Impregnable Biometric - A Survey

Srividya R*, Ramesh B **

* Telecommunication Engineering, KSIT, Bengaluru, Karnataka, India
** Computer Science Engineering, MCE, Hassan, Karnataka, India

Abstract - In recent year’s person identification using his physical or behavioral trait has become one of the ground breaking formulas for authentication. Authentication is the primary step in access control of any system. In accessing ones elementary mobile device to ingressing huge industrial server authentication plays a significant role. Authentication can be based on something one knows, something one has or something one is. Biometrics is a genre of something one is, it can either be a physical or a behavioral trait of a person. This work presents a survey on secure biometric genres used in authentication techniques with major outlook on comparison of passwords with gesture biometric.

Index Terms - Biometric, Gesture, Password, Pattern, Trait.

I. INTRODUCTION

The idiom Biometric conventionally means life measurement, “bio” means “life” and “metric” means “measurement”. Biometrics universally is the study of automated identification of an individual, by utilizing one’s own behavioral or physical attributes. Application of Biometric dates back to ancient Egypt, during the construction of the great pyramid of Khufu, it is a ground breaking concept to apply biometrics in Encryption techniques and authentication process. Biometrics is fascinating because they are instinctive possessions of an individual and there is no necessity to remember them like passwords [1].

Biometrics as stated earlier can be broadly classified into behavioral biometrics and physical or physiological biometrics which can be either unimodal or multimodal. Physical biometric represents physical characteristics of a person and this list includes face [2], fingerprint, finger-knuckle print, ear, palm print, iris, hand geometry, Dental X-ray, Deoxyribonucleic Acid (DNA) and retina, to mention a few. Behavioral biometric is an avant-garde technology which involves uniquely identifying humans based on few measurable patterns in human activities. Few of its types include voice of a person, signature, odor, keystroke, gait, Electrocardiogram (ECG), Thermogram and gesture limiting to only few of the examples being mentioned [9].

This paper is organized into following sections. Section II briefs about related work in the area of biometrics. Section III details different Biometric genre. Section IV throws light into the comparison of password based authentication and Gesture based authentication considering various parameters into account for the study and also lists the areas of biometric application. Section V concludes the comparison between these authentication techniques.

II. RELATED WORK

Shantanu Rane, Ye Wang, Stark C. Draper and Prakash Ishwar [1], provided an insight into secure biometrics or in a layman’s language known as protection of the generated biometric template from an attacker. They also discussed about biometric signal model for processing biometric signals and biometric performance measures.

Unsang Park and Anil K. Jain, explained about face biometric recognition [2]. They initiated to use analytical information and soft facial biometric features for improving face image matching and retrieval performance. They developed an automatic facial mark detection method and provided experimental results based on FERET database and forensic domain based mugshot databases. They proved that face-recognition performance of state-of-art matcher improves by use of soft biometric traits.

Xi Zhao, Shi and Ioannis A. Kakadiaris, illustrated the application of statistical touch dynamics image to retain discriminative power for user authentication [3]. The proposed method significantly reduced computational time in online authentication processes. They also evaluated the usability and effectiveness of this method and implemented as App in Android based phones.

Shuang Wang, Xiaqian Jiang, Lucila, Ohno-Machado, Lijuan Cui, Samuel Cheng, Hongkai Xiong, proposed a method that involves non-asymmetric SW codes [4]. This method involves following steps, biometric feature extraction, non-asymmetric SW encryption/decryption and lastly Privacy preserving authentication, which aims at fixing security holes within existing biometric systems.

Ali Fahmi P.N, Elyor Kodirov, Deok-Jai Choi, Guee-Sang Lee, Mohd Fikri Azli A and Shohel Sayeed, proposed a novel approach for implicitly authenticating smart phone users using both shape and texture information of an ear image captured during the call [5]. This approach involves extracting and combining all Local Binary Pattern to form a histogram and also involves extracting ear geometry features by using ear location centre that can be adjusted very easily by users. The authors concluded that is method is easy and simple to employ.

Kresimir Delac and Mislav Grgic, provided an overview of biometric methods. They provided an insight into both the unimodal and multimodal biometric and their advantages and disadvantages.

III. BIOMETRIC GENRE
As already stated, Biometric is broadly classified into two genres with many types falling under each category. A third genre of biometric can be formed by amalgamation of physical and behavioral biometric and it is avowed as Hybrid Biometric [13] [15]. This section describes various biometrics employed in diverse spheres.

1.1. Finger print Biometric
Fingerprint technology is the most widely accepted form of biometric authentication method. The fingerprint specimen consists of minutiae, furrows, valleys and ridges at its tip. These features may be used for feature detection, feature extraction and matching. The accuracy of fingerprint feature matching the template with the input biometric is very high since the input directly is in contact with the reader device. In real-time fingerprint matching, matching can be performed using any of these methods, minutiae based, ridge based or correlation based methods [4] [16].

1.2. Finger-Knuckle Print Biometric
Finger-knuckles are the joints of fingers that are visible prominently when fist is made by clenching the hand. Finger-Knuckle Print (FKP) biometric is an upcoming technology which is gaining popularity in recent years in authentication process. FKP biometric is relatively stable since it remains unchanged throughout the lifetime of a person. In methods using FKP biometric, Region of Interest (RoA) is first determined and then nearest neighbor classifier is used for recognition and comparison. To obtain 100 percent accuracy using FKP in authentication process, multiple finger types yield better result [8] [16].

1.3. Palm print Biometric
Palm print biometric is similar to Fingerprint in having principle lines, valleys and ridges similar to a finger print. Palm print can be characterized as having distinctive features like wrinkles, width of fingers, Meta Carpo Phalangeal (MCP), Distal Inter Phalangeal (DIP), Proximal Inter Phalangeal (PIP), overall palm area and circularity, the perimeter and elongation fingers indices, which varies for every person. Systems involving this method for authentication uses Principle Component analysis strategy and hand geometry features [10].

1.4. Hand Geometry Biometric
Hand Geometry features may involve height of fingers and distance between them, width of the palm, angle between the fingers and hand dimensions. Systems employing this form of biometric processing for authentication may have error rates lesser than 10 percent in verification process. When combined with other forms of biometric to form a multimodal biometric, hand geometry can be reliable for identification [11].

1.5. Iris Biometric
Iris is complex human phenotype (externally visible trait) and that portion of eye which surrounds the pupil and is colored. It is also claimed that the combination of dark spots, filaments, pits, striations, rings, and freckles add for the accuracy of iris biometric identification. It is believed that iris texture patterns are so unique that both the eyes of same individual are different. [6] [15] [22]

1.6. Retina Biometric
Retina is that portion of the eye embedded deep in its rear hemisphere with tissues and vessels, forming a person’s unique identity. Retina recognition technology is based on the differentiation of unique vascular patterns from eye to eye and person to person and nearly impossible to acquire retina images of a person without his consent [14] [15].

1.7. Face Biometric
Face detection, face recognition, face analysis and retrieval system uses facial images consisting of local and global texture features. The prominent components of face include eyes, nose, mouth, ears and chin. Face matching can also be performed using soft facial biometric traits unique to an individual and they include moles, scars, pockmark which may be permanent and the non permanent facial features may include wrinkle, freckle, scares, abrasion, acne, dark skin, whitening and many more [2]. Accuracy of face matching may increase if expressions of subjects are not taken into account.

1.8. Ear Biometric
Ear biometric is one of the easily employed passive forms of biometric. The merits of using ear biometrics in authentication process over other forms of biometrics are, shape of the ear and the cartilage tissue of the pinna are distinctive and does not change during life time of a person, color distribution of ear remains uniform and unchanged so much information is not lost during ear image processing, since ear size is small, one can work efficiently and effectively with lower resolution involved [5].

1.10. Vein Biometrics
Veins are elastic blood vessels that transport blood to heart from various regions of the body and are prominent features of any person’s hand. These Vascular patterns have strong immunity to forging since they are not visible to naked eyes and lie underneath the skin. To capture subjects vein pattern infrared sensors are used and when the palm is illuminated a dark pattern appears which is visible due to deoxidized hemoglobin in the palm veins [23].

1.11. Voice Biometric
Voice biometric has made the world of technology more easily adoptable and is true since most of devices used by humans today work on speech commands. Voice of an individual is predominantly dependent on his physical traits used in creation of sound like mouth, vocal tracts, larynx, pharynx, nasal cavities and lips. The behavioral trait of an individual may change according to his emotional state, medical conditions and age. Recorded audio files of varying types and conditions and age.
their differing qualities are the primary challenge in voice recognition systems. Obtaining all levels of training data is an added issue and also the distance of the individual from the recording device can be a problem [17].

1.12. Signature Biometric or Hand Writing recognition

Signature or hand writing is an unique expression by an individual’s hand geometry and is a traditional style of metric for person authentication and identification. Though many theories relating to signature based authentication systems are proposed, no due attention is rendered in employing them. In some instances handwriting or signatures belonging to different subjects may look similar and two genuine signature instances of same user may have variations in texture and other dynamic property. To declare a signature genuine an Elastic distance matching algorithm may be made use of and the signature characteristics considered [18].

1.13. Gait Biometric

Gait of a person is the way he walks and is influenced by his physical or psychological status such as emotion, fatigue, well-being, etc. In addition, external factors such as clothing, shoes, carried loads, and ground characteristics also influence gait. Gait is a complex spatio-temporal biometrics measured using the concept of Bio-kinematics and is not a distinctive feature [21].

1.14. Keystroke Biometric

A prevalent belief in major class of society is that every individuals typing style or pattern on keyboard is unique. It provides discriminatory information even though not completely distinctive. The merits of using keystroke biometrics is that since the person using the system is keying information he can be easily monitored, but it majorly does not contribute to privacy and in turn security. The application of keystroke biometrics and databases consisting of keystroke templates majorly affect the performance of keystroke biometrics system [20].

1.15. Odor Biometric

Odor is a predominant feature of every individual and is caused generally at a very lesser concentration by one or more volatilized chemical composition. They are spread around and can either be pleasant or unpleasant. To employ this type of biometric in authentication process an array of sensors are to be used, to identify the odor and it becomes a complex process to synchronize the array of sensors. Though this is a promising approach it is still in infancy and needed to be well established in the field of Biometric authentication systems [19].

1.16. DNA Biometric

DNA technology is the most widely accepted form of complex human genotypes biometric authentication means. DNA or Deoxyribonucleic acid of an individual is very unique and probably most reliable feature which cannot be forged. The DNA pattern in fact is a one dimensional code which is unique to a person and preset in every cell of an individual’s body. The limitations of DNA biometrics are, since it is present in every cell of a person’s body, it is easy to steal, but DNA matching involves complex process so it is difficult to employ in real time by the masses [22].

1.17. ECG Biometric

Electrocardiogram (ECG) is an emerging modality in the field of Biometric recognition systems which are difficult to counterfeit. ECG depends on structural and functional characteristics of the heart and contains information pertaining to the electrical operations of the heart which are unique and highly personalized. In short ECG is a record of heart’s electrical activity. Researchers have stated several issues that need to be solved before using ECG in biometric systems for authentication few of them are ECG signal changes over time and heart rate variability due to ageing [24].

1.18. Thermogram Biometric

It is an emerging modality in the field of Biometric Authentication Techniques. Thermo gram relates to capturing heat radiation pattern emitted from human body parts like face, hand, veins and so on, using infra-red cameras and since humans maintain constant temperature and are homoeothermic When compared to visual images, thermal imaging has better accuracy. Facial Thermo gram allows one to passively perform detection in different circumstances by recording facial temperature variations caused by vein structure on facial surface [25].

1.19. Gesture Biometric

Gesture biometrics is one of the most interesting and trendsetting innovation of previous few decades. Gesture refers to non verbal communication or movement of body parts usually hand or fingers to indicate a person’s intention. It involves edge detection methods. Gestures are revocable that is when a gesture is no longer effective it can be replaced and since it does not involve touch on any device, forging is difficult. Having these merits gestures are widely used now a days in person identification and authentication process [3] [7] [26].

IV. ANALYSIS AND DISCUSSION

This section provides an insight into the comparison of passwords with one of the biometrics based authentication methods and also the areas of application of biometrics.

1.1. Comparison between Passwords and Gesture Biometric Authentication Methods

The comparative study between two classes of authentication is tabulated in Table 1. The two authentication classes that are gesture authentication represented in table as “Ges” and the classical password authentication method represented as “Pwd” are compared with respect to the parameters Interest, Ease of Use and Ease of remembrance.

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>Interest</th>
<th>Ease of Use</th>
<th>Ease of Remembrance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classic Password</td>
<td>N</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Gesture Authentication</td>
<td>E</td>
<td>VD</td>
<td>VD</td>
</tr>
</tbody>
</table>


Table 1 was formulated by giving same type of gesture and password to each of the subjects under study. With respect to their Interest in using the password or gesture, Ease of their Use and Ease of remembrance the results are correlated, compared and tabulated. This study was consolidated for a period of nine months involving 63 subjects belonging to different age group.

www.ijsrp.org
For a period of three months first study was conducted. Involving same subjects, for a period of next six months, second study was conducted and the third study was done for a period of successive nine months.

Table 1 Comparative Analysis of Password and Gesture authentication Approaches

<table>
<thead>
<tr>
<th>Age</th>
<th>Time Duration</th>
<th>Interest</th>
<th>Ease of Use</th>
<th>Ease of Remembrance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Pwd</td>
<td>Ges</td>
<td>Pwd</td>
</tr>
<tr>
<td>20-30</td>
<td>3months</td>
<td>I</td>
<td>I</td>
<td>NI</td>
</tr>
<tr>
<td></td>
<td>6months</td>
<td>I</td>
<td>I</td>
<td>NI</td>
</tr>
<tr>
<td></td>
<td>9months</td>
<td>NI</td>
<td>I</td>
<td>NI</td>
</tr>
<tr>
<td>30-40</td>
<td>3months</td>
<td>I</td>
<td>I</td>
<td>NI</td>
</tr>
<tr>
<td></td>
<td>6months</td>
<td>NI</td>
<td>I</td>
<td>D</td>
</tr>
<tr>
<td></td>
<td>9months</td>
<td>NI</td>
<td>I</td>
<td>D</td>
</tr>
<tr>
<td>40-50</td>
<td>3months</td>
<td>NI</td>
<td>I</td>
<td>D</td>
</tr>
<tr>
<td></td>
<td>6months</td>
<td>NI</td>
<td>I</td>
<td>D</td>
</tr>
<tr>
<td></td>
<td>9months</td>
<td>NI</td>
<td>I</td>
<td>VD</td>
</tr>
<tr>
<td>50-60</td>
<td>3months</td>
<td>NI</td>
<td>I</td>
<td>D</td>
</tr>
<tr>
<td></td>
<td>6months</td>
<td>NI</td>
<td>I</td>
<td>VD</td>
</tr>
<tr>
<td></td>
<td>9months</td>
<td>NI</td>
<td>I</td>
<td>VD</td>
</tr>
</tbody>
</table>

Fig.1 depicts the tabulated comparative study between password and gesture based authentication methods graphically.

Fig.1. Comparision between Password and Gesture authentication

X-axis represents Range of Ages (RoA) i.e., different age group considered for study of the two methods of authentication and Y-axis represents Average Percentage of Correlation between the Parameters considered for Gesture and Password (APCPGP) for 9 months. The graph was derived by assuming values for all the variables considered in Table I.

Different biometric genre can also be evaluated based on the Biometric characteristics listed here and they are universality, uniqueness, permanence, measurability, performance, acceptability, circumvention. There can also be many other parameters not listed here that can be used to evaluate various biometric genre.

When conducting this study special case related to memory loss like Dementia, Alzheimer’s and mental illness were not taken into account.

1.2. Areas of Applications

The most revolutionary idea of using what a person himself is, in various fields, is a cutting edge technology and known as Biometric as already stated. Biometric concept can be employed in various areas and few of them are listed here.

- Biometric are used in access control systems to provide various levels of security.
- Biometric are used in person recognition or identification and authentication.
- They are used in Biometric linked Encryption algorithms in various Networks.
- They are increasingly useful for security applications in the banking industry and various web applications.
- Biometric systems are used in home automation and security applications like video surveillance, airport checking, computer or mobile devices systems, etc.
- Used in the field of medical applications, forensic medicine and forensic science to find culprits in the area of crime.

V. CONCLUSION

The study of biometric has a voluminous scope and future. Biometric and its use in security solutions for networks and in authentication process is a ground breaking technology. Biometrics can be easily employed since the burden of remembering neither the passwords nor the issues related to maintaining any smart cards is involved.

Biometric and its applications will rule the world of encryption and authentication in mere future. Biometric applications not limiting to only above said areas, currently their usage in home automation is catching an eye. In mere future there will be no area spared where in biometric technology is not made use of.

This paper is an effort to provide an insight into biometrics and its classes. There are currently ample of ongoing researches in this field to explore the unexplored within us and use them for the benefit of mankind.

ACKNOWLEDGMENT

The authors would like to extend their thanks to all those subjects involved in study and also the researchers, academicians and corporate employees, who have lend their support directly or indirectly in carrying out this research work.

www.ijsrp.org
REFERENCES


[3] Xi Zhao, Member, IEEE, Tao Feng, Student Member, IEEE, Weidong Shi, Senior Member, IEEE, and Ioannis A. Kakadiaris, Senior Member, IEEE, “Mobile User Authentication Using Statistical Touch Dynamics Images”, This paper appears in IEEE Transactions on Information Forensics and Security, Vol 9, No 11, November 2014


AUTHORS

First Author – Sridivya R, B.E., M.Tech, Asst. Professor Department of Telecommunication Engg., Kamvvari Sangham Institute of Technology, Bengaluru, India. sridivya.ramisetty@gmail.com

Second Author – Ramesh B, B.E, M.Tech, PhD, Professor, Department of Computer Science Engg, Maldan College of Engineering, Hassan, India. sanchara@gmail.com

www.ijsrp.org