.13, these images are taken from Caltech 101 dataset at [24].

![Sample of Caltech 101 dataset as cover images](image1)

One image of size 256×256 pixels is used as a secret image as shown in Fig.14.

In our experiment we try to find the relationship between cover shares and secret image in order to get a clear picture of the visual quality of the reconstructed secret image.

![Secret image](image2)

In our experiment we try to find the relationship between cover shares and secret image in order to get a clear picture of the visual quality of the reconstructed secret image.

VIII. EXPERIMENTAL RESULTS AND ANALYSIS OF CASE STUDY NO.2

To improve the visual quality of the reconstructed secret image, we choose cover images that are related to the secret image, i.e. by measuring the difference between the cover images and secret image. To measure the difference between two images we use MSE, PSNR and AD.

According to numerical measurements values of MSE, PSNR and AD, we choose the two covers that have the least differences with the secret image, relatively close in similarity, as displayed in Fig.15, and also we choose the two cover that have the most differences with the secret image as displayed in Fig.16.

![Two cover images with lowest difference with the secret image](image3)

![Two cover images with highest difference with the secret image](image4)
The result of embedding secret image into the least differences shares and reconstructing the secret are shown in Fig.17.

The result of embedding secret image into the most differences shares and reconstructing the secret are shown in Fig.18.

According to results appeared in Figures 17 and 18, reconstructed secret images have good visual quality when we using shares that are similar to secret image as we summarized the results in Fig.19. (a) Reconstructed secret image using two shares with highest differences from original secret image (b) reconstructed secret image using two shares with lowest differences from original secret image.
IX. CONCLUSION

Traditional visual cryptography schemes encode secret image into shares that are meaningless which cause security problem, since the meaningless shares can attract intruders and hackers.

Our objective is to propose a (2-2) visual cryptography scheme for embedding secret image into two meaningful shares and improving the visual quality of the generated shares and reconstructed secret.

In this paper, we proposed a visual cryptography scheme for embedding secret image into two meaningful shares. To improve the visual quality of the reconstructed secret image and shares ,which is important to avoid attacks of hackers, we check to use shares that are almost similar to secret by using numerical measurements , such as MSE and PSNR, to check which shares have less or more differences from the secret.

Experimental results show that using shares that are less different from secret, we obtained relative good visual quality shares which helps in avoiding unwanted attacks and as a result, relatively better good visual quality reconstructed secret than using any shares.

The proposed scheme works for one secret to generate two meaningful shares with 2x2 pixel expansion.

Embedding more than one secret into meaningful shares and improving the visual quality of the shares and reconstructed secret are considered as the future work.

REFERENCES

[1] Suchethana H C, Visual Cryptography and Its Challenges, International Journal of Computer Engineering and Applications, Volume XII, Issue I, 2018.
[2] M. Ulutas, "Meaningful Share Generation for Increased Number of Secrets in Visual Secret-Sharing Scheme", Hindawi Publishing Corporation, Mathematical Problems in Engineering, Article ID 593236, 18 pages, 2010.
[3] K. Brindha, and N. Jeyanthi, "Secret Image Enhanced Sharing Using Visual Cryptography", Cybernetics and Information Technologies, Volume 17, No 3, 2017.
[4] J. Weir , and W. Yan , "Visual cryptography and its applications" Jonathan Weir and WeiQi Yan & Ventus Publishing ApS ISBN 978-87-403-0126-7, 2012.
[5] M. Nakajima , and Y. Yamaguchi," Extended visual cryptography for natural images", in the Journal of WSCG, Volume 10, No.1-3, 2002.
[6] J. Verm, and V. Khemchandani,"A Visual Cryptographic Technique to Secure Image Shares", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 1, pp.1121-1125, 2012.
[7] D. Wang, L. Zhang, N. Ma and X. Li " Two secret sharing schemes based on Boolean operations", Pattern Recognition Society, Published by Elsevier Ltd. 2007.
[8] A. V. Dahata , and P. V. Chavanb, "Secret Sharing Based Visual Cryptography Scheme Using CMY Color Space", International Conference on Information Security & Privacy (ICISP2015), pages 563 – 570, 2015.
[9] Y. H. Ismaiel, and M. M. Khether, "Binary Image Visual Cryptography", International Journal of Computer Applications, Volume 177, No 6, 2017.
[10] Chin-Chen Chang, Bo Li, and Jung-San Lee, "Secret Sharing Using Visual Cryptography", Journal of Electronic Science and Technology, Volume 8, NO 4, 2010.
[11] Asha S.N. ,Shreedhara K.S.M.Tech., and Smt. Anitha G. BE "Performance Evaluation Of Extended Visual Cryptography Schemes With Embedded Extended Visual Cryptographic Scheme ", International Journal of Scientific & Engineering Research Volume 3, Issue 4, 2012.
[12] Chang-Chou Lin, and Wen-Hsiang Tsai, "Visual cryptography for gray-level images by dithering techniques", Pattern Recognition Letters 24 pages 349–358, 2003.
[13] C. S. varnan, A. Jagan, J. Kaur, D. Jyoti , and D. S. Rao "Image Quality Assessment Techniques on Spatial Domain", International Journal of Computer Science and Technology, Vol. 2, Issue 3, September 2011.
[14] K. Thung, and P. Raveendran, "A Survey of Image Quality Measures", International Conference for Technical Postgraduates (TECHPOS), 2010.
[15] P. Gupta, P. Srivastava, S. Bhardwaj , and V. Bhateja ,"A HVS based Perceptual Quality Estimation Measure for Color Images", Signal & Image Processing, Volume 03, No. 01, 2012.
[16] M. Fathimal, and A. Jansirani, "New Fool Proof Examination System through Color Visual Cryptography and Signature Authentication", the International Arab Journal of Information Technology, Vol. 16, No. 1, 2019.
[17] S. B. Patel, and V. L. Desai, “Evaluation of Visual Cryptography Halftoning Algorithms ”, International Journal of Latest Technology in Engineering, Management & Applied Science, Volume III, Issue VIII, 2014.
[18] V. S. Vora,. A. C. Suthar, Y. N. Makwana, and S. J. Davda, "Analysis of Compressed Image Quality Assessments ", International Journal of Advanced Engineering & Application, 2010.
[19] R. Wajid, A. B. Mansoor and M. Pedersen, "A Human Perception Based Performance Evaluation of Image Quality Metrics", Springer International Publishing Switzerland LNCS 8887, pp. 303–312, 2014.
[20] D. Singh, and P. Sharma, "Comparison of various Error Diffusion Algorithms Used in Visual Cryptography with Raster scan ", International Journal of Engineering Development and Research, Volume 5, Issue 2,2017.
[21] A. Horé, and D. Ziou," Image quality metrics: PSNR vs. SSIM", International Conference on Pattern Recognition, 2010.
[22] Z. Wang, and Q. Li, "Information Content Weighting for Perceptual Image Quality Assessment", IEEE Transactions on Image Processing, Volume 20, NO 5, 2011.
[23] G. P. Renieblas, A. T. Noguès, A. M. González, N. Gómez-Leon, and E. G. del Castilloa, "Structural similarity index family for image quality assessment in radiological images", Journal of Medical Imaging, Volume 4, 2017.
[24] http://www.vision.caltech.edu/Image_Datasets/Caltech101/Caltech101