A STUDY ON VISUAL CRYPTOGRAPHY SYSTEM IN BIOMETRIC AUTHENTICATION SYSTEM

[1]Ms. S. Neethu, [2]Mr. C. Moudeesh, [3]Mr. V. Sadhasivam.

[1]Assistant Professor, Department of Computer Applications, Dr. SNS Rajalakshmi College of Arts & Science, Coimbatore.

[2]PG Student, II MCA, Department of Computer Applications, Dr. SNS Rajalakshmi College of Arts & Science, Coimbatore.

[3]PG Student, II MCA, Department of Computer Applications, Dr. SNS Rajalakshmi College of Arts & Science, Coimbatore.

Abstract: - *Biometrics deals with recognizing a person or verifying the identity of a person based on physiological or behavioral characteristics. Visual cryptography is a secret sharing idea where a secret image is encrypted into the number of shares which independently reveal no information about the original image. There are various biometric templates like fingerprints, face, voice, signature, iris and odor. Preserving the privacy of biometric data such as fingerprint images stored in central database has become vital importance. This can be primed achievable using visual cryptography for biometric privacy such as fingerprint images. A private fingerprint image is flustered into two host images that are gathered in two separate database servers such that the private image can be discovered only when both sheets are concurrently available; at the same time, the individual sheet images do not reveal the uniqueness of the private image. The images are saved in database by employing encryption .The stored images are encrypted and during verification process that images are decrypted. So we propose biometric privacy using visual cryptography with pixel sharing. In this paper, we discuss about the visual cryptography system for fingerprint authentication.*

Keywords **-** *Visual cryptography, Fingerprint, Privacy, Biometrics.*

1. INTRODUCTION

Now a day, increasing use of internet has a great impact in human beings. They become more dependent on the computer system and networks. This dependency has brought many threats to the network security. Due to this reason, need a secure mechanism which protects our information through unauthorized access. Biometric authentication system is example of the technologies which widely used in various applications like ID cards, banking etc [1]. The importance of utilizing biometrics to establish personal authenticity and to detect imposters is growing in the present scenario of global security concern. Also the Development of a biometric system for personal identification, which fulfills the requirement for access control of secured areas and other applications like identity validation for social welfare, crime detection, ATM access, computer security, etc. is felt to be the need of the day. The human tongue promises to deliver a level of uniqueness to identification applications that other biometrics cannot match in context of that it is well protected in mouth and is difficult to forge [2]. The tongue also presents both geometric shape information and physiological texture information which are potentially useful in identity verification applications.

It is one of the authentication system it comes from the Greek words 'bios and metrics' which means 'life measure'. It is the science of establishing the identity of on individual based on physical or behavioral traits such as face, finger print, Iris. It is more reliable, consistent and also user friendly. So it is used for many applications. The biometric data classified as physiological or behavioral. Physiological biometrics based on the physical part of the body such as fingerprint, iris, eye, retina, face, palm, hand. Behavioral type is based the on behavior of human such as voice, signature and keystroke. Biometrics is a technology that uses physiological or behavioral characteristics to authenticate identity of persons [3]. For automated personal identification biometric authentication is getting more attention. There are various application where personal identification is required such as passport control, computer login control, secure electronic banking, bank ATM, credit cards, premises access control, border crossing, airport , mobile phones, health and social services, etc. Many biometric techniques are available such as facial thermogram, hand vein, gait, keystroke, odor, ear, hand geometry, fingerprint, face, retina, iris, palm print, voice and signature. Among those iris recognition is one of the most promising

approach because of stability, uniqueness and noninvasiveness [4]. A biometric system is essentially a pattern recognition system that recognizes a person based on a feature vector derived from a specific physiological or behavioral characteristic that the person possesses [5]. Advantages of using biometrics characteristics are reliability, convenience, universality, and so on. But biometrics system does not provide privacy because biometric data is not replaceable and is not secret. There exist several types of attacks possible in a biometric system.

A. The Properties of Biometric Template

- Security**:** This property prevents the biometric template from stolen template.
- Diversity: The secure template must not allow cross matching across databases.
- Revocability: It should be straight forward to revoke a compromised.
- Performance: The recognition performance of the biometric system should not reduced by biometric template protection scheme.

B. Modules in Biometric System

There are basically two phases in biometric system. There are enrollment phase and authentication phase. In these two phases there are four modules. The sensor module is used in extracting the biometric data which may be image, audio or video. The feature extraction module is used in obtaining the template that is generated from the features of the biometric data.

Each feature is labeled with a user's identity. The Matching module is used in authentication phase, where the template data is compared with data which is obtained from user and that it estimates the similarity between these data. These similar elements are processed in Decision making module which is used to identify the individual.

C. Vulnerabilities in Biometric system

The biometric system failures are classified into two types, intrinsic system and adversary attack. Intrinsic attack is due to the incorrectness in the decision making of biometric system which may lead to false accept and false reject. In adversary attack the hacker will try to circumvent the biometric systems for personal gains. These are classified into three types administrator attack, Non-secure Infrastructure and Biometric overtone [6].

2. RELATED WORK

2.1 Biometric template attacks

Biometrics is the detailed measurements of the human body. A brief comparison of nine biometric techniques made by A. Jain et al. in 1997 is provided in Table 2.1 below.

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance
Face	High	Low	Medium	High	Low
Fingerprint	Medium	High	High	Medium	High
Iris	High	High	High	Medium	High
Signature	Low	Low	Low	High	Low
Voice	Medium	Low	Low	Medium	Low

Table 2.1: - Comparison of biometric technologies

Now-a-days, recognizing person using alphanumeric passwords is not sufficient for the identity determination because they can be easily guessed or stolen [7]. Therefore using biometric system is generally pattern recognition system that determines person based on his physiological characteristic. Use of the biometric templates provides advantages like convenience, reliability, universality etc. Several places were attacks are possible in biometric system are shown in Figure[1] below.

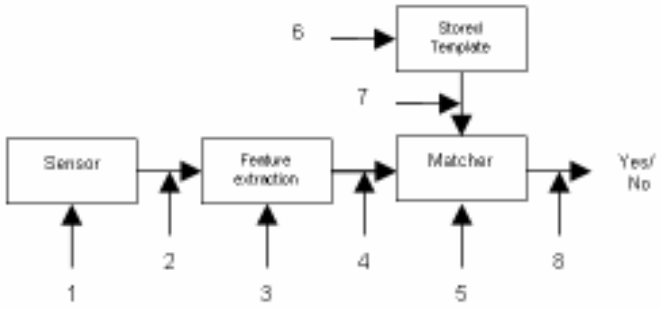

Fig 2.1: - Possible attack points in generic biometric systems

2.2. Visual Cryptography

The basic visual cryptography scheme was proposed by Naor and Shamir's [8] .In this scheme for sharing a single Pixel p, in a binary image Z into two shares A and B is illustrated in Table 2.1. If p is white, one of the first two rows of Table 2.1, is chosen randomly to encode A and B. If p is black, one of the last two rows in Table 2, is chosen randomly to encode A and B. Thus, neither A nor B exposes any clue about the binary color of p. When these two shares are superimposed together, two black sub-pixels appear if p is black, while one black sub-pixel and one white sub-pixel appear if p is white as indicated in the rightmost column in Table[2]. Based upon the contrast between two kinds of reconstructed pixels can tell whether p is black or white. Performance of visual cryptography scheme mainly depends on pixel expansion and contrast. Pixel expansion refers to the number of sub pixels in the generated shares that represents a pixel of the original input image. It represents the loss in resolution from the original picture to the shared one. Contrast is the relative difference in weight between combined shares that come from a white pixel and a black pixel in the original image. Plenty of research has been made to improve the performance of basic visual cryptography scheme. Many authors have proposed the visual cryptography schemes in which pixel expansion is 1 [9, 10]. These schemes can be used as quality of retrieved images is good.

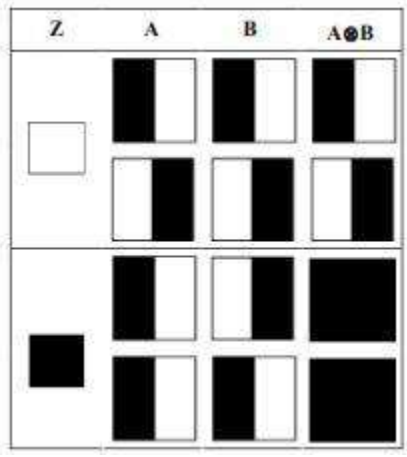

Table 2.2: - Visual Cryptography

A pixel P is split into two sub pixels in each of the two shares. If P is white, then a coin toss is used to randomly choose one of the first two rows in the figure above. If P is black, then a coin toss is used to randomly choose one of the last two rows

in the figure above. Then the pixel P is encrypted as two sub pixels in each of the two shares, as determined by the chosen row in the figure. Every pixel is encrypted using a new coin toss. Suppose we look at a pixel P in the first share. One of the two sub pixels in P is black and the other is white. Moreover, each of the two possibilities "black-white" and "white-black" is equally likely to occur, independent of whether the corresponding pixel in the secret image is black or white.

The extracted iris template is stored in the database and using Random number generator algorithm, a random number is generated and is stored in the database as the extracted template image‟s name. This number is given as input to the VC module which then generates two shares, out of which one share is stored in the database and the other is stored on the user ID card. This ends the enrollment module. 3.2 Authentication For this phase, user will come and give his eye image. His eye image will go through the SNF process. Then this extracted image will be compared with the extracted image stored in the database while enrollment phase. If both the templates match then we consider that the user is a registered employee and he can proceed for the further Login process. But, if the templates do not match, then the user is asked to go through the enrollment phase. Once he proceeds to the Login process, he will provide the ID card on which the share is stored. At the same time system will find his corresponding second share from the database. These both shares will be superimposed and will be decrypted to find the number. The decrypted number will be compared with the image name which was also stored as the number. If both the numbers match then the user is This demonstrates the security of the scheme. Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by humans (without computers). It involves breaking up the image into n shares so that only someone with all n shares could decrypt the image by overlaying each of the shares over each other. As we can see in the figure below, original image is encrypted into the two shares by using visual cryptography and as we can see these shares are not understandable to the naked eyes but by decrypting them we can again get the original image.

3. FINGERPRINT AUTHENTICATION PROCESS

Fingerprints are graphical flow-like ridges present on human fingers (Figure [3]). Their formations depend on the initial conditions of the embryonic mesoderm from which they develop [11].

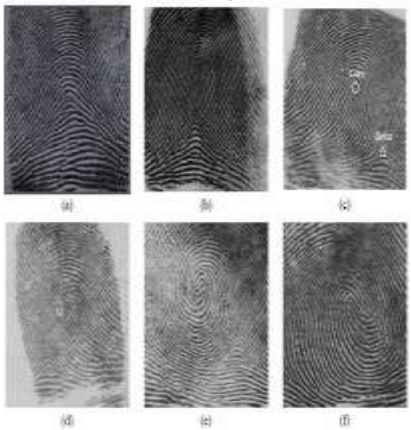

Fig 3.1: - A fingerprint classification schema of six categories: (a) arch, (b) tented arch,(c) right loop, (d) left loop, (e) whorl, and (f) twin loop.

Modern fingerprint techniques were initiated in 1684 by English plant morphologist Nehemiah Grew. Starting from 1809, Thomas Bewick began to use his fingerprint as his trademark, which is believed to be one of the most important contributions in the early scientific study of fingerprint identification [12].

Later fingerprint identification systems were involved in criminal identification process. Nowadays these systems are widely used in multiple civil areas, such as in prevention of multiple enrollments in an electoral, welfare, custom control, employee attendance logging, security desk in banks, security installations, visitor verification, member verification in clubs, member organizations etc.

The first stage makes use of global fingerprint characteristics while the second stage is the minutiae matcher (point pattern matching). Authors state that typically, automatic fingerprint identification and authentication systems rely on representing the two most prominent structures: ridge endings and ridge bifurcations. These two structures are background-foreground duals of each other and pressure variations could convert one type of structure into the other [13]. Therefore, many common representation schemes do not distinguish between ridge endings and bifurcations. Both the structures are treated equivalently and are collectively called minutiae. The simplest of the minutiae-based representations constitute a list of points defined by their spatial coordinates with respect to a fixed image-centric coordinate system. Typically, though, these minimal minutiae-based representations are further enhanced by tagging each minutia (or each combination of minutiae subset, e.g., pairs, triplets) with additional features. For instance, each minutia could be associated with the orientation of the ridge at that minutia; or each pair of the minutiae could be associated with the ridge count: the number of ridges visited during the linear traversal between the two minutiae.

A feature extractor finds the ridge endings and ridge bifurcations from the input fingerprint images. If ridges can be perfectly located in an input fingerprint image, then minutiae extraction is just a trivial task of extracting singular points in a thinned ridge map. However, in practice, it is not always possible to obtain a perfect ridge map [14].

Finely, the researchers have listed the stages required for the biometric authentication as following:

- **Capture:** A raw biometric sample is captured by a sensing device, such as a fingerprint scanner or video camera.
- **Process:** The distinguishing characteristics are extracted from the raw biometric sample and converted into a processed biometric identifier record (sometimes called biometric sample or biometric template).
- **Enrol:** The biometric template is stored in a storage medium for comparison during an authentication phase. Notice that the original biometric sample cannot be reconstructed from this identifier.
- **Verification:** In this mode (\1 to 1 matching"), a newly captured/processed biometric sample taken for instance during a login, is compared against a previously enrolled sample to address the question \Are you the person you claim to be?"
- **Identification:** In this mode (\1 to N matching"), the individual does not claim an identity. The individual presents a biometric sample and the system tries to identify the individual from a database of stored biometric samples.

4. CONCLUSION AND FUTURE ENHANCEMENTS

Various approaches adopted by researchers to secure the raw biometric data and template in database. In this paper, we discussed about the the visual cryptography system for fingerprint authentication. This kind of approach solves two major problems related to fingerprint based automatic access control systems such as falsification and costly maintenance of the large fingerprint database. For the purposes of identification and authentication, biometric methods use distinctive physical traits (such as fingerprints, eyes, or faces) or behavioural characteristics (such as signature, voice, etc.). The biometric approach has more benefits than the conventional password approach. For instance, a password is easy to forget, easy to steal, and tough to remember. Simple passwords are easy to crack, whereas complicated passwords are challenging to remember. However, biometrics can be more trustworthy than the conventional password strategy. At the time of authentication, biometric data are modified according on the owner's emotional or physical state. The database contains the two fingerprint templates that were created by Chen and Wu using various secret sharing image strategies. It improves the confidentiality of the sensitive information.

REFERENCES

[1] Pant, B., Shukla, S., & Bordoloi, D. (2021). Visual Cryptography: A Study And Its Application To Biometric Authentication. Webology, 18(3), 1502-1509.

[2] Ibrahim, D. R., Teh, J. S., & Abdullah, R. (2021). Multifactor authentication system based on color visual cryptography, facial recognition, and dragonfly optimization. Information Security Journal: A Global Perspective, 30(3), 149-159.

[3] Chutake, V., Hatiskar, N., & Dhas, A. (2014). Secure Biometric Authentication using Visual Cryptography. International Journal of Engineering Research and Technology, 3(2), 881-884.

[4] Gupta, H., & Sharma, N. (2016, September). A model for biometric security using visual cryptography. In 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) (pp. 328-332). IEEE.

[5] Nandhinipreetha, A., & Radha, N. (2016, January). Multimodal biometric template authentication of finger vein and signature using visual cryptography. In 2016 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-4). IEEE.

[6] Kaur, H., & Khanna, P. (2020). Remote multimodal biometric authentication using visual cryptography. In Proceedings of 3rd International Conference on Computer Vision and Image Processing: CVIP 2018, Volume 2 (pp. 13-25). Springer Singapore.

[7] Singh, P., & Bordoloi, D. (2021). Visual Cryptography Authentication for Locker Systems using Biometric Input. Webology, 18(5), 3126-3131.

[8] Ibrahim, D. R., Abdullah, R., Teh, J. S., & Alsalibi, B. (2019, January). Authentication for ID cards based on colour visual cryptography and facial recognition. In Proceedings of the 3rd International Conference on Cryptography, Security and Privacy (pp. 164-167).

[9] Dwivedi, A., Khandare, G., Shaikh, M., & Morey, M. A. (2021). ONLINE VOTING SYSTEM BASED ON VISUAL CRYPTOGRAPHY AND BIOMETRIC.

[10] Mohan, J., & Rajesh, R. (2021). Enhancing home security through visual cryptography. Microprocessors and Microsystems, 80, 103355.

[11] Kakkad, V., Patel, M., & Shah, M. (2019). Biometric authentication and image encryption for image security in cloud framework. Multiscale and Multidisciplinary Modeling, Experiments and Design, 2(4), 233-248.

[12] Suganya, M., & Suganya, S. (2017). A Fingerprint Biometric Privacy Using Visual Cryptography.

[13] Gulsezim, D., Zhansaya, S., Razaque, A., Ramina, Y., Amsaad, F., Almiani, M., ... & Oun, A. (2019, October). Two factor authentication using twofish encryption and visual cryptography algorithms for secure data communication. In 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS) (pp. 405-411). IEEE.

[14] Udayini, V., Bindu, C. H., & Malleswari, P. N. (2019). Iris Image Authentication using Visual Cryptograph. International Journal of Recent Technology and Engineering, 8, 288-291.