Visual Cryptography Scheme for Color Images Using Half Toning Via Direct Binary Search with Adaptive Search and Swap

N Krishna Prakash, *Member, IACSIT* and S Govindaraju

***Abstract*—This paper proposes a method of encoding a color image into *n* meaningful halftone shares using the scheme of halftone visual cryptography. The proposed method encrypts the color image into high-quality *n* halftone shares generated via direct binary search (DBS) with adaptive search and swap method. This scheme achieves lossless recovery and reduces the noise in the shares without any computational complexity. Simulation results show that the visual quality of the obtained halftone shares are observably better compared with previous algorithms.**

***Index Terms*—Visual secret sharing, halftone visual cryptography, direct binary search, adaptive search.**

I. Introduction

The visual cryptography (VC) scheme is used to encode a secret image into several shares, each of which does not reveal any information of the secret image. Shares are printed on transparencies for example, and distributed to *n* participants. The secret image can easily be decrypted only by staking the shares in an arbitrary order. This property needs no computation in decryption.

The basic concept of visual cryptography [6] states that a secret message is divided into *n* partitions, share1, share2,… and share *n*, which are viewed as random noise images. Here a secret contains two levels of illumination: bright areas are labeled with level 0.5 and level 0 is used to represent dark areas. Fig.1 illustrates two simple examples of secret sharing from two shares of size 2x2. The first example indicates that if two shares are the same, then bright illumination will be shown, while the second one shows that if two shares are different, then dark illumination will be shown. Based on the process described above, two shares for secret image are constructed. Superimposing the two shares leads to the output secret image. The decoded image is clearly identified, although some contrast loss occurs. A practical example of visual cryptography is shown in Fig. 2.

Naor and Shamir [6] applied this idea on black and white images only. Different schemes were developed [8, 13] that can be applied on color images. The inconvenient with these new schemes is that they use meaningless shares to hide the secret and the quality of the recovered image is poor.

More advanced schemes based on visual cryptography were introduced in [10, 11] where a colored image is hidden into multiple meaningful shares. Zhi Zhou and G.R.Arce introduced in [1] a Halftone Visual Cryptography (HVC) scheme which utilizes the void and cluster algorithm [7] to encode a secret image into n halftone shares. HVC gives better quality of halftone shares and is applied to grayscale images only. This paper introduces a scheme based on Zhongmin Wang et al. technique, for hiding a colored image. We also extend our previous work on secret sharing schemes for color images using halftoning [2] and propose a method based on Zhongmin wang et al. technique that can encode the secret pixels into the shares via the direct binary search (DBS) halftoning method [3]. This technique improves significantly the quality of the shares compared with previous algorithms.

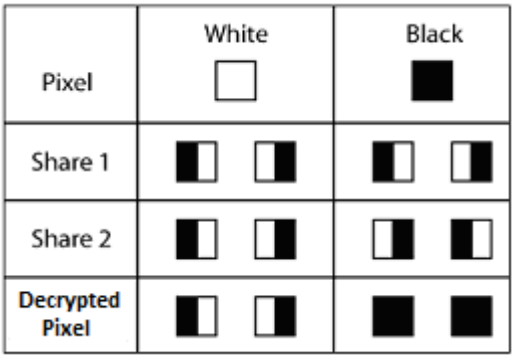


Fig. 1. Construction of 2-out-of-2 scheme

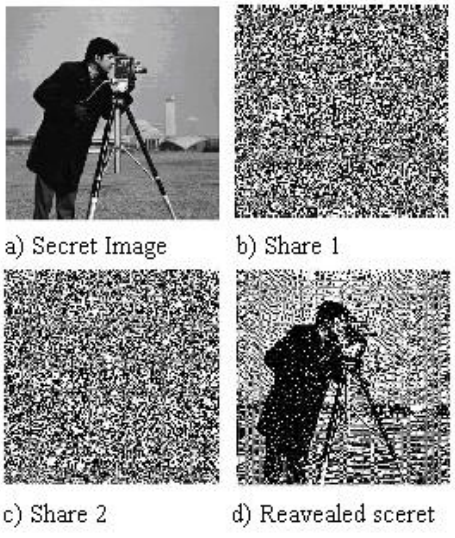


Fig. 2. Image visual cryptography

This paper is organized as follows: Section II & III introduces the Halftone Visual Cryptography for gray scale and color images. Section IV is devoted to our proposed

Manuscript received February 27, 2011; revised July 22, 2011.

N Krishna Prakash is with the Electrical and Electronics Engineering Department, Sri Krishna College of Engineering and Technology, Coimbatore, India (e-mail: nkrishnaprakash@rediffmail.com).

S Govindaraju is with the Electronics and Communication Engineering Department, Kumaraguru College of Technology, Coimbatore, India (e-mail: sgraju_kct@hotmail.com).

method for encoding secret images via DBS. Section V shows the simulation results of the proposed method. Finally section VI draws conclusions.

II. Halftone Visual Cryptography

A. Halftoning via Error Diffusion

Halftone image is obtained by applying the error diffusion [16] algorithm. This method is used as it is simple and effective. The Error Diffusion algorithm is designed to preserve the average intensity level between input and output images by propagating the quantization errors to unprocessed neighboring pixels according to some fixed ratios.To produce the *i*-th halftone share, each of the three color layers are fed into the input. Let $x_{ij}(m, n)$ be the (m, n)-th pixel on the input channel j $(1 \le i \le n,\ 1 \le j \le 3))$ of i-th share. The input to the threshold quantization is:

$$q_{ij}(m, n) = x_{ij}(m, n) - \sum_{k,l} f(k, l) d_{ij}(m - k, n - l) \quad (1)$$

where $f(k, l) \in F$ and F is a two dimensional error filter. The $d_{ij}(m, n)$ is a difference between $q_{ij}(m, n)$ and $g_{ij}(m, n)$.

$$d_{ij}(m, n) = q_{ij}(m, n) - g_{ij}(m, n) \quad (2)$$

The $g_{ij}(m, n)$ is a quantized output pixel value given by :

$$g_{ij}(m, n) = \{\ 1, \text{ if } q_{ij}(m, n) \ge t_{ij}(m, n), \quad (3)$$
$$0, \text{ otherwise, } \}$$

where $t_{ij}(m, n)$ is the threshold. The quantization error $d_{ij}(m, n)$ depends on current input and output and also on the entire past history. Fig. 3. shows the block diagram of the Error Diffusion algorithm and Fig. 4. shows the Floyd and Steinberg error filter.

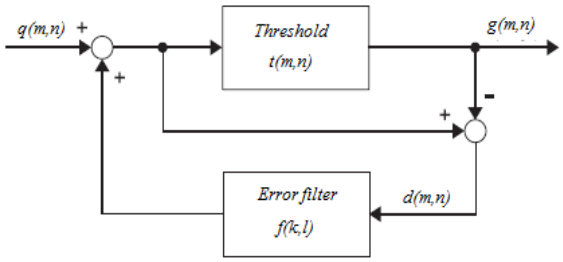


Fig. 3. Error diffusion block diagram

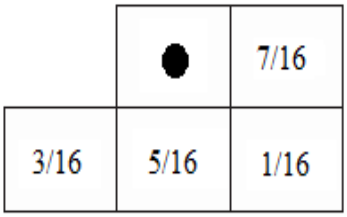


Fig. 4. Error filter

The error filter minimizes low frequency differences between the input and an output image, in addition the error is high frequency or "blue noise". The message information components are not modified during the halftone process.

B. Visual Secret Sharing Scheme

In two-out-of-two halftone visual threshold scheme, a halftone image I, obtained by applying the error diffusion algorithm on a grey level image, is assigned to participant 1. Its complementary image $\bar{I}$, obtained by reversing all black/white pixels of I to white/black pixels, is assigned to participant 2. To encode a secret pixel p into a Q1 x Q2 halftone cell in each of the two shares, only two pixels, referred to as the secret information pixels, in each halftone cell need to be modified. The two secret information pixels should be at the same positions in the two shares. The resulting structure can be described by a Boolean matrix $M = m(i, j)_{nxm}$. Let m represents the number of pixels in a share, α represents the relative difference in the weight between the combined shares that come from a white pixel and a black pixel in the original image, γ represents the size of the collection of C_0 and C_1. C_0 refers to the sub-pixel patterns in the shares for a white pixel and black refers to the sub-pixel patterns in the shares for the 1 pixel. If p is white, a matrix M is randomly selected from the collection of matrices C_0. If p is black, M is randomly selected from C_1. The secret information pixels in the ith (i = 1, 2) share are replaced with the two sub pixels in the ith row of M. These modified pixels carry the encoded secret. The other pixels in the halftone cell which were not modified are referred to as ordinary pixels, maintaining halftone information. The secret pixel p can be visually decoded with contrast $1/Q_1Q_2$ [1].

In the above procedure, the selection of the secret information pixels in a halftone cell is important as it affects the visual quality of the resultant halftone shares. The simplest method to select the locations of the secret information pixels is random selection. The corresponding pixel replacements, however, are equivalent to adding white noise, which leads to poor visual quality. To obtain better visual results, the void and cluster algorithm [7] is applied to choose these pixel locations. This spreads the minority pixel as homogeneously as possible to achieve improved halftone image quality in each share. The void and cluster algorithm, performed on the halftone cell, first applies a low-pass filter to obtain a measure of minority pixel density (m.p.d) at each minority pixel location. The minority pixel is white/black and the majority pixel is black/white, if the halftone cell contains more black/white pixels. The minority pixel with the highest density, denoted as pixel A, is replaced with a majority pixel.

The dither pattern is then filtered again by the same low-pass filter to obtain a measure of m.p.d at each majority pixel location. The majority pixel with the lowest density, denoted as pixel B, is then replaced with a minority pixel. Since the complementary pair has the same distribution of the minority and majority pixels, the located pixels A and B are at the same positions in the two shares. The void and cluster algorithm identifies the minority pixel A with the highest m.p.d. and the majority pixel B wit the lowest m.p.d., and switches their locations. This spreads the minority pixels as homogeneously as possible leading to an improved blue noise halftone cell in each share. If the conventional void and cluster algorithm [7] is performed on each share, it may result in different locations of the secret information pixels in the two shares, which is highly undesirable in the halftone VC

scheme. This problem is addressed using a slightly modified void and cluster algorithm [14]. The void and cluster algorithm uses a Gaussian filter to determine the locations of voids and clusters in the halftone images.

III. Halftone Visual Cryptography for Color Images

The color image is split into channels of cyan, magenta and yellow. Each channel is treated as a grayscale image to which halftoning and visual cryptography are applied independently. After the monochrome shares are generated for each channel, channels are combined separately to create the color shares [2]. There are many halftoning techniques available, of which error diffusion produces superior results [16]. The encryption starts with color channel splitting first and then grayscale halftoning for each channel.

$$I \xrightarrow{\text{split CMY}} [\mathrm{I^C}, \mathrm{I^M}, \mathrm{I^Y}] \xrightarrow{\text{halftoning}} [I_H^C, I_H^M, I_H^Y] \quad (4)$$

The technique presented in section II is applied to each halftone channels. The algorithm begins with finding the position of the largest density value that is the largest density value in all three separations of the original color image. Then a dot is placed at the same position in the corresponding separation of the halftoned image. Gaussian filter is chosen to have a good structure of the placed dots.

$$I_H^C \xrightarrow{(2,2)\text{- VSS}} [S_0^C, S_1^C] \quad (5)$$

$$I_H^M \xrightarrow{(2,2)\text{- VSS}} [S_0^M, S_1^M] \quad (6)$$

$$I_H^Y \xrightarrow{(2,2)\text{- VSS}} [S_0^Y, S_1^Y] \quad (7)$$

This stage is followed by the reconstruction of the original secret image which is done by stacking the halftone shares.

$$[S_0^C, S_1^C] \xrightarrow{\text{Stacking}} I_C^S \quad (8)$$

$$[S_0^M, S_1^M] \xrightarrow{\text{Stacking}} I_M^S \quad (9)$$

$$[S_0^Y, S_1^Y] \xrightarrow{\text{Stacking}} I_Y^S \quad (10)$$

The final step includes combining the stacked images to a single color image.

$$[I_C^S, I_M^S, I_Y^S] \xrightarrow{\text{Combining CMY}} I^S \quad (11)$$

IV. Direct Binary Search Half Toning

Direct Binary search (DBS) uses a human visual system (HVS) model to minimize the error between the continuous tone image and the output halftone image by searching for the best possible configuration of the binary values in the halftone image iteratively [12]. The HVS model is a linear shift invariant low pass filter based on the contrast sensitivity function (CSF) of the human visual system. Each color channel splitted is treated as a grayscale image to which DBS is applied. In DBS [5], an initial halftone image $I_h(m,n)$ in which the positions and values of the secret information pixels are preserved is provided for a continuous-tone image $I_o(m,n)$. Then the algorithm evaluates the difference between $I_o(m,n)$ and $I_h(m,n)$ to produce the error image e(m,n) and filters e(m,n) through the HVS model. The error metric □ is evaluated for the first time. Then the algorithm starts to evaluate changes in the initial halftone image $I_h(m,n)$ that could lead to a decrease in error □. The main operations are change in the status of the current pixel and swapping the values of the current pixel and one of its 8 nearest neighboring pixels that has a different value. When all the pixels in the image have been visited, the first iteration is over. The process is iteratively repeated over the newly obtained halftone image until the error □ has converted to a local minimum.

$$e(m,n) = I(m,n) - I_o(m,n) \quad (12)$$

The filtered error is

$$\hat{e}(m,n) = e(m,n) \otimes h(m,n) \quad (13)$$

where ⊗ indicates convolution. The error metric is defined as

$$\varepsilon = \Sigma |\hat{e}(m,n)|^2 \quad (14)$$

An outline of the basic steps of the algorithm is given below:

1. Generate an initial halftone image $I_h(m,n)$
2. Compute the error $e(m,n)$ in approximating $I(m,n)$ by $I_h(m,n)$
3. Iterate the following: For each pixel (m, n):
   a) Check which of the following changes to I_h decreases e the most:
      • swapping pixel (m, n) with one of its 8 nearest neighbors
      • toggling pixel (m, n) to the opposite color
   b) if any of the possible actions decreases e, perform the best one
   c) update e

The DBS algorithm needs to evaluate many trial toggles and swaps; recomputing the full matrix $\hat{e}$ at each trial is infeasible. The swapping or toggling introduces only a small, localized change to $\hat{e}$. To reduce computation in DBS, it is attempted to avoid swaps and toggles that do not decrease the error significantly [17]. The adaptive search and swap is given below:

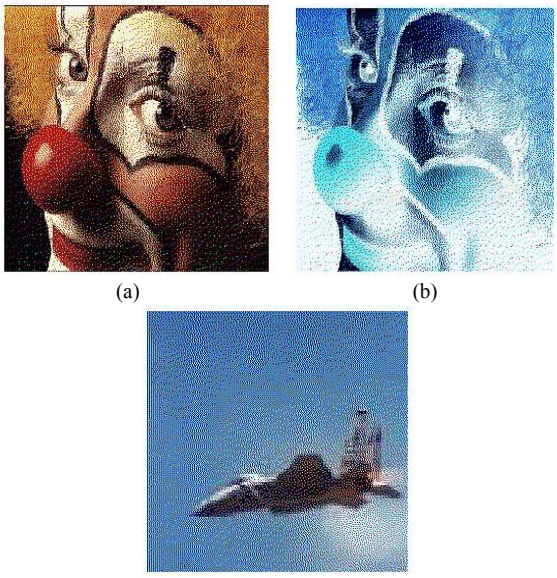
1. Split the image into m × m size blocks
2. Sort each block based on $|\hat{e}(i, j)|$
3. Generate an initial search set S
4. Repeat the following until the ending criteria $(\varepsilon_n - \varepsilon_{n-1})/\varepsilon_{n-1} < 0.01$ is met. For each pixel (m, n) in S:
   a) Remove (m, n) from S
   b) Process pixel (m, n)
   c) if pixel (m, n) is changed, add its neighborhood to S
5. For each pixel to process:
   (a) If the best trial change is a toggle, perform the change and continue to the next pixel. Otherwise:
   (b) If the best trial swap gives ε< threshold, then
      • Perform the change
      • Update ε

Thus halftone shares are produced that has minimal difference with respect to the original continuous-tone image in the sense of HVS and also contains the secret image information. All the shares except the complementary share are produced via DBS with adaptive search and swap. The

complementary image which is a structured image but not a natural image is obtained by reversing all pixels of its complementary pair except the secret information pixels.

V. Simulation Results

Simulation results for the proposed secret sharing scheme for color images are illustrated in this section. The experiment was conducted for different color images of size 512 x 512. The embedded secret image is of same size as the original image. The obtained encoded halftone shares via DBS are shown in Fig. 5(a) and Fig. 5(b). Fig.5(c) shows the decoded secret image by stacking the shares together. The simulation result for the multiple color images is shown in Fig.6.

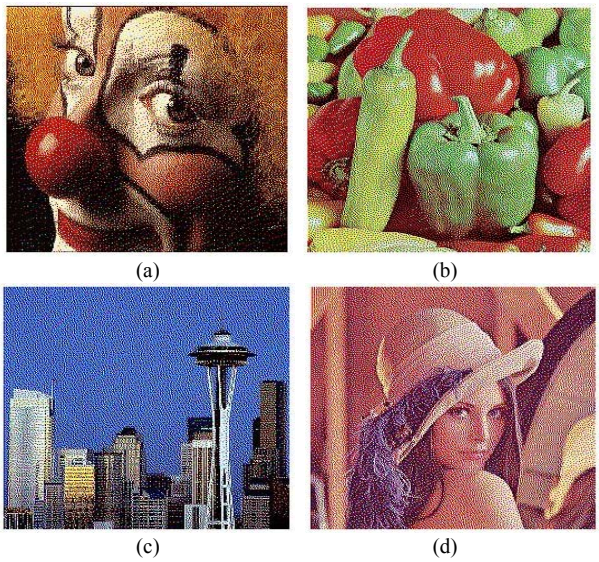


(a) (b)

(c)

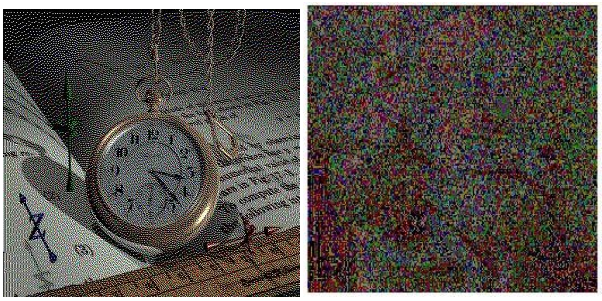
Fig.5. Simulation result 5(a), 5(b) share 1 and share 2 (complementary pair) via DBS; 5(c) decoded image by superimposing the shares

The obtained encoded four shares via DBS are shown in Fig. 6(a) to Fig. 6(d). The decoded secret image by stacking all four shares together is shown in Fig. 6(e). The secret image is clearly revealed. No information can be obtained by stacking share 1 and 2, as shown in Fig. 6(f).



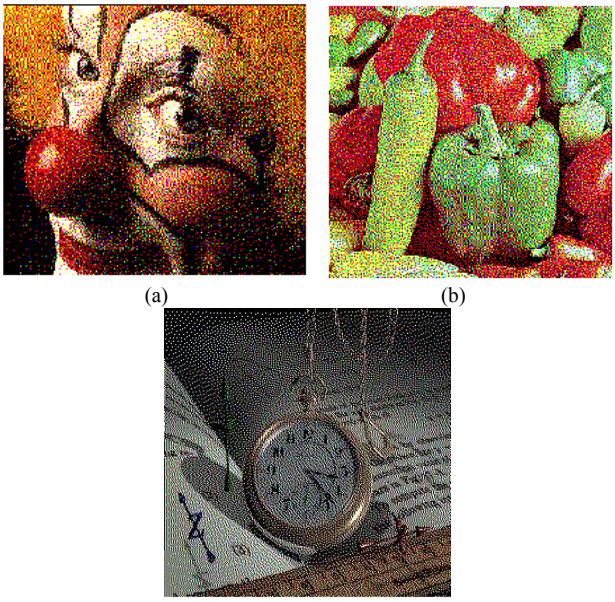
(a) (b)

(c) (d)



(e) (f)

Fig. 6. Simulation result. (6(a), 6(b), 6(c), 6(d)) share 1, share 2, share 3 and share 4 via DBS; 6(e) result of stacking 6(a)-6(d); 6(f) result of stacking 6(a), 6(b).



(a) (b)

(c)

Fig.7. Simulation result of Halftone VC 7(a), 7(b) share 1 and share 2 by halftone VC; 7(c) Decoded image by superimposing the shares by halftone VC.

The proposed method is compared with previously proposed method, Halftone VC. Fig. 7. shows the results of the previously proposed method. The image quality deterioration is obvious on HVC. Though the results are visually comparable, it is important to measure whether the decoded image is visually acceptable. Peak signal to noise ratio (PSNR) is used as the performance metric for the visual comparison between the original images and the encrypted image. The proposed method resulted in a PSNR of 10.37dB and Fig. 6(d) produced by halftone VC has PSNR of 9.62dB. The proposed method shows a difference of 0.75dB in the visual quality. It is observed that the visual quality of decrypted image deteriorates when the number of input shares increases.

VI. Conclusion

Halftone visual cryptography is improved to achieve better halftone images by simultaneously encoding the secret image and producing the halftone shares via DBS. The DBS algorithm with adaptive search and swap improves runtime performance while still generating a halftone with low error. Simulation results show that the proposed method outperforms the other techniques and the recovered image is of high quality. The proposed method achieves i) better

quality of halftone images and the revealed secrets, ii) holds good for multiple colored images also, iii) does not require any additional computational complexity.

REFERENCES

[1] Z. Zhou, G.R. Arce, and G. Di Crescenzo, "Halftone visual cryptography" *IEEE Transactions on Image Processing*, vol.15, No.8, August 2006, pp. 2441-2453.

[2] N. Krishna Prakash and S. Govindaraju, "Visual secret sharing schemes for color images using halftoning," in *Proc. of International Conference on Computational Intelligence and Multimedia Applications*, vol. III, Dec 2007, pp. 174-178.

[3] Z. Wang, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography via direct binary search," *IEEE Tans. On Image Processing*, 2006.

[4] N. Krishna Prakash, S. Govindaraju, "Visual secret sharing schemes for color images using halftoning via direct binary search" in *Proc. of 2nd International Conference on Computer control and communication*, 2009, pp. 1-4.

[5] A. J. Gonzalez, G. R. Arce, J. Bacca Rodriguez, and D. L. Lau, "Human visual alpha-stable models for digital halftoning," in *18th annual Symposium on Electronic Imaging Science and Technology: Human* Vision *and Electronic Imaging XI*, San Jose, CA, Jan 2006

[6] M .Naor and A. Shamir, "Visual Cryptography," in *Proceedings of Eurocrypt*, Lecture notes in computer science, vol. 950, 1994, pp. 1-12,

[7] R. Ulichney, "The void-and-cluster method for dither array generation," *IS,T/SPIE Symposium on Electronic Imaging and Science*, San Jose, CA, vol.1913, pp.332-343. 1993.

[8] E .R. Verheul and H.C.A. Van Tilborg, "Constructions and properties of k out of n visual secret sharing scheme," *Designs, Codes, and Cryptography*, vol.1, 1997, no.2, pp.179-196.

[9] D. L. Lau, R. Ulichney, G. R. Arce, "Fundamental Characteristics of Halftone Textures: Blue- Noise and Green-Noise," Image Systems Laboratory, HP Laboratories Cambridge, March 2003

[10] C. Yang and C. Laih, "New colored visual secret sharing schemes," *Designs, Codes and Cryptography*, vol.20, 2000, pp.325-335

[11] C.Chang, C.Tsai, and T.Chen, "A new scheme for sharing secret color images in computer network", in *Proc. of International Conference on Parallel and Distributed Systems*, pp. 21-27.2000.

[12] S. H. Kim and J. P. Allebach, "Impact of HVS models on model-based halftoning," *IEEE Transactions on Image Processing*, vol.11, Mar pp.258-269. 2002.

[13] R. Lukac, K. N. Plantaniotis, B. Smolka, "A new approach to color image secret sharing," EUSIPCO 2004, pp.1493-1496

[14] H. Ancin, A. K. Bhattacharjya, J. Shu, "Improving void- and- cluster for better halftone uniformity," International Conference on Digital Printing Technologies in SPIE volume. Giordano B. Beretta; Reiner Eschbach (eds), 1998.

[15] M. Iwanmoto and H. Yamamoto, "The Optimal n-out-of-n Visual Secret Sharing Scheme for GrayScale Images," *IEICE Trans. Fundamentals*, vol.E85-A, No.10, October 2002, pp. 2238-2247

[16] Doron Shaked, Nur Arad, Andrew Fitzhugh, Irwin Sobel, "Color Diffusion: Error Diffusion for Color Halftones", HP Laboratories Israel, May 1999.

[17] S. Bhatt, J. Harlim, J. Lepak, R. Ronkese, J. Sabino, "Direct Binary Search with Adaptive Search and Swap," in the college of information sciences and technology, August. 2005.

N Krishna Prakash received the B.E. degree in Electrical and Electronics Engineering, from Maharaja Engineering College, Coimbatore in 2001 and M.E. degree in Applied Electronics, from Kumaraguru College of Technology, Coimbatore in 2004.

He has 8 years of teaching experience and he is currently with Department of Electrical and Electronics Engineering, Sri Krishna College of Engineering and Technology, Coimbatore as Assistant Professor. He has to his credit 5 pulications in refereed conferences in the areas of signal and image processing. His research interests include statistical and nonlinear signal processing, wavelets, halftone visual cryptography and analog VLSI.

Krishna Prakash is a member of IEEE.

S Govindaraju graduated from PSG College of Technology, Coimbatore and obtained his masters at College of Engineering, Chennai.

After 10 year stint in Industry, he migrated to teaching profession out of passion. Since 1997, he is with Kumaraguru College of Technology, Coimbatore. As a professor, he has guided both under-graduate and post-graduate students in their project work. His areas of interest include Digital Signal Processing algorithms, hardware structures for real-time image processing, ASIC/FPGA platforms and bio-inspired computing.