iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 Issue: I Month of publication: January 2019

DOI: http://doi.org/10.22214/ijraset.2019.1104

An Efficient Image Hiding Technique based on Secret Fragment Visible Mosaic Images using DCT Algorithm

Vaishma K[1], Karthik M[2], Usha S[3]
[1]Department of EEE, Kongu Engineering College, Erode

Abstract: This paper presents a new secure image transmission technique called secret fragment visible mosaic image. The secret image is embedded into the created mosaic image by a lossless data hiding scheme using a key and the secret image cannot be recovered without the key. DCT algorithm is proposed to find a similar tile image in the secret image to fit into each block in the target image. The given original image divides into smaller tiles of images and these tiles are rearranged to become the final carrier image looking like a mosaic image. A new technique for secure image transmission in which transforming a secret image into a meaningful mosaic image with the same size and looking like a preselected target image. The main issue is for hiding data in images is the difficulty to embed a large amount of message data into a single image. The mosaic image is the result of rearrangement of the secret image in disguise of another image called the target image preselected from a database. The generated mosaic image is similar to the selected target image. The transformation process is controlled by a secret key and only with the help of secret key a person can able recover the secret image nearly lossless from the mosaic image. The simulated version of the proposed system is developed using MATLAB R2017b and desktop application of the project is developed using MATLAB GUIDE.

Keywords: Color Transformation, Data Hiding, Image Encryption and Decryption, Mosaic Image, DCT Algorithm, Secure Image Transmission.

I. INTRODUCTION

Internet has become more popular and common now-a-days. Sending the vital information through cyber web has become a significant threat. Moreover routing the information in associate in nursing encrypted format is extremely common and embedding the key message in a picture may be a challenge. To safeguard the pictures from the embezzled hindrance or interception, techniques like watermarking, image concealment is employed for the safe transmission of pictures [5]. Image processing is a method used to convert an image into digital form and it performs some operations on it. In order to induce associate in nursing increased image or to extract some helpful data from it. It is a type of signal dispensation. The input is image, like video frame or photograph and the output may be image or characteristics associated with that image. Usually this type of Image Processing system includes treating images as two dimensional signals while applying already set signal processing methods to them. It is among quickly growing technologies nowadays, with its applications in various aspects of a business. Image process forms core analysis space at intervals engineering and computing disciplines too [12]. Image processing basically includes the following three steps,

A. Importing the image with by digital photography or optical scanner.
B. Analyzing and manipulating the image and also it includes data compression.
C. Image enhancement and spotting patterns that are not to human eyes like satellite photographs.

Analog or visual techniques of image process are often used for the laborious copies like printouts and pictures. Image analysts use numerous fundamentals of interpretation whereas mistreatment these visual techniques. The image process isn't simply confined to space that should be studied however on data of analyst [2]. Association is the another vital tool in image process through visual techniques. Information from the imaging sensors from satellite platform contains deficiencies. To get over such flaws and to induce originality of knowledge, it has to undergo various phases of processing. The 3 general phases that each one styles of information need to endure whereas mistreatment digital technique area unit,

1) Pre - processing.
2) Enhancement and display.
3) Information extraction.

Mosaic is a type of art work created by composing small piece of materials, such as stone, glass, tile, etc. They are still used in many applications today. Creation of mosaic images by computer is a new search direction in recent years. Image Mosaicing could be a methodology of constructing multiple pictures of an equivalent scene into a bigger image [14]. The output of the image mosaic are the union of 2 input pictures. Image mosaicing is wide utilized in making 3D pictures, medical imaging, computer vision, data from satellites, and military automatic target recognition. Image mosaics area unit collections of overlapping pictures that area unit reworked so as to lead to an entire image of a good angle scene. The transformations are often viewed as easy relations between coordinate systems.

II. LITERATURE SURVEY

A SYMMETRIC IMAGE ENCRYPTION SCHEME BASED ON 3D CHAOTIC CAT MAPS [3], By analyzing and researching several digital chaotic image encryption algorithms, this paper designs a symmetric image encryption scheme supported the 3 dimensional Henon chaotic map and also the general Cat chaotic map. In this theme, the chaotic sequence of general Cat map is employed because the data format sequence to confuse the positions of image pixels; the 3 dimensional Henon chaotic map will diffuse the image pixels; Then, repeat the confusing and diffusing process to increase the resistance to statistical and related attacks. Thorough experimental tests area unit distributed with elaborate analysis, demonstrating the high security and fast encryption speed of the new scheme.

A NOVEL ALGORITHM FOR IMAGE ENCRYPTION BASED ON MIXTURE OF CHAOTIC MAPS [18], In this paper, an implementation of digital image encryption scheme based on the mixture of chaotic systems is according. The chaotic cryptography technique utilized in this paper may be a isobilateral key cryptography. In this algorithmic program, a typical coupled map was mixed with a 1 dimensional chaotic map and used for prime degree security image coding whereas its speed is appropriate. The projected algorithmic program is delineate intimately, in conjunction with its security analysis and implementation. The experimental results supported mixture of chaotic maps approves the effectiveness of the projected technique and therefore the implementation of the algorithmic program. This mixture application of chaotic maps shows benefits of huge key area and high-level security. The cipher text generated by this method is the same size as the plain text and is suitable for practical use in the secure transmission of confidential information over the Internet.

HIDING DATA IN IMAGES BY SIMPLE LSB SUBSTITUTION [9], In this paper, a data hiding scheme by simple LSB substitution is proposed. By applying associate degree optimum pel adjustment method to the stego image obtained by the straight forward LSB substitution technique, the image quality of the stego-image can be greatly improved with low extra computational complexity. The worst case mean square-error between the stego image and therefore the cover-image springs. Experimental results show that the stego-image is visually indistinguishable from the initial cover-image. The obtained results conjointly show a major improvement with reference to a previous work.

AN IMAGE ENCRYPTION APPROACH BASED ON CHAOTIC MAPS [27], It is well-known that images are different from texts in many aspects, such as highly redundancy and correlation, the local structure and the characteristics of amplitude–frequency. As a result, the strategies of typical coding can't be applicable to pictures. In this paper, we have a tendency to improve the properties of confusion and diffusion in terms of distinct exponential chaotic maps, and style a key scheme for the resistance to data point attack, differential attack and grey code attack. Experimental and theoretical results conjointly show that our theme is economical and really secure.

III. PROPOSED METHOD

Fig. 1 represents the block diagram of proposed method. Selecting the key image for making mosaic image, at that time choosing the foremost similar target image for the chosen supply image. We have an efficient similarity algorithm for comparing similarity value between both the images. Then we've got produce the tile pictures for making a mosaic image, we want to split the source image into particular size small image called as tile. The tile pictures are compared with the target image to obtaining the position for putting the tile into the target image. Then we have to search out the position that is dead matching for every tile of secret image. After finding the position of every tile, then we have to create a new blank image for placing the tile in it. Then placing the tile images based on the information presented in the fitting sequences. We can generate the duplicate tile pictures for finishing the image as target image. Then embedding the fitting sequence file into the created mosaic image by using the algorithm to hide the fitting sequence information. By using this the receiver can able to reconstruct the original image as it send by the sender. The fitting sequence containing the knowledge regarding the image name and wherever it's utterly matched in target image position. After receiving the mosaic image, we can first de-embedding the fitting file, because with the help of this only we split the tile images presented in the mosaic image. Then we've got to separate the mosaic created image. Finally compared the images got from the mosaic image that sender can send.

A. Mean Square Error (MSE)

The MSE assesses the standard of associate computer (i.e., a function mapping a sample of knowledge to associate estimate of a parameter of the population from that the info is sampled) or a predictor (i.e., a perform mapping arbitrary inputs to a sample of values of some random variable). The definition of associate MSE differs consistent with whether or not one is describing associate computer or a predictor [6]. Ifˆ is a vector of n predictions generated from a sample of n data points on all variables, and Y is the vector of observed values of the variable being foreseen, then the among sample MSE of the predictor is computed as,

$$\text{MSE} = \frac{1}{n}\sum_{i=1}^{n}(Yi - \hat{Y}i)2$$

i.e., the MSE is the mean ($\frac{1}{n}\sum_{i=1}^{n}$) of the squares of the errors $(Yi - \hat{Y}i)2$.

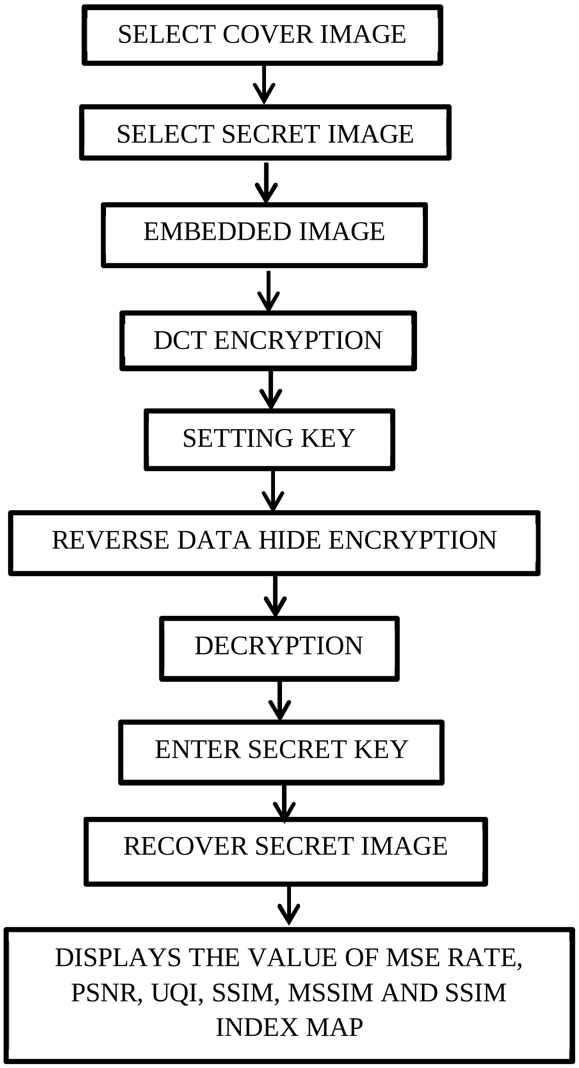


Fig. 1 Block diagram of Proposed method

B. Peak Signal to Noise Ratio (PSNR)

The PSNR block computes the height S/N, in decibels, between 2 pictures. This quantitative relation is usually used as a top quality measuring between the initial and a compressed image. The higher the PSNR, higher the standard of the compressed or reconstructed image. The Mean sq. Error (MSE) and therefore the Peak Signal to Noise quantitative relation (PSNR) are the 2 error metrics wont to compare compression quality [10]. The MSE represents the accumulative square error between the compressed and therefore the original image, whereas PSNR represents a live of the height error. The lower value of MSE is lower the error. To cipher the PSNR, the block initial calculates the mean-squared error victimization the next equation,

$$\mathrm{MSE} = \frac{1}{M * N} \sum_{M,N} [I1(m,n) - I2(m,n)]2$$

In the previous equation, M and N square measure the amount of rows and columns within the input pictures, severally. Then the block computes the PSNR subsequent equation,

$$\mathrm{PSNR} = 10 \log10(R2/\mathrm{MSE})$$

C. Universal Quality Index (UQI)

The universal image quality index, which is easy to calculate and applicable to various image processing applications. This index is mathematically defined and no human visual system model is explicitly employed.

The UQI is computed as,

$$Q = 4\, \sigma_{xy}\, \bar{x}\bar{y} \,/\, (\sigma_z^2 + \sigma_y^2)\, [(\bar{x})^2 + (\bar{y})^2]$$

D. Structural Similarity Index (SSIM)

SSIM is employed for measuring the similarity between 2 pictures. The SSIM index may be a full reference metric; in alternative words, the measurement or prediction of image quality is based on an initial uncompressed or distortion-free image as reference. SSIM is intended to boost on ancient strategies like peak signal-to-noise ratio (PSNR) and mean squared error (MSE).

$$\mathrm{SSIM}\,(x,y) = (2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2) \,/\, (\mu_x^2\mu_y^2 + c_1)(\,\sigma_x^2 + \sigma_y^2 + c_2)$$

E. Mean Structural Similarity Index (MSSIM)

MSSIM is layered on SSIM. It is based on SSIM metric of several downscaled levels of original images. Result is weighted average of those metrics. At the m^{th} scale, contrast and structure comparisons are evaluated and denoted as $c_m(x,y)$ and $s_m(x,y)$ respectively.

$$\mathrm{MSSIM}(x,y) = [I_M(x,y)]^a \,.\, \prod_{m=1}^{M} [c_m(x,y)]^{\beta} \,.\, [s_m(x,y)]^{\gamma}$$

IV. EXPERIMENTAL RESULTS

A series of experiments are conducted to check the planned technique exploitation several secret and target pictures. To show that the created mosaic image looks like the preselected target image, the quality metric of Mean Square Error (MSE) is utilized, which is defined as the mean square distinction between the component values of the 2 pictures. The mosaic image is yielded by dividing the secret image into tile images and transforming their color characteristics to be those of the corresponding target blocks, the global color characteristics of a transformed tile image and its corresponding target block are the same but the color distributions of them maybe quite different. Hence, although the mosaic image has the visual appearance of the target image, the details of each fragment in the mosaic image may have low similarity to those of its corresponding target block. To measure this mosaic effect, we adopt the Metric of Mean Structural Similarity (MSSIM) to compare the similarity of the created mosaic image and the target image.

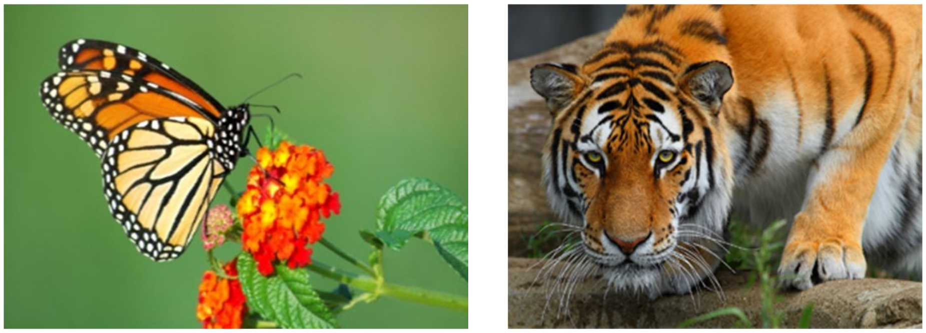


Fig. 2 (a) Secret Image (b) Target Image

Fig. 2 shows the secret image and the target image that is the host image. User can select any image as the target image.

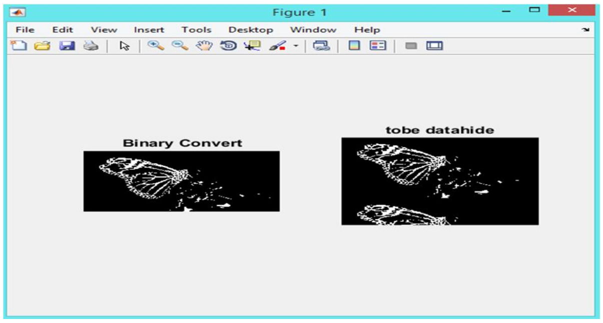


Fig. 3 Binary Image of Secret Image

Fig. 3 shows the output of binary image of secret image because for embedding the secret image and the target image should be in the same size.

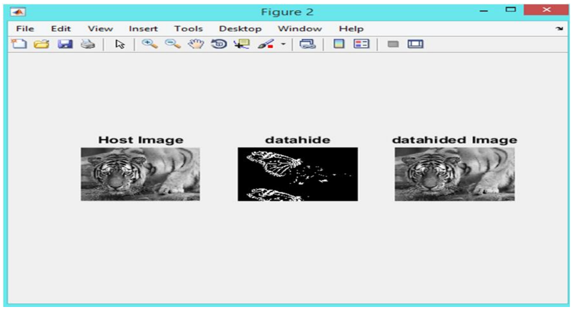
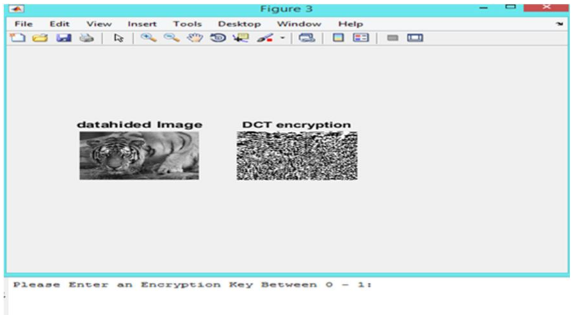


Fig. 4 Embedded Image of Secret and Target Image

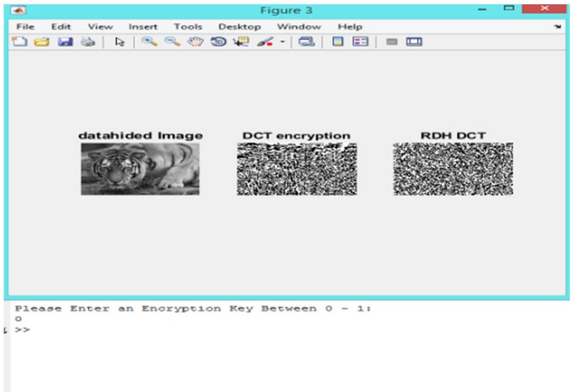
Fig. 4 shows the host image, binary image of secret image and the embedded image of the secret image and the target image.



```
Please Enter an Encryption Key Between 0 - 1:
```

Fig. 5 Generating DCT Encryption Image

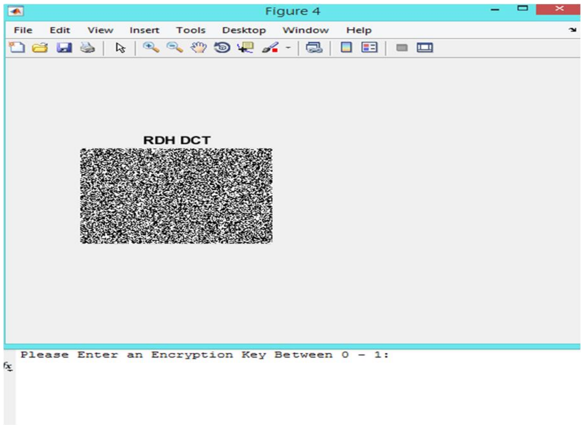
Fig. 5 shows the embedded image and the generation of DCT encryption image from the embedded image.



```
Please Enter an Encryption Key Between 0 - 1:
0
>>
```

Fig. 6 Generating RDH DCT Image

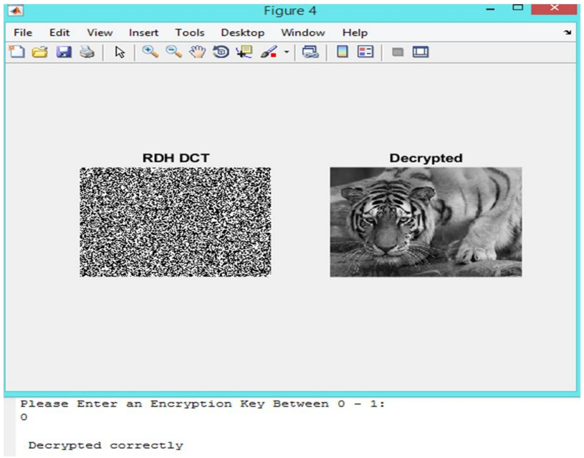
Fig. 6 shows the embedded image, DCT encryption image and generation of RDH DCT image from the DCT encryption image after setting the secret key.



```
Please Enter an Encryption Key Between 0 - 1:
```

Fig. 7 Decryption Image

Fig. 7 shows the RDH DCT image in the decryption side to recover the secret image.



```
Please Enter an Encryption Key Between 0 - 1:
0

 Decrypted correctly
```

Fig. 8 Decrypted the Original Image

Fig. 8 shows the decrypted image from RDH DCT image by entering the correct secret key.

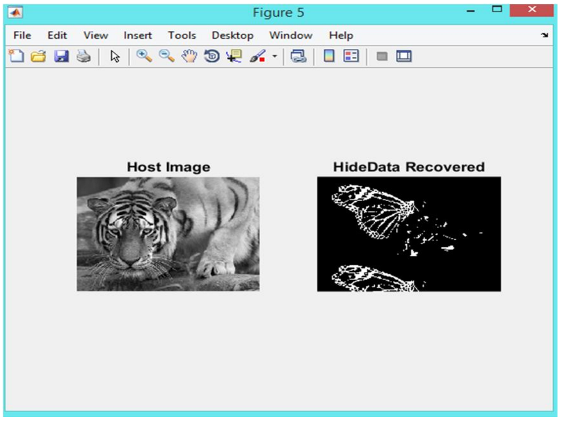
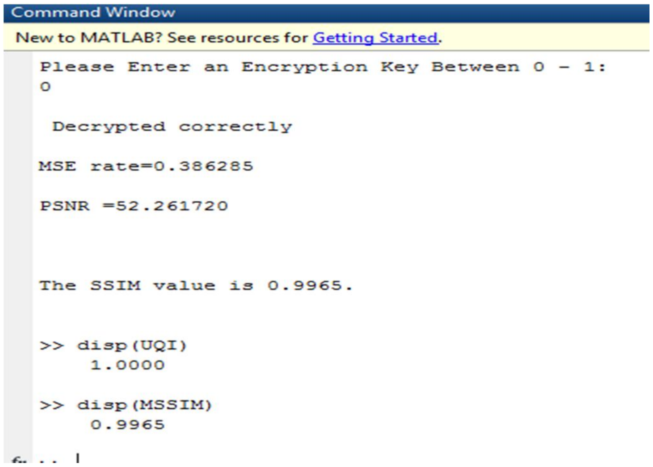


Fig. 9 Decrypted Target Image and Secret Image

Fig. 9 shows the recovered cover image that is host image and the binary image of the secret image.



```
Please Enter an Encryption Key Between 0 - 1:
0

 Decrypted correctly

MSE rate=0.386285

PSNR =52.261720


The SSIM value is 0.9965.


>> disp(UQI)
    1.0000

>> disp(MSSIM)
    0.9965
```

Fig. 10 Command Window Output Image

Fig. 10 shows the output of MSE, PSNR, UQI, SSIM and MSSIM values which displays in the command window.

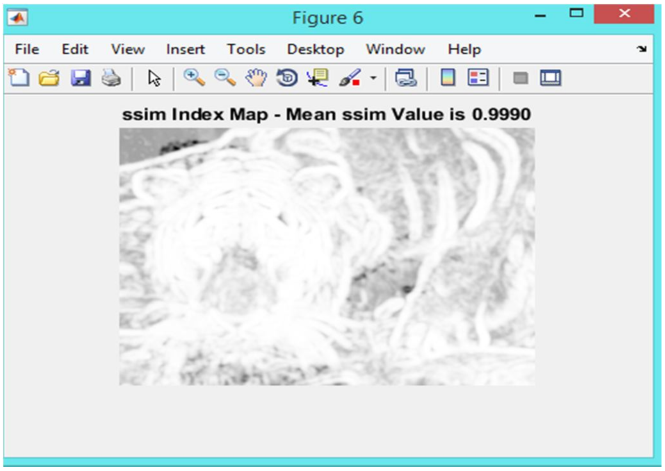


Fig. 11 SSIM Index Map Image

Fig. 11 shows the output of Structural SIMilarity index map image for the value 0.9990.

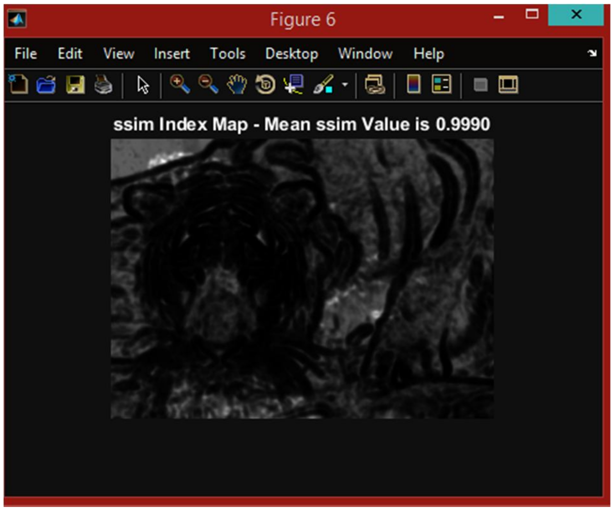


Fig. 12 Invert Color of SSIM Index Map Image

Fig. 12 shows the output of inverted color of Structural SIMilarity index map image for the value 0.9990.

Table 1
Tabulation of MSE, PSNR, UQI, SSIM and MSSIM Value for No Noise and Adding Salt & Pepper Noise, Poisson Noise, Speckle Noise and Gaussian Noise

S. N O.	IMAGES	NO NOISE				
		SALT & PEPPER NOISE				
		POISSON NOISE				
		SPECKLE NOISE				
		GAUSSIAN NOISE				
		MSE	PSNR	SSIM	UQI	MSSIM
1		0.4628	51.476	0.9966	0.9999	0.9966
2		0.4624	51.479	0.9955	0.9875	0.9955
3		0.4507	51.591	0.9974	0.9976	0.9974
4		0.4543	51.557	0.9966	0.9880	0.9966
5		0.4632	51.472	0.9971	0.9933	0.9971
6		0.4418	51.678	0.9971	0.9999	0.9971
7		0.4428	51.668	0.9972	1.0000	0.9972
8		0.4424	51.671	0.9970	0.9999	0.9970
9		0.4626	51.478	0.9990	1.0000	0.9990
10		0.2952	53.428	0.9980	0.9306	0.9980

Table 1 shows the value of MSE, PSNR, UQI, SSIM and MSSIM for no noise and adding salt & pepper noise, Poisson Noise, Speckle Noise and Gaussian Noise for different secret images. From the table it shows that the values are same. So the images are insensitive to noise.

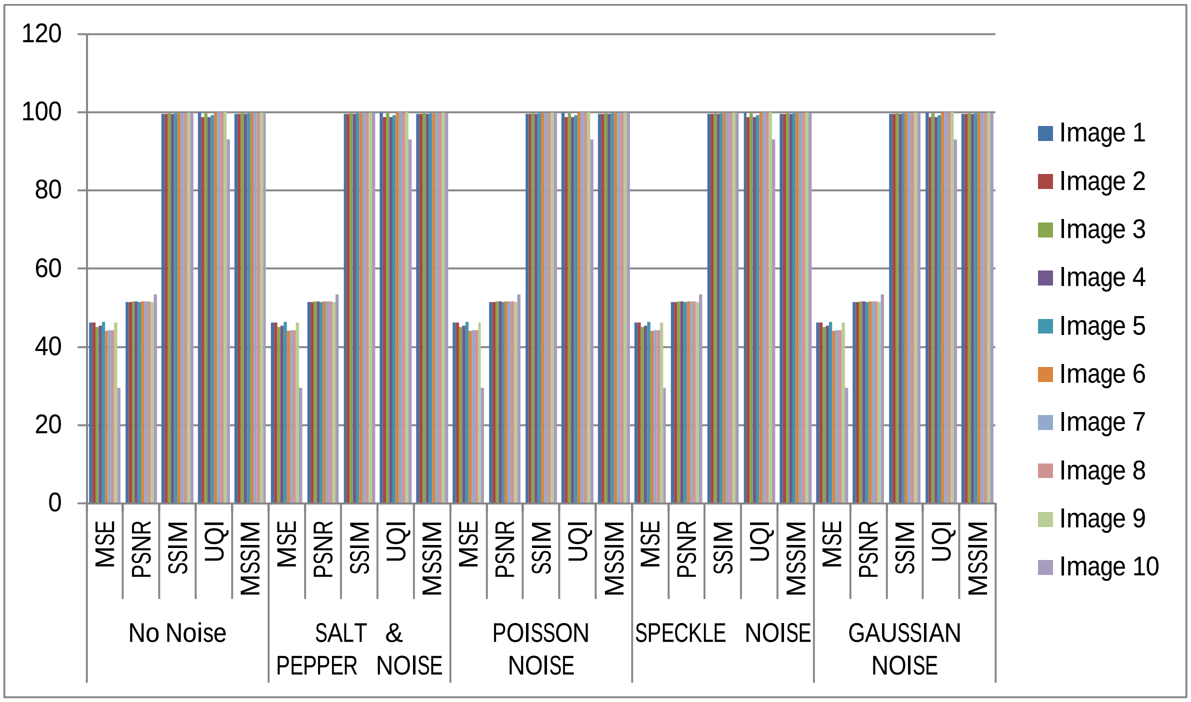


Fig. 13 Graph diagram for different secret images

Fig. 13 This graph represents the MSE, PSNR, SSIM, UQI and MSSIM value for different secret images and also clearly shows that the images are insensitive to the noise.

V. CONCLUSION

A new secure image transmission method has been proposed, which not only create meaningful mosaic images but also transform a secret image into a mosaic one with the same data size to be used as a camouflage of the key image. By the use of proper pixel color transformations as well as a skillful scheme for handling overflows and underflows in the converted values of the pixels colors, secret-fragment visible mosaic images with very high visual similarities to arbitrarily-selected target images are created with no need of a target image database. Also, the initial secret pictures are often recovered nearly losslessly from the created mosaic pictures. Good experimental results have shown the feasibleness of the planned technique. The mosaic image was created, encryption and decryption process was done successfully by entering the secret key and also analyzed the MSE, PSNR, UQI, SSIM and MSSIM values for different secret images to show the images are strong and robustness.

VI. FUTURE SCOPE

The future enhancement is to apply the proposed method to the images of color models other than the RGB. Furthermore, an additional secret key can be used to prevent hackers from trying to extract the secret key. So without the help of the second key, the original bit pattern cannot be recovered. Even if a hacker's random trial leads to correct extraction, the extracted index will be still in the form of random bit pattern. The main problem of today's world is to secure their data confidentially and can be applied differently in digital image, audio and video file but it can be done faster with the large number of software.

REFERENCES

[1] Digvijay Singh Chauhan, Abhinav Adarsh, Basant Kumar, Rajeev Gupta and J P Saini, (2017) 'Double Secret Key Based Medical Image Watermarking For Secure Telemedicine In Cloud Environment', 978-1-5090-3982-1/17 IEEE.

[2] Nguyen, Sy C., Ha Hoang Kha, and Hoang M. Nguyen. (2017) 'An efficient image watermarking scheme using the Laplacian Pyramid based on projection', International Conference on, pp. 103-108 IEEE.

[3] G. Chen,Y. Mao, and C. K. Chui, (2004) 'A symmetric image encryption scheme based on 3D chaotic cat maps', Chaos Solit. Fract., vol. 21, no. 3, pp. 749–76.

[4] Miyake S, Nakamae K. (2016) 'A quantum watermarking scheme using simple and small-scale quantum circuits', PP.15 (5):1849-64.

[5] X. Hu, W. Zhang, X. Hu, N. Yu, X. Zhao, and F. Li, (2013) '"Fast estimation of optimal marked-signal distribution for reversible data hiding', IEEE Trans. Inf. Forens. Secur., vol. 8, no. 5, pp. 187–193.

[6] D. Xiao, X. Liao, and P. Wei, (2009) ‘Analysis and improvement of a chaos based image encryption algorithm’, Chaos Solit. Fract., vol. 40, no. 5, pp. 2191–2199.

[7] Ya-Lin Lee and Wen-Hsiang Tsai, (2014) ‘A New Secure Image Transmission Technique Via Secret-fragment-visible Mosaic Images By Nearly Reversible Color Transformations’, IEEE transactions on circuits and systems for video technology, vol. 24, no. 4.

[8] D. Coltuc and J.-M. Chassery, (2007) ‘Very fast watermarking by reversible contrast mapping’, IEEE Signal Process. Lett., vol. 14, no. 4, pp. 255–258.

[9] C. K. Chan and L. M. Cheng, (2006) ‘Hiding data in images by simple LSB substitution’, Pattern Recognit.., vol. 37, pp. 469–474, Mar. 2004.

[10] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, “Reversible data hiding,” IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362.

[11] W. Zhang, X. Hu, X. Li, and N. Yu, (2013) ‘Recursive histogram modification: Establishing equivalency between reversible data hiding and lossless data compression’, IEEE Trans. Image Process., vol. 22, no. 7, pp. 2775–2785.

[12] I. J. Lai and W. H. Tsai, (2011) ’Secret-fragment-visible mosaic image—A new computer art and its application to information hiding’, IEEE Trans. Inf. Forens. Secur., vol. 6, no. 3, pp. 936–945.

[13] V. Patidar, N. K. Pareek, G. Purohit, and K. K. Sud, (2011) ‘A robust and secure chaotic standard map based pseudorandom permutation substitution scheme for image encryption’, Opt. Commun., vol. 284, no. 19, pp. 4331–4339.

[14] X. Li, B. Yang, and T. Zeng, (2011) ‘Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection’, IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524–3533.