Image Authentication Scheme with Self Repair Capability for Grayscale Images

Anushri Shinde, Prital Salunkhe, Prajakta Mane, Arjun Nichal

Abstract— Image authentication is one of the methods which can detect the any tampering data. The original grayscale document image is converted into stego image by adding the alpha channel plane. The stego image is in the Portable Network Graphics (PNG) format. This stego image is transmitted over the network. The authentication process is applied on the stego image on the receiver side. In the authentication process the data extracted from this stego image is compared with the data computed from the binary version of the stego image. If the data is matched the image is considered to be authentic. Else the tampered blocks are marked and the image is self-repaired. In our methods we can resist the Cropping, Noise addition, Enhancement, Complement, Translation and Blurring attacks. Furthermore, those attacks can be completed by using image enhancement techniques. We proposed security enhanced authentication scheme. Our proposed scheme is capable of repairing the content of the given stego-image if attacked by the methods mentioned above

.

Index Terms — Data hiding, watermarking, authentication, tampering, data repair, grayscale image

1 Introduction

Authentication is the process or action of verifying the identity of user or process. Image authentication technique have a recently gained great attention due to its importance for a large number of multimedia application. With the fast development of information technology, the digital image has become an important way of preserving and communicating important information; however, the wide application of image editing software makes it easy to modify the contents of digital images without visual perception. Therefore, how to ensure the credibility of image content has become a challenge. Image authentication technology is an efficient method of overcoming this challenge. Among all kinds of the images, the document images need more protection. The reason is that a document image consists of text, tables, line art, etc., and a little change in it can cause a large amount of meaning to be changed. Therefore, authentication of a document image is more meaningful for practical application. Digital image can be used to preserve important information such as important certificates, signed documents, scanned checks, circuit diagrams, art drawings, design drafts, last will and testaments, and so on. Image transmission is a major activity in today's communication. Digital images are now widely distributed via the internet and various public channels. With the advance of digital technologies; it is now easy to modify digital images without causing noticeable changes, resulting possibly in tampering of transmitted images. It is desirable to design effective method for image authentication, aiming to check the fidelity and integrity of received images. Authentication without any perceptible distortion as well as ability to repair tampered image parts. In this method the original image is binary like grayscale image. This image is transformed into a stego image which is in the PNG format. PNG is an extension to the stego image. This image is then sent to the receiver. The stego image is then verified by the proposed authentication method. If the image has not undergone any attack it is verified. Otherwise, the tampered blocks are identified and the image is repaired. In our method we can tempered the image by using various image enhancement techniques such as Cropping, noise addition, Enhancement, Complement, Translation and Blurring. These attack operations are very common for images but cause a greater amount of meaning to be changed for comparing with the original document image. In our scheme we can detect these attacks and repair the original document image.

2. METHODOLOGY

2.1 Block Diagram

The proposed method which aims to authenticate the gray scale image and after detection of tampering in original image, the method is also able to repair the tampered areas of the image. Conventionally, the concept of data hiding for image authentication is irrelevant issue in the domain of information security.

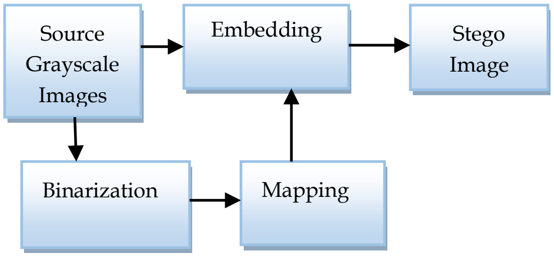


Figure .1.Creation of Stego Image from Grayscale Image

For the authentication process we used the stegnography technique. Steganography is the process of hiding a secret message within a larger one in such a way that someone can not know the presence or contents of the hidden message. The purpose of Steganography is to maintain secret communication between two parties. The basic structure of Steganography is made up of three components: the "carrier", the message, and the key. The carrier can be a painting, a digital image, an mp3, even a TCP/IP packet among other things. It is the object that will 'carry' the hidden message. A key is used to decode the hidden message. This can be anything from a password, a pattern, a black-light.

In our scheme the source image is gray scale image which is also called as cover image. For the authentication of the image we embed the watermark image or authentic layer into the cover image by using the steganography technique. Then after that process we get stego image which is very similar to grayscale image, but it is authentic image, as the data for authentication and Self repairing is embedded into it. Stego-image with the Portable Network Graphics format with an additional alpha channel for network transmission or archiving in the databases. Now tampering is done as the title of the image is altered with name Test image. Then after applying the Enhancement techniques such as Cropping, noise addition, Enhancement, Complement, Translation and Blurring to it ,it will be successfully tempered the image.This tempered image is recovered.The results are taken from the Matlab Output Window for better understanding. In that a method of document image authentication with an additional self-repair capability to fix data of tampered image.

A major topic of discussion in the self-repairing of tampered data at attacked image parts is that, after the original cover image data is embedded into the image itself to use in data repairing later on, the cover image is itself destroyed in the first place and the original data is now no longer available for the purpose of data repairing, which results in a contradiction. A solution to this difficulty is to embed the original image data somewhere else without varying the cover image itself. The technique proposed in this paper to implement this solution is to utilize the extra alpha channel in a PNG image so as to embed the original image data. However, the use of alpha channel of the PNG image is done to create a desired degree of transparency for the image. Moreover, data embedding into the alpha channel will create random transparency in the resulting PNG image, which will produce an unwanted opaque effect. In this paper, is to map the resulting alpha channel values into a small range near their extreme value of 255, resulting in an almost undetectable transparency effect on the plane of alpha channel. There is another difficulty faced during the self-repairing of the original image data, that the data to be embedded in the carrier are often large in size. This is not a problem for our case where with the alpha channel as the carrier, the cover image that is dealt with is basically binary-like, and hence, we may just embed into the carrier a binary version of the cover image, which includes much less data.

In this proposed method the input cover image is transformed into PNG format, with scrambled form in a supplementary alpha channel for transmission on networks or archiving in database. By using proposed method the stego image retrieved or received may be verified for its authenticity. Integrity modification of the stego image can be detected by the method at the blocklevel and repaired at the pixel level. In case the alpha channel is totally destroyed from the stego image, the entire resulting image is regarded as in authentic.

2.2 Least significant bit [LSB] substitution mehod:

The Least Significant Bit (LSB) insertion method is a common, simple approach to embedding information in a graphical image file. In LSB insertion method the LSB of every pixel is replaced by every message bit. the change occurs only in the bit which is least significant, thus keeping the other more significant bits unaltered. Therefore, this does not affect the original image perceptibility. Hence it is a very popular technique. However, it is extremely vulnerable to attacks. Any image manipulations such as cropping, intensity changes for any enhancements such as contrast stretching, histogram equalization, addition of noise etc will destroy the embedded message. The techniques other than LSB technique are complicated although they are robust to most attacks. LSB technique can therefore be used wherever we want to store confidential information on a standalone PC or one which is shared among several users. LSB technique can be used to store personal data such as ATM PIN, Credit card details, salary statement, income tax data, passport information etc in an imperceptible way.

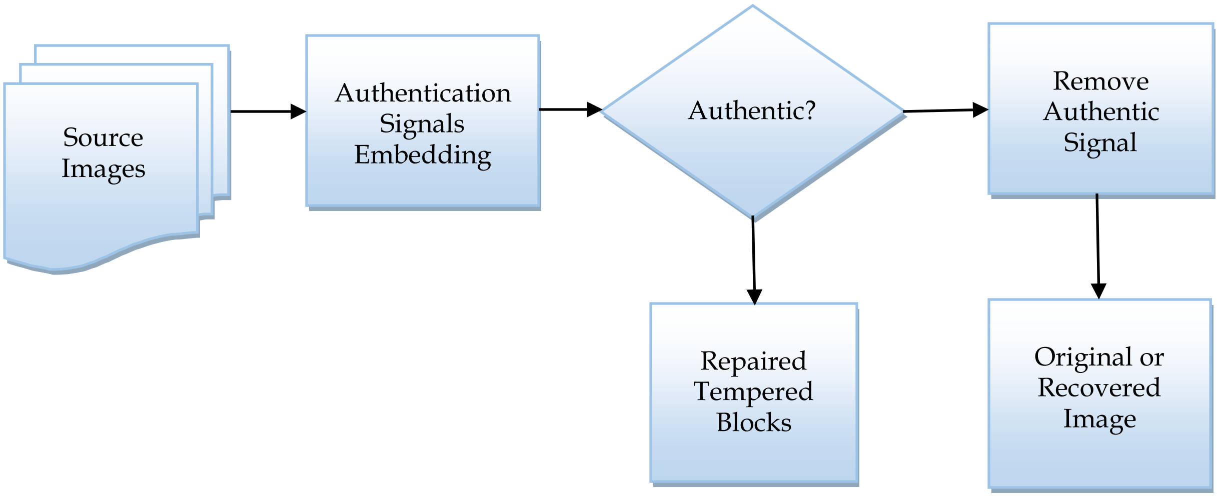


Figure 2 Framework of Proposed Document Image Authentication Method

3. Literature Summary

In [1] Image Authentication and data repaired techinique is used.It can resist attacks but in that Color image is not used. In [2] Image authentication technique is used.In that message is secretely embed into data.Grayscale via PNG fomat image is not used. In [3] Image authentication and Data Repaired technique is used.In that attacks cannot be resist. In [5] Image Quality assessment technique is proposed in that data hiding scheme with high capacity for binary images.Data is not repaired.In [6] LAHLVDSMTTM algorithm is proposed it secures message transmission technique by embedding message/image into color image. In [7] Lossless Data hiding Algorithm is proposed on Histogram modification for image authentication. In [4] Image authentication and data repaired is proposed in that attacks cannot be resist. In [8] Steganography algorithm is proposed for passport protection mechanism is supported at both stages of encryption and data hiding. In [9] Robust lossless image data hiding algorithm is proposed.It can be readily applied in the medical field, law enforcement remote sensing. Data is not repaired. In Multipurpose watermarking algorithm is proposed for image authentication and protection.

4. Results Analysis and Discussion:

a) Quality Parameters

To analyze or compare the result we check some quality parameters as follows:

PSNR
MSE

PSNR (Peak Signal to Noise Ratio)

The PSNR is most commonly used as a measure of quality of reconstruction of lossy compression codec's (e.g., for image Compression).

The signal in this case is the original data, and the noise is the error introduced by compression. When comparing compression codec's it is used as an approximation to Perception of reconstruction quality., therefore in some cases one reconstruction may appear to be closer to the original than another, even though it has a lower PSNR (a higher PSNR would normally indicate that the reconstruction is of higher quality).

MSE (Mean Square Error)

Mean Square Error (MSE) is the cumulative squared error between the compressed and the original image.A lower value for MSE means lesser error .

If MSE is low that means we get higher output if an image or good quality of image.

If MSE is high then we get low quality of image.

b)Actual Implementation of Results:

i) Generation of Authentic Image

The Authentic Image is generated after embedding the Watermark image into the Cover image.In that firstly alpha channel added into the gray scale image then PNG image is generated.

(a)

(b)

(c)

Figure.4.1 Generation of a Authentic image
(a)Cover Image (b) Watermark Image (c) Stego Image

Grayscale image+Alpha channel plane=PNG image

Input: a grayscale image gray and a watermark image/authentic layer.

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

Steps

Stage I—generation of authentication image

1. Cover image and watermark image is given.we have to embed the watermark image into the cover image for authenitication of cover/original image.
2. On the cover image we apply the Least Significant Bit (LSB) substitution technique which is also called steganography technique.
3. In that the cover image is divided into eight planes by using bit plane slicing technique.
4. In the first plane we have to embed the waternark image/authetic layer.
5. After embedding the data Stego image is obtained.

ii) Tempring the data from image

Input: A stego image

Output: Tempered Image

Steps

Stage II -Generation of Temperd image

There are following techniques are used to generate tempering data from images:

1.Cropping: This focuses the viewer's attention on a specific portion of the image and discards areas of the image that contain less useful information. Using imge cropping in conjunction with image magnification allows you to zoom in on a specific portion of the image.

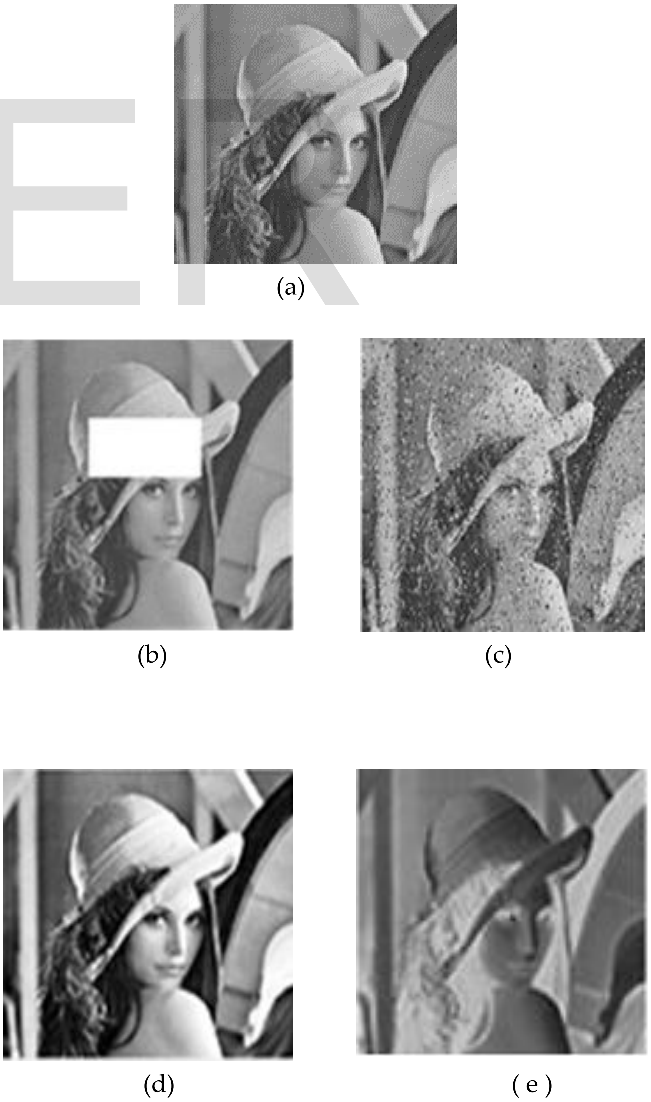
2. Noise Addition: Image noise is random variation of brightness or color information in images, and is usually an aspect of electronic noise. It can be produced by the sensor and circuitry of a scanner or digital camera.

3. Enhancement: Image enhancement is the process of adjusting digital images so that the results are more suitable for display or further image analysis. For example, you can remove noise, sharpen, or brighten an image, making it easier to identify key features.

4. Complement: In the complement of a binary image, zeros become ones and ones become zeros. Black and white are reversed. In the complement of a grayscale or color image, each pixel value is subtracted from the maximum pixel value supported by the class (or 1.0 for double-precision images).

5. Translation: The treatment of elements near image edges varies with implementation. In a translation, you shift an image in coordinate space by adding a specified value to the x- and y-coordinates.

6. Blurring: In blurring, we simple blur an image. An image looks more sharp or more detailed if we are able to perceive all the objects and their shapes correctly in it. This shape of an object is due to its edges. So in blurring, we simple reduce the edge content and makes the transition form one color to the other very smooth.



(a)

(b)

(c)

(d)

(e)

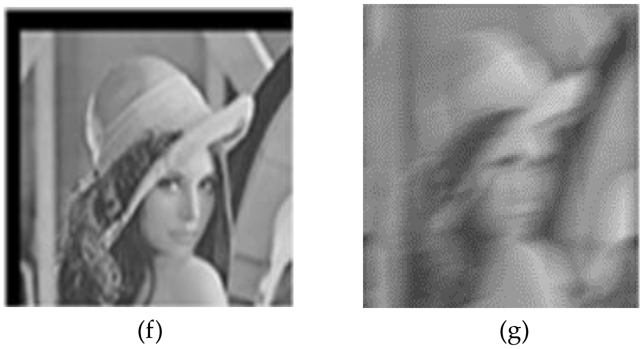

(f) (g)

Figure.4.2 Generation of Tempered Image
(a)Stego Image (b) Cropped Image (c) Noise added Image
(d) Enhancement Image (e) Complement Image
(f) Translation Image (g) Blurred Image

iii)Recovering the Data/Original image from Tempered Image

Input:Tempered Image.

*Output:*Recovered Original image.

Steps
Stage III –Recover the Original image.

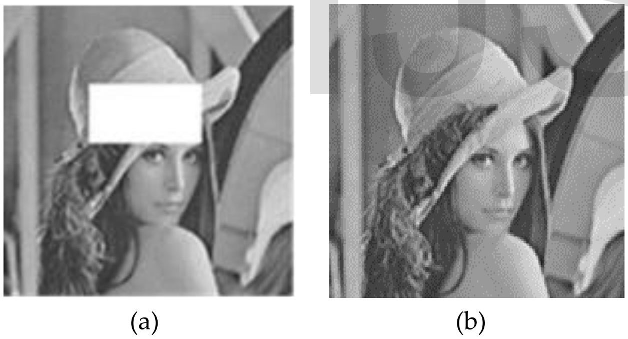
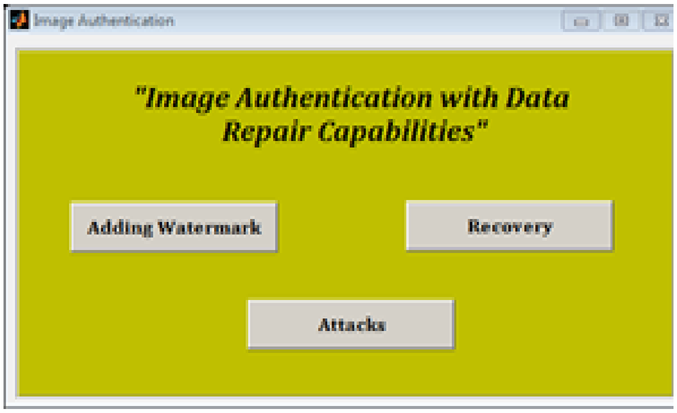

(a) (b)

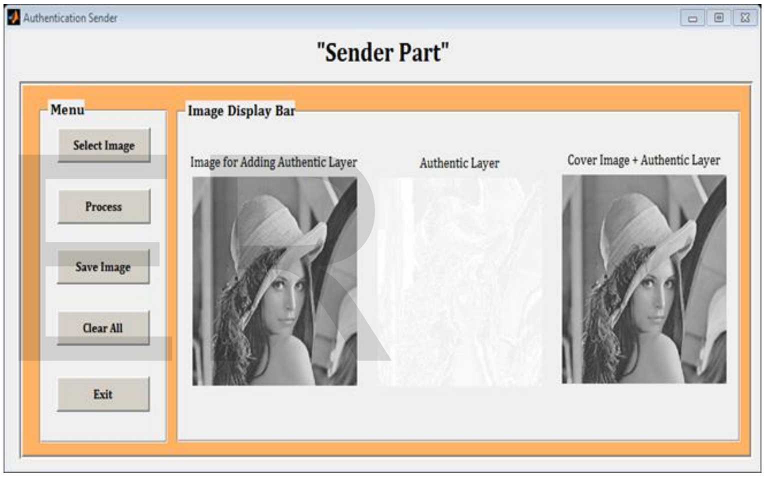
Figure.4.3 Generation of Recovered Image
Fig.5.(a)Tempered Image (b) Recovered Image

c)GUI Implementation

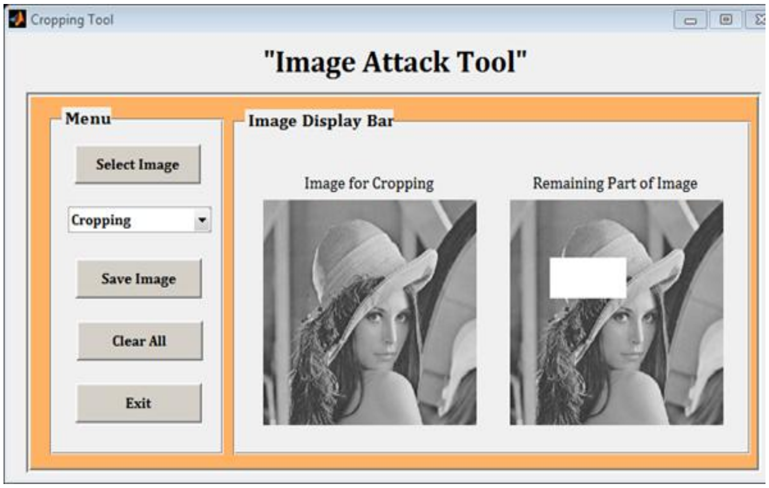
i)Main GUI of Image Authentication with Data Repair Capabilities.



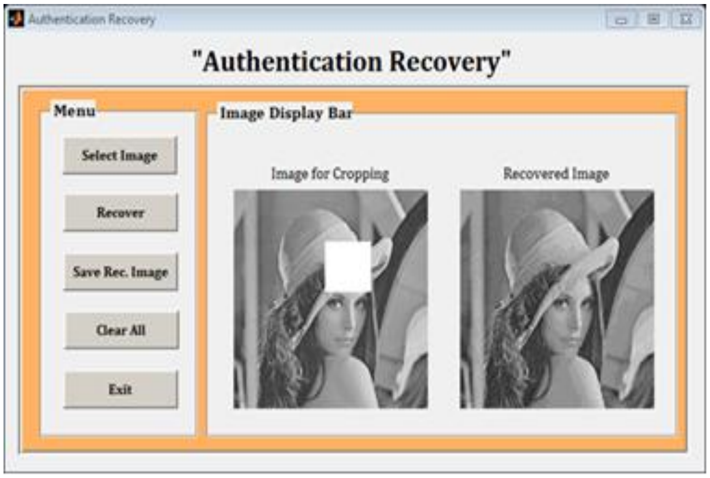
ii) GUI of Generation of Authentic Image



iii) GUI of Generation of Tempered Image



iv) GUI of Generation of Recovered Image



5.ACKNOWLEDGMENT

I owe my sincere thanks towards my Project Guide Prof. A. R. Nichal for his constant guidance during my Paper and forencouraging me to do selective paper work. With his guidance I have overcome, all the intricacies that I came across during the course of time.He has always kept up the work environment full of zeal and enthusiasm, right from beginning to end, without letting me go into the resilient mode. I am thankful to college, especially to the Electronics and Telecommunication Department for making its equipment and facilities like computing lab available to me.

6. CONCLUSION

The authentication method for grayscale document images via the use of PNG with an additional self repair capability has been proposed. This is the only method as compared to earlier methods which uses the concept of alpha channel plane. It is basically used as a carrier for authentication signals.for the authentication of image we used steganography technique.In this method we used different techniques for tempering the image and also repaired the original image.

7.REFERENCES

1)Che-Wei-Lee & Wen Hsiang Tsai proposed [2]"A Secret-Sharing-Based Method for Authentication of Gray scale Document Images via the Use of the PNG Image With a Data Repair Capability",IEEE transactions on image processing,vol.21,No.1,January 2012.pg. no. 207-218

2) Chin-Chen Chang,Wei-Liang Tai&Kuo-Nan Chen [3]proposed a" Lossless Data Hiding Based on Histogram Modification for Image Authentication", 2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing.pg no. 506-511.

3) Ankur Dauneria, Kumari Indu proposed [4]" Encryption Based Data Hiding Architecture with Text Pattern Authentication and Verification", IEEE 8th International Conference on Computer and Information Technology Workshops, pg.no. 236-241.

4) Nabin Ghoshall, J. K. Mandal,etl. Proposed [5]" Image Authentication by Hiding Large Volume of Data and Secure Message Transmission Technique using Mask (IAHLVDSMTTM). 2009 IEEE International Advance Computing Conference (IACC 2009),pg.no.1103-11

5) Meng Guo& Hangbin Zhang proposed [6] "High Capacity Data Hiding for Binary Image Authentication", 2010 International Conference on Pattern Recognition. IEEE computer society, pg. no.1441-1444.

6) Patel Roshani, Prof Aslam Durvesh, etl proposed [7] "Lossless Method for Data Hiding In Encrypted Image",2015, IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems
.

7) K.V.Arya & Akanksha Bandil proposed[8] "An Improved Image Authentication Technique using Random-Sequence based Secret-Sharing Scheme",Arya 2014.

8) Zhicheng Ni, Yun Q. Shi proposed [9]"Robust Lossless Image Data Hiding Designed for Semi-Fragile Image Authentication" IEEE Transactions on circuits and systems for video technology,vol.18,No.4,April 2008,pg no.497-509
.

9) Feng Wang & Won-Li-Lyu,Jeng [1]Shyang-Pan proposed a"Robust image authentication scheme with self-repair capability for gray scale source document images via PNG format",IET image process,2016 ISS.12,pp.971-978

8.BIOGRAPHY

Anushri Shinde
Pursuing her BE in Electronics and Telecommunication from Adarsh Institute Of Technolology and Reaserch Centre Vita. Her area of interest is Image Processing And Embedded System.

Prital Salunkhe
Pursuing her BE in Electronics and Telecommunication from Adarsh institute Of Technology and Reasearch centre,Vita. Her area of interest is Image Processing And Embedded System.

Prajakta Mane
Pursuing her BE in Electronics and Telecommunication from Adarsh Institute Of Technology and Reaseach Centre,Vita. Her area of interest is Image Processing And Embedded System.

Arjun Nichal
Received his M.tech degree from Walchand College of Engineering,Sangli in 2012. Pursuing Ph.D from Shivaji University Kolhapur.Working as an Assistant Professor In Adarsh Institue Of Technology and Research Centre,Vita.His area of interest is Image Processing, Embedded System.Published one E-book and 19 International Journal papers.He has one blog on Fundamentals of image processing,Matlab Basics and embedded system. Blog:www.image1pcmatlab.blogspot.in