International Journal of Information & Computation Technology.
ISSN 0974-2239 Volume 4, Number 14 (2014), pp. 1419-1427

http://www. irphouse.com

Halftone Visual Cryptography with Pixel Expansion through Error Diffusion

Prateek Kumar[1], Suneeta Agarwal[2], and Shivendra Shivani[3]

1, 2, 3MNNIT Allahabad, Uttar Pradesh

Abstract

Extended Visual Cryptography (EVC) concept provides meaningful shares instead of non meaningful shares. In this paper we proposed an algorithm based on EVC which enhances the contrast of the recovered secret image. Here the size of image visible on shares is taken to be three times as that of secret image, both the images are assumed in grey level.

In the proposed algorithm secret image and the visible image are first converted to halftone image using Halftone error diffusion method. Recovered image from the shares generated by is found to be of better quality. Standard parameters like Negative Rate Matrix, Recall, Precision, F-Measure, Balanced classification rate (BCR), Balanced error rate (BER) of visual cryptography are used to compare the quality of recovered image by our proposed scheme with other state of art EVC approaches.

Keywords: Error diffusion, Halftone visual cryptography (HVC), Halftoning, Visual cryptography (VC), Cryptography, Image processing, Secret sharing.

Introduction.

Visual cryptography (VC), first proposed by Naor and Shamir [1] in 1994, is a secret sharing method, which is based on black and white or binary images. Naor and Shamir [1] proposed a cryptography platform, called visual cryptography (VC) or visual secret sharing (VSS), which attempts to reveal the secret image via the human perception of visual system by stacking two or more share [6]. Visual cryptography is a unique concept of secret sharing method, in this when the shares are stacked, a hidden secret image is revealed.

In extended visual cryptography, the secret share images are transformed into meaningful shares. EVC with halftone image improves the quality of the recovered secret image and size is equal to the original image [3]. The (k, n)-threshold visual cryptography (VC) scheme is to share a secret image with n participants. In this if we have k or more shares then only secret image can be revealed otherwise not, this follows the concept of ”All or Nothing”[6].

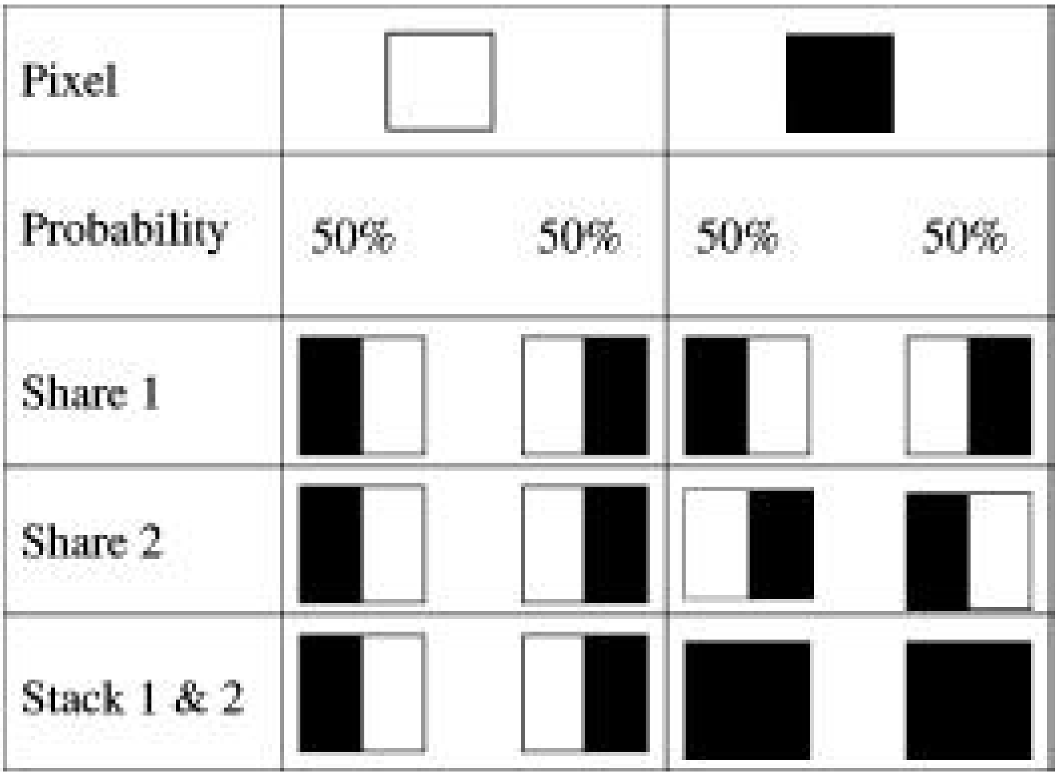

Fig. 1: Construction of 2-out-of-2 scheme [4]

In Progressive Visual Cryptography the secret image gradually revealed by superimposing more and more shares [8]. If we have only some pieces of secret shares, we could get an outline of the secret input image, by raising the number of the shares being superimposed, the details of the hidden information can be recovered progressively[5].

To illustrate the principles of VC, consider a simple 2-out-of-2 VC scheme shown in Figure 1. Each pixel p from a secret binary image is encoded into a pair of black and white sub pixels in each of the two shares. If pixel is white then we can make shares in two ways and after superimposing we get 50% white and black as shown in Figure 1. Similarly if pixel is black then after superimposing we get complete black pixel means 100% black pixel, as shown in Figure 1.

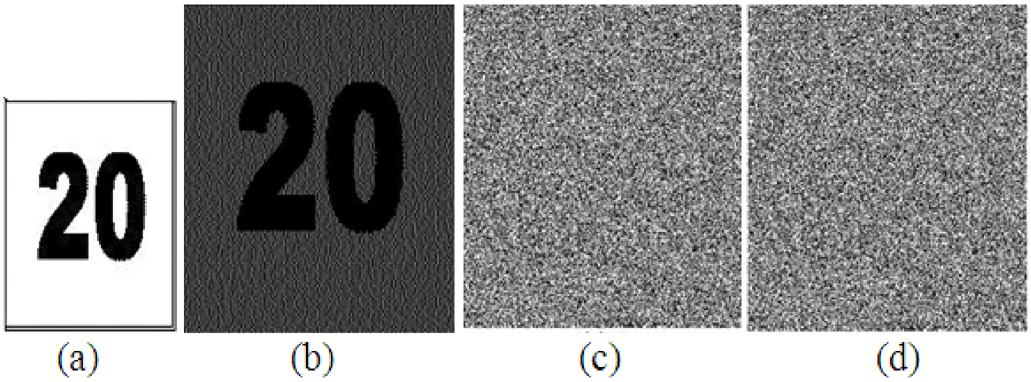

Fig. 2: Example of a (2; 2) VC Scheme with 4 Sub pixels: (a) secret 20 image, (b) recovered 20 image, (c) first share, (d) second share.

Figure 2, uses the visual cryptography concept that generates two non meaningful shares, that shows recovered image has degradation in visual quality, and also has pixel expansion [7].

Previous Work. In 1996, Ateniese, Blundo, and Stinson proposed extended visual cryptography (EVC) schemes that can construct meaningful share images [3]. Figure 3, shows the concept of extended visual cryptography, in this there are two input images one visual halftone image, MNNIT, 3(a) and other input halftone secret image, PRAEEK, 3(b) then using these images construct the share1, 3(c) and share2, 3(d) after superimposing the share1 and share2 recovered the secret image, 3(e)[9-11].

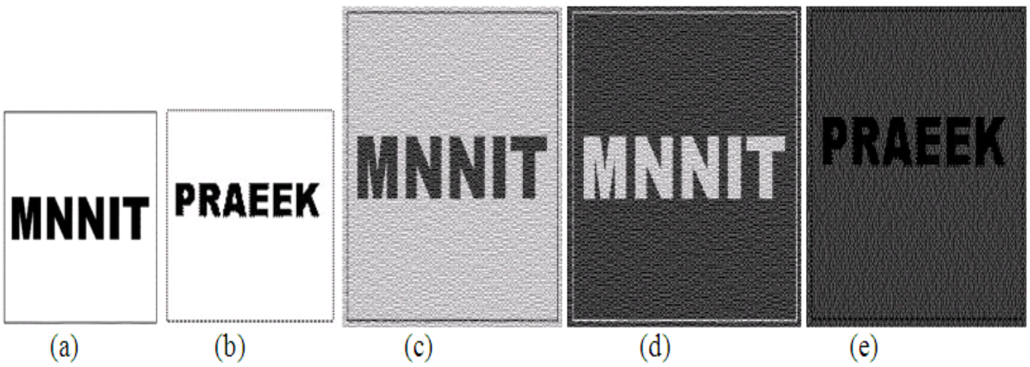

Fig. 3: Example of (2; 2) EVC Scheme: (a) visual image (b) secret image, (c) share 1, (d) share 2, (e) recovered secret image.

Extended visual cryptography scheme, yet preserves a good quality image for both the shares and the recovered image. The basic difference between visual cryptography and extended visual cryptography[8] is constructing meaningful shares that add security measure and contrast of recovered secret image. In this paper extended visual cryptography concept used for constructing meaningful shares[7]. Extended visual cryptography also provides higher contrast level than the visual cryptography [15].

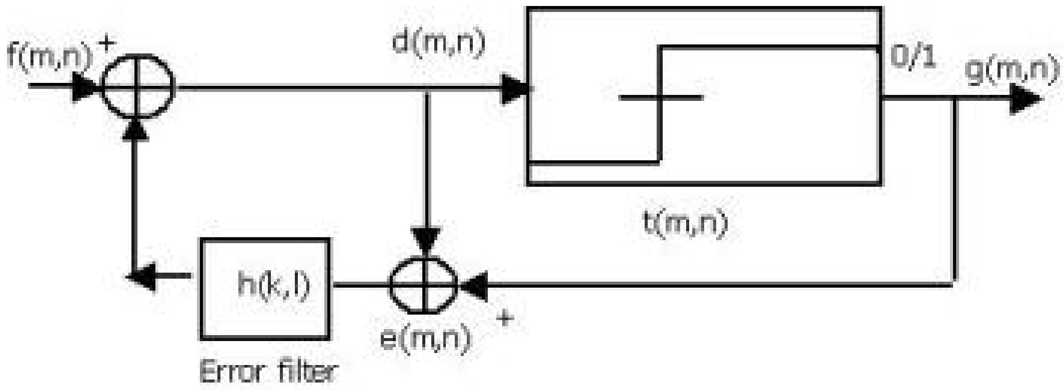

Fig. 4. Block diagram for binary error diffusion [4].

Proposed Work.

(a) Halftone the input gray scale image and visual image.
(b) Construct the meaningful shares using both input halftone image and visual halftone image.

Halftone Image through Error Diffusion.

Error Diffusion.

Error Diffusion method is easy and simpler to other half toning technique [2, 4]. This is efficient algorithm for half-toning gray scale image [12-14]. The quantization error is filtered at each pixel and fed back to set of future input samples. Figure 4, represents a binary error diffusion where f(m, n) represents the (m, n)th pixel of the input grayscale image, d(m, n) is the sum of the input pixel value and the diffused past errors, and is the output quantized pixel value[2-4]. The pixel f(m, n) passes through a quantizer to get the corresponding pixel of the halftone image g(m, n). The difference between these two pixels is diffused to the neighboring pixels by means of the error filter h(k, l)[4]. Error diffusion consists of two main components. The first component is the thresholding block where the output g(m, n) is given by-

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

The t(m, n) is the threshold position-dependent value. The second parameter is error filter h(k, l) whose input e(m, n) is the difference between d(m, n) and g(m, n). Finally we calculate d(m, n) as-

$$d(m,n) = f(m,n) - \sum h(k,l)e(m-k, n-l)$$

$$1/16 * \begin{array}{|c|c|c|}\hline & \bullet & 7 \\ \hline 3 & 5 & 1 \\ \hline\end{array}$$

Floyd Steinberg error filter[2].

Represent the current pixel. The weights are given by h(0, 1)=7/16, h(1, -1)=3/16, h(1, 0)=5/16, and h(1, 1)=1/16[2].

Construction of Meaningful Shares.

Using halftone image of both input secret image and visual image, we construct the meaningful shares. We have halftone visual image of 384*384 and halftone input secret image of 128*128 because each pixel of input secret image is represented by 3*3 of visual image.

Procedure For Meaningful Share.

1. For each pixel of input halftone image we have block of 3*3 halftone visual image and block of 3*3 complementary halftone visual image.
2. Then if input halftone image pixel value is == 0
3. Then take block of 3*3 from halftone visual image and
4. Also take block of 3*3 from complementary halftone visual image.
5. Select four pixels of 3*3 block of both halftone visual image and complementary halftone visual image.

Block (2, 2)
Block (2, 3)
Block (3, 2)
Block (3, 3)

r/c	1	2	3
1			
2		*	*
3		*	*

Assign the value on place of * in 3*3 block

$$M_1 = \begin{bmatrix}1 & 1\\0 & 0\end{bmatrix} \text{ or } \begin{bmatrix}0 & 0\\1 & 1\end{bmatrix} \text{ and } M_0 = \begin{bmatrix}0 & 0\\1 & 1\end{bmatrix} \text{ or } \begin{bmatrix}1 & 1\\0 & 0\end{bmatrix}$$

6. if input halftone image pixel value is == 1

Assign the value on place of * in 3*3 block

$$M_1 = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \text{ or } \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \text{ and } M_0 = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \text{ or } \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$$

7. After this process we will get two shares, one from the halftone visual image and other from the complementary halftone visual image.
8. These shares named as Share1 and Share2.
9. After superimposing these two shares we will get *Recovered Secret Image*.

Full Procedure in Algorithm Form.

Algorithm1 (Halftoning Process).

Initially we have two gray scale image one input secret image and other input visual image.

1. Using Error Diffusion halftoning method construct halftone image of secret image.
2. Using Error Diffusion halftoning method construct halftone image of visual image.
3. Constructs complement of halftone visual image.
4. Size of visual image is 3 times of input secret image (because every pixel of secret image represent by 3*3 block of pixel in recovered image).

Algorithm 2 (For Constructing Initial Share).

1. *For* (i =1 to size of input secret image)
2. *If* (pixel value of halftone secret image(i) ==1) *then*
3. Sec_1 = (1, 1, 0, 0) or (0, 0, 1, 1)
4. Sec_0 = (1, 1, 0, 0) or (0, 0, 1, 1)
5. *else*
6. Sec_1 = (1, 1, 0, 0) or (0, 0, 1, 1)
7. Sec_0= (0, 0, 1, 1) or (1, 1, 0, 0)

Algorithm 3 (For Constructing Final Share).

1. $outImage_1$=Halftone visual image
2. $outImage_2$= Complement Halftone visual image
3. x=1, z=1
4. For (kk =1 to size of input secret image)
5. $Block_1$= $outImage_1$ (z to z+3-1, x to x+3-1)
6. $Block_2$= $outImage_2$ (z to z+3-1, x to x+3-1)
7. $Block_1$ (2, 2)= Sec_1(kk, 1), $Block_2$ (2, 2)=Sec_0(kk, 1)
8. $Block_1$ (2, 3)= Sec_1(kk, 2), $Block_2$ (2, 3)=Sec_0(kk, 2)
9. $Block_1$ (3, 2)= Sec_1(kk, 3), $Block_2$ (3, 2)=Sec_0 (kk, 3)
10. $Block_1$ (3, 3)= Sec_1(kk, 4), $Block_2$ (3, 3)=Sec_0 (kk, 4)
11. After this process we have two meaningful share one $outImage_1$ and other from complement share $outImage_2$.
12. Then superimposing these two share 1 and share 2.
13. After superimposing we will get *Recovered secret image.*

14. Recovered secret image is 3 times larger than the input secret image.

.

Simulation Results

In this section, examples are present to illustrate the effectiveness of proposed work. In all simulation result, we have input secret halftone image of 128*128 and recovered image of 384*384 size so there is pixel expansion in EVC. We represent one pixel of input secret image by 3*3 pixel so recovered image is 3 times larger than the input secret image.

Here we use two step for recovering secret image, In first step halftoning and in second step making meaningful shares, in halftoning process there is no pixel expansion we get same size of halftone image as we give input image but in making meaningful shares we represent one pixel of input secret halftone image by 3*3 pixels, So finally we will get 3 times larger image than the secret image.

Figure 5, 6 and 7 shows the experimental results.

In all experimental results we get good quality and better contrast of Recovered image with pixel expansion.

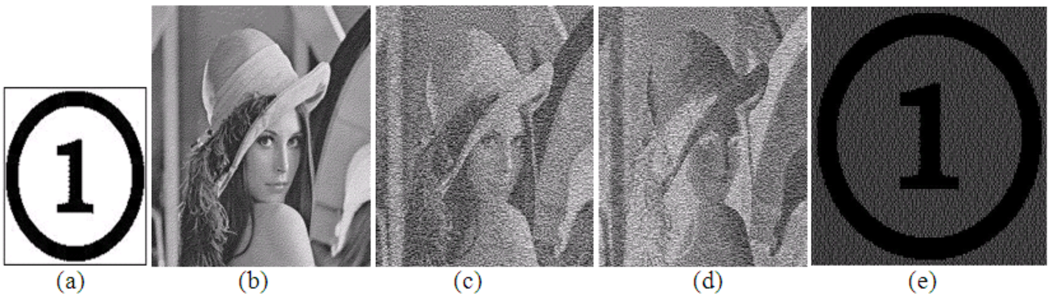

Fig. 5: (a) halftone secret Image, (b) halftone visual image, (c) share 1, (d) share 2, and (e) recovered secret image.

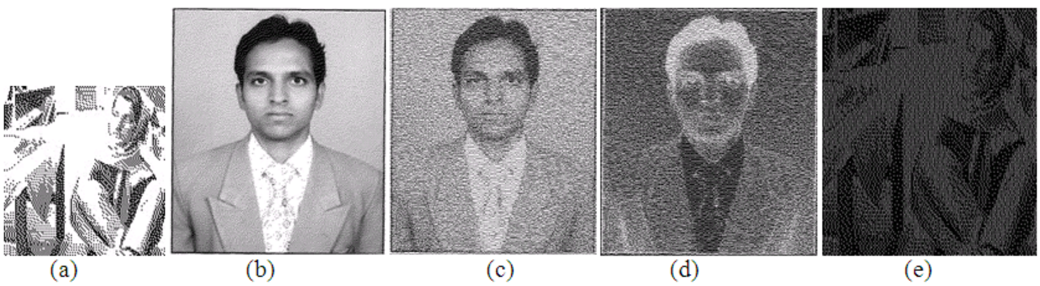

Fig. 6: (a)) halftone secret Image, (b) halftone visual image, (c) share 1, (d) share 2, and (e) recovered secret image.

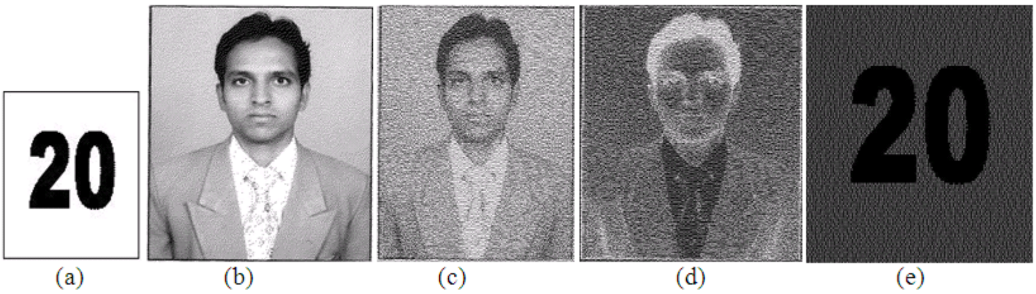

Fig. 7: (a) halftone secret Image, (b) halftone visual image, (c) share 1, (d) share 2, and (e) recovered secret image.

Parameter Analysis

In this section, we present experimental results, using standard visual cryptography parameters like NRM, Recall, Precision, F-Measure, Specificity, BCR, BER. Table I shows the values of these parameters based on the results shown in Fig. 5, 6 and 7. Comparing these results with earlier EVC results, we can say that, the results are approaching towards standard value of parameters.

Table I: Simulation Result Table

Parameter Analysis	Standard value	Previous EVC Results[3]	Figure 5	Figure 6	Figure 7
NRM	0	0. 5799	0. 3895	0. 3893	0. 3893
Recall	1	0. 1110	0. 2219	0. 2223	0. 2221
Precision	1	0. 5454	0. 9984	0. 9983	0. 9993
F-Measure	1	0. 2195	0. 3631	0. 3637	0. 3634
Specificity	1	0. 5932	0. 9991	0. 9990	0. 9993
BCR	1	0. 5231	0. 6105	0. 6107	0. 6107
BER	0	78. 3231	38. 9501	38. 9316	38. 9336

Conclusion

In the proposed method of EVC, the pixels that carry the secret information are preset before meaningful shares are generated from halftone images. Error diffusion is used to construct the halftone image so that the noise introduced by the preset pixels is diffused away. When halftone shares are generated, the secret information is originally embedded into the halftone shares, thus leading to shares with high image quality. Our proposed method follows the basic principle of EVC. It is clear that there is a tradeoff between the share image quality and the contrast loss of the decoded image. The method used in this paper for making meaningful shares is very simple, easy to understand and recovered good quality of image.

References

[1] M. Naor and A. Shamir. *Visual cryptography*. in EUROCRYPT94 Proceedings, Lecture Notes in Computer Science, Springer-Verlag; vol. 950, pp. 1-12, 1995.

[2] Zhongmin Wang, Student Member, IEEE, Gonzalo R. Arce, Fellow, IEEE, and Giovanni Di Crescenzo. *Halftone Visual Cryptography Via Error Diffusion*. IEEE Transactions on Infomation Forensics and Security; VOL. 4, NO. 3, SEPTEMBER 2009.

[3] N. Askari, H. M. Heys, and C. R. Moloney. *An Extended Visual Cryptography Scheme Without Pixel Expansion For Halftone Images*. 26th IEEE Canadian Conference Of Electrical And Computer Engineering; (CCECE)-2013.

[4] Zhongmin Wang, Student Member, IEEE, Gonzalo R. Arce, Fellow, IEEE, and Giovanni Di Crescenzo. *Halftone Visual Cryptography*. IEEE Transactions on Image Processing; VOL. 15, NO. 8. AUGUST 2006.

[5] Young-Chang Hou and Zen-Yu Quan. *Progressive Visual Cryptography with Unexpanded Shares*. IEEE Transaction on circuit and system for video technology; VOL. 21, NO. 11, NOVEMBER 2011.

[6] Kai-Hui Lee and Pei-Ling Chiu. *An Extended Visual Cryptography Algorithm for General Access Structures*. IEEE Transactions on Infomation Forensics and Security; VOL. 7, NO. 1, FEBRUARY 2012.

[7] Alekya K, Dr. R. V. Krishnaiah. *Secret Image Sharing System UsingMeaningful Covering Shares*. International Journal of Computer Science and Network (IJCSN); Volume 1, Issue 6, December 2012 www. ijcsn. org ISSN 2277-5420.

[8] Giuseppe Ateniese, Carlo Blundo, Alfredo De Santis and Douglas R. Stinson. *Extended Capabilities for Visual Cryptography*. Theoretical Computer Science; vol. 250, pp. 143-161, 2001.

[9] M. Nakajima and Y. Yamaguchi. *Extended Visual Cryptography for Natural Image*. in Proceeedings of WSCG; pp. 303-310, 2002.

[10] Y. T. Hsu and L. W. Chang. *A new construction algorithm of visual cryptography for gray level images*. in Proc. IEEE ISCAS, Island of Kos, Greece; May 2006.

[11] C. C. Lin and W. H. Tsai. *Visual cryptography for gray-level images by dithering techniques*. Pattern Recognit. Lett. vol. 24; pp. 349358, Jan. 2003.

[12] N. D. Venkata and B. L. Evansi. *Adaptive threshold modulation for error diffusion halftoning*. IEEE Trans. Image Process; vol. 10, no. 1, pp. 104116, Jan. 2001.

[13] P. Li and J. P. Allebach. *Tone-dependent error diffusion* ", ", IEEE Trans. Image Process; vol. 13, no. 2, pp. 201215, Feb. 2004.

[14] R. Eschbach, Z. Fan, K. T. Knox, and G. Marcu. *Threshold modulation and stability in error diffusion* IEEE Signal Process. Mag; vol. 20, no. 4, pp. 3950, Jul. 2003.

[15] D. L. Lau, G. R. Arce, and N. C. Gallagheri. *Digital halftoning by means of green-noise masks*. J. Opt. Soc. Amer. A, Opt. Image Sci., vol. 16, no. 7, pp. 15751586, Jul. 1999.