College of Engineering Chengannur
Department of Computer Engineering
M. Tech. Computer Science (Image Processing)
03CS7903 Seminar II
Abstract of Proposed Seminar Topic

A safe and secured iris template using steganography and cryptography

15/MCS/2019 CHN19CSIP04 Sudhi G. K.

September 7, 2020

Keywords: Irisrecognition, Cryptography, Steganography, Algorithm

Abstract

The utmost need for applications of biometrics-based authentication in access control, banking, healthcare among other in recent years are for reliable and accurate identification among users. There are still various privacy and performance issues exist in biometrics-based system such as absence of revocability in biometric system techniques, lack of uniqueness, noisy data, sensitivity to outliers, and identity invasion.Therefore, the two main param- eters issue for biometric-based recognition systems are security and performance, thus there is need for a system that can achieve template protection and as well as performance improvement to produce strength to the biometric system. To prevent any possibility of security theft and ensure the privacy of any user, three criteria must be satisfied namely: diversity, revocability, and non-invertibility.three criteria must be satisfied namely: diversity, revocability, and non-invertibility.

Iris recognition is one of the utmost dependable, unique, steady and sure preference traits of all biometric system. Iris templates are extracted features from the iris sample, which are used during the verification process. Though the iris system enhances security, it is still prone to attacks. Imposters can break through the system deceitfully in the name of a genuine user. Hence, there is a need to secure the iris template.

Cryptography is the science and art of concealing the messages to introduce secrecy in information security. It provides several encoding schemes for achieving the security while communicating in a public domain or network. Steganography is related but adds another measurement to cryptography. In steganography, people not only want to protect the secrecy of an information by concealing it, but they also want to make sure any unauthorized person gets no evidence that the information even exists.

Cryptography does not guard against the vulnerabilities and treats that emerge from the poor design systems, protocols and procedures. Hence, there is need to fixed it with another method through proper design and setting up of a defensive infrastructure. In steganography if image is subject to attack such as translation and rotation, message is hard to recover. Message is difficult to recover, if significant damage occurs to picture appearance in steganography and relatively easy to detect.The iris images can be vulnerable to the third party using only one of these techniques, thus the combination of Steganography and Cryptography will enhance the security and robustness of iris template protection. Therefore the algorithms were combined to enrich and complement each other.

This study combines Cryptography (Twofish and Triple data decryption (3DES)) algo- rithms and Steganography (Least Significant Bits) to solve the problem of attacking or hacking biometric template for a malicious act, which has become a huge problem in the iris recognition system. Twofish and Triple data encryption are good and secured cryptography algorithms which are used to change readable secret data (plain image) into an unreadable format (cipher image) while least significant bits (LSB) is a steganog- raphy algorithm which embeds ciphertext/image directly into a cover image to produce an image known as stego image.

Several systems have been projected to safeguard the bio-

metric (iris) templates from any unlawful or unintentional tampering.

Grover et al. proposed a hybrid approach that is based on Run Length Encoding together with Steganography for Iris template security. The proposed technique accomplished a compression of the template together with providing two-fold security of the iris template. The original template is compressed in the proposed technique and the subsequent template is extra safeguarded when compared with the application of steganography only. The method fail to reported on the difficulty of access even for legitimate user at a crucial time of decision- making using a strongly encrypted, authentic, and digitally signed information in cryptography.

Taha et al. conducted a survey on the use of steganographic and cryptographic techniques to achieve a hybrid system and reports the differences between both techniques. After the comparison between the two methods, it was established that steganography cannot be used as an alternate to Cryptography as each aspect has its individualities and uniqueness.

Yang et al. propose a system to provide user authentication and secure the original iris data called cancelable iris and steganography-based user authentication system. The paper established that most existing cancelable iris biometric systems need a user-specific key to guide feature transformation because this user-specific key is compromised, some useful information can be leaked and exploited by attackers to restore the original iris feature data. Therefore, to overcomes the risk, the paper enhances the system security by integrating an effective information-hiding technique called steganography.

Chai et al. proposed a cancelable iris key binding scheme without Elliptic Curve Cryptography and an alignment-free. The system protects the binary biometric data IrisCodes, from security and privacy attacks through a strong and size varying non-invertible cancelable transform. Through the controllable hashed code length, the system provides flexibility in system storage and authentication speed.

Maček et al. designed an iris based system in mobile banking using modular authen- tication framework. System keeps biometric templates encrypted or at least cancelable during all stages of storage, transmission and verification.As templates are stored on clients in encrypted form and decryption keys reside on bank's authentication server, original plaintext templates are unavailable to an adversary if the phone gets lost or stolen.

Anuja et al. conducted a survey of iris template security using different techniques.Template transformation methods, biometric cryptosystems, steganography, and visual cryptography among other are schemes proposed to provide security to iris templates in a database. The paper suggested that a single template protection scheme might not be sufficient to fulfill the needs of requests. Therefore, hybrid systems that are build use of the benefits of various template protection approaches should be created.

Zhao et al. [25] designed a system using local ranking to secure iris template. The iris data are first XORed (Exclusive OR operation) with an application-specific string; and divide the results into blocks and then partition the blocks into groups. The blocks in each group are ranked according to their decimal values, and original blocks are transformed to their rank values for storage.

This work combined Twofish, 3DES, and LSB to develop improved security for iris template in the database. The iris template is divided into two segments, segment A and segment B. Segment A was encrypted with Twofish to produce a cipher image A while segment B is encrypted with 3DES to produce cipher B. Both ciphers were embedded into the cover image using LSB, this produces a stego image that will not display the cipher image while the cover image is visible. The process will be reversed to get the iris template.

The Chinese Academy of Science -Institute of Automation (CASIA) eye image database dataset was used for this research work. The iris images are extracted and stored in a database and the images were loaded from the database.

Generation of template is done using Iris segmentation algorithm using Hough Transform. This can be connected to distinguish the nearness of a circular shape in a given image. It is utilized to distinguish any shape or to find the iris in. characteristic equation of a circle of radius r and center (a, b) is given by $(x-a)^2-(y-b)^2$. This circle can be explained by the two following equations $x=a+r\cos\theta$, $x=b+r\sin\theta$ .It is used to work out the radius and center of the user and iris circles. To detect the edges in the iris image, the Canny edge detection operator is utilized.

The next phase is to a fix size of the image in order to allow comparisons by transforming the iris region. Generally, the dilation of a pupil from difference illumination resulted in stretches of the iris image. The remap of each iris region's point to the polar coordinates (r, θ) was done using Daugman's rubber sheet model. Where r is the distance $(0, 1)$ and the angle θ is $(0, 2\pi)$.

Daugman's rubber sheet model is used for normalization of iris regions because the pupil can be non-concentric to the iris, the formula for remapping is required to rescale points, which depending on the angle around the circle. The formula is given as $r' = \sqrt{\alpha\beta} \pm \sqrt{\alpha\beta^2 - \alpha r_l^2}$, Where $\alpha\beta$ represent the centre of the pupil in relation to the centre of the iris as shown by $X-0, y_0, r$ represent the distance between the edge of pupil and the edge of iris at an angle, θ is around the region while I_r is the radius of the iris

Iris feature extraction is done by Log-Gabor Filters. Modification to Gabor function is the log Gabor function that served as an amendment to the basic Gabor function, which the frequency response is a Gaussian on a log frequency axis as defined.

The iris template generated is divided into two segments. Segment A and B. Encryption of segment a is done with 3DES algorithm. The use of many and different length keys led to the use of Triple-DES algorithm by applied DES three times. The triple length key is assumed of having three 56-bit keys represented as K1, K2, K3. Encryption of segment B is done with two-fish algorithm.

The encrypted iris cipher image A and B was combined to get cipher image C and embedded into a cover image using LSB, then the stego image was loaded into the database.

The result of the proposed system was compare with some existing iris template protection that use different methods. Genuine Acceptance Rate (GAR) was used as the benchmark for the performance evaluation. The probability of confusing two identities is FAR, and the GAR is defined as $GAR = 1 - FRR$, where the rejection probability of the authorized users is the false reject rate (FRR) .Here securing iris template before it is stored in database is done using Twofish, Triple Data Encryption system algorithm and Least Significant Bits of image steganography.The developed system performs two main operations which are securing and retrieving. Each of these operations accept two inputs, iris template and cover image for securing, stego image and cover image for retrieving. At the end of each successful operation a single output is obtained that is, stego image and iris template form securing and retrieving operation respectively. The negligible changes in the master file after embedding the secrete text message or stego file cannot be identify by the human eyes. With the level of security of the system, the problem of panicking with information in transit or information stored in the database will be reduced to the barest minimum if not totally eradicated in information communication technology environment. The application of steganography and cryptography in iris recognition brings about stronger security platform.

References

[1] Anuja JS, Praveen K, and Amritha PP. A Survey of Iris Template Security Aspects. *International Journal of Pure and Applied Mathematics*, 119(15):1471–1481, 2019.

[2] Canuto AM, Pintro F, and Xavier-Junior JC. Investigating Fusion Approaches in Multi-Biometric Cancellable Recognition. *Expert Syst Appl*, 40(6):1971–1980, 2013.

[3] Kelkboom EJC, Zhou X, Breebaart J, Veldhuis RNJ, and Busch C. Multialgorithm Fusion with Template Protection. In *In IEEE 3rd International Conference on Biometrics:Theory, Applications, and Systems*, pages 1–8, 2009.