Multilevel Biometric Based Authentication System

[#1]Rabiya Shaikh, [#2]Prof. G .A. Patil
[1]M.E., Student, Department of Computer Science & Engineering, Dr.D.Y.Patil College of Engineering & Technology, Kolhapur.
[2]Prof. Department of Computer Science & Engineering, Dr.D.Y.Patil College of Engineering & Technology, Kolhapur.

Abstract : Security-sensitive environments protect their resources against unauthorized access by enforcing access control mechanisms. Text based passwords are not secure enough for such applications. User authentication can be improved by using both Biometrics and structured images. The system developed displays an image or set of images to the user, who would then select one to identify them. The system uses such image based passwords and integrates image registration and notification interfaces. Image registration enables users to have their own image compared with image stored in database.

I. INTRODUCTION

There are two types of systems that help automatically establish the identity of a person: 1) authentication (verification) systems and 2) identification systems. In a verification system, a person desired to be identified submits an identity claim to the system, usually via a magnetic stripe card, login name, smart card, etc., and the system either rejects or accepts the submitted claim of identity (Am I who I claim I am?). In an identification system, the system establishes a subject's identity (or fails if the subject is not enrolled in the system data base) without the subject's having to claim an identity (Who am I?). Identity verification is a general task that has many real-life applications such as access control, transaction authentication (in telephone banking or remote credit card purchases for instance), voice mail, or security. Most of the biometric applications are related to security and are used extensively for military purposes and other government purposes. The goal of an automatic identity verification system is to either accept or reject the identity claim made by a given person. A key advantage of biometric authentication is that biometric data is based on physical characteristics that stay constant throughout one's lifetime and are difficult to fake or change. We have investigated how the security of user authentication can be improved by using both finger print biometrics, structured images and text-based-passwords with virtual keyboard.

Authentication is a function where a user presents some credentials to the system. If the system recognizes this set of credentials or the credentials match a given set on the system, then the user is said to be authorized otherwise the user is not authorized. Authentication is needed to let the system perform some tasks for the user. The user needs to be authorized to request services from the system. So, for a new user, he has to get registered with a system and then authenticated before he can request services. In a basic authentication process, a user presents some credentials like user ID and some more information to prove that the user is the true owner of the user ID. This process is simple and easy to implement. A complicated process involves a user ID, password and a key value generated with time and which changes constantly at fixed intervals. A user is authenticated only if all three values are right. This is better and more secure than the basic authentication process as the user has to be there physically to use the changing key. An example of this process is use of smart cards. The third authentication process uses biometrics. Biometrics can measure finger prints, facial image scan and many more. In this case, a user always has these credentials on him. User has to present physically for authentication. The most widely used authentication process uses user ID and a password.

II. LITERATURE SURVEY

Biometric based authentication system

To prevent mishandling of secured data and misuse of it by unauthorized persons particularly hackers and anti social elements, these biometric systems are used. The technology to prevent unauthorized usage of secured resources, ensuring unique identity and safety with the usage of fuzzy logic, and neural networks in implementing face recognition techniques and also an advanced technique on fingerprint recognition. Fingerprint recognition technique is used for allowing access only to the stored fingerprints, S. Santtosh, Fred Kaggwa[1] [2] say that, multiple enrollments can also improve the recognition accuracy of a fingerprint recognition system by lowering the error rates, allowing robustness by lowering the False Rejection Rates for low quality or worn-out fingerprint images and also make spoofing harder. Multiple enrolled fingerprints per individual can be collected in a onetime session (within the same period of time and day) or at multiple sessions for example after a three to five weeks time. Biometrics, the application of statistical analysis to identify individuals through their biological or physiological characteristics, is emerging as a key aspect in new security systems as stated in [3]. Takada Tetsuji [4] states that, using biometrics, it is possible to avoid pitfalls encountered with traditional security systems where users are required to keep information, such as passwords, safe. Biometric authentication systems may be very safe and secure and reliable as well as cost effective and provide additional support in security. Deploying such systems for internet may be very easy suitable.

Content based image retrieval (CBIR) :

Content-based image retrieval system retrieves an image from a database using visual information such as color, texture, or shape as given in [5]. In most systems, the user queries by presenting an example image that has the intended feature [6]. Although this approach has advantages in effective query processing, it is inferior in expressive power and the user cannot represent all intended features in his query.

Rui.Y [7] has proposed a survey of technical achievements in area of image retrieval. He has brought into light, the demand for the CBIR in real time application. He also proposed the past and current achievements in indexing and extracting the visual

feature of the images. A.W.M.Smeulders [8] has provided the steps carried out in content based image retrieval process. The features used for retrieval are also spoken here. The disadvantages like need for databases, role of similarity and problems of evaluation are also discussed. Subrahmanyam Murala [9] presented a novel image indexing and retrieval algorithm using local tetra patterns (LTrPs) for content-based image retrieval (CBIR). The standard local Ternary pattern (LTP) and local Binary pattern (LBP) encode the relationship between the referenced pixel and its surrounding neighbours by computing gray-level difference .Using this difference, the images are compared and retrieved. Color is one of the most important features that make possible the recognition of images by humans and color feature is one of the most commonly used visual features in image retrieval. Texture is defined as structure of surfaces formed by repeating a particular element or several elements in different relative spatial positions. Gabor wavelet is widely adopted to extract texture from the images for retrieval and has been shown to be very efficient [9].

The text-based-password using virtual keyboard: So far there have been several research proposals for mitigating the shoulder surfing problem of virtual keyboards. Ankit Parekh, Ajinkya Pawar, Pratik Munot, Piyush Mantri [10] have proposed an anti-screen shot virtual keyboard. In this idea, the keys on a particular row of the keyboard would be replaced by some special characters when the mouse cursor moves over it. When the user click on a particular key, all the keys would be replaced by the special character such that a screen shot at that moment will not reveal the actual key aimed by the user. In another work, Dhamija Rachna, Perrig Adrian [11] have proposed a colored keyboard implementation. The alphabets and numbers in the keyboard are given different colors. The whole keys on the keyboard are shuffled every time after the user clicks a particular key. Before clicking on the desired key, the users have to note down the position of the key. Then a button captioned 'Hide Keys' have to be pressed. That will hide the characters from the keys and empty keys will be displayed. Users have to click on the key that contained the desired key earlier. They may utilize the key color for remembering this. A spy-resistant virtual keyboard for password entry in public touch screen displays was proposed in [12]. This approach is based on creating a tile of characters underlined in red, blue and green colors and hiding the keys at the moment when user makes a key selection.

III. PROPOSED WORK

The proposed system can be classified into three distinct levels for authentication. First level will use the image as password and use the Content based image retrieval technique to detect and compare the images. Then for improving the efficiency of the system, next level would be the fingerprint biometric. Here the user will enroll its fingerprint into the system via a R305 module. Then finally, to make the authentication process successful, the user will input its text based password through a virtual keyboard. This three level authentication system will ensure the users identity and make the system secure.
Fig 1. shows the system architecture for the proposed work. It consists of the following modules.

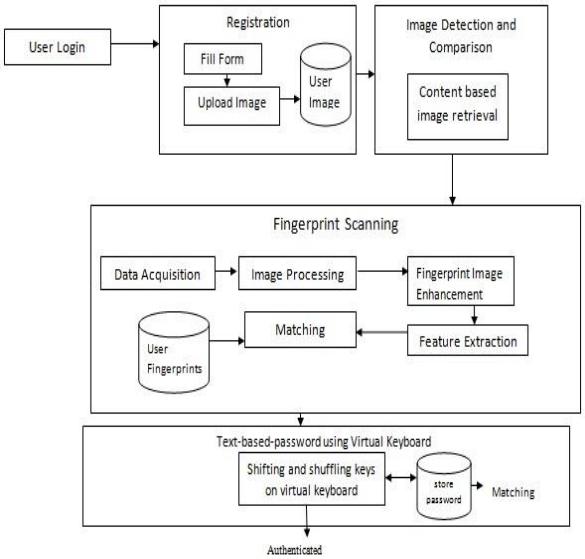

Fig. 1. System architecture

Modules:

Registration:

User friendly graphical user interface is developed for registration of the new users. A user is registered using his user name and an image. Once the user selects his own image, it is displayed on the window for the user to verify his image. He can bring his own image in a storage device. The images are read byte wise and hashed using a secure hashing function SHA-1. Images are large files. But SHA-1 algorithm produces a 20 byte output which is very secure and requires less memory. This system is implemented in Matlab Image Processing. Matlab Image Processing is platform independent, portable and most suitable for Internet applications.

Image Identification:
Content Based Image Retrieval (CBIR), by which images would be indexed by their visual content such as color, texture, shape etc. and the desired images are retrieved from a large collection, on the basis of features that can be automatically extracted from the images themselves.

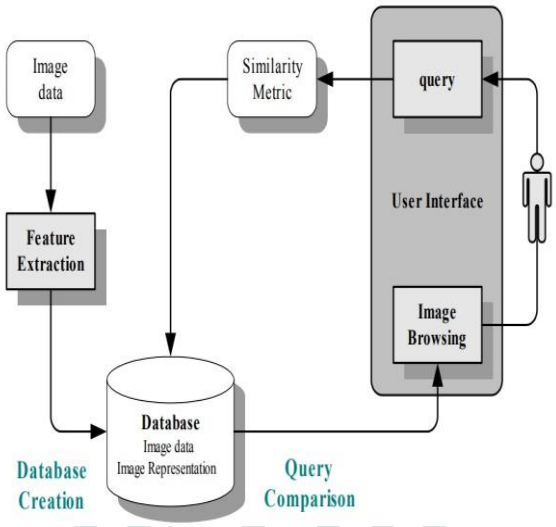

fig 2. Content Based Image Retrieval Process

Watermarking of Images:
Digital watermarking comprises various approaches for the hiding of information behind the cover image. In this process the cover image is divided into smaller regions by using various approaches and then the watermark is embedded to these different approaches by using an embedding algorithm.

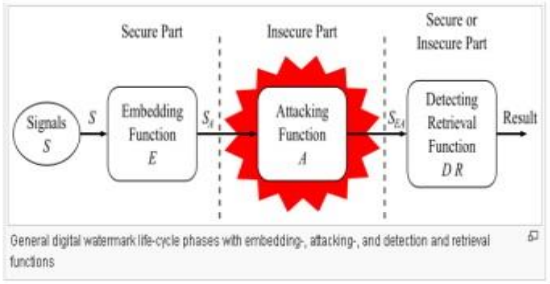

fig 3. Digital Watermarking life-cycle phases

Biometric Fingerprint Scanning:
A fingerprint recognition system can be used for both verification and identification. In verification, the system compares an input fingerprint to the "enrolled" fingerprint of a specific user to determine if they are from the same finger (1:1 match). In identification, the system compares an input fingerprint with the prints of all enrolled users in the database to determine if the person is already known under a duplicate or false identity (1:N match).

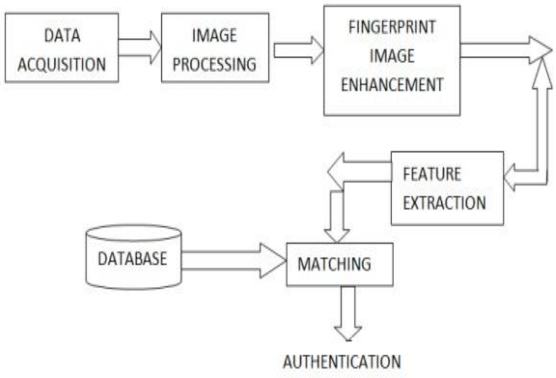

fig. 4: Fingerprint matching mechanism.

IV. EXPERIMENTS & RESULTS

Image Matching: The most common evaluation measures used in image retrieval are precision and recall. The performance of a retrieval system can be measured in terms of its precision and recall. Precision measures the ability of the system to retrieve only models that are relevant, while Recall measures the ability of the system to retrieve all models that are relevant. They are defined as,

$$\text{Precision} = \frac{\text{Number of relevant images retrieved}}{\text{Total number of images retrieved}} = \frac{A}{A+B} \qquad \text{Recall} = \frac{\text{Number of relevant images retrieved}}{\text{Total number of relevant images}} = \frac{A}{A+C}$$

Where A represents the number of relevant images that are retrieved, B represents the number of irrelevant items and C the number of relevant items those were not retrieved.

If Precision (P), and recall (R) for query image I_k (k=1,…..1000) are defined as:

$$P(I_k, N) = \frac{\text{Number of relevant images retrieved}}{\text{Total number of images retrieved (N)}}$$

$$R(I_k) = P(I_k, |A(I_k)|)$$

Where, $_k A(I_k)$ represents the numbers of relevant images in the respective category.

Watermarking: In this process big issue of digital watermarking is security and distortion occurred in different formats of the cover image. Due to distortion the predictions is easy and data at receiver end does not get properly. To overcome these issues in the previous approaches, the bit plane image encryption scheme is used for encryption of watermark and implements DWT at fourth level for hiding information using DCT on the cover image and secret image.

Image	DCT	DWT	SVD	Proposed
1	52.36	39.56	5.36	101.96
2	50.23	39.45	5.56	99.67
3	50.67	40.18	4.73	98.23
4	54.72	38.97	4.94	100.34
5	51.98	39.97	4.95	99.93

Table 1: Different values derived using Digital Watermarking

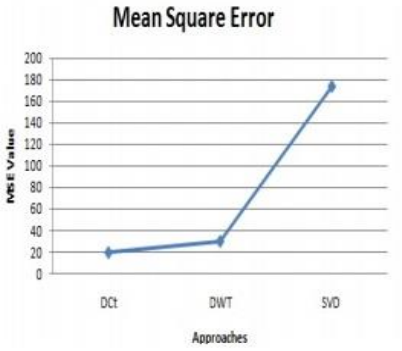

fig 5. Graph for PSNR

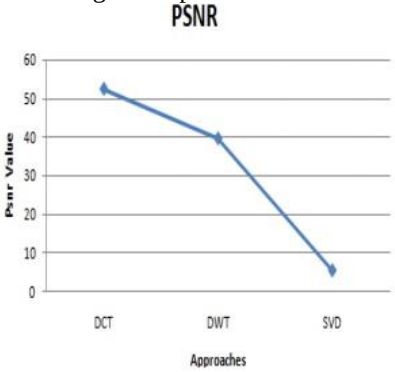

fig 6. Graph for Mean Square Error

Above fig. 5 and fig. 6 represents graphs for PSNR and Mean Square Error methods. The term peak signal-to-noise ratio (PSNR) is an expression for the ratio between the maximum possible value of a signal and the power of distorting noise that affects the quality of its representation. Mean square error (MSE) of an estimator measures the average of the squares of the "errors", that is, the difference between the estimator and what is estimated.

Biometric Fingerprint Identification: False Matching Ratio : It is the probability that the system will decide to allow access to an (FMR) imposter is given in an equation (1)

$$FMR = \frac{FalseMatches}{\text{Im } posterAttempts} \quad \text{---------- (1)}$$

The imposter attempts are implemented by matching each input image with all the template images. False match was recorded for each imposter attempt when the matching score was greater than the established threshold.

- False Non Matching Ratio (FNMR): It is the probability that the system denies access to an approved user is given in an equation (2)

$$FNMR = \frac{FalseNonMatches}{EnrolleAttempts} \quad \text{---------- (2)}$$

Enrollee attempts are implemented by matching each input image with corresponding template image, hence it is one-to-one matching. A False Non-match was recorded when the matching score between an enrollee and its template was less than the established threshold.

Matching Score: it is used to calculate the matching score between the input and template data is given in an equation (3)

$$Matchingscore = \frac{MatchingMinutiae}{Max(NT, NI)} \quad \text{------ (3)}$$

Where, NT and NI represent the total number of minutiae in the template and input matrices respectively. By this definition, the matching score takes on a value between 0 and 1. Matching score of 1 and 0 indicates that data matches perfectly and data is completely mismatched respectively.

Threshold Value	False Acceptance Rate (MSU)(ms)	False Reject Rate (MSU) (ms)	False Acceptance Rate (NIST 9)(ms)	False Reject Rate (NIST 9)(ms)
1	0.07%	7.1%	0.073%	12.4%
2	0.02%	9.4%	0.023%	14.6%
3	0.01%	12.5%	0.012%	16.9%
4	0	14.3%	0.003%	19.5%

Table 2: False Acceptance and False Reject Rates on Test sets with different Threshold Values

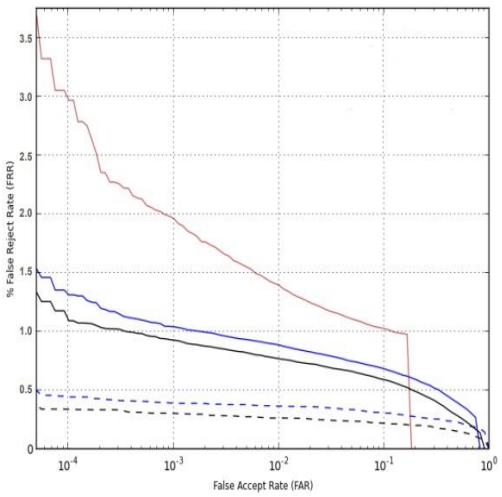

fig. 7: Graph showing FAR and FRR.

Text-Based Passwords:
A virtual keyboard environment is developed which is used for entering text based password. The keyboard will be given as: The keyboard will consist of 72 keys, out of which there are 26 alphabets (a-z), 10 numbers (0-9), 32 special characters ($, #, ? etc.) and 4 virtual additional special characters.

Operating the Virtual Keyboard for Password Entry:
The keys in the virtual keyboard are logically divided into four groups- A, B, C and D, each comprising of 18 keys. When the keyboard is shown to the user, the keys are randomized such that they are not in any fixed positions. But to reduce the difficulty in locating the keys from the keyboard, the randomization is confined at the group levels and not at the entire keyboard level. That is, the 18 keys in each group are randomized only within themselves not across other groups. Then the user has to locate and remember the current position of the target key that is the next password character to be entered. To simplify the process of remembering key positions, an index for each key numbered from 1 to 18 are associated with each key in the keyboard. Similarly the group ids are also attached with each group. So the user simply needs to note down the index value and group id pertaining to the required key, for example A4 where A is the group id the 4 is the index of the required key.
Once they are noted down, user should click on the button captioned as "Hide Keys". Then a key transfer operation carried out according to the user's selection during the sign up phase. Accordingly, all the 18 keys in the 4 groups are transferred to other groups. Here time is measured in milliseconds.

TESTED VALUE	PHYSICAL KEYBOARD	VIRTUAL KEYBOARD
Failure	0	18
Time Taken	51.8	461.3
Right character	140	140
Total character	140	158
Time per character	0.37	2.92
Accuracy	100	88.61

Table 3: Comparison between physical keyboard and Virtual Keyboard based on different factors.

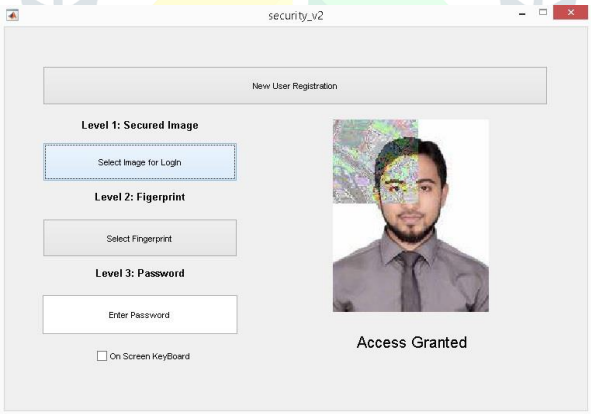

fig. 8: Watermarked image

In Fig. 18, we can see that the user provided image is now being watermarked the system. Also, below the image the STATUS is given as ACCESS GRANTED. If the user did not provide the correct watermarked image, the system will show the STATUS as ACCESS REJECTED. After the user has given correct watermarked image to the system, the user has to provide the previously enrolled fingerprint to the system.

fig. 9: All the credentials are entered.

V. CONCLUSION

In this paper we have presented different techniques used for image retrieval. Some of these approaches were single feature based and some of them were the combinations of these features (Texture, Color, Shape and region). Most of the studied techniques lack accuracy and are unable to overcome the semantic gap between the user and the CBIR system. This area of CBIR systems is a hot research area with huge potential for research and development of better image retrieval techniques. The proposed technique is less prone to errors and watermarks the image accurately. Digital watermarking is the process of hiding the secret data behind any image or signal. In first phase the cover image is reflected behind which data has to be hidden. After this discrete wavelet transformation is implemented to that image which divides the image into four different resolution regiments. This transformation is implemented up to fourth level. In the next phase secret image is reflected which has to be encrypted using bit phone encryption approach and that has to be embedded behind the cover image extracted region.

Along with image retrieval, this paper has presented the design and development of portable system which is based on fingerprint identification. The system helped to reduce many issues such as, denying the possibilities of breaking the security of the system, also the encryption technique adds more security so there will be no anonymous fingerprint which is able to tamper with the recorded data, and the portability saves time in taking user records instead of queuing in a line. Future works will be making this system wireless and using IOT (internet of things) concept.

From the above discussions it is concluded that finally, the user can enter its password using the virtual keyboard and login into the system. If the user's credentials are matched with the systems database, access to the system will be given to the user.

REFERENCES

[1] S. Santhosh, "Design and development of a security module with inbuilt neural network methodologies and an advanced technique on fingerprint recognition", Circuit, Power and Computing Technologies (ICCPCT), 2014 International Conference.

[2] Fred Kaggwa, "Evaluation of Multiple Enrollment for Fingerprint Recognition" ,IEEE Transaction on System Analysis, vol 8, April 2014.

[3] Takada Tetsuji, Koike Hideki, "Awase-E: Image-based Authentication for Mobile Phones using User's Favorite Images", 5th International Symposium, Udine, Italy, vol 2, March 2013.

[4] Ross A.J. Everitt, Peter W. McOwan, "Java-Based Internet Biometric Authentication System", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 26 pp. 1166-1172 July 2012.

[5] S. Mangijao Singh , K. Hemachandran, "Content-Based Image Retrieval using Color Moment and Gabor Texture Feature" , IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 5, No 1, September 2012.

[6] Sue J. Cho, Suk I. Yoo, "A Matching Algorithm for Content-Based Image Retrieval", IEEE Trans. Pattern Analysis and Machine Intelligence, January 2008.

[7] Smeulders.A.W.M, Worring.M, Santini.S,Gupta.A, and R. Jain, "Content- based image retrieval at the end of the early years," IEEE Trans. Pattern Anal.Mach. Intell.,vol. 22, no. 12, pp. 1349–1380, Dec. 2007.

[8] Subrahmanyam Murala, R. P. Maheshwari, and R. Balasubramanian, "Local Tetra Patterns: A New Feature Descriptor for Content-Based Image Retrieval," IEEE Trans. Image Process., vol. 21, no. 5, pp. 2874–2886, May 2012.

[9] Art Conklin, Glenn Dietrich, Diane Walz, "Password-Based Authentication: A System Perspective", Proceedings of the 37th Hawaii International Conference on System Sciences – 2004.

[10] Ankit Parekh, Ajinkya Pawar, Pratik Munot and Piyush Mantri, "Secure Authentication using Anti-Screenshot Virtual Keyboard", International Journal of Computer Science Issues, September 2011.

[11] Dhamija Rachna, Perrig Adrian, "Déjà Vu: A User Study Using Images for Authentication", 9th Usenix Security Symposium, August 2009.

[12] Hyun-Sung Kim, Sung-Woon Lee, Kee-Young Yoo, "ID-based password authentication scheme using smart cards and fingerprints", ACM SIGOPS Operating Systems Review, Volume 37, Issue 4 (October 2012), Pages: 32 – 41.

[13] Ragini Sharma, Er. Surbhi Gupta, "Digital Watermarking with DWT & DCT using Bit Plane Encryption", International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 12, December 2015.

[14] Syed Hamad Shirazi, Arif Iqbal Umar, "Content-Based Image Retrieval Using Texture Color Shape and Region", International Journal of Advanced Computer Science and Applications, Vol. 7, No. 1, 2016.

[15] Ravi. J , K. B. Raja, Venugopal K. R, "Fingerprint Recognition using Minutia Score Matching", International Journal of Engineering Science and Technology Vol.1(2), 2009, 35-42 .