International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 4, April 2013)

A Fast Encryption Algorithm for Color Extended Visual Cryptography

Anuprita Mande[1], Manish Tibdewal[2]

[1]*Student, M.E. (4th Semester), Shri Sant Gajanan Maharaj College of Engineering, Shegaon*
[2]*Associate Professor, Shri Sant Gajanan Maharaj College of Engineering, Shegaon*

***Abstract*— Color visual cryptography (VC) encrypts a color secret image into *n* halftone image shares. The secret image can be recovered simply by stacking these shares together without any complex computations involved. The shares are very safe because separately they reveal nothing about the secret image. This paper introduces a faster and easier color visual cryptography encryption method that produces meaningful color shares via error diffusion halftoning. An error diffusion technique for halftoning produces shares which are more pleasant to human eyes. The algorithm proposed by this scheme reduces a considerable time for encryption and decryption in a much easier way. Comparisons with previous approaches show the superior performance of the new method.**

***Keywords*—Color meaningful shares, digital halftoning, error diffusion, secret sharing, visual cryptography (VC).**

I. INTRODUCTION

"Visual cryptography" was first proposed by Naor and Shamir which is also called as the "*k*-out-of-*n* visual secret sharing scheme" [1]. The major feature of this scheme is that the secret image can be decrypted simply by the human visual system without any complex computations. This scheme can hide the secret image in *n* distinct images called shares. The secret image can be revealed by simply stacking together as many as *k* of the shares. Each of the shares looks like a collection of random pixels and of course appears meaningless by itself. Any single share before being stacked up with the others, reveals nothing about the secret image. This way, the security level of the secret image can be effectively lifted up. VC scheme has been applied to many applications which include general access structures [2], copyright protection [3], watermarking [4], [5], visual authentication and identification [6], print and scan applications [7], etc.

To illustrate the basic principles of VC scheme, consider a simple (2, 2)-VC scheme in Fig. 1. Each pixel from a secret binary image is encoded into black and white subpixels in each share. If *p* is a white (black) pixel, one of the six columns is selected randomly with equal probability, to replace *p*.

Regardless of the value of the pixel *p*, it is replaced by a set of four subpixels, two of them are black and two white. Thus, the subpixel set gives no clue of the original value of *p*. When two subpixels originating from two white *p* are superimposed, the decrypted subpixels have two white and two black pixels. On the other hand, a decrypted subpixel having four black pixels indicates that the subpixel came from two black *p* pixels.[1]

Fig. 2 shows an example of a simple (2, 2)-VC scheme with a set of subpixels shown in Fig. 1. Fig. 2(a) shows a secret binary message, Fig. 2(b) and (c) depicts encrypted shares for two participants. Superimposing these two shares leads to the output secret message as shown in Fig. 2(d). The decoded image is clearly identified, although some contrast loss is observed.

Several new methods for VC have been introduced later. In 1996, Ateniese [2] proposed a more general method for VC scheme based upon general access structure. This paper provided a more efficient construction of threshold schemes. The VC scheme concept has been extended to grayscale share images by L. A. MacPherson [8]–[11]. Blundo [9] proposed VC schemes with general access structures for grayscale share images. In this paper, it is assumed that the secret image consists of a collection of pixels, where to each pixel is associated a grey level ranging from white to black and each pixel is handled separately. Hou [12] transformed a gray-level image into halftone images and then applied binary VC schemes to generate grayscale shares. Although the secret image is grayscale, shares are still constructed by random binary patterns carrying visual information which may lead to suspicion of secret encryption. Ateniese [13] developed a method of extended visual cryptography (EVC) in which shares contain not only the secret information but are also meaningful images. Zhou *et al.* [14] used halftoning methods to produce good quality halftone shares in VC. Wang *et al.* [15] produced halftone shares showing meaningful images by using error diffusion techniques. This scheme generates more pleasing halftone shares by diffusing errors to the neighbor pixels.

Visual secret sharing for color images was introduced by Naor and Shamir [16] based upon cover semigroups. Hou [12] in 2003 proposed schemes for color shares by applying halftone methods and color decomposition. Hou decomposed the secret color image into three (yellow, magenta and cyan) halftone images. All of the previously mentioned methods discuss color schemes for *2*-out-of-*2* or *2*-out-of-*n* secret sharing where the reconstructed colors are interpreted by some mixing rules of colors.

Ching-Nung Yand and Tse-Shih Chen proposed a VC scheme for color images based upon an additive color mixing method [17]. In this scheme, each pixel is expanded by a factor of three. We found that this scheme suffers from the problem of pixel expansion in the size of encrypted shares. In order to reduce the size of encrypted shares a new VC scheme was proposed by Gonzalo R. Arce [18] for color visual cryptography which introduces Visual Information Pixel (VIP) synchronization to generate high quality shares. This paper has also introduced an error diffusion technique for generating halftone shares which are more pleasant to human eyes. However, the algorithm proposed by this scheme takes a long time for encryption and decryption.

In order to reduce the time required for encryption and decryption, a new VC scheme for color visual cryptography is proposed in this paper which provides a faster algorithm to generate the meaningful shares. This paper also uses error diffusion halftoning to generate the shares that are much pleasant to human eyes.

The paper is organized as follows: Section II provides preliminaries about standard VC, extended VC scheme, and the fundamentals of halftone techniques for easy understanding of the proposed VC method. Section III describes the proposed encryption algorithm to generate final shares. Section IV shows simulation results of the new scheme and we conclude this paper in Section V.

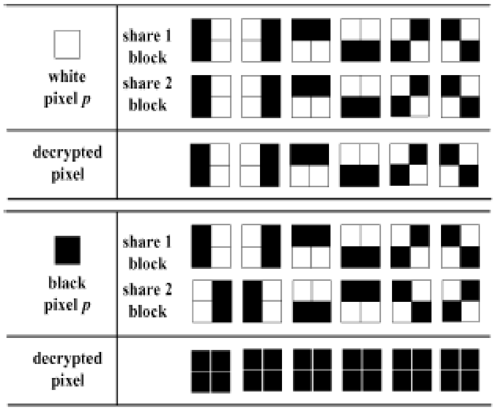


Fig.1. Construction of (2, 2) VC scheme

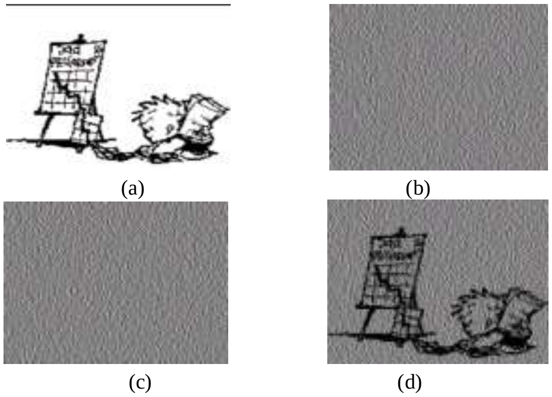

(a) (b) (c) (d)

Fig.2. (a) Binary secret image (b) Encrypted share 1. (c) Encrypted share 2. (d) Decrypted secret message.

II. Preliminaries

This section gives a brief description of VC, extended VC and an error diffusion halftoning.

A. Fundamentals of VC

Generally, a *(k, n)* VC scheme encrypts a secret message into *n* distinct shares. Each share shows noise-like random black and white patterns and does not reveal any information of the secret image by itself. In a *k*-out-of-*n* scheme, access to more than *k* shares allows one to recover the secret image by stacking them together, but access to less than *k* shares is not sufficient for decryption. [1]

B. Extended VC

Generally, a *(k, n)*-Extended VC scheme takes a secret image and *n* original images as input and produces *n* encrypted shares with approximation of original images that satisfy the following three conditions:

- Any *k* out of *n* shares can recover the secret image;
- Any less than *k* shares cannot obtain any information of the secret image;
- All the shares are meaningful images; encrypted shares and the recovered secret image are colored. [13]

C. Error Diffusion

Error diffusion is a simple but efficient way to halftone a grayscale image. There are various error diffusion algorithms that are applied to halftone an image. This includes Floyd-Steinberg algorithm [19], Jarvis algorithm [20], Stucki algorithm [21], etc.

III. Color Encryption and Decryption

In this section, we describe the encryption method for color meaningful shares with the proposed scheme. First, we describe the process of halftoning with error diffusion method. We need to halftone the secret image as well as the share images ahead of the encryption stage. We then introduce the proposed encryption as well as decryption process.

A. Halftoning with error diffusion method

In this method of halftoning, the quantization error at each pixel is filtered and fed into a set of future inputs. Fig. 3(a) shows a binary error diffusion diagram where *f(m,n)* represents the pixel at *(m,n)* position of the input image. *d(m,n)* is the sum of the input pixel value and the diffused errors, *g(m,n)* is the output quantized pixel value. Error diffusion consists of two main components.

The first component is the thresholding block where the output *g (m,n)* is given by

$$g(m,n) = \begin{cases} 1, & if\ d(m,n) \geq t(m,n) \\ 0, & otherwise \end{cases} \qquad (1)$$

The threshold *t (m,n)* can be position dependant.

The second component is the error filter *h (k,l)* where the input *e (m,n)* is the difference between *d (m,n)* and *g (m,n)*. Finally, we compute *d (m,n)* as

$$d(m,n) = f(m,n) - \sum_{k,l} h(k,l)e(m-k, n-l) \qquad (2)$$

Where $h(k,l) \in H$ and H is a 2-D error filter. A widely used filter is the error weight originally proposed by Floyd and Steinberg. [19]

$$h(k,l) = \frac{1}{16} \times \begin{bmatrix} & \blacksquare & 7 \\ 3 & 5 & 1 \end{bmatrix} \qquad (3)$$

Where ● is the current processing pixel. The error filter is designed in such a way 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" [14]. These features of error diffusion produce halftone images that are pleasant to human eyes with high visual quality. [18]

The process of error diffusion halftoning can be explained with an example of Floyd-Steinberg algorithm. Consider an *n* by *m* grayscale image. The boundary conditions are ignored. It is convenient to compute the output pixels in scan line order from upper left to lower right.

At every step, the algorithm compares the grayscale value of the current pixel J (i, j) which is represented by an integer between 0 and 255, to some threshold value (typically 128). If the grayscale value is greater than the threshold, the output pixel I (i, j) is considered black (value 0), else it is considered white (value 1). The difference between the pixel's original grayscale value and the threshold is considered as an error. Because we don't want to alter the already computed pixels, we spread this error intensity only to the pixels on the right, the right diagonal, the left diagonal and the bottom. The amount of error which is spread to each neighbor may be varied, but sending 3/8 of the error to the right and lower pixels and 1/8 to the two diagonal neighbors gives good results. Algorithm 1 given below illustrates the Floyd-Steinberg algorithm. The matrix shown graphically in Fig. 3(b) is an error-diffusion matrix proposed by Floyd and Steinberg [19].

Algorithm 1:

```
Procedure HALFTONING AN IMAGE
for i = 1,……,n do
    for j = 1,…..,m do
        if  J(i, j) < 128 is found then J(i, j) = 0
        else J(i, j) = 1
        error = J[i, j] - I[i, j]*255
        Distribute (3/8) error to the right pixel
        Distribute (1/8) error to right diagonal pixel
        Distribute (1/8) error to the bottom pixel
        Distribute (3/8) error to the left diagonal pixel
    end for
end for
```

As observed from figure 3(b), halftoning is a very time consuming process. In fact, it requires four floating-point multiplication operations and six memory accesses to process each pixel of the image. For an image with dimensions *n* by *m* it takes *10·n·m* such operations, and is therefore computationally quite expensive. Another two error diffusion algorithms has been proposed by Jarvis, Judice and Ninke [20] and Stucki [21]. The error diffusion matrices of Jarvis and Stucki algorithm are shown in Fig.3(c) and (d). These algorithms diffuse the error in the 12 neighboring cells instead of 4 cells as in the Floyd-Steinberg algorithm. As a result, this algorithm is even slower, requiring at least *24·n·m* floating point and memory access operations. However, increasing the number of elements over which the error is diffused improves the visual quality [22]. The flowchart of Error Diffusion halftoning is shown in Fig. 4 [23].

Table 1 shows the comparison of all these algorithms with respect to perceived error and peak signal to noise ratio (PSNR). At this stage of the scheme, halftoning of the secret image as well as the share images is performed.

B. Declaration of shares

Two random shares *S0* and *S1* of size 256 × 256 are to be declared prior to the encryption. These shares are used for the encryption process.

C. Encryption process

The proposed encryption process starts with segmentation of the halftoned secret image. The halftoned secret image is partitioned into four segments. These segments also called as 'message images' are to be interpolated to match with the size of halftoned share images. After interpolation, every pixel of the message image is verified for two values, '0' or '1'. If the message pixel is '0', it is EX-ORed with share *S0* otherwise EX-ORed with share *S1* and the resultant pixel is stored.

D. Decryption Process

The decryption process is exactly reverse to that of the encryption process. The decrypted images are to be decimated to obtain the original message images. The four message images retrieved so are concatenated to obtain the secret image.

The complete algorithm of the proposed encryption method is given in algorithm 2.

Algorithm 2:

```
1.  Procedure PROPOSED ENCRYPTION SCHEME
2.  Read secret image
3.  Perform halftoning of the secret image
4.  Read share images
5.  Perform halftoning of the share images
6.  Perform partition of the secret image into four
    segments
7.  Each segment is called as message image
8.  Perform interpolation of each message image to match
    with the size of the share images
9.  Declare two random shares S0 and S1 equal to the size
    256 × 256
10. Do for Message image 1 of dimension n × m
11. for i = 1,……,n do
12.   for j = 1,…..,m do
13.     if  M (i, j) = 0 is found then EX-OR M (i, j) with
         S (i, j) of share S0
14.     else EX-OR M (i, j) with S (i, j) of share S1
15.     End if
16.  End for
17. Repeat step 11 to 16 for message images 2,3 and 4
18. Retrieve the message images from encrypted shares by
    performing decryption
19. Decimate the decrypted message images to obtain the
    original message images
20. Concatenate the decimated message images to obtain
    the complete secret image
```

IV. SIMULATION RESULTS

In this section we will discuss the simulation results of the proposed encryption scheme. Fig. 5(a) shows the secret message of size 128×128 pixels which shows letters "U," "D," "E," and "L" in red, green, blue and yellow, respectively. Fig. 5(b) to (e) shows "Lena," "Baboon," "Pepper," and "Flower" of size 256×256 in natural colors for share generation. Fig. 6(a) shows the halftoned secret message of size 128×128 pixels. Fig. 6(b) to (e) shows halftoned share images "Lena," "Baboon," "Pepper," and "Flower" of size 256×256. Fig. 7(a) to (d) shows the encrypted share images of size 256×256 by the proposed scheme. Fig. 7(e) shows the retrieved secret image.

We use two different metrics for visual quality comparison between the original images and the encrypted shares. First, we use the peak signal-to-noise ratio (PSNR) distortion measure. Second, we measure the visual quality of the encrypted shares using the perceived error method between the original images and the encrypted shares. The perceived error is the difference between perceived continuous-tone images and perceived halftone images calculated by employing an approximated human visual system (HVS) model [24]. Let *f (m,n)* be the continuous-tone image and *f (x,y)* be the continuous-tone image by an ideal printer. An ideal printer is one that can reproduce an ideal square pixel equal to that of the continuous-tone pixel. Likewise, let *g [m,n]* = 0 or 1 represent the halftone image. Then, the perceived halftone image $\tilde{g}(x,y)$ is written as

$$\tilde{g}(x,y) = \sum_{m,n} g[m,n]\tilde{p}\,(x-mX, y-nY)$$

and the perceived continuous-tone image is written as

$$\tilde{f}(x,y) = f(x,y) ** h(x,y)$$

$$\tilde{f}(x,y) = \sum_{m,n} f[m,n]\tilde{p}\,(x-mX, y-nY)$$

The $**$ denotes 2-D convolution and $h(x,y)$ denotes point spread function of the HVS.

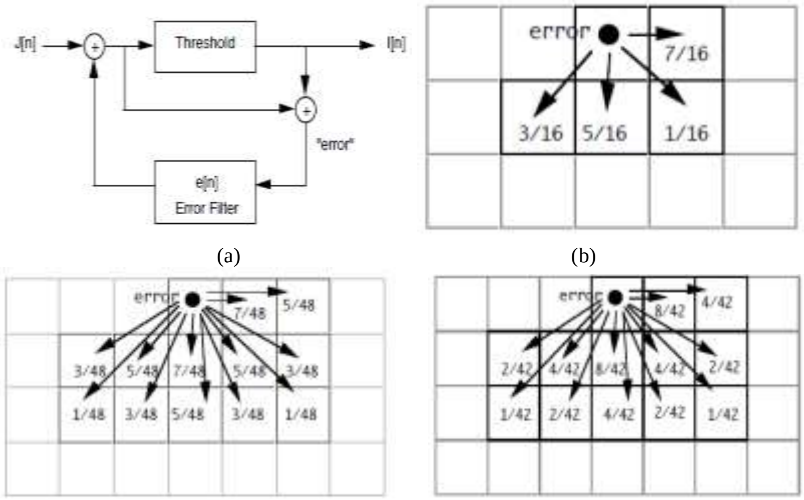
$$p(x,y) = rect(x|X,y|Y)$$

Above equation is the dot rendering function of an ideal printer. [18]

The perceived error between the continuous-tone image and the halftone image is given by

$$\tilde{e}(x,y) = \tilde{g}(x,y) - \tilde{f}(x,y)$$

Table 2 gives the comparison of Perceived error of the secret image as well as the share images using the proposed encryption algorithm for (2, 2), (4, 4) and (8, 8) shares. Table 3 gives the comparison of PSNR of the secret image as well as the share images using the proposed encryption algorithm for (2, 2), (4, 4) and (8, 8) shares.



(a) (b)

(c) (d)

Fig.3. a) The Floyd-Steinberg halftoning, b) Floyd-Steinberg error-diffusion matrix, c) Jarvis error-diffusion matrix, d) Stucki error-diffusion matrix,

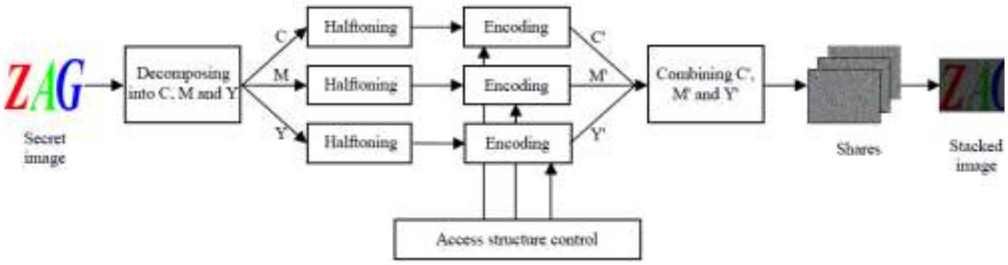
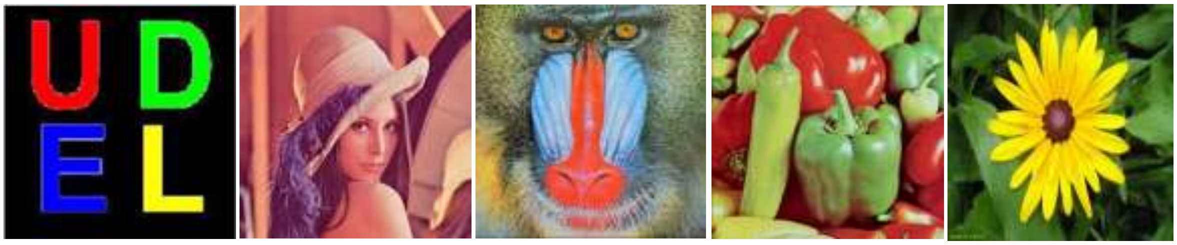
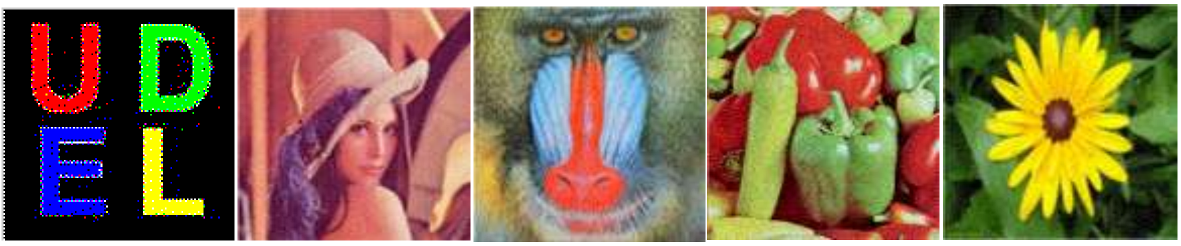


Fig.4 Flowchart of Error diffusion halftoning



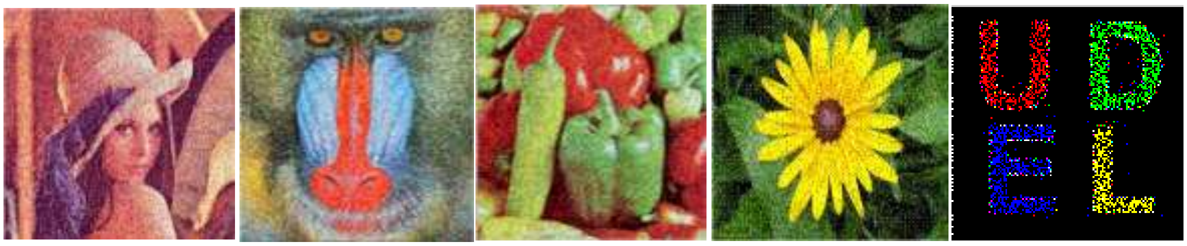
(a) (b) (c) (d) (e)

Fig.5. (a) Original Secret image of size 128 × 128 (b) to (e) Lena, Baboon, Pepper and Flower respectively of size 256 × 256



(a) (b) (c) (d) (e)

Fig.6. (a) Halftoned secret image of size 128 × 128, (b) to (e) Halftoned shares using error diffusion with the Floyd and Steinberg error filter; Lena, Baboon, Pepper and Flower respectively of size 256 × 256



(a) (b) (c) (d) (e)

Fig.7. Experimental results of (4, 4)-proposed CEVC scheme. (a) to (d) Encrypted Shares of proposed VC scheme. (e) Decrypted message from shares (a) and (d) of (4, 4)-proposed VC scheme

V. CONCLUSION

This paper develops a faster and easier encryption method to construct a color VC scheme with error diffusion halftoning. An error diffusion halftoning is used to construct the shares such that the noise introduced by the preset pixels is diffused away to the neighbors. This improves the visual quality of the encrypted shares as well as the decrypted secret image. From Table 1 we can observe that Stucki algorithm gives maximum PSNR and minimum perceived error. Hence, we can conclude that Stucki algorithm is best suited for the proposed VC scheme. The proposed encryption method provides easy way of encryption as well as decryption by simple EX-OR operations. It also takes less time i.e. only 7.552531 seconds to perform encryption and decryption. This time is very much less as compared to the previous methods. From Table 2 we can conclude that, if we increase the number of shares to hide the secret image, the amount of perceived error decreases. It is minimum i.e. 2175759 for (8, 8) VC scheme. However, it is observed from Table 3 that, PSNR also decreases with the increase in the number of shares, which is not desirable.

TABLE 1
PERCEIVED ERROR AND PSNR FOR ALL THE HALFTONING ALGORITHMS

Type of halftoning Algorithm	**Perceived Error**	**PSNR**
Original Floyd-Steinberg algorithm	4213223	18.2995
Modified Floyd-Steinberg algorithm	4.2132e+006	18.2995
Jarvis algorithm	4206273	18.2975
Stucki algorithm	4.2019e+006	18.3104

TABLE 2
PERCEIVED ERROR FOR PROPOSED ENCRYPTION ALGORITHM

Image(s)	**Perceived Error**		
	2 Shares	4 Shares	8 Shares
Secret Image	545799	5.4527e+005	2175759
Lena	8.3063e+006	8306336	8.3063e+006
Baboon	8.2697e+006	8.2697e+006	8.2697e+006
Pepper		7.2407e+006	7.2404e+006
Flower		5.4748e+006	5.4740e+006
Sunset			5.4837e+006
Mixed Fruit			6.8041e+006
Apple			1.1116e+007
Ice cream			7.9624e+006

TABLE 3
PSNR FOR PROPOSED ENCRYPTION ALGORITHM

Image(s)	PSNR		
	2 Shares	4 Shares	8 Shares
Secret Image	23.2554	23.2747	22.7850
Lena	12.0650	12.0651	12.0640
Baboon	12.5358	12.5359	12.5349
Pepper		13.7787	13.7778
Flower		15.7006	15.6995
Sunset			16.8809
Mixed Fruit			14.0239
Apple			5.7146
Ice cream			12.2028

REFERENCE

[1] M. Naor And A. Shamir, “Visual Cryptography,” In Proc. Eurocrypt, 1994, Pp. 1–12.

[2] G. Ateniese, C. Blundo, A. D. Santis, And D. R. Stinson, “Visual Cryptography For General Access Structures,” Inf. Comput., Vol. 129, No. 2, Pp. 86–106, 1996.

[3] A. Houmansadr And S. Ghaemmaghami, “A Novel Video Watermarking Method Using Visual Cryptography,” In Proc. Ieee Int. Conf. Eng. Intell. Syst., 2006, Pp. 1–5.

[4] M. S. Fu And O. C. Au, “Joint Visual Cryptography And Watermarking,” In Proc. Ieee Int. Conf. Multimedia Expo, 2004, Pp. 975–978.

[5] C. S. Hsu And Y. C. Hou, “Copyright Protection Scheme For Digital Images Using Visual Cryptography And Sampling Methods,” Opt. Eng., Vol. 44, P. 077003, 2005.

[6] M. Naor And B. Pinkas, “Visual Authentication And Identification,” Adv. Cryptol., Vol. 1294, Pp. 322–336, 1997.

[7] W. Q. Y, J. Duo, And M. Kankanhalli, “Visual Cryptography For Print And Scan Applications,” In Proc. Ieee Int. Symp. Circuits Syst., 2004, Pp. 572–575.

[8] L. A. Macpherson, “Gray Level Visual Cryptography For General Access Structrue,” M. Eng. Thesis, Univ. Waterloo, Ontario, Canada, 2000.

[9] C. Blundo, A. D. Santis, And M. Naor, “Visual Cryptography For Grey Level Images,” Inf. Process. Lett, Vol. 75, No. 6, Pp. 255–259, 2000.

[10] Y. T. Hsu And L. W. Chang, “A New Construction Algorithm Of Visual Crytography For Gray Level Images,” In Proc. Ieee Int. Symp. Circuits Syst., 2006, Pp. 1430–1433.

[11] C. C. Lin And W. H. Tsai, “Visual Cryptography For Gray-Level Images By Dithering Techniques,” Pattern Recognit. Lett., Vol. 24, Pp. 349–358, 2003.

[12] Y. C. Hou, “Visual Cryptography For Color Images,” Pattern Recognit., Vol. 36, Pp. 1619–1629, 2003.

[13] G. Ateniese, C. Blundo, A. Santis, And D. R. Stinson, “Extended Capabilities For Visual Cryptography,” Acm Theor. Comput. Sci., Vol. 250, Pp. 143–161, 2001.

[14] Z. Zhou, G. R. Arce, And G. D. Crescenzo, “Halftone Visual Cryptography,” Ieee Trans. Image Process., Vol. 18, No. 8, Pp. 2441–2453, Aug. 2006.

[15] Z. M. Wang, G. R. Arce, and G. Di Crescenzo, “Halftone visual cryptography via error diffusion,” IEEE Trans. Inf. Forensics Security, vol. 4, no. 3, pp. 383–396, Sep. 2009.

[16] M. Naor And A. Shamir, “Visual Cryptography Ii: Improving The Contrast Via The Cover Base,” Lect. Notes Comput. Sci., Vol. 1189, Pp. 197–202, 1997.

[17] C. N. Yang and T. S. Chen, “Visual cryptography scheme based on additive color mixing,” Pattern Recognit., vol. 41, pp. 3114–3129, 2008.

[18] Gonzalo R. Arce, Color Extended Visual Cryptography Using Error Diffusion Ieee Transactions On Image Processing, Vol. 20, No. 1, January 2011

[19] Robert W. Floyd And Louis Steinberg, An Adaptive Algorithm For Spatial Grayscale. Proceedings Of The Society For Information Display 17 (2) 75-77, 1976

[20] J. F. Jarvis, C. N. Judice And W. H. Ninke, A Survey Of Techniques For The Display Of Continuous Tone Pictures On Bi-Level Displays. Computer Graphics And Image Processing, 5 13-40, 1976

[21] P. Stucki, Mecca - A Multiple Error Correcting Computation Algorithm For Bi-Level Image Hard Copy Reproduction. Research Report Rz1060, Ibm Research Laboratory, Zurich, Switzerland, 1981.

[22] Panagiotis Takis Metaxas- Parallel Digital Halftoning By Error-Diffusion

[23] Haibo Zhang, Xiaofei Wang, Wanhua Cao and Youpeng Huang, “Visual Cryptography for General Access Structure Using Pixel-block Aware Encoding”, Journal Of Computers, Vol. 3, No. 12, December 2008

[24] S. H. Kim and J. P. Allebach, “Impact of hvs models on model-based halftoning,” IEEE Trans. Image Process., vol. 11, no. 3, pp. 258–269, Mar. 2002.

Anuprita U. Mande received the B.E. degree in Electronics & Telecomm. Engineering in 2002. Now, she is a student of 4th Semester M.E. in Shri Sant Gajanan Maharaj College of Engineering, Shegaon, Maharashtra, India.

Manish N. Tibdewal received the B.E. Industrial Electronics Engg. degree in 1990 and M.E. Electronics Engineering degree, from Amravati University,Amravati, Maharashtra, India, in 2001. Presently, he is working as an Associate Professor with Electronics and Telecommunication Engineering Department in Shri Sant Gajanan Maharaj College of Engineering, SHEGAON, Maharashtra, India.

He is currently working toward the Ph.D. degree in Biomedical Neuro-Signal and Image Analysis and processing in School of Medical Science and Technology, **Indian Institute of Technology, Kharagpur,W.B., India**. He is a student member of IEEE and life member of ISTE and IETE. He is co-opted as an executive member of IETE Centre Amravati, Maharashtra,India.

His research interests encompass Bio-Signal and Image Analysis, Image Processing, Signals and Image Parameter Quantification, disease prediction, and computational intelligence methods with emphasis on adaptive signal processing with an embedded system design.