An Improved Approach in Visual Cryptography Using Error Diffusion Technique

Ms. Shital B Patel[1], Dr. Vinod L Desai[2]

[1] Research Scholar, RK University, Kastubadham, Rajkot, India.
[2] Assistant Professor, Department of Computer Science, Gujarat Vidyapith, Ahmadabad ,India.
Corresponding Author: Ms. Shital B Patel[1]

ABSTRACT

Visual Cryptography (VC) is a special type of technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes the job of the person to decrypt via sight reading. Visual cryptography can be used to protect biometric templates in which decryption does not require any complex computations. A secret image which is encoded into N shares printed on transparencies. The shares appears random and contain no decipherable information about the underlying secret image, however if any 2 of the shares are stacked on top of one another the secret image becomes decipherable by the human eye. This paper focuses on halftoning method named as error diffusion method used for the better generation of halftoned shares. In this paper, three existing error diffusion algorithms and proposed algorithm are compared on the basis of execution time of various parameters such as PSNR, WSNR, SNR and UQI and highlights how the proposed enhanced work increases the overall performance of visual cryptography.

KEYWORDS: Halftoning, Error diffusion, PSNR, WSNR, SNR and UQI.

Date of Submission: 27-07-2018 Date of acceptance: 11-08-2018

I. INTRODUCTION

Visual Cryptography is a cryptographic technique, that allows visual information is encrypted in such a way that decryption becomes a mechanical operation that does not require a computer. In present day's computer generation data security, hiding and all such activities have become probably the most important aspect for most organizations. The organizations expend millions of currency to just secure their data. This need has risen due to increase in cyber theft/ crime. Now technology has grown so enough that criminals have found multiple ways to perform cybercrime to which the concerned authorities have either less or not sufficient answer to counter. Visual cryptography is used specifically in the field of Biometric security, Watermarking, Remote electronic voting, Bank customer identification etc.

One of the well-known techniques has been recognized to Moni Naor and Adi Shamir[1], who developed it in 1994. They established a visual secret sharing scheme, where an image is fragmented up into n shares so that only somebody with all n shares could decrypt the image, while any n − 1 shares revealed no information about the original image. Each share was reproduced on a separate transparency, and decryption was executed by overlaying the shares. When all n shares were covered, the original image would appear. There are several generalizations of the basic scheme including k-out-of-n visual cryptography.

For instance in the (2, 2) sharing case (the secret is split into 2 shares and both shares are required to decode the secret) we use complementary matrices to share a black pixel and identical matrices to share a white pixel. Stacking the shares we have all the subpixels associated with the black pixel now black while 50% of the subpixels associated with the white pixel remain white.

Horng et al [2]. recommended a method that allows N − 1 colluding parties to cheat an honest party in visual cryptography. They take advantage of knowing the underlying distribution of the pixels in the shares to create new shares that combine with existing shares to form a new secret message of the cheaters choosing. We know that 2 shares are enough to decode the secret image using the human visual system. But examining two shares also gives some information about the 3rd share. For instance, colluding participants may examine their shares to determine when they both have black pixels and use that information to determine that another participant will also have a black pixel in that location. Knowing where black pixels exist in another party's share allows them to create a new share that will combine with the predicted share to form a new secret message. In this way a set of colluding parties that have enough shares to access the secret code can cheat other honest parties.

II. REVIEW OF LITERATURE

To affect this issue, G. Ateniese, C. Blundo, A.DeSantis, and D. R. Stinson deliver a general access structure [2] in 1996. In which disposed set of n shares is distributed into two subsets specifically qualified and forbidden subset of shares each the interest of shares. Any subset of 'k' or further qualified shares can decoded the secret image but no data can be recover by stacking lower number of qualified shares or by bundle disqualified shares. As far as year 1997 visual cryptography systems were suitable to only black and white images.

Zhou, Arce, Gonzalo R, et al. [3] in "Halftone Visual Cryptography" given halftone visual cryptography which expansion the quality of the purposeful shares. In halftone visual cryptography a secret pixel 'P' is encrypted into an array of Q1 X Q2 sub pixel, introduce to that halftone cell, in respectively of the 'n' shares. By applying halftone cells with a proper size, preserve contrast and safety. Apply Void and Cluster algorithm to encrypt a secret binary image into n halftone share.

D. Jena, and S. Jena [4] in "A Novel Visual Cryptography Scheme" investigate vital visual cryptography model for achieve shares and then enclose them into cover image applying a DHCOD technique, so that share will be higher secure and essential. It implement superior security so it is greater effective in transformation of financial evidences.

Nakajima, M. and Yamaguchi, Y. [5] ,developed Extended visual cryptography scheme (EVS) in 2002. An EVC implement technique to initiate meaningful shares rather of random shares of classic visual cryptography and provide to escape the possible issues, which may happen by noise-like shares in classic visual cryptography.

Chang-Chou Lin and Wen-Hsiang Tsai [6] in 2003 , "Visual Cryptography for gray-level images by dithering techniques" specified modern dithering techniques rather than applying gray pixel straight to create shares, A dithering technique is used to transform gray level images into relative binary images. Later current visual cryptography systems for binary images are utilized to produce the work of generating the shares.

Sandeep Katta [7] in "Recursive Information Hiding in Visual Cryptography" given to work out problems of hiding of lesses secret in shares bigger secret with secret sizes increase at every step. When recursive threshold visual cryptography is applied in network application, network load is decrease. Later simulation result the contrast will be loss. Tested algorithm usage amounts of factors and invested disclose image.

Nakajima and Yasushi [8] in "Extended Visual Cryptography for natural images" they recommended spread visual cryptography for natural images establish meaningful binary images as shares. This will decrease the cryptanalysts to suspect secret from a separate shares. While the preceding investigator essentially handle only binary images.

Anuprita U Mande and Manish N Tibdewal [9] in "Parameter Evolution and Review of various Error-Diffusion Half toning algorithms used in color Visual Cryptography" ,they offered on various error-diffusion algorithm and analyze the a few parameters such as PSNR and perceived error. They offered half toning method .They also do comparison on various Error-Diffusion algorithms. The comparison is done on the vital of contrast loss, perceived error between original and half toned image and the PSNR values. From the implementation of all the algorithm, it observed that Visual quality of haft toned image is better when Jarvis algorithm is applied.

Shital patel , Dr. Vinod Desai [11] in "Performance Evaluation: Analyzed parameter tuning for Halftone secure with Error Diffusion techniques for Visual Cryptography" has proposed algorithms to analyze different error diffusion algorithm. They compared few parameters, such as PSNR, MSE, SNR , WSNR and UQI with other error diffusion algorithm. In this paper, they got better result than other algorithm and got higher quality result.

III. RELATED WORK

3.1 Error Diffusion for Visual Cryptography

Error diffusion is a simple but it is very efficient algorithm to halftone a gray scale image compared with other halftoning algorithms. In Error diffusion technique, the quantization error is distributed to neighboring pixels and fed-back to set of future input pixels. The quantization error depends upon not only the current input and output but also the entire past history. The error filter designed in such a manner that the low frequency difference between the input and output image is minimized. The error that is diffused away by the error filter is high frequency or "blue noise". These features of error diffusion produced halftone images that are good to human eyes with high visual quality. he more popular technology of halftoning algorithms is error diffusion. This technology propagates quantization errors to unprocessed neighboring pixels according to some fixed ratios. The error diffusion preserves the average intensity level between the original input images and the binary output image.

Further, the error diffusion produces good halftone image despite relatively low cost.

In Figure 1 show an error diffusion diagram where f(m ,n) represents the (m.n)th pixel of input gray scale image, d(m,n) is the input to the threshold block t(m,n) and g(m,n) is the output quantized pixel value is either 1 or 0. Error diffusion consists of two main component is define , the block t(m,n) and another is the error filer h(k,l) whose input e(m,n) is the difference between d(m,n) and g(m,n) .

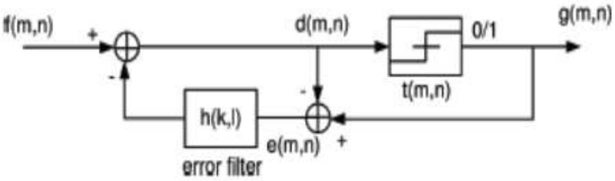


Fig. 1 Error Diffusion Algorithm.

In this paper, we will analysis of the three error diffusion halftoning algorithm used in visual cryptography.

3.2. Floyd-Steinberg halftoning algorithm

The error-diffusion algorithm is suggested by Floyd and Steinberg [12]. The algorithm implements the error-diffusion halftoning of an n by m grayscale image. First, the quantization error is scaled an added to the nearest gray scale pixels. The scaling factor for Floyd-Steinberg algorithm filter is given below.

	X	7/16
3/16	5/16	1/16

The error filter proposed by Floyd-Steinberg algorithm [10]
where x indicates the current pixel.
Floyd-Steinberg halftoning Algorithm :

```
Step 1 Procedure HALFTONE AN IMAGE
Step 2 for i=1… n do
Step 3    for j=1... m do
Step 4           if J (i ,j) < 128 is found then c0
Step 5                 else J (i ,j) = 1
Step 6           error = J [i, j] - I[i, j]* 255
Step 7           Distribute (3/8) errors to the right pixel
Step 8           Distribute (1/8) errors to the right diagonal pixel
Step 9           Distribute (1/8) errors to the bottom pixel
Step 10        Distribute (3/8) errors to the left diagonal  pixel
Step 11         end for
Step 12     end for
```

3.3 Jarvis halftoning algorithm

The error diffusion algorithm has been proposed by Jarvis, Judice and Ninke.. It diffuses the error in the 12 neighboring cells instead of 4 cells as in Floyd-Steinberg algorithm. Second, Jarvis's halftoning algorithm the quantization error is scaled added to nearest gray scale pixels. The scaling factor is given below.

		x	7/48	5/48
3/48	5/48	7/48	5/48	3/48
1/48	3/48	5/48	3/48	1/48

The error filter proposed by Jarvis's algorithm
Jarvis halftoning Algorithm:
Step 1 Procedure JARVIS HALFTONING AN IMAGE

```
Step 2 for i = 1,….., n do
Step 3 for j = 1 ,….., m do
Step 4   if f ( i , j ) < 128 THEN
                  b [i, j] = 1
             else
                  b[ i , j] = 0
Step 5 since the pixel value in f, which is a real number between 0 and 255, has been replaced by 0 or 1 in b and "error" has been calculated.
Step 6   The error occurred at the position (i, j) is weighted by 7/48 and added to the pixel value at (i+1, j). The same error is weighted by 5/48 and added to the pixel at (i+1,j+1) and so on.
Step 7     end for
Step 8    end for
Step 9 End procedure
```

3.4 Stucki halftoning algorithm

Third, Stucki halftoning algorithm the quantization error is scaled added to nearest gray scale pixels. The scaling factor is given below.

		x	8/42	4/42
2/42	4/42	8/42	4/42	2/42
1/42	2/42	4/42	2/42	1/42

The error filter proposed by Stucki algorithm.

The effect of error diffusion with Floyd and Stenberg, Jarvis's and Stucki algorithm error filter for gray scale ramp, the test image is shown in below.

Stucki halftoning Algorithm:

```
Step 1 Procedure STUCKI HALFTONING AN IMAGE
Step 2 for i = 1,….., n do
Step 3 for j = 1 ,…..,m do
Step 4   if f( i , j ) < 128 THEN
                 b[ i , j] = 1
             else
                 b[ i , j] = 0
Step 5 since the pixel value in if, which is a real number
           between 0 and 255, has been replaced by 0 or 1 in b
           and "error" has been calculated.
The "error" is the difference between the pixel value in l and t at that position.
Step 6  The error occurred at the position (i, j) is weighted by
           8/42 and added to the pixel value at (i+1, j). The        same error is weighted by  4/42 and added  to the pixel at (i+1, j+1) and so on .

Step 7   end for
Step 8    end for
Step 9 End procedure
```

IV. PROPOSED METHOD

In this paper, we propose the secure visual quality of secret images by halftone scheme with diffusion techniques. At first, the visible images is translated into binary image. Next, the binary image is converted into halftone shares containing efficient visual information. Thus the shared images are disseminated to particular participants and then they are extremely enforced to reveal the secret images. When the shares are generated, it is uses the halftone processing, which first the encryption the images with high quality secret images and then decryption the secret images with same image quality by using diffusion methodology.

The proposed methodology is consists of following process:

1. Input Gray scale image.
2. Convert gray scale image into Binary image

3. Calculate error by subtracting from binary pixel into original pixel.
4. Apply halftone scheme with error diffusion technique.
5. Retrieving high quality image.

By using proposed algorithm we get higher quality image, where the quality is computed by comparing different image quality metrics.

4.1 Performance Measurement Standard

The result of proposed work is measured using different quality measurement parameters. These all parameters (like PSNR , MSE , WSNR , SNR, and UQI) are discuss in [10]. And one more criteria add which is related with execution time see in this paper. To measure the performance of the overall execution time required for various algorithms by calculating the time of all quality measurement parameters.

A. Execution time for PSNR Value

Table-1 shows the execution time needed for calculating PSNR value along with all other algorithms.

Types of Algorithm	Floyd-Steinberg	Jarvis et al	Stucki	Proposed Algorithm
Time (seconds)				
Lena	0.0059	0.0109	0.0143	0.0019
Peppper	0.0036	0.0138	0.0054	0.0032
Barbra	0.0062	0.0073	0.0031	0.0023
Boat	0.0052	0.0059	0.0053	0.0045
Tree	0.0054	0.0135	0.0056	0.0049
Clock	0.0056	0.0165	0.0058	0.0035

Table -1 : Execution time for PSNR value of various Algorithms .

In below table, execution time of proposed algorithm is less than as compare to other algorithms. A graphical comparison for time required of various images between proposed method and various Error diffusion algorithms is depicted in Figure 2.

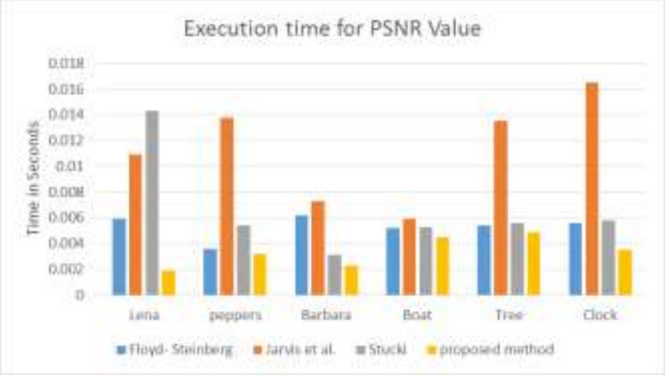


Figure 2 : Execution time comparison between Floyd-Steinberg, Jarvis, Stucki and proposed algorithm on PSNR value.

B. Execution time for WSNR value

Weighted Signal-to-Noise Ratio (WSNR) is calculated in the spatial frequency domain. Human Visual System is a nonlinear, spatially varying system. Table-2 shows the execution time required for calculating WSNR value along with all other algorithms.

Types of Algorithm	Floyd-Steinberg	Jarvis et al	Stucki	Proposed Algorithm
Time (seconds)				
Lena	0.0281	0.0287	0.0314	0.0195
Peppper	0.0263	0.0289	0.0284	0.0149

Barbra	0.0265	0.0252	0.0269	0.0145
Boat	0.0252	0.0291	0.0283	0.0128
Tree	0.0260	0.0265	0.0248	0.0143
Clock	0.0284	0.0253	0.0303	0.0154

Table - 2 : Execution time for WSNR value of various Algorithms .

A graphical comparison for time required of various images between proposed method and various Error diffusion algorithms is depicted in Figure 3.

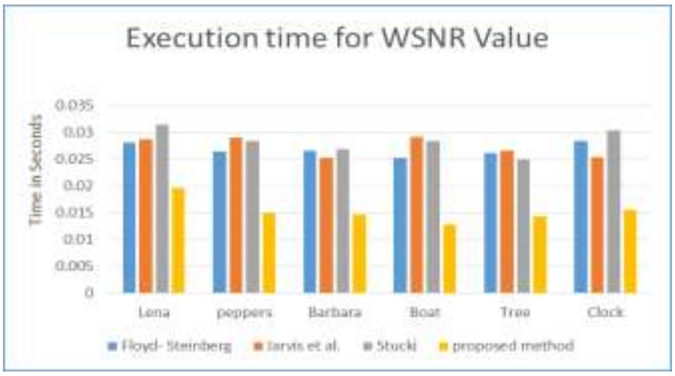


Figure 3 : Execution time comparison between Floyd-Steinberg, Jarvis, Stucki and proposed algorithm on WSNR value.

C. Execution time for SNR value

SNR is the ratio of signal power to the noise power. In terms of images, how the original image is affected by the added noise. The SNR are used to measure the quality of an image after the reconstruction. Table-3 shows the execution time required for calculating SNR value along with all other algorithms.

Types of Algorithm	Floyd-Steinberg	Jarvis et al	Stucki	Proposed Algorithm
Time (seconds)				
Lena	0.0075	0.0089	0.0077	0.0072
Peppper	0.080	0.0113	0.0086	0.0078
Barbra	0,.0042	0.0073	0.0043	0.0038
Boat	0.0078	0.0081	0.0075	0.0067
Tree	0.0053	0.0080	0.0082	0.0045
Clock	0.0039	0.0045	0.0043	0.0032

Table - 3: Execution time for SNR value of various Algorithms .

A graphical comparison for time required of various images between proposed method and various Error diffusion algorithms is depicted in Figure 4.

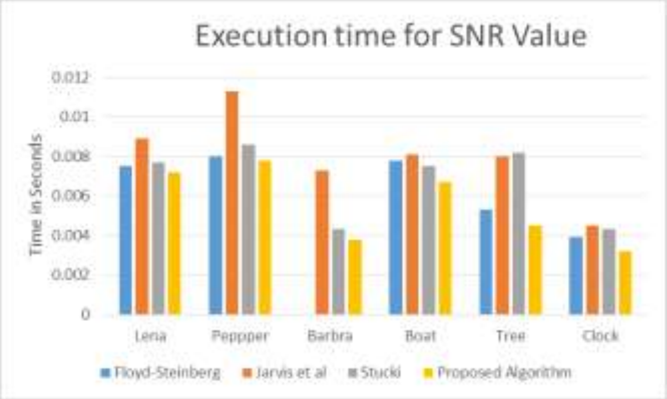


Figure 4 : Execution time comparison between Floyd-Steinberg, Jarvis, Stucki and proposed algorithm on SNR value.

D. Execution time for UQI value

Universal Image Quality Index (UQI) is measure, the comparison between original and distorted image into three comparison: luminance, contract and structural comparison. Table-4 shows the execution time required for calculating UQI value along with all other algorithms.

Types of Algorithm	**Floyd-Steinberg**	**Jarvis et al**	**Stucki**	**Proposed Algorithm**
Time (seconds)				
Lena	0.0158	0.0209	0.0178	0.0092
Peppper	0.0178	0.0186	0.0188	0.0103
Barbra	0.0226	0.0248	0.0234	0.0178
Boat	0.0148	0.0172	0.0151	0.0087
Tree	0.0163	0.0256	0.0153	0.0078
Clock	0.0155	0.0162	0.0149	0.0122

Table - 4: Execution time for UQI value of various Algorithms.

A graphical comparison for time required of various images between proposed method and various Error diffusion algorithms is depicted in Figure 5.

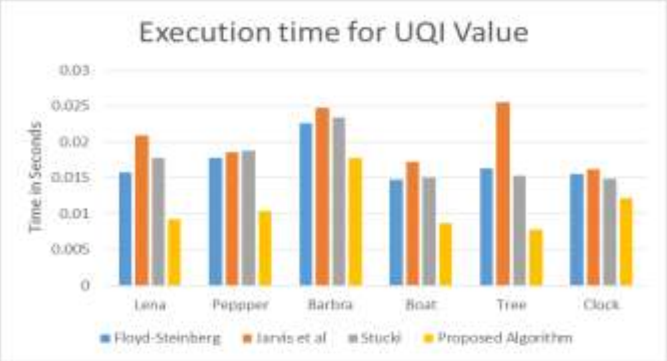


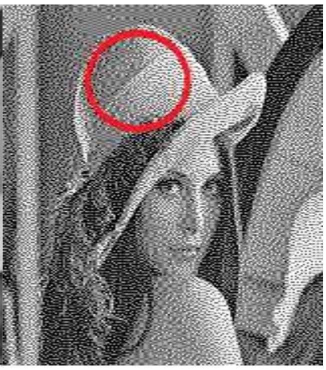
Figure 5: Execution time comparison between Floyd-Steinberg, Jarvis, Stucki and proposed algorithm on UQI value.

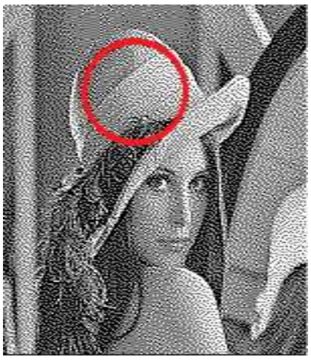
methods. In above Figure 2, Figure 3, Figure 4 and Figure 5 shows that proposed algorithm take less execution time then all other existing algorithms.

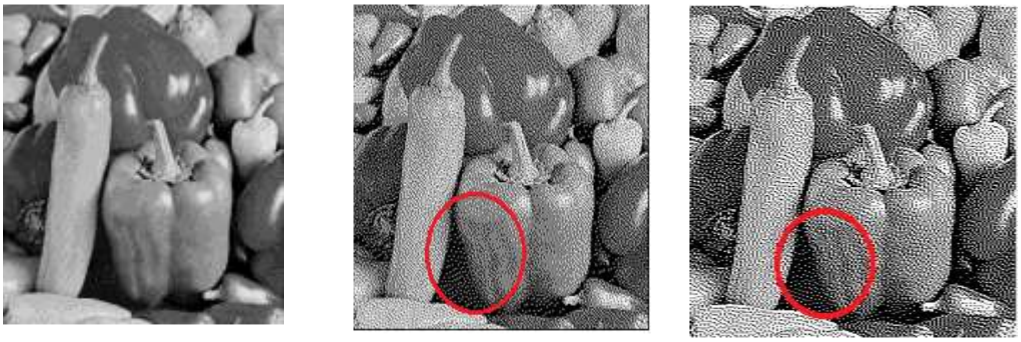
V. SIMULATION RESULTS AND ANALYSIS

The proposed algorithm, implemented using MATLAB R2012a and tested performance of these algorithms and evaluated the result. A number of images including Lena, Peppers, Barbara, boat, tree and clock were tested. These test images were degraded in a variety of ways such as impulsive salt-pepper noise interference, additive Gaussian noise, blurring, and compression. Figure 6 shows the results.

(a1)


(b1)


(c1)



(a2) (b2) (c3)

Figure 6: The result images of various methods (a) Original Image , (b) Floyd- Steinberg halftone and (c) Proposed halftone image

VI. CONCLUSION

In this research paper performance of the visual cryptography is improved base on proposed and implemented work. The proposed work used error diffusion method. We enhanced the error diffusion method and the goal of error diffusion. First the continuous-tone image is transformed into a binary image and scan pixel from top to bottom and left to right. After that calculated error by subtracting binary pixel from original pixel. At last error distributed among its neighbor pixel and provided halftone share with good image quality. The recovered secret image (share) are better quality means better secret hiding and for better secrecy. The overall enhanced work increases the overall performance of visual cryptography.

REFERENCES

[1]. M. Naor and A. Shamir (1994). "Visual Cryptography" In Proc. Eurocrypt, 1-12.

[2]. Ateniese, G., Blundo, C., De Santis, A., & Stinson, D. R. (1996). Visual cryptography for general access structures. Information and Computation, 129(2), 86-106.

[3]. Zhou, Z., Arce, G. R., & Di Crescenzo, G. (2006). Halftone visual cryptography. Image Processing, IEEE Transactions on, 15(8), 2441-2453.

[4]. Jena, D., & Jena, S. K. (2009, January). A Novel Visual Cryptography Scheme. In Advanced Computer Control, 2009. ICACC'09. International Conference on (pp. 207- 211). IEEE.

[5]. Nakajima, M., & Yamaguchi, Y. (2002). Extended visual cryptography for natural images.

[6]. Lin, C. C., & Tsai, W. H. (2003). Visual cryptography for gray-level images by dithering techniques. Pattern Recognition Letters, 24(1), 349-358.

[7]. Katta, S. (2010). Recursive information hiding in visual cryptography. arXiv preprint arXiv:1004.4914.

[8]. Nakajima, M., & Yamaguchi, Y. (2002). Extended visual cryptography for natural images.

[9]. Mande, A. U., & Tibdewal, M. N. (2013). Parameter Evaluation and Review of Various Error-Diffusion Half toning algorithms used in Color Visual Cryptography. International Journal of Engineering and Innovative Technology (IJEIT) Volume, 2.

[10]. T. D. Kite, B. L. Evans and A. C. Bovik, "Modeling and quality assessment of halftoning by error diffusion", in IEEE Trans. Image Processing, vol. 9, pp. 909-922, May 2000 .

[11]. Shital Patel , Dr.V.L.Desai "Evaluation of visual cryptography halftoning algorithms" in IJLTEMAS vol.3,Issue 8, pp. 65-69, August 2014.

[12]. Soltani, M. (2013). A New Secure Image Encryption Algorithm using Logical and Visual Cryptography Algorithms and based on Symmetric Key Encryption.

[13]. Wang, Zhongmin, Gonzalo R. Arce, and Giovanni Di Crescenzo. "Halftone visual cryptography via error diffusion." Information Forensics and Security, IEEE Transactions on vol. 4, pp.383-396,2009.

Ms. Shital B Patel1 "An Improved Approach In Visual Cryptography Using Error Diffusion Technique" International Journal of Computational Engineering Research (IJCER), vol. 08, no. 08, 2018, pp. 51-58.