Passport Authentication Using PNG Image with Data Repair Capability

Aswathi Muralidharan, Maria Johnson, Roshna Raj, Deepika M P

Abstract— **The system Passport Authentication Using PNG Image with Data Repair Capability introduces a passport authentication method for preventing the criminals and terrorists to travel between countries with fake or forged documentation. The more effort those countries, universities and other organizations put into verifying the identity of foreign nationals, the better the chance of keeping criminals and terrorists from entering a country and causing problems. The main aim of the proposed system is to design innovative system which deals with passport authorization management. The motto of the project is *to develop a new and secure passport system and* to simplify the job of the security people. In short, have a flawless passport verification system. In the proposed system, as first phase the stego image formation and as second phase, the verification stage, in this the authentication and self repairing are carried out. If part of a document image is verified to have been illicitly altered, the destroyed content can be repaired in the second phase. Such image content authentication and self-repair capabilities are useful for this security protection. In short the system proposes an authentication method that deals with *binary like color document* images instead of binary, grayscale ones and simultaneously solves the problem of image tampering detect `ion and visual quality keeping.**

Index Terms— **alpha channel, PNG image, secret sharing.**

I. INTRODUCTION

Security is a growing issue in international travel for both travelers and governments. It is an important issue with the potential for criminals and terrorists to travel between countries with fake or forged documentation.

The existing passport authentication system is by using watermarking technique. The aim of the system is to provide a firm association between the passport holder's photo and the holder's details by embedding hidden information in the passport photograph. During the issue of passport, a watermark can be created based on the details of the holder full name and passport number and this invisible watermark is embedded inside the passport photo such that it satisfies all the requirements of the watermarking technique. This process is carried out during the issue of the passport document at the passport office. With the help of this technique, during the passport verification process at the checkpoint, computer can be used in scanning the passport photo to check whether the passport photo has been replaced by comparing the invisible watermark hidden in the passport photo with the holder's details including the full name and passport number.

The existing procedure consists of three phases. The first phase deals with acquiring the required parameters for creating the watermarking. The second phase converts the holder's details into a watermark that can be embedded into the digital image. The third phase hides the watermark obtained inside the passport photo such that it meets the requirements of the watermarking.*Table.1* shows the comparison table of previous methods in document authentication. [4][5][6][7][8][9]

Computerized technologies in authentication systems are emerging to help security professionals in handling the security of passport data explosion and increasingly complex security information. Current and future authentication systems require large amounts of information to be collected, stored, processed and managed. The security of these information systems and data is important. In order to deal with the security in passport authentication field in this paper we present a secret sharing technique with a data repair capability for color document images via the use of the Portable Network Graphics (PNG) image. Actually it is an enhancement to the already existing passport system. An authentication signal is generated for each block of the color document image. It ensures the integrity and the authenticity of a digital image.

II. PROPOSED SYSTEM

In our system, a method for authentication of document images/passport with an additional self-repair capability for fixing tampered image data is proposed. Data hiding which destroys the cover image and the original image along with it prevents self-repairing capability. A solution to this problem is to embed the original image data somewhere else without altering the cover image itself. An extra alpha channel in a PNG image is utilized to embed the original data image. The input cover image/photograph is assumed to be/or converted to a binary-like color image with three planes. After the proposed method is applied, the cover image is transformed into a stego-image in the PNG format with an additional alpha channel for transmission on networks or archiving in databases. The stego-image, when received or retrieved, may be verified by the proposed method for its authenticity.

Manuscript received May, 2014.
Aswathi Muralidharan *,IT Department ,ASIET, Kalady, Kerala ,India*
Maria Johnson, *IT Department ,ASIET, Kalady, Kerala ,India*
Roshna Raj, *IT Department ,ASIET, Kalady, Kerala ,India*
Deepika M P, *IT Department ,ASIET, Kalady, Kerala ,India*

ISSN: 2278 – 1323

Table 1: Comparison of previous authentication methods

	Advantages	Disadvantages
M. Wu & B. Liu	Manual Scoring method is automated to score pixels dynamically. Can embed large amount of data	Flippablity score lookup table may exceed the available memory size for the large neighborhoods.
H.Yang & A.C Kot	Locating embeddable pixels in a block for different block scheme are addressed.	Difficult to locate tampering occurred at each block.
Hae Yong Kim & Amir Afif	Binary/Halftone watermarking is possible.	Smaller the host image the more visually noticeable will be the watermark. Printed images cannot be authenticated.
C.H.Tzeng & W.H Tsai	Image distortion is reduced	There is a trade of between distortion reduction and security enhancement.
Y.Lee,H.Kim & Y.Park	small distortion	Limited amount of embeddable data.

Integrity modifications of the stego-image can be detected by the method at the block level and repaired at the pixel level. In case that the alpha channel is totally removed from the stego-image, the entire resulting image is regarded as inauthentic, meaning that the fidelity check of the image fails.

An authentication signal is generated for each block of a passport document image, which, together with the binarized block content, is transformed into several shares using the Shamir secret sharing scheme. The involved parameters are carefully chosen so that as many shares as possible are generated and embedded into an alpha channel plane. The alpha channel plane is then combined with the original passport image to form a PNG image. In this system, we propose an authentication method that deals with color document images converted into binary-like images instead of pure binary ones and simultaneously solves the problems of image tampering detection and visual quality keeping. The two main phases of the system are one the stego image formation and second, in the verification stage, the authentication and self repairing. *Fig: 2 and 3* shows the different operations in these two phases.

In the proposed method, a PNG image is created from a binary-like color document image with an alpha channel plane. Data for authentication and repairing are then computed from and taken as input to the Shamir secret sharing scheme to generate secret shares. The share values are subsequently 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.Fig:1 shows the overall structure of the proposed passport authentication system. Fig.1 (a) shows the authorization part and Fig.1 (b) shows the verification part.

Advantages of proposed system:

- The authentication is not based on only passport number or emblems or photos. The authentication is provided to the entire page of the passport.
- It provides data repair capability i.e., after applying the proposed method if any distortions are occurred to the image, it would be altered.
- Having higher possibility to survive image content attacks.
- Enhancing data security by secret sharing.
- Making use of a new type of image channel for data hiding

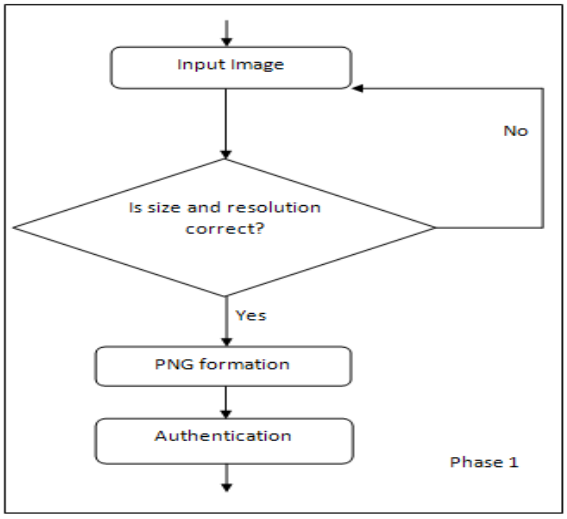

Fig.1 (a).

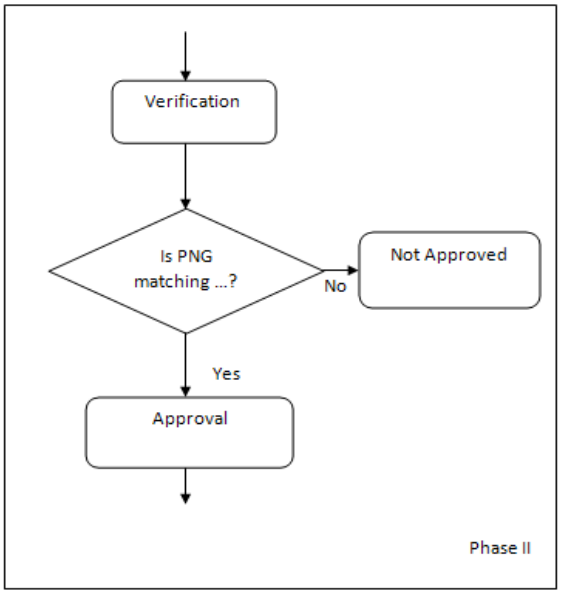

Fig.1 (b).

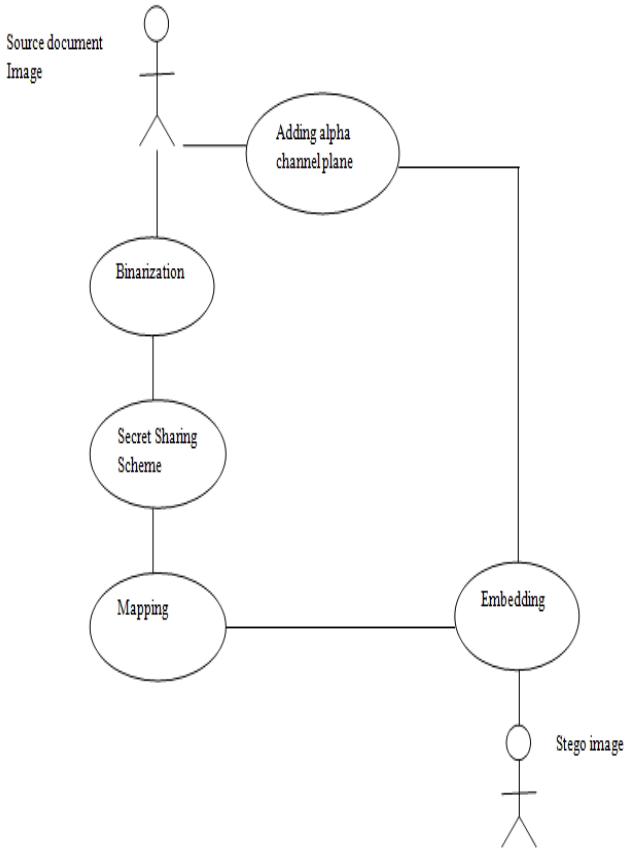

Fig: 2 Stego image formations.

III. CONCLUSION

Passport is the most important document while travelling from one country to another. It is the proof of citizenship of the country. Hence, it needs to keep secure from unauthorized use. Authentication and security of passport and checking integrity of a person on the airport is a challenging task. In order to face this challenge of security and privacy, we are proposing a secret sharing scheme based authentication method for the passport authentication via the use of PNG image with a data repair capability. The system Passport Authentication Using PNG Image with Data Repair Capability introduces a passport authentication method for preventing the criminals and terrorists to travel between countries with fake or forged documentation. In this system, a method for authentication of color passport document images with an additional self-repair capability for fixing tampered image data is proposed.

IV. FUTURE WORK

We have implemented the proposed system as a standalone system. It can be implemented as a website in future. Thus PAS can be accessed from anywhere in the world for both the passport issuing authorities and for the verifying authorities.

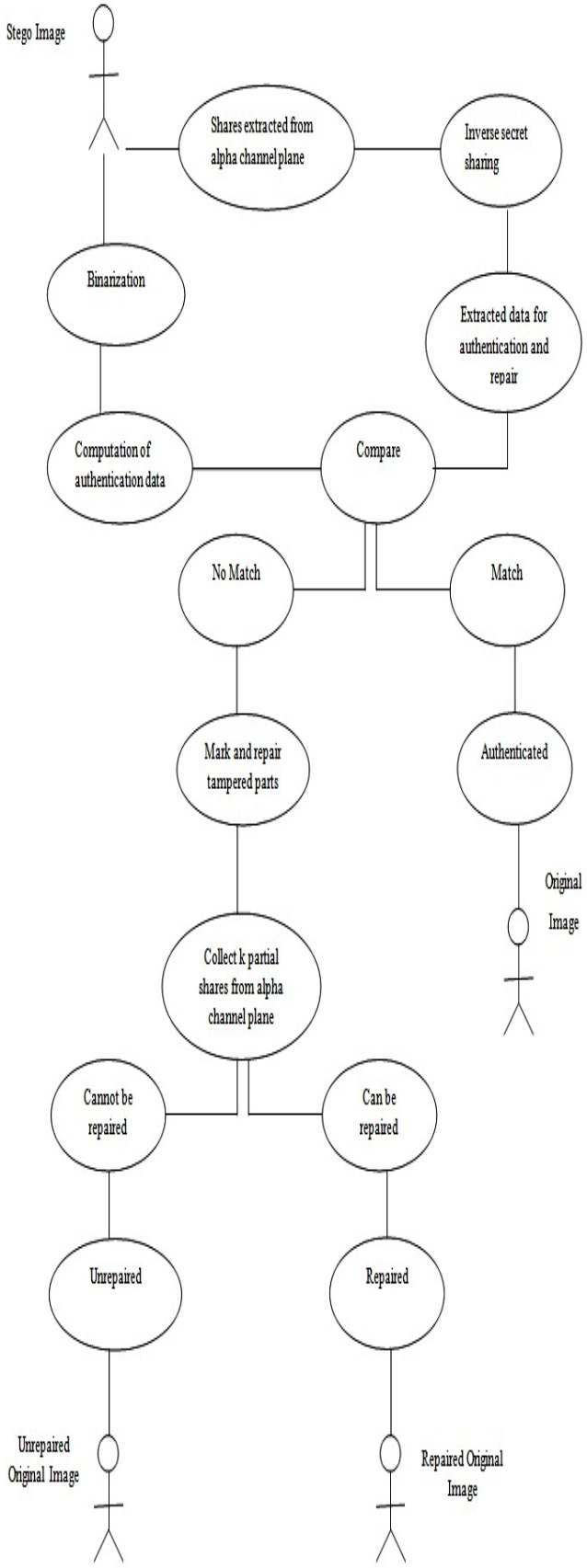

Fig: 3 Authentication and repairing.

ISSN: 2278 – 1323

APPENDIX

Fig .5 shows the authentication window of the system
Fig.6 shows the verification window of the system.

Registration:

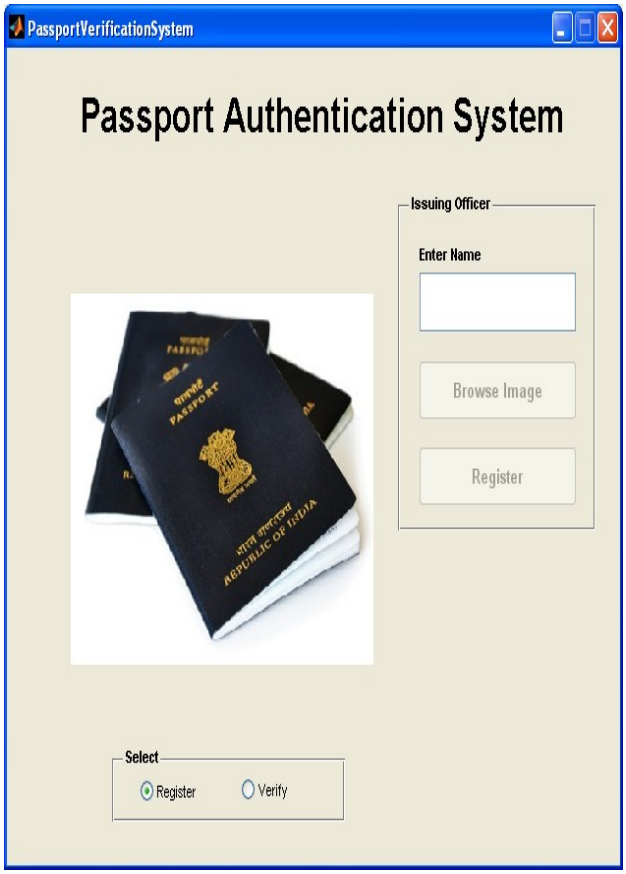

Fig.5(a)

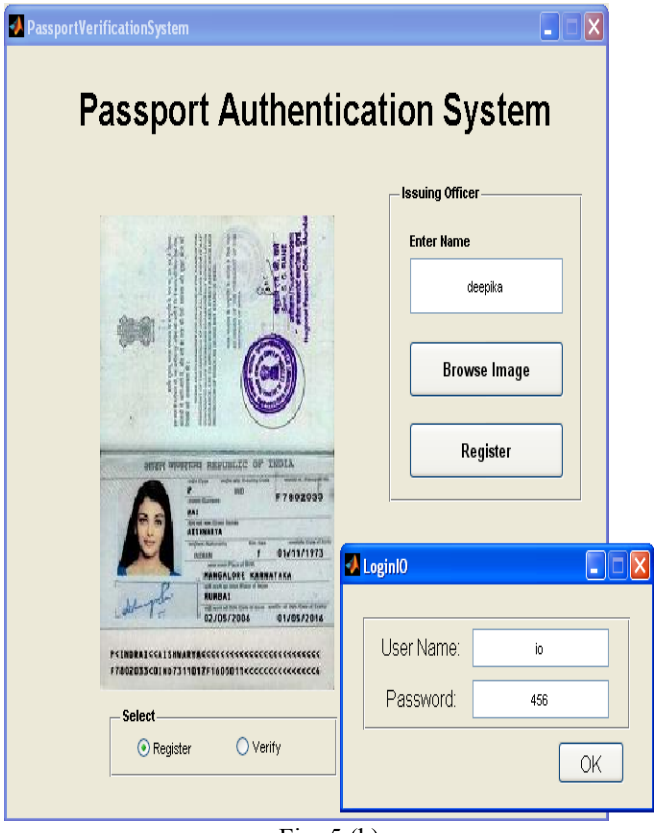

Fig .5 (b)

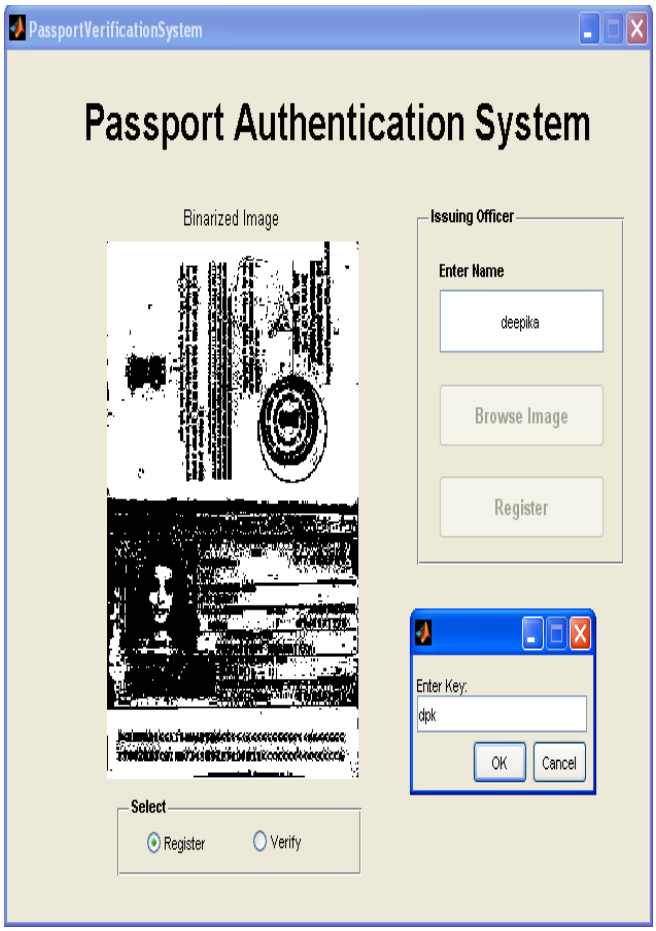

Fig 5.(c)

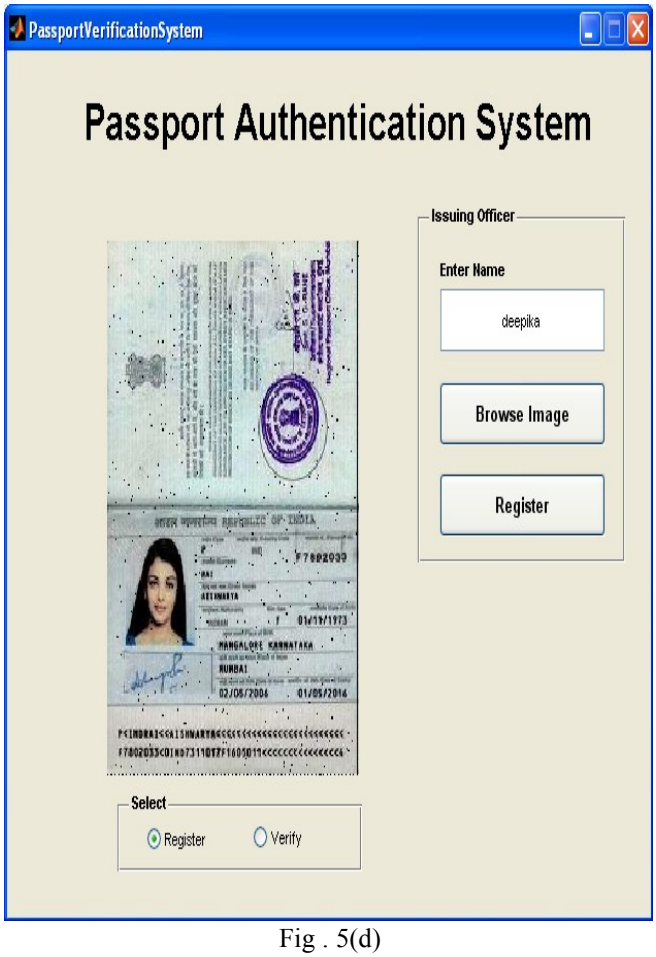

Fig . 5(d)

Verification:

Fig. 6

Registration stage:

1. Issuing officer registering the passport holder with his/her name and a key unique of the holder that is provided.
2. For doing that Issuing officer has to authenticate himself first.
3. Stego image is formed using the given data of the passport holder. (say, *PASSPORT,* based on our system)

Verification stage*:*

1. Using the same key and the details, the stego image is verified by the verifier.
2. The passport is verified and authenticated, even if some part of the passport is tampered.

ACKNOWLEDGMENT

To the light, our god, who guided us through the way. To our institution Adi Shankara institute of Engineering and Technology, Management and our department head, for their timely support. To the project coordinators, for their great efforts of supervising and leading us, to accomplish this fine work. Extreme gratitude is conveyed to all the staff members of our department for extending their helping hands to make this project a success. To our friends and families, they were a great source of support and encouragement; we thank them all and wish them all the best in their lives. To our mothers and fathers, for their warm, kinds, encourages, and love. To every person gave us something to light our pathway, we thank them for believing in us.

REFERENCES

[1]M.Naor, A. Shamir, Visual cryptography, in: *Proceedings of the Advances in Cryptology, Eurocrypt '94, in:LNCS*, vol.950, 1995,pp.1–12.
[2].A. Shamir, _How to share a secret,_ Communications of the *ACM*, vol. 22, no. 11, pp.612_613, 1979.
[3].P.S.Revenkar, Anisa Anjum, W .Z.Gandhare,_ Survey of Visual Cryptography Schemes _*International Journal of Security and Its Applications* Vol. 4, No. 2, April, 2010
[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, _Binary image authentication with tampering localization by embedding cryptographic signature and block identi_er,_ *IEEE Signal Process. Lett.,* vol. 13, no. 12, pp. 741_744, Dec.2006.
[6]. 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.
[7]. H. Y. Kim and Amir A_f, _Secure authentication watermarking for halftone and binary images,_ *Int. J. Imag. Syst. Technol*., vol. 14, no. 4, pp. 147_152, 2004.
[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., Sep. 2003.
[9]. 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.
[10]. Che-Wei Lee and Wen-Hsiang Tsai, _A Secret-Sharing-Based Method for Authentication of Grayscale 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.

Ms.Aswathi Muralidharan Pursuing B.Tech in Information Technology, Adi Shankara institute of Engineering and Technology, Affiliated to M.G University, Kerala

Ms.Maria Johnson Pursuing B.Tech in Information Technology, Adi Shankara institute of Engineering and Technology, Affiliated to M.G University, Kerala

Ms. Roshna Raj Pursuing B.Tech in Information Technology, Adi Shankara institute of Engineering and Technology, Affiliated to M.G University, Kerala.

Ms.Deepika M P working at Adi Shankara institute of Engineering and Technology as Assistant Professor in Information Technology Department. Received her M.Tech degree in Software engineering from CUSAT. Her area of interest is in Visual Cryptography.

ISSN: 2278 – 1323