International Journal of Electronics Communication and Computer Engineering
Volume 3, Issue 6, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

New Approach of Visual Cryptography Scheme for Hiding Color Images

Katta Swamy Mergu

***Abstract* — Cryptography is the science of hiding information. The word is derived from the Greek kryptos meaning hidden. Visual Cryptography is a special type of encryption technique which is used to hide the information and data in images. In this technique the decryption process is done without any complex cryptographic computation. The encrypted data is decrypted using Human Visual System (HVS). This is the benefit of the visual secret sharing scheme. Visual Cryptography, introduced by Naor and Shamir in 1995. This paper presents an improved algorithm based on Chang's and Yu visual cryptography scheme for hiding a colored image into multiple colored cover images. This scheme achieves lossless recovery and reduces the noise in the cover images without adding any computational complexity.**

***Keywords* — Image processing, visual Cryptography, secret sharing.**

I. INTRODUCTION

Cryptography is the study of hiding some confidential information. The current cryptography crosses over the mathematics, engineering, and computer science. The applications of cryptography embrace all cases in our daily life, e.g. ATM cards, network security, video and audio. The cryptography covered field is very extensive.

Naor and Shamir [2] proposed a new cryptography area, visual cryptography, in 1994. The most notable feature of this approach is that it can recover a secret image without any computation. It exploits the human visual system to read the secret message from some overlapping shares, thus overcoming the disadvantage of complex computation required in the traditional cryptography. The simplest case is the 2 out of 2 scheme where the secret message is hidden in 2 shares, both needed for a successful decryption [2]. This can be further extended to the k out of n scheme where a secret message is encrypted into n shares but only *k* shares are needed for decryption where $k \le n$. If *k*-1 shares are presented, this will give no information about the secret message. Naor and Shamir applied this idea on black and white images only. Few years later, Verheul and Tilborg [4] developed a scheme that can be applied on colored images. The inconvenient with these new schemes is that they use meaningless shares to hide the secret and the quality of the recovered plaintext is bad. More advanced schemes based on visual cryptography were introduced in [1, 3, 5] where a colored image is hidden into multiple meaningful cover images. Chang et al. [3] introduced in 2000 a new colored secret sharing and hiding scheme based on Visual Cryptography schemes (VCS) where the traditional stacking operation of subpixels and rows interrelations is modified [5]. This new technique does not require transparencies stacking and hence, it is more convenient to use in real applications. However, it requires the use and storage of a Color Index Table (CIT) in order to losselessly recover the secret image. CIT requires space for storage and time to lookup the table. Also, if number of colors c increases in the secret image, CIT becomes bigger and the pixel expansion factor becomes significant which results in severe loss of resolution in the camouflage images.

The next scheme Chang et al. algorithm is a new secret color image sharing scheme [1] based on modified visual cryptography. The proposed approach uses meaningful shares (cover images) to hide the colored secret image and the recovery process is lossless.

II. DEVELOPMENT

A. Chang, Tsai and Chen's Scheme

Since that general data hiding technology comes short of quantity and security, in visual cryptography fails to detect color contrast and to stack images with precision, and thereby a new technique is proposed to share a secret color image improves data hiding and visual cryptography to transmit secret color images. Basically, this scheme is at first to convert confidential information into a color image. Next, two significant color images are selected at random as cover images which share the same size as the image with confidential information. Finally, the secret image with all the pixels will be hidden into two cover images, called camouflage images. An established CIT will help to hide the secret image in the two camouflage images. As for recovering, stack the two camouflage images, and through inverted look-up of CIT, the secret image will returns with ease. Detailed description will be given next about how to hide and share the confidential information between two camouflage images for secure transmission.

B. Chang's et al. Algorithm

Chang et al. proposed in 2002 a new secret color image sharing scheme [1] based on modified visual cryptography. The scheme defines a new stacking operation (XOR) and requires a sequence of random bits to be generated for each pixel. Chang's scheme can be generalized to an *n* out of *n* approach as opposed to Chang Tsai's scheme presented previously.

Method description:

Consider a gray image with 256 colors constitute a secret to be hidden. Each color can be represented as an 8-bit binary vector. The main idea is to expand each colored pixel into *m* subpixels and embed them into *n* shares. This scheme uses *m*=9 as an expansion factor. The resulting structure of a pixel can be represented by an n x 9 Boolean matrix $S=[S_{ij}]$ where $(1 \le i \le n, 1 \le j \le 9)$ and S_{ij} =1, if and only if, the j^{th} subpixel in the i^{th} share has a non-white color. To recover the color of the original secret pixel, an "XOR" operation on the stacked rows of the *n* shares is performed.

A Uniform 2 Out of 2 Construction:

International Journal of Electronics Communication and Computer Engineering
Volume 3, Issue 6, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

We now describe the construction details of a uniform (2,2) secret color image sharing scheme and extend it to a uniform (n; n) scheme in the next subsection. Suppose we take a gray-level secret image I and two significant cover images, O^1 and O^2 whose sizes are the same as that of I.

To share the p^{th} pixel with color k = $(k_1\ k_2\ k_3\ k_4\ k_5\ k_6\ k_7\ k_8)_2$ in I, the dealer randomly chooses an integer r_p, $(1 \le i \le n, 1 \le j \le 9)$. According to r_p and k = $(k_1\ k_2\ k_3\ k_4\ k_5\ k_6\ k_7\ k_8)_2$ S is constructed to satisfy Equation (2). After constructing S, in case that the color of the p^{th} pixels in the cover image $O(i)$ is $k_p(i)$, then the dealer arranges row i in S as a 3 x 3 block $B_p(i)$ and fills the subpixels valued 1 with color $k_p(i)$ for block Bp(i). The resulting blocks B^1_p and B^2_p are the supixels of the p^{th} pixel after expanding. Following the above description, a uniform construction of B^1_p and B^2_p for the p^{th} pixel with color k in I can be constructed by using Algorithm 1. After processing all the pixels in I, two camouflage color images O^{1}'and O^{2}' are generated. In other words, O^{1}' and O^{2}' share the secret image I.

Later, after receiving camouflage images O^{1}'and O^{2}' as well as a sequence of random bits R = {r_1; r_2;…. $r_{|1|}$}, the hidden secret image is recovered without any distortion by performing Algorithm 2.

Steps of Hiding Algorithm

Algorithm 1 [Sharing a pixel among two blocks]

Input: a colored secret image I_{HL} of size H x L and two colored cover images O^1_{HL} and O^2_{HL}.

Output: two camouflage images $O^{1'}$ and $O^{2'}$.

Step1: Scan through the I_{HL} and convert each pixel in I_{ij} to an 8 bits binary string denoted as k=$(k_1,k_2,k_3,k_4,k_5,k_6,k_7,k_8)_2$.

Step 2: Set all elements in S to be null, noofone = 0, randomly select an integer r, where 1 ≤ r ≤ 9 for each pixel of I_{ij}.

Step 3: For i = 1 to 8 do
if (k_i = 1 and i < r) then
noofone = noofone + 1;
S_{1i} = (1; if (noofone % 2 = 1)
(0; if (noofone % 2 = 0)
(where % denotes "MOD" operation)
else if (k_i = 1 and i ≥ r) then
noofone = noofone + 1;
j = i + 1;
S_{1i} = (1; if (noofone % 2 = 1)
(0; if (noofone % 2 = 0)

Step 4: If (noofone%2 = 1) then S_{1r} = 0.

Step 5: Randomly assign the rest null elements in row 1 to 0 or 1, let the total number of 1s be more than the number of 0s by one.

Step 6: Let j=0, for i = 1 to 9 do
if (i ≠ r) then
j = j + 1;
$S_{2i} = S_{1i}$ xor k_j
else
if (noofone%2 = 1) then S_{2i} = 1
else $S_{2i} = S_{1i}$ xor 0

Step 7: Arrange each row in S to two 3 x 3 blocks B^1 and B^2, respectively.

Step 8: Fill the 1s subpixels in B^1 and B^2 with colors k^1 and k^2, respectively, the rest of subpixels are transparent.

Step 9: After processing all the pixels in $I_{HL,}$ two camouflage colored images $O^{1'}$ & $O^{2'}$ are generated. In order to losselessly recover I_{HL}, both $O^{1'}$ & $O^{2'}$ as well as a sequence of random bits R={r_1; r_2;…. $r_{|1|}$} are needed.

Recovering Algorithm:

Algorithm 2 [Recover the hidden secret image]

Input: two camouflage images O^{1}'and O^{2}'with image size of n x m pixels, a sequence of random bits R = r_1; r_2; ….; $r_{|1|}$,

Output: the hidden secret image I ' with image size of n /3 x m /3 pixels.

Step 1: For r = r_1 to $r_{|1|}$ do Step 2 to Step 4.

Step 2: Set V^1_r and V^2_r the rth 3 x 3 block in O^{1}'and O^{2}', respectively.

Step 3: Arrange V^1_r and V^2_r to two 1 x 9 matries S^1_r and S^2_r , respectively.

Step 4: The r^{th} pixel in I'is
I'[r] = $(k_1\ k_2\ k_3\ k_4\ k_5\ k_6\ k_7\ k_8)_2$,
Where $k_i = S_{1j} \oplus S_{2j}$
and

$$j = \begin{cases} i & if\ i < r \\ i+1 & if\ i \ge r \end{cases} \qquad (1)$$

Step 5: After determining all the pixels in G', the secret image G(t)hidden in $O^{1'}$and $O^{2'}$ is recovered.

A Uniform n Out of n Construction:

In this subsection, we extend the proposed 2 out of 2 scheme to construct a uniform *n* out of *n* secret color image sharing scheme. The encryption process for *n* out of *n* scheme is shown in fig.1 and the decryption process for *n* out of *n* scheme is shown in fig.2.

To share a pixel with color k = $(k_1\ k_2\ k_3\ k_4\ k_5\ k_6\ k_7\ k_8)_2$ among n shares, the dealer first chooses an integer r, $(1 \le i \le n, 1 \le j \le 9)$, and then constructs the n x 9 matrix S´ by the following procedure.

Step 1: Randomly assign n – 2 rows $\{S_{i1}\ S_{i2}\ S_{i3}\ \ldots.\ S_{in-2}\}_n$ S_0 with five 1s and four 0s.

Step 2: Compute t, such that t=$(t_1\ t_2\ t_3\ t_4\ t_5\ t_6\ t_7\ t_8\ t_9)_2$

$$Where\ t_i = \begin{cases} k_i & if\ i < r \\ 0 \cup 1 & if\ i = r \\ i+1 & if\ i > r \end{cases} \qquad (2)$$

Step 3: Compute t_0 by "xoring" t, S_{i1}; S_{i2}; ::: and S_{in-2} .
That is, t'=t $\oplus$ S_{i1} $\oplus$ S_{i2} $\oplus$ ….. $\oplus$ S_{in-2} (3)

Step 4: Apply the uniform 2 out of 2 scheme to compute row S_{in-1} and S_{in}, such that
t'= S_{in-1} $\oplus$ S_{in} (4)

Proof: From Equation (5), the following equation holds.
t= S_{i1} $\oplus$ S_{i2} $\oplus$ ….. $\oplus$ S_{in-2} $\oplus$ t'. (5)
Since there exists a uniform 2 out of 2 construction for any t_0 such that t'= S_{in-1} $\oplus$ S_{in} in, the following equation holds,
t= S_{i1} $\oplus$ S_{i2} $\oplus$ ….. $\oplus$ S_{in-2} $\oplus$ S_{in-1} $\oplus$ S_{in} (6)

This also means that the result of "xoring" all the rows in S´ satisfies Equation (1). Furthermore, since each row in S´ contains five 1s and four 0s, S´ is a uniform n out of n scheme with a 9-pixeled expansion.

International Journal of Electronics Communication and Computer Engineering
Volume 3, Issue 6, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

III. RESULTS

In Chang T Sai and Chen's algorithm a 100 x 100 secret image (fig.4(a)) is hidden into two 100 x 100 meaningful cover images (fig.4(b) & fig.4(c)). As seen in fig.4(d) and fig.4(e), the camouflage images obtained the original algorithm. In order to get the lossless original image from camouflage images, Color Index Table (CIT) must be needed.

The quality of recovered image can be quantified by using the Peak Signal to Noise Ratio (PSNR).

The PSNR is defined as

$PSNR=20 \log_{10}(255/\text{mean square error})$ (7)

The Peak Signal to Noise Ratio for the Chang Tsai and Chen's Scheme is 18.7 dB.

Next we discuss the results improved secret sharing n out of n scheme (chang et al. algorithm). Suppose a gray secret image of 100 x 100 pixels as shown in Fig. 5(a) is given. Next, we select three cover images, as shown in Fig.5(b) Fig.5(c) and Fig.5(d). After performing the secret sharing scheme, three corresponding camouflage images are generated as shown in Fig.5, Fig.5(f) and Fig.5(g). Later, the original secret image is shown in Fig.(h), will be revealed without any distortion by performing the recovery algorithm.

By using the equation (7), we can quantify the quality of recovered image, is 19.2 dB.

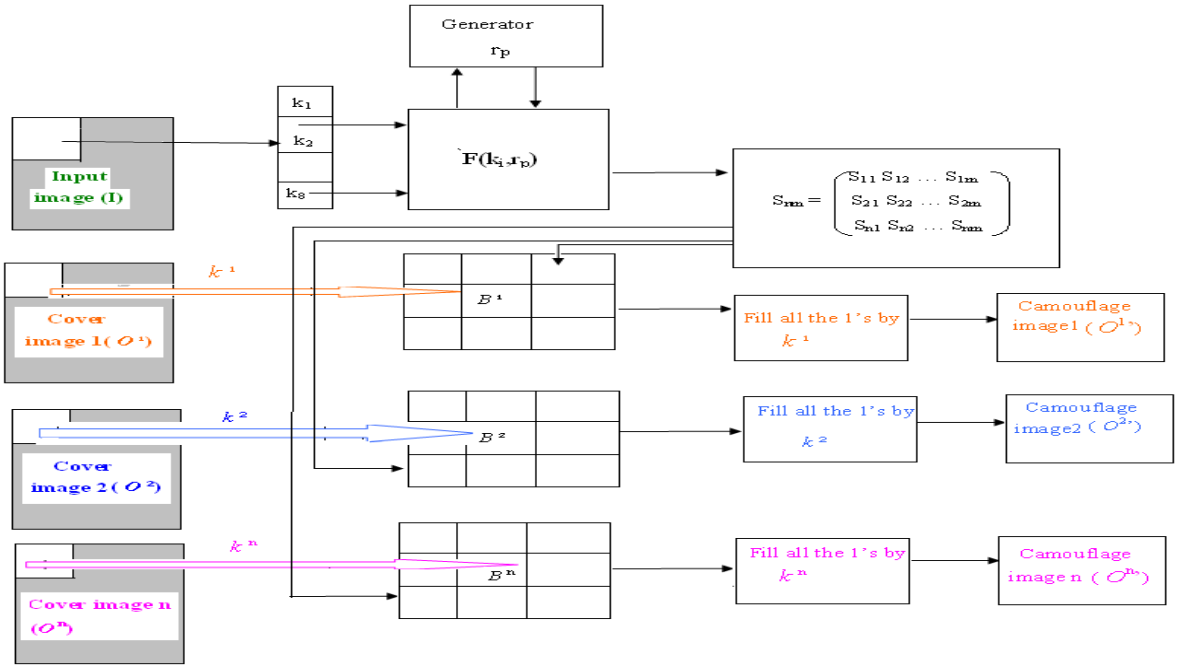

Fig.1. Chang's et al. secret sharing algorithm flowchart

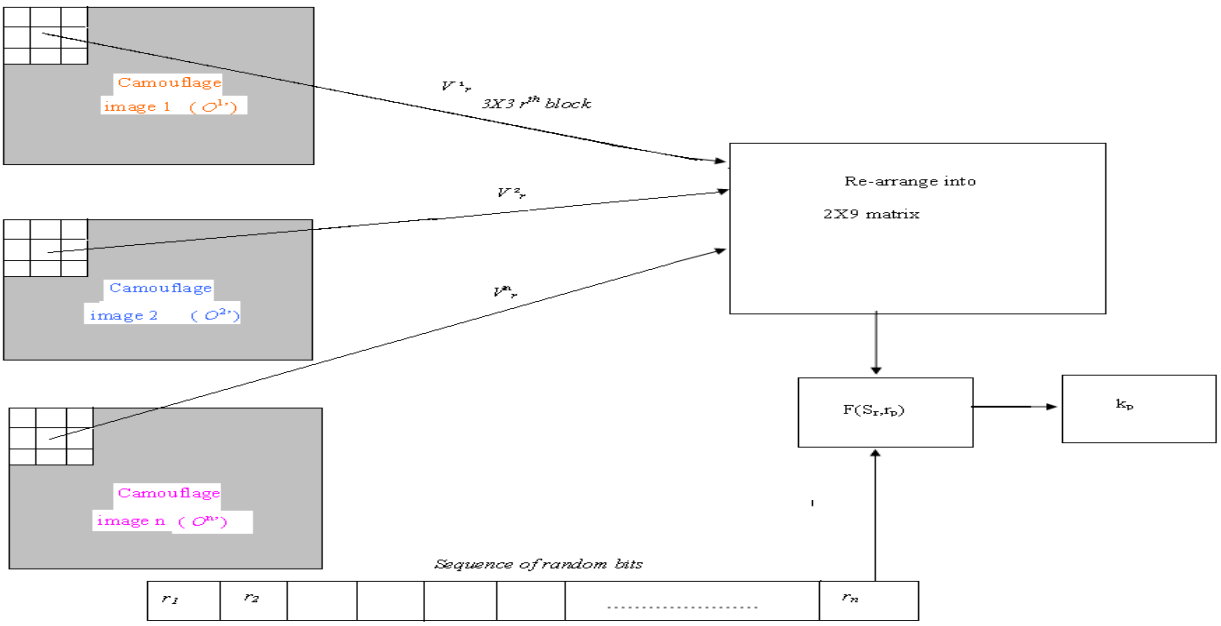

Fig.2. Chang's et al. secret sharing recovering algorithm

International Journal of Electronics Communication and Computer Engineering
Volume 3, Issue 6, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

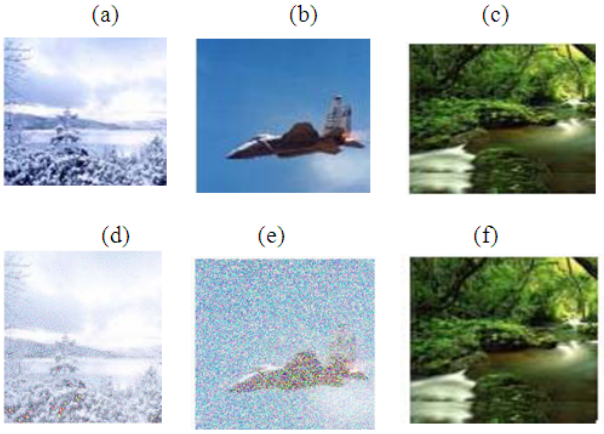

Fig.4. Chang's T Sai and Chen's secret sharing algorithm results: (a) cover image #1, (b) cover image #2, (c) secret Image(d) camouflage #1 (e) camouflage #2, (f) recovered image

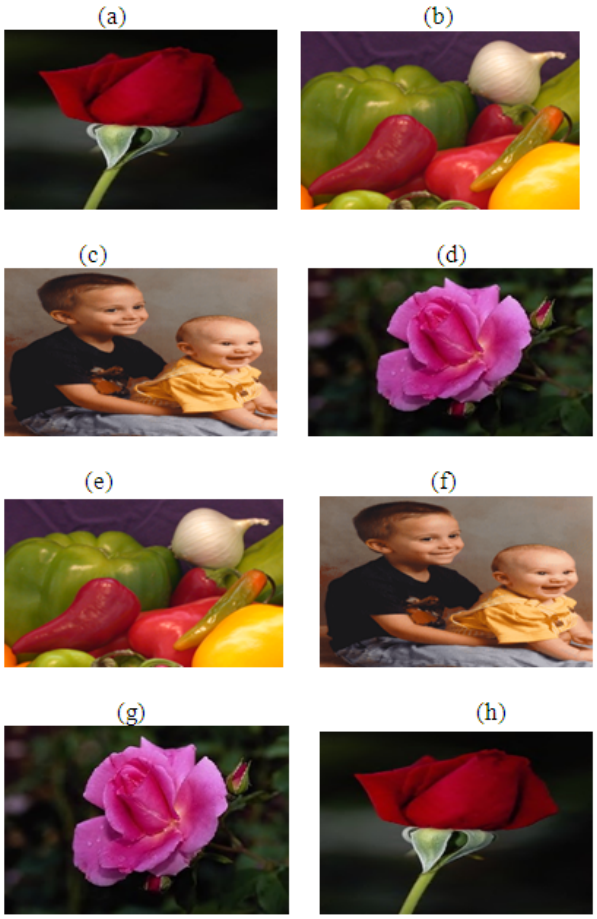

Fig.5. Chang's secret sharing algorithm results: (a) secret Image (b) cover image #1, (c) cover image #2, (d) cover Image #3,(e) camouflage #1 (f) camouflage #2, (g) camouflage #3, (h) recovered image.

IV. Comparisons

In this section we discuss the comparisons between the three methods. Those are Chang, T Sai & Chen's algorithm and Chang's et al. algorithm.

Table1: Comparisons between three Algorithms

Chang , Tsai and Chen's Scheme	**Chang's et al. Algorithm:*(2 out of 2)***	**Chang's et al. Algorithm:*(n out of n)***
Only one secret image and two cover images	Only one secret image and two cover images	Only one secret image and n no. cover images
Basic operation is "AND"	Basic operation is "XOR"	Basic operation is "XOR"
Moderately Securable	Moderately Securable	More Securable comparing with other two methods.
Processing time for both encryption and decryption is 26 min	Processing time for both encryption and decryption is only 8 min.	Processing time for both encryption and decryption is 46 min.
Additional space for CIT is needed	No need of additional space	Additional space is needed for more no. of cover images.

V. Applications

Visual Cryptography Schemes can decode concealed images based purely on human visual systems, without any aid from cryptographic computation. This nice property gives birth to a wide range of encryption applications. In this section, we will discuss how VCS is used in applications such as E-Voting system, financial documents and copyright protections.

VI. Conclusion and Future Scope

In this paper, we have presented (2, 2) and (n; n) secret color image sharing schemes in two different algorithms. Based on the modified visual cryptography, these two schemes provides an efficient way to share a gray image among different images. In Chang, T sai and Chen's algorithm to hide and recover the secret image a Color Index Table is needed and it takes more space to store CIT and spend more time to look-up the CIT. But Chang et al. algorithm [5] improves the pixel expansion quite substantially. Furthermore, the construction does not need any special *image editing package* or extra *color index table*; it only needs the basic XOR operation and a sequence of random bits for each pixel. This developed method does not require any additional cryptography computations and achieves a lossless recovery of the secret image.

Since the chang et al. algorithm has the advantage of low computation and avoids the drawbacks mentioned in the previous approach, it is indeed suitable for today's requirement of low power. Because of these advantages, we can infer that some practical applications, such as using some low computation, compact memory devices to reach the goal of mobile authentication or identification, will be available to all soon.

As future work, this scheme can possibly be modified to hide two or more independent colored secret images into n meaningful colored cover images. The recovery process of both secret images should remain lossless while using the same expansion factor as described.

REFERENCES

[1] Chang, C. C. and Yu. T. X., Sharing a Secret Gray Image in Multiple Images, in the Proceedings of International Symposium on Cyber Worlds: Theories and Practice, Tokyo, Japan, Nov. 2002, pp.230-237.

[2] M. Naor and A. Shamir, Visual cryptography. Advances in Cryptology EUROCRYPT '94. Lecture Notes in Computer Science, (950):1–12, 1995

[3] C. Chang, C. Tsai, and T. Chen, A new scheme for sharing secret color images in computer network. In the Proceedings of International Conference on Parallel and Distributed Systems, pages 21–27, July 2000.

[4] E. Verheul and H. V. Tilborg., Constructions and properties ofk out of n visual secret sharing schemes. Designs, Codes and Cryptography, 11(2):179–196, 1997.

[5] C. Yang and C. Laih., New colored visual secret sharing schemes. Designs, Codes and Cryptography, 20:325–335, 2000.

[6] R.L. Lagendijk and J. Biemond, Iterative Identification and Restoration of Images. Norwell, MA: Kluwer Academic Publishers, 1991.

AUTHOR'S PROFILE

Katta Swamy Mergu
received his B. Tech. Degree from KITS(S), JNTU at Hyderabad, India. After that he received his M. Tech Degree from JNTU, Ananthapur, A.P, India. Presently he is working as Asst. Professor at Vignana Bharathi Institute of Technology, Hyderabad, Andhra Pradesh, India. His research interests include Digital Image Processing and its applications; Signal processing, Digital Communication and Coding Theory and Techniques.
E-mail: kattaswamy@gmail.com