3-Stage Authentication System

Mrs. Dhanamma Jagli[1], Mrs. Geocy Shejy[2] , Shrimant Gauda[3], Dinesh Makhijani[4]

1,2 ASSISTANT PROFESSOR

Department of MCA, V.E.S. Institute of Technology, Mumbai, India

3,4 MCA THIRD YEAR STUDENT

V.E.S. Institute of Technology, Mumbai, India

{[1]dhanamma.jagli, [2]geocy.shejy, [3]shrimant.gauda, [4]dinesh.makhijani}@ves.ac.in

Abstract— 3-stage Authentication system is a system which identifies the user who wishes to gain access to the system .Our proposed system overcomes the shortcomings of the current authentication system like textual password, graphical password etc and providing a cheap and effective solution for authentication by using digital watermarking and other techiques to hide the password. Here we have used the digital watermarking technique based on joint DWT and DCT transform.

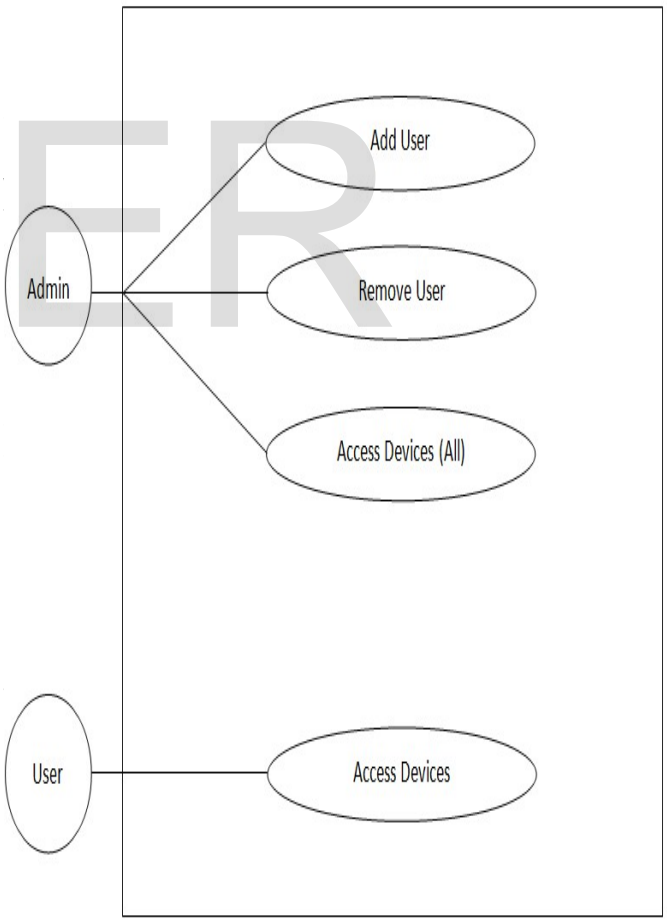
Index Terms—Digital Watermarking, DWT (Discrete Wavelet Transform), DCT (Discrete Cosine Transform)

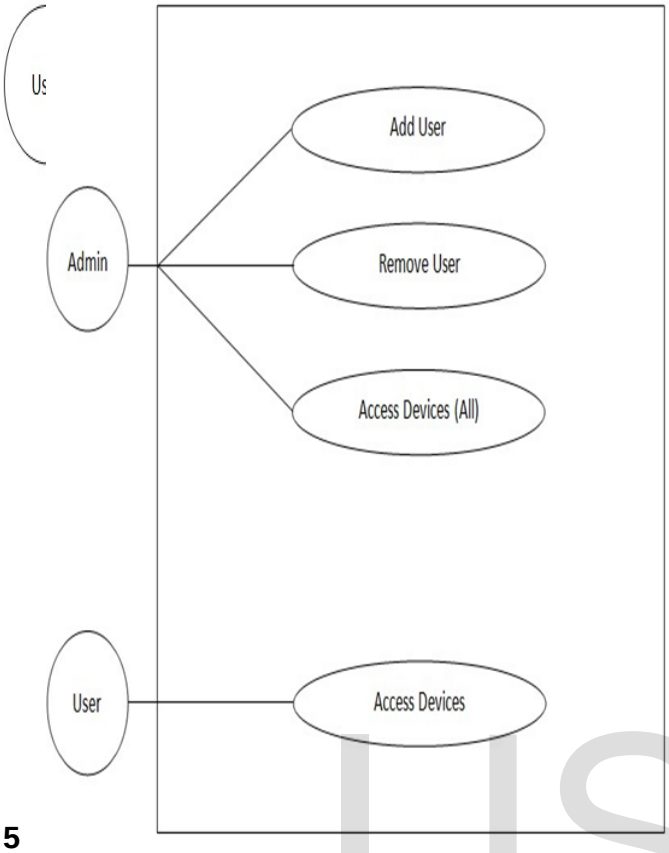
1 Introduction

There are different techniques used for authentication such as textual password, graphical password etc. However they have their own disadvantages. Random and lengthy passwords difficult to remember. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can be easily guessed or cracked. The alternative techniques are graphical passwords and biometrics. But these two techniques have their own disadvantages. Biometrics, such as finger prints, iris scan or facial recognition have been introduced but not yet widely adopted.

The major drawback of this approach is that such systems can be expensive and the identification process can be slow. There are many graphical password schemes that are proposed in the last decade. But most of them suffer from shoulder surfing which is becoming quite a big problem. There are graphical passwords schemes that have been proposed which are resistant to shoulder- surfing but they have their own drawbacks like usability issues or taking more time for user to login or having tolerance levels. In our paper we suggest a three level security system which provides higher level of security than the existing one.The new technology of digital watermarking has been advocated by many specialists as the best method to such multimedia copyright protection problem. It's expected that digital watermarking will have a wide-span of practical applications such as digital cameras, medical imaging, image databases, and video-on-demand systems, among many others[3].In order for a digital watermarking method to be effective it should be imperceptible, and robust to common image manipulations like compression, filtering, rotation, scaling cropping, collusion attack.

Among many other digital signal processing operations. Current digital image watermarking techniques can be grouped into two major classes: spatial-domain and frequency-domain watermark-





5

fig 2.1 Logical design

Embedding Block Diagram

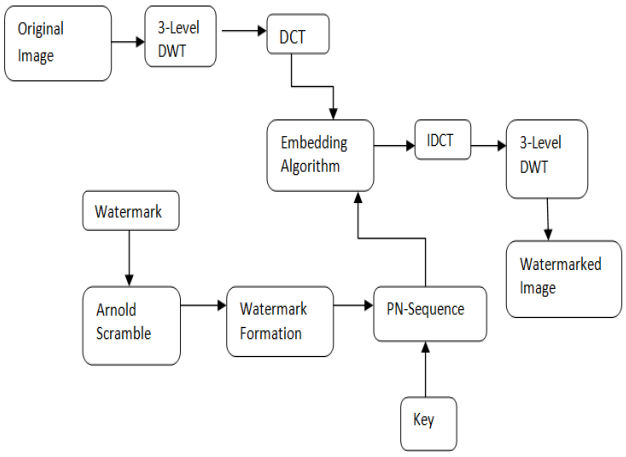
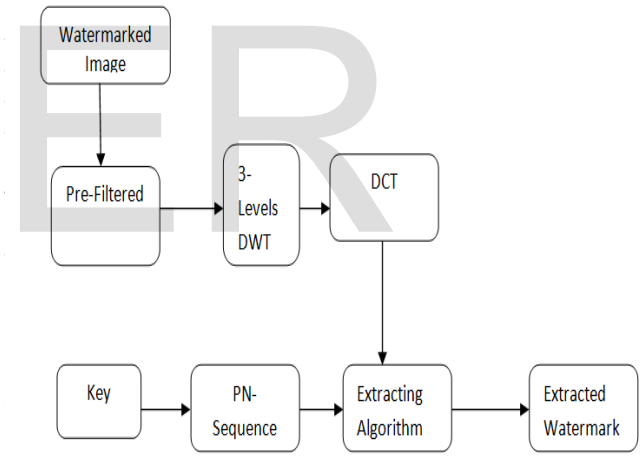


fig 2.2 Embedding Block Diagram

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should, but does not need to, contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyright infringements and for banknote authentication. Like traditional watermarks, digital watermarks are only perceptible under certain conditions, i.e. after using some algorithm, and imperceptible otherwise. If a digital watermark distorts the carrier signal in a way that it becomes perceivable, it is of no use. Traditional Watermarks may be applied to visible media (like images or video), whereas in digital watermarking, the signal may be audio, pictures, video, texts or 3D models. A signal may carry several different watermarks at the same time. Unlike metadata that is added to the carrier signal, a digital watermark does not change the size of the carrier signal.

Extraction Block Diagram

Watermark extraction assumes to have some original data, e.g. the original image, eigenvectors, etc. Watermark extraction is performed in two different ways – Independent Component Analysis (ICA) is applied to the bands of original and watermarked images and extraction by the



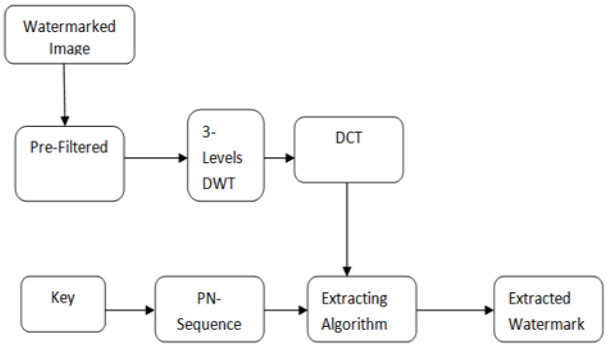


fig 2.3 Extraction Block diagram

3 UI Design

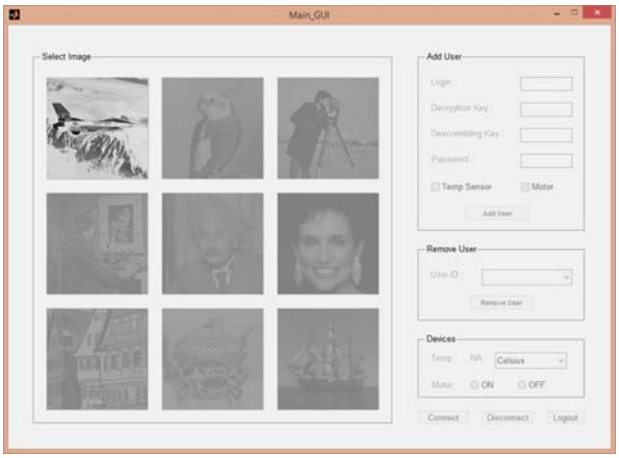


fig 3.1

The above screenshot shows a Graphic User Interface which is prepared using various tools. The fig 5.1 shows the selection of the first image which has been allocated to the admin of the system.

fig 3.2

This step shows that after correctly entering the descrambling key and the decryption key the admin has correctly obtained captcha image which needs to be entered to gain the complete access to the system.

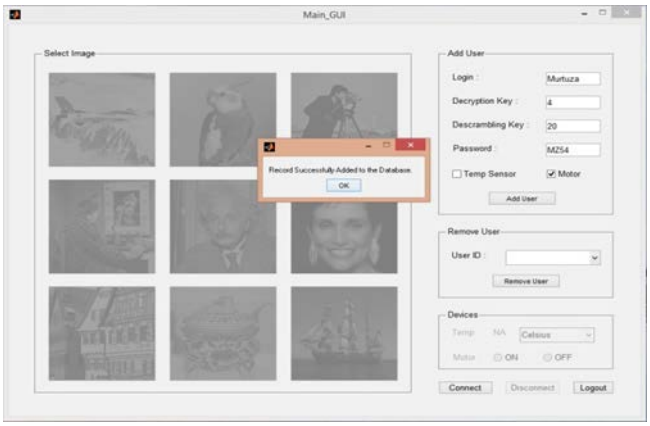


fig 3.3

This figure shows that the admin has correctly entered the password and he has finally gained access to the dialog boxes which are available on the right hand side of the image through which he can add/delete user and give them access to a particular system

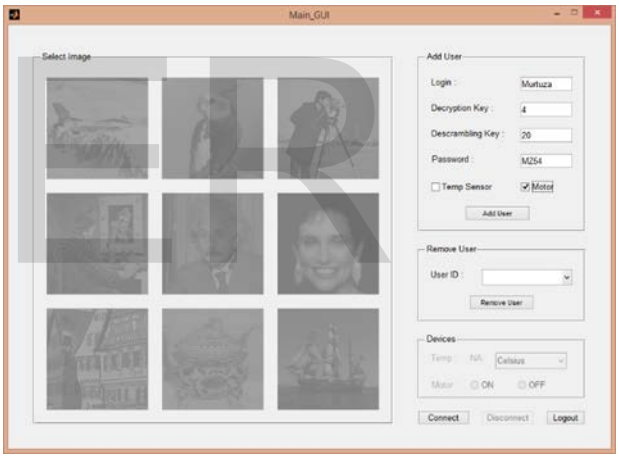


fig 3.4

The above screenshots shows the admin adding a user by assigning him the decryption key, descrambling key and password.

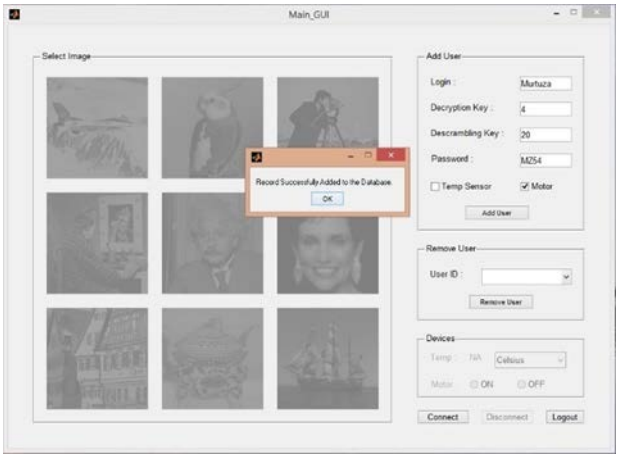


fig 3.5

This figure shows that the data has been added to the Microsoft Access which is being used as a database in our project.

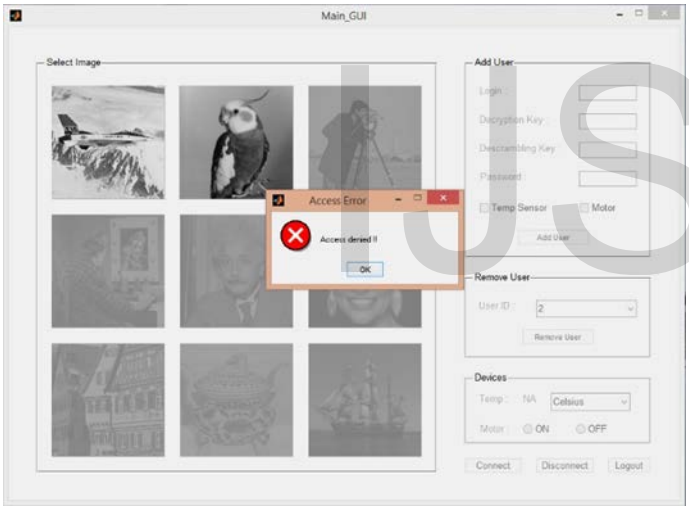


fig 3.6

This page shall appear only if the user which was created by the admin in the previous step enters a wrong key at the time of log in. If the user enters the descrambling key and decryption key wrongly then the captcha image will appear in the form of noise, however if the user enters the correct password access shall be denied as the image created will not match with the original image.

4 Workflow Architecture

i. Original image is a 512X512 image.

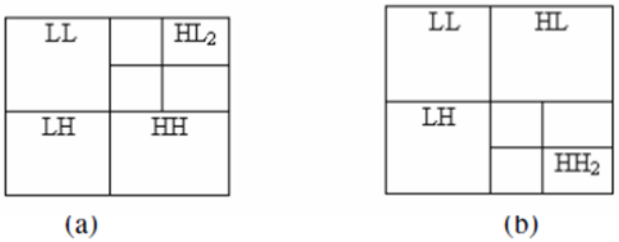


Fig.4.1 Multi-resolution DWT sub-bands of the original

ii. Watermark image (Data) is 32X32 image.
iii. The image to be embedded as watermarked image it is converted into 64X64.
iv. Then the watermark image is added bit by bit to the original image to obtain the final watermarked image.(Encryption And Decryption)
v. For high security Scramble-Descramble algorithm is used to avoid hacking.
vi. For high security Scramble-Descramble algorithm is used to avoid hacking.
vii. Which will create some random number which is actually not random but computer generated but unauthorized user will see as a noise.
viii. And finally a capcha image will be used as a third level of security. This will be predefined by the admin during selections of users.
ix. And even if the hacker knew the capcha already he/she should get access to previous 2 security levels , otherwise the image obtain will be a noise as the situation is shown in results.

5 Conclusion

In this paper, we have presented the design and implementation of a 3-Stage Authentication system. The main advantage of this authentication technique will be that even if a hacker gets access to a password he would have to go through other levels which would be a difficult task to perform. After completing all the three levels the user will get access to a remotely placed electronic device which is a sensor & simple dc motor.

REFERENCES

[1] Ali Al Haj, *Combined DWT-DCT Digital Image Watermarking*, Princess Sumaya University for Technology, PO Box 1928, Al- Jubeiha, Amaan, Jordon.

[2] Sonkar S.K. , 2012, *Graphical Password Authentication Scheme Based on Color Image Gallery*, International Journal of Engineering and Innovative Technology (IJEIT).

[3] N.S. Joshi, 2013, *Session Password using Grids and Colors for Web based Application and PDA*, International Journal of Engineering and Innovative Technology (IJEIT).

[4] V.M. Lomte, *Authentication Schemes for Session Password using Color and Grid*, IOSR-JCE, Pune.

[5] Rafael C. Gonzalez& Richard Eugene Woods,*Digital Image Processing Using MATLAB codes*, Pearson Prentice hall publications, Second Edition.

[6] http://www.digi.com/technology/rf-articles/wireless-zigbee

[7] http://www.atmel.com/

[8] http://www.keil.com/

[9] http://www.mathworks.in/products/matlab/

[10] "Digital Watermarking"
http://en.wikipedia.org/wiki/Digital_watermarking