International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Gray Scale Image Authentication Using SSS Technique

Vandana Navale[1], Archana Lomte[2]

[1]Pune University, BSIOTR(W),Wagholi , Pune 411014, India

[2]Bhivrabai Sawant Institute of Technology And Research Pune University, Wagholi, Pune, India

Abstract: ***This is a blind authentication method for Gray Scale image that is in PNG (Portable Network Graphics) Format. This method is based on SSS (Shamir's Secret Sharing) technique. This technique used to reduce risk of data loss. Authentication is done for Gray Scale Image by generating secrets for each block of gray image. Block content are in binary forms. That shares are embedded in to Alpha channel Plane .Then alpha channel plane is combined with the original Gray scale image to form a PNG image. When image authentication is done image blocks are marked as tampered the shares embedded in the alpha channel plane are match with current image block shares by applying reverse Shamir secret sharing technique repaired tampered block contents.***

Keywords: SSS (Shamir's Secret Sharing) technique, PNG (Portable Network Graphics), Data repair, Authentication, Data Hiding

1. Introduction

Important information can be preserve in digital images, today's day it is very easy to modify in digital images content because of advance digital technology .The security problem regarding this type of images are major issue. So to solve image authentication problem required some method [1][2]. Gray scale image have two major gray values one for background and one for foreground as shown in Fig.1. The image contents circuit diagrams, certificates, Last will, art drawing, scanned check etc.

Figure 1: Binary like Gray scale image

Gray scale image overcomes the Visual quality problem of binary image. In this paper we proposed new blind authentication method for Gray scale images with data repair capability. After the proposed method applying the gray scale image converted into stego image that stego image is in PNG format that is in scrambled form in a alpha channel plane and that stego image with alpha channel is for transmission on network. In put image is Gray image shown in Fig 1. The stego image is received may be verified for its authenticity. The stego images integrity modifications can be detected by the method at block level and it's repaired at pixel level. The proposed method is based on shamir's method [3] .The secret is transform into n shares and when k of the n shares is collected the secret message can be recovered without data loss not necessary all of them are collected the secret message can be recovered. This technique is useful to reduce data loss. In proposed method two information security issues are combined data hiding and secret sharing. The secret sharing scheme is used in contents data and also it help to repair tampered data through the use of shares self repairing of tampered data at attacked image parts is that after the original data of the cover image are embedded into the image itself. For use in later data repairing the cover image is removed in the first place and original data are no longer available for data repairing resulting is not accretion.

To solve the original image data other place without change in cover image itself to solve this problem use extra alpha channel plane will create random transparency in the formed PNG image. As proposed in this paper is to map the resulting alpha channel values into a small range near their extreme value of 255. Another problem is data embedded in carrier that is of large sized for my case here with the alpha channel as the carrier, this is not a problem because the cover image that I deal with is binary like and thus may just embed into the carrier a binary version of cover image that contain much less data.

2. Literature Survey

Some methods for image authentication have been proposed; authentication with embedding special codes Yang and Kot [4] proposed a two layer binary image authentication method in which one layer is used for checking image fidelity and the other for checking image fidelity and the other for checking image integrity. Latter Yang and Kot [5] proposed a pattern based data hiding method for binary image authentication in which three transition criteria are used to determine the flip abilities of pixels in each block and the watermark is adaptively embedded into embedded blocks to deal with host image. In Tzeng and Tsai's method [6], randomly generated authentication codes are embedded into image blocks for use in image authentication, and a so-called code holder is used to reduce image distortion resulting from data embedding. Lee *et al.* [7] proposed a Hamming-code-based data

embedding method that flips one pixel in each binary image block for embedding a watermark, yielding small distortions and low false negative rates. Lee *et al.* [8] improved the method later by using an edge line similarity measure to select flappable pixels for the purpose of reducing the distortion.

3. Algorithms

3.1 The Shamir Secret Sharing Method

Proposed method's first review is the SSS method. In this (k, n)-threshold secret sharing method of Shamir [3], secret d form of an integer vale is convert into shares, that shares are distributed to n participants for them to keep; and as long as k of the n shares are collected, the original secret can be accordingly recovered , where $k \leq n$

Algorithm 1: secret sharing By using threshold values.

Input: Take secret d as integer values, number n of participants, and threshold $k \leq n$.

Output: n shares in the form of integers for the n participants to keep.

Step 1. Choose randomly a prime number p that is larger than d.

Step 2 .Select $k-1$ integer values $c1, c2, \ldots \ldots c_{k-1}$ within the range of 0 through p-1.

Step3. Select n distinct real values $x_1, x_2 \ldots\ldots\ldots$

Step 4.Use the following ($k-1$) degree polynomial to compute n function values $F(x_i)$, called partial shares for $i = 1,2,3, \ldots \ldots \ldots n$ i.e.

$$F(x_i) = (d + c_1 x_i + c_2 x_i^2 + \cdots c_{k-1} x_i^{k-1}) \ mod \ p \quad (1)$$

Step 5. Deliver the two-tuple $(xiF(xi))$ as a *share* to the ith participant where $i=12\ldots n$.

Since there are k coefficients, namely, d and c_1 through c_{k-1} in (1) above, it is necessary to collect at least k shares from the n participants to form k equations of the form of (1) to solve these k coefficients in order to recover secret d. This explains the term threshold for k and the name (kn) -threshold for the Shamir method [11]. Below is a description of the just-men-tioned equation-solving process for secret recovery.

Algorithm 2: Equation solving process for secret recovery

Input: 1.prime no p

2. k shares that collected from n participants

Output: secret d hidden in the coefficients c_i

Where $i = 1,2, \ldots, k-1$

Step 1: By using k shares

$$x_1, F(x_1)), (x_2, F(x_2)) \ldots \ldots, (x_k, F(x_k))$$

to set up

$$F(x_j) = (d + c_1 x_j + c_2 x_j^2 + \cdots + c_{k-1} x_j^{k-1}) mod \ p$$

(2) where ,

$$j = 1,2,3 \ldots . k$$

Step 2: Apply Lagrange's interpolation to obtain d as follows[9]:

$$d = -1^{k-1} \left[F(x_1) \frac{x_2 x_3 \ldots \ldots x_k}{(x_1 - x_2)(x_1 - x_3) \ldots (x_1 - x_k)} + F(x_2) \frac{x_1 x_3 \ldots . x_k}{(x_2 - x_1)(x_2 - x_3) \ldots . (x_2 - x_k)} + F(x_k) \frac{x_1 x_2 \ldots \ldots x_{k-1}}{(x_k - x_1)(x_k - x_2) \ldots . . (x_k - x_{k-1})} \right] mod \ p$$

Step 3: compute c_1 using c_{k-1} by expanding equality and

$$j = 1,2,3 \ldots . k$$

comparing the result with(2) in step 1 while regarding variable x in the equality below to be x_j in (2)

$$F(x) = \left[F(x_1) \frac{(x-x_2)(x-x_3) \ldots \ldots (x-x_k)}{(x_1 - x_2)(x_1 - x_3) \ldots (x_1 - x_k)} + F(x_2) \frac{(x-x_1)(x-x_3) \ldots (x-x_k)}{(x_2 - x_1)(x_2 - x_3) \ldots (x_2 - x_k)} + F(x_k) \frac{(x-x_1)(x-x_2) \ldots \ldots (x-x_{k-1})}{(x_k - x_1)(x_k - x_2) \ldots \ldots (x_k - x_{k-1})} \right] mod \ p$$

In above algorithm step 3 is added extra for computing values of parameters c_i if only secret value d needed to convert this step is not required.

2. Data Repairing and Image Authentication

In the proposed method, a PNG image is created from a bi-nary-type grayscale document image I by using an alpha channel plane. The original image I may be considered as a grayscale channel plane of that PNG image. Generating s process of PNG image creation is shown in Fig. 2.

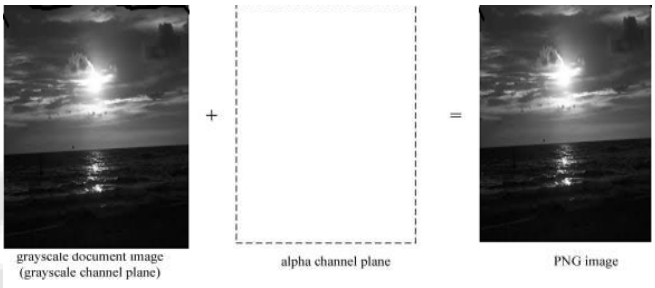

Figure 2: Creation of a PNG image from a grayscale document image and an additional alpha channel plane.

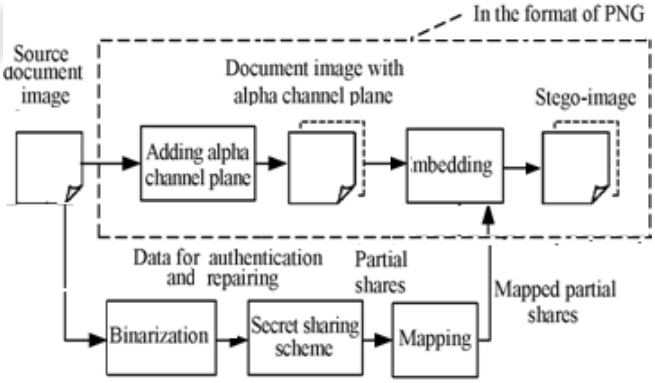

Figure 3: Creating a PNG image from a grayscale document image and an alpha channel

Next, is binaries by moment-preserving thresholding [10], yielding a binary version of , which I denote as I_b. Data used for repairing and authentication are then computed from I_b and taken as input to the SSS scheme to generate n secret shares. The share values are mapped into a small range of alpha channel values near the maximum transparency value to create an imperceptibility effect. Finally, the mapped secret shares are randomly embedded into the alpha channel for the purpose of promoting the security protection and data repair capabilities. Two block diagrams describing the proposed method are shown in Figs. 3 and 4.

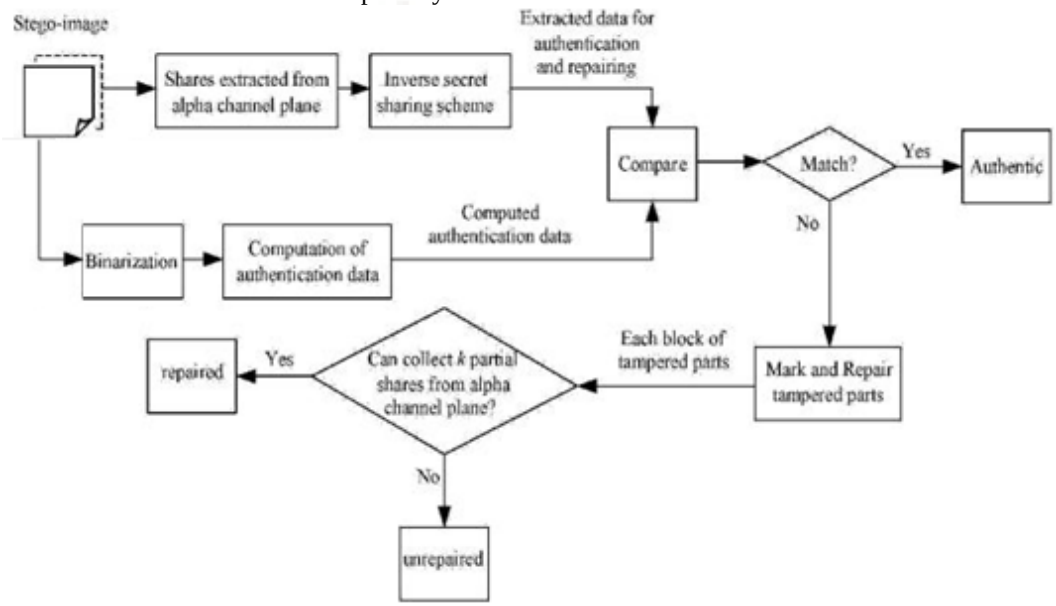

Figure 4: Authentication process including verification and self-repairing of a stego-image in PNG format.

Algorithm 3:

A. Generation of stego image from given Grayscale Image

Input: 1.a secret key K.

2. a grayscale document image I with two major gray values

Output: stego-image I' in the PNG format with relevant data embedded, including the authentication signals and the data used for repairing.

Stage 1. An Authentication signal genration

Step 1. Input image binarization

Consider Gray values and as a threshold to binarize compute yielding a binary version with "0" representing and "1" representing

Step 2. cover image is converted into PNG format

Transform I into a PNG image with an alpha channel plane I_α by creating a new image layer with 100% opacity and no color as I_α and combining it with I using an image processing software package.

Step 3. Start the looping

Take in an unprocessed Take in an unprocessed raster-scan order a 2 ×3 block of with pixels .....

Step 4. Create an authentication signals

First generate 2 bit authentication signals with and , where denotes the exclusive-or operation.

Stage 2. Embedding and creation of shares.

Step 5. For secret sharing creation of data
Concatenate the 8 bits of , , and through to form an 8-bit string, divide the string into two 4-bit segments, and transform the segments into two decimal numbers and , respectively.

Step 6. Generation of Partial Shares

Set , , and in (1) of Algorithm 1 to be the following values: 1) =17 (the smallest prime number larger than 15); 2) = and = ; and 3) =1, =2, =6. Perform Algorithm 1 as a (2, 6)-threshold secret sharing scheme to generate six partial shares through using the following equations (3):

$$q_i = F(x_i) = (d + c_1 x_i) \bmod p$$

where 1 2 , ,6. .

Step 7. Mapping of partial shares

Add 238 to each of through, resulting in the new values of through respectively which fall in the nearly total

transparency range of 238 through 254 in the alpha channel plane I_α.

Step 8. Two partial shares embedding in current block

Take block B_α in I_α corresponding to B_b in I_b, select the first two pixels in B_α in the raster-scan order, and replace their values by q_1' and q_2' ,respectively.

Step 9. Embedding remaining partial shares at random pixels

Use key K to select randomly four pixels in I_α but outside B_α, which are unselected yet in this step, and not the first two pixels of any block; in the raster-scan order, replace the four pixels values by the remaining four partial shares q_3' through generated above, respectively.

Step 10. End of loop

If there exists any unprocessed block in I_b, then go to Step 3; otherwise, take the final I in the PNG format as the desired stego-image I'. The possible values of q_1 through q_6 yielded by (3) above are between 0 and 16 because the prime number p used there is 17. After performing Step 7 of the above algorithm, they become q_1' through q_6' , respectively, which all fall into a small interval of integers ranging from 238 to 254 with a width of 17 (the value of the prime number). The subsequent embedding of q_1' through q_6' in such a narrow interval into the alpha channel plane means that very similar values will appear everywhere in the plane, resulting in a nearly uniform transparency effect, which will not arouse notice from an attacker.

The reason why we choose the prime number to be 17 in the above algorithm is explained here. If it was instead chosen to be larger than 17, then the aforementioned interval will be enlarged, and the values of q_1' through q_6' will become possibly smaller than 238,creating an undesired less transparent but visually whiter stego image As to the choice of the block size, the use of a larger block size, such as 2×4 or 3×3, will reduce the precision of the resulting integrity authentication (i.e., the stego-image will be verified in a spatially coarser manner). On the other hand, it seems that a smaller block size such as 2×2 instead of 2×3 may be tried to increase the authentication precision. However, a block in the alpha channel with a size of 2×2 can be used to embed only four partial shares instead of six (see Steps 6–9 of Algorithm 3). This decreases the share multiplicity and thus reduces the data repair capability of the method. In short, there is a tradeoff between the authentication precision and the data repair capability, and our choice of the block size of 2×3 is a balance in this aspect. Finally I use Fig.5 to executing steps 8 and 9 in algorithm 3 where a core idea of the proposed method is presented, i.e., two shares of the generated six are embedded at the current block and the other four are embedded at four randomly selected pixels outside the block, with each selected pixel not being the first two ones in any block

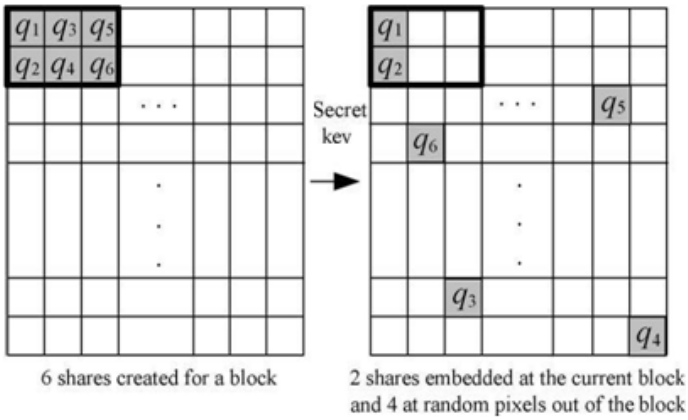

Figure 5: Embedding six shares created for a block

B. Stego-Image Authentication Algorithm

This algorithm describing the proposed stego-image authentication process, including verification and self-repairing of the original image content, is presented in the following.

Algorithm 4: Authentication of a given stego-image in the PNG format
Input: stego-image I', the representative gray values g_1 and g_2 , and the secret key K used in Algorithm 3.
Output: Image I_r with tampered blocks marked and their data repaired if possible.

Stage 1. **Extraction of the embedded two gray values.**
Step 1. Stego image Binarization
Calculate $T=(g_1+g_2)/2$, and use it as a threshold to I' binarize here "0" representing g_1 and "1" representing g_2

Stege 2.Stego image verification

Step 2. Starting of loop

Take in a rasterscan order an unprocessed block B_b' from I_b' with pixel values through ,and find the six pixels value q_1' through q_6' of the corresponding block B_α' in alpha channel plane I_α' of I'

Step 3. Hidden authentication signal extraction

Following steps to extract the hidden two bits authentication signal $s = a_1 a_2$ from B_α'

1.Subtract 238 from each of q_1' and q_2' to obtained two partial shares q_1 and q_2 of B_b' resp.

2.With shares and as input, perform algorithm 2 to extract two values and as out put

3.Transform and into two 4 bit memory values concat them to from 8 bit string s, take the first 2 bit of s to compose the hidden authentication signals $s = a_1 a_2$

Step 4. computation of the authentication signal from current block content

Compute a 2 bit authentication signal $s' = a_1' a_2'$ from values p_1 through p_6 of the six pixels of by and B_b' by

$a_1' = p_1 \oplus p_2 \oplus p_3$ and $a_2' = p_4 \oplus p_5 \oplus p_6$

Step 5. Matching of hidden and computed authentication signals and marking of tampered blocks Match s and by checking if $a_1 = a_1'$ and $a_2 = a_2'$, and if any mismatch occurs, mark B_b', the corresponding block B' in I', and all the partial shares embedded in B_α' as tampered [9].
Step 6. End of looping

If there exists any unprocessed block in, then go to Step 2; otherwise, continue.

Stege 3. Self repairing of the original image content

Step 7. Extraction of the remaining partial shares For each block in perform the following steps to extract the remaining four partial shares through of the corresponding block B_b', in I_b' from I_α' blocks in other than B_α' 1.Use key K to collect the four pixels in I_α' in the same order as they were randomly selected for B_b',in step 9 of algorithm 3 and take out the

respective data and q_6' embedded in them. 2. Subtract 238 from each of q_3' through q_6' to obtain through

Step 8. Tampered region repairing

For each block B' in I' marked as tampered previousliy, perform the following steps to repair it if possible.

1. From the six partial shares q_1 through q_6 of block

With shares (k, q_k) and (l, q_l) as input, perform
1. Algorithm 2 to extract the values of d and a_1 (the secret and the first coefficient value, respectively) as output.
3. Transform d and a_1 into two 4-bit binary values, and concatenate them to form an 8-bit string s'
4.Take the last 6 bits $b_1', b_2', \ldots b_6'$ from s' and Check their binary values to repair the corresponding tampered pixel values $y_1', y_2', \ldots y_6'$ of block by the following way:

Step 9. Take the final I' as the desired self-repaired image I_r.

4. Merits of Proposed Method

Along with being capable of data repairing and being blind in nature. The proposed method has several other merits which are described as following.

1. Higher data security and possibility to survive image content attacks: Due to the use of encryption the data become scrambled, therefore the hackers doesn't see the document data, and also by the use of sharing method , the proposed method can survive malicious attacks of common content modification, such as super imposition, painting etc
2. Providing pixel level repairing of tampered image parts: After collecting two non tampered partial shares, we can repair the tampered block at the pixel level.
3. Making the use of new type of image channel for data sharing: Rather than common type of image a PNG image has the extra alpha channel plane , which is normally used to produce transparency of the image .

5. Experimental Result

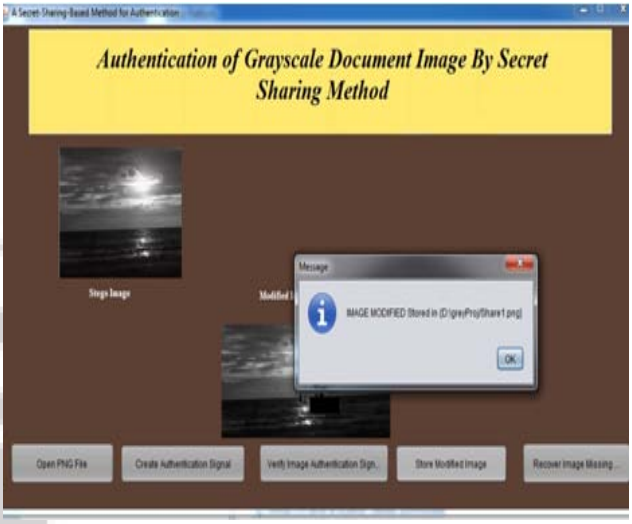

Figure 6: Authorization result of an image in PNG format Original cover image. ,Stego image i.e. Binarized imageof original image with alpha channel.

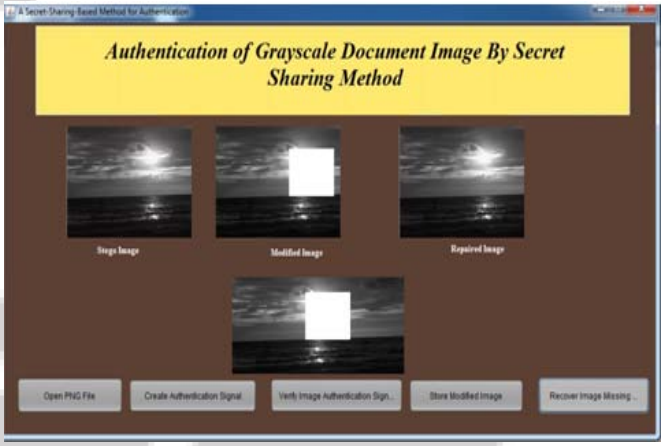

Figure 7: Authorization result of a image of a Art in the form of PNG, tampered image ,Repaired image

6. Conclusion

A new blind image authentication technique with an information repair capability for binary-like grayscale document images based on secret sharing technique has been proposed. The generated authentication signal and also the content of a block are converted into partial shares by using shamir technique, that are then dispersed in a well designed way to make a stego image with in the PNG format. The unwanted opaque result visible within the stego-imag Returning from embedding the partial shares has been excluded by mapping the share values into a low range of

alpha channel values close to their most transparency value of 255. In the procedure of image block authentication, block within the stego-image has been thought to be having been tampered with if the computed authentication signal doesn't match that extracted from corresponding partial shares within the alpha channel plane. Experimental results have been shown to prove the efficiency of the proposed method.

7. Future Scope

Future studies could also be directed to decisions of alternative block sizes and connected parameters (prime range, coefficients for secret sharing, range of authentication signal bits, etc.) to boost data repair effects. Applications of the projected technique to the authentication and also the repairing of attacked color pictures may be conjointly tried.

References

[1] C. S. Lu and H. Y. M. Liao, "Multipurpose watermarking for image authentication and protection," *IEEE Trans. Image Process.*, vol. 10, no. 10, pp. 1579–1592, Oct. 2001.
[2] Z. M. Lu, D. G. Xu, and S. H. Sun, "Multipurpose image watermarking algorithm based on multistage vector quantization," *IEEE Trans. Image Process.*, vol. 14, no. 6, pp. 822–831, Jun. 2005.
[3] Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.
[4] M. Wu and B. Liu, "Data hiding in binary images for authentication and annotation," *IEEE Trans. Multimedia*, vol. 6, no. 4, pp. 528–538, Aug. 2004.
[5] H. Yang and A. C. Kot, "Pattern-based data hiding for binary images authentication by connectivity-preserving," *IEEE Trans. Multimedia*, vol. 9, no. 3, pp. 475–486, Apr. 2007.
[6] H. Yang and A. C. Kot, "Binary image authentication with tampering localization by embedding cryptographic signature and block identifier," *IEEE Signal Process. Lett.*, vol. 13, no. 12, pp. 741–744, Dec. 2006.
[7] Y. Lee, J. Hur, H. Kim, Y. Park, and H. Yoon, "A new binary image authentication scheme with small distortion and low false negative rates," *IEICE Trans. Commun.*, vol. E90-B, no. 11, pp. 3259–3262, Nov. 2007.
[8] C. H. Tzeng and W. H. Tsai, "A new approach to authentication of binary images for multimedia communication with distortion reduction and security enhancement," *IEEE Commun. Lett.*, vol. 7, no. 9, pp. 443–445, Sep. 2003.
[9] Y. Lee, H. Kim, and Y. Park, "A new data hiding scheme for binary image authentication with small image distortion," *Inf. Sci.*, vol. 179, no. 22, pp. 3866–3884, Nov. 2009.
[10] C. C. Lin and W. H. Tsai, "Secret image sharing with steganography and authentication," *J. Syst. Softw.*, vol. 73, no.3, pp. 405–414, Nov./Dec. 2004.
[11] W. H. Tsai, "Moment-preserving thresholding: A new approach,"*Comput. Vis. Graph. Image Process.*, vol. 29, no. 3, pp. 377–393, Mar.1985.

Author Profile

Vandana Navale received the B.E. degree in Computer Engineering from Terna college of Engineering 2002.