EFFICIENT AND PRIVACY PRESERVING ONLINE FINGERPRINT AUTHENTICATION SCHEME OVER OUTSOURCED DATA

к. Steephenraj[1], Vishnupriya. N[2], Priyalatha. S[3], Pavyasri. S[4], Vasantha. S[5]

[1]Assistant Professor, Department Of Computer Science & Engineering. Vivekanandha College Of Technology For Women, Namakkal Tamilnadu, India.

[2,3,4,5]Ug Scholar, Department Of Computer Science & Engineering. Vivekanandha College Of Technology For Women, Namakkal, Tamil nadu, India

ABSTRACT

Frameworks for Programmed Finger Impression Acknowledgment from that point forward, Show Assault (Dad) has undermined (AFRSs). its presence Subsequently, it is liked to foster a compelling show. Approaches for assault identification (Cushion). In any case, the unexpected as make Cushion a troublesome issue. This article recommends once more Optical Intelligibility One-Class Cushion (OCPAD) move toward Innovation based unique mark Dad discovery utilizing pictures (OCT). The recommended OCPAD model was found during preparing. Set just incorporates Huge fires (for example genuine fingerprints). The Inert coding and remaking mistake got from the prepared. The proposed model purposes an auto-encoder network as the accompanying spoons score calculation depends on. To get We give an initiation technique to a more exact recreation blunder. Utilizing a guide based weighting approach, the precision of error in recreation. We test different insights and distance measures lastly utilize a choice level combination to make the forecast. Our tests are performed utilizing a dataset with 93200 huge fire examines and 48400 Dad checks. The outcomes show that the proposed OCPAD can accomplish a Genuine Positive Rate (TPR) of 99.43% when the Bogus Positive Rate (FPR)equals to 10% and a TPR of 96.59% when FPR = 5%, which essentially beat an element based approach and regulated learning based model requiring PAs for preparing.

1. INTRODUCTION

1.1 IMAGE PROCESSING

Picture handling includes changing the idea of a picture either work on its pictorial data for human translation or render it more appropriate for independent machine discernment. The advanced picture handling, which includes utilizing a PC to change the idea of a computerized image. The computerized picture characterizes as a two-layered capability, f (x, y), where x and y are spatial (plane) arranges, and the sufficiency off at any sets of directions (x, y) is known as the power or dim level of the picture by then. At the point when x, y, and the sufficiency upsides off are limited, discrete amounts. The field of computerized picture handling alludes to handling computerized pictures through a computerized PC. Note that a computerized picture is made out of a limited number of components, every one of which has a specific area and worth and the components are alluded to as picture components, picture components, pels, and pixels. Pixel is the term most broadly used to mean the components of a computerized picture.

1.2 CSC DETECTOR IMAGE DATA HIDING

Somewhat recently many advances have been made in the space of computerized media, and much concern has emerged with respect to steganography for computerized media. Steganography is a solitary strategy for data concealing methods. It implants messages into a host medium to cover secret messages so as not to stimulate doubt by a busybody. A regular steganography application incorporates secretive correspondences between two gatherings whose presence is obscure to a potential assailant and whose achievement relies upon recognizing the presence of this correspondence. By and large, the host medium utilized in steganography incorporates significant advanced media like advanced picture, text, sound, video, 3D model, and so forth. An enormous number of picture stenographic calculations have been researched with the rising ubiquity and utilization of computerized pictures. Most picture stenographic calculations embrace a current picture as a cover medium. The cost of inserting secret messages into this cover picture is the picture mutilation experienced in the stego picture. This prompts two downsides. In the first place, since the size of the cover picture is fixed, the more mystery messages which are implanted consider more picture mutilation. Subsequently, a trade off should be arrived at between the implanting limit and the picture quality which brings about the restricted limit gave in a particular cover picture. Review that picture steganalysis is a methodology used to identify secret messages concealed in the stego picture. A stego picture contains some bending, and paying little mind to how minute it is, this will slow down the regular elements of the cover picture. This prompts the second disadvantage since it is as yet conceivable that a picture steganalytic calculation can overcome the picture

steganography and subsequently uncover that a secret message is being passed on in a stego picture. This paper proposes an original methodology for steganography utilizing reversible surface blend. A surface union cycle re-tests a little surface picture drawn by a craftsman or caught in a photo to combine another surface picture with a comparable nearby appearance and erratic size. We mesh the surface amalgamation process into steganography covering secret messages as well as the source surface. Specifically, as opposed to utilizing a current cover picture to conceal messages, our calculation hides the source surface picture and installs secret messages through the course of surface union. This permits us to extricate the mystery messages and the source surface from a stego engineered surface. Supposedly, steganography exploiting the reversibility has at any point been introduced inside the writing of surface combination. This approach offers three benefits. To begin with, since the surface union can integrate an erratic size of surface pictures, the inserting limit which our plan offers is corresponding to the size of the stego surface picture. Furthermore, a steganalytic calculation isn't probably going to overcome this stenographic approach since the stego surface picture is made out of a source surface instead of by changing the current picture contents. Third, the reversible ability acquired from our plan gives usefulness to recuperate the source surface. Since the recuperated source surface is the very same as the first source surface, it tends to be utilized to continue onto the second round of mystery messages for steganography if necessary. Trial results have checked that our proposed calculation can give different quantities of installing limits, produce outwardly conceivable surface pictures, and recuperate the source surface. Hypothetical examination shows that there is an irrelevant likelihood of separating our stenographic approach, and the plan can oppose a RS steganalysis assault.

2. LITERATURE REVIEW

2.1 Fingerprint Identification Combining the Discrete Wavelet Transform with the Support Vector Machine

In this review, Shahid Akbar proposes Unique mark acknowledgment is frequently used in biometric and security frameworks, which are generally utilized for various wellbeing estimates in different areas of public guard associations. Given the significance of biometric frameworks, various endeavors to identify fingerprints have been grown, yet there are as yet specific issues that request further consideration and request. In such manner, we need to create a solid biometric framework for unique finger impression acknowledgment. The computational model proposed utilizes three discrete element extraction strategies: The Discrete Wavelet change, Head Part Examination, and the Discrete Cosine Change. The classification suspicions utilized are Backing Vector Machine (SVM) and K-closest neighbor. Three free benchmark unique finger impression datasets and 10-overlap cross approval are used to assess the proposed model's exhibition. SVM performed really well on every one of the three benchmark datasets, as per the exact outcomes. The proposed model has been laid out to be a valuable and high-throughput device for scholastics and security-related sectors. The name "biometric" is gotten from the Greek expression "to quantify life." Biometrics is the investigation of physiological or social qualities of people to recognize people. To recognize an individual, the biometrics framework utilizes data that is extraordinary, invariant, reliable, and dependable, instead of run of the mill secret key based ID strategies. Finger impression ID is perceived as one of the most experienced and reliable biometrics strategies because of its one of a kind and unmistakable characteristics.

2.2 The State of Fingerprint Recognition Today

In this review, U. U. Manikdurge proposes. A biometric framework utilizes conduct and physiological biometric data to recognize an individual. The perceiving framework underscores on nearby edge properties like edge endpoints, small details, center point, delta, etc. Be that as it may, unique finger impression pictures are of low quality because of varieties in skin and engraving settings. Unique finger impression acknowledgment is habitually perceived as the most prestigious and dependable strategy for matching kept fingerprints in a data set in the field of individual character. A few systems and calculations for accomplishing precise acknowledgment results are examined. A more fundamental stage in unique finger impression matching is the extraction of details. The reason for this work is to introduce an outline of various element extraction and matching calculations for finger impression acknowledgment frameworks to figure out which system is the most dependable and secure. Biometrics is the investigation of human uniqueness in light of at least one physical or conduct qualities. Since biometrics is a special characteristic that each human has, no passwords or ID papers are required. Biometric attributes are grouped into two sorts. Physiological person: This is connected with body shape thus differs from one individual to another. Models incorporate fingerprints, face acknowledgment, finger math, and iris acknowledgment. It is worried about an individual's way of behaving like mark, voice, etc. Conduct attributes might change with age. The biometric framework can be utilized in confirmation or recognizable proof mode, contingent upon the requests of the application. The correlation of properties in a question finger impression picture with those in a data set is known as distinguishing proof. 1: n correlations are expected by the strategy. Thus, the activity is tedious. Conversely, confirmation is a moderately simple and quick

activity where a question unique mark picture matched with a personality number is given to the framework, and the framework looks at this biometric information to data set data in setting with the character number. Check is a quicker, more dependable, more vigorous interaction than recognizable proof since it includes a 1:1 correlation.

2.3 A Reliable Fingerprint Recognition System

As per Dr. R. Satya Prasad, fingerprints have been one of the most broadly involved strategies for human acknowledgment for more than 100 years; computerized biometric innovations have simply of late been accessible. Most biometric frameworks catch perceptions of a person's biometric utilizing normal sensors, like a computerized camera; elective sensors should be explored. This exploration will offer a compelling unique finger impression acknowledgment framework that will be utilized in a few cycles, including finger impression picture catch, finger impression disengagement, finger impression upgrade, and component extraction. The introduced framework is said to have tried two unique finger impression pictures for the left and right thumbs, with great outcomes. Biometrics can be utilized to distinguish individuals in circumstances where they should be recognized. Applications length from coherent PC admittance to actual admittance to a solid working environment or office. They might be utilized as distinguishing proof frameworks in an assortment of assortment conditions. Biometrics are likewise utilized in responsibility applications, for example, recording the biometric characters of travelers on an airplane, getting paperwork done for a piece of hardware, or following the chain of proof. Obviously, biometrics work better in controlled conditions like workplaces and labs than in uncontrolled conditions like the outside. A standard biometric framework comprises of five connected parts. A sensor is utilized to gather information and convert it to computerized design. Quality control obligations are performed by signal handling calculations, and the biometric layout is made. An information stockpiling part saves information that will be contrasted with new biometric formats. The new biometric format is contrasted with at least one recently put away layouts by a matching calculation. At last, a choice interaction (either mechanized or human-helped) goes with a framework level choice in light of the matching part results.

2.4 A reliable fingerprint matching algorithm

In this review, Ying HAO proposes in computerized finger impression recognizable proof frameworks, unique mark matching is a fundamental stage (AFIS). Customary methods treat this issue as point design coordinating, which is successfully an unmanageable issue because of the different nonlinear misshapenings usually saw in unique finger impression pictures. In this paper, we portray a compelling unique mark matching strategy in view of mistake spread. To start, edge data and the Hough change are utilized to track down a few sets of matching particulars, which are then used to work out the normal area of two fingerprints and the arrangement boundaries. A Matched Set is shaped by consolidating the correspondence and its encompassing matching particulars matches. The accompanying matching method is persuaded by the idea of mistake engendering: the matching blunders of each unequaled details are assessed in light of those of its most pertinent neighbor particulars. To forestall being deceived by befuddled details pairings, we utilize an adaptable engendering methodology. The consequences of the analyses uncover that our strategy is vigorous to nonlinear misshaping. The matching stage looks at the closeness of two unique finger impression includes and chooses if they have a place with a similar finger in light of a reference portrayal in the data set and an info portrayal got from an info picture. Most AFIS frameworks portray fingerprints utilizing particulars, for example, edge finishing and edge bifurcation, with each element separated by its area and direction. Utilizing this methodology, the matching issue is decreased to a point design matching issue. Matching in Jain's ideal model is all around as straightforward as counting the quantity of spatially covering highlights. Nonetheless, by and by, the detecting framework transforms the three-layered finger into two-layered pictures. At the point when the position, tension, and heading of the engraving change, so does the planning, bringing about nonlinear distortion of unique finger impression pictures. Between two finger impression pictures, interpretation, pivot, and, surprisingly, nonlinear disfigurement can happen. On the off chance that there is a huge time defer between two impressions, the pictures might vary because of finger wounds or skin disorder.

2.5 A Novel Thinning Algorithm for Fingerprint Recognition

This work was provided by Muzhir Shaban Al-Ani in this work. Many unique finger impression acknowledgment methods, with differed levels of exactness, were distributed a long time back. This examination takes a gander at existing unique mark acknowledgment calculations to expand the presentation of the proposed finger impression calculation and make a productive progressive framework. The proposed unique mark calculation expects to further develop the diminishing system. Finger impression improvement and details extraction are achievable with adequate diminishing. The outcomes uncover that the finger impression acknowledgment design has significantly better. The term biometric comes from the Greek words profiles (life) and measurements (estimating) (measure). People normally

perceive themselves by actual attributes like the face, eyes, finger, finger, iris, step, or voice. Perceiving individuals in view of their actual qualities has developed seriously fascinating in new innovations and applications on the grounds that a great many applications require exact check ways to deal with affirm a singular's recognizable proof. Passwords and ID cards have for quite some time been utilized to restrict admittance to safeguarded frameworks, but the two strategies are effortlessly broken and dishonest. Biometrics can't be acquired, taken, or neglected, and it is exceedingly difficult to produce one. In light of an impression of the edges in the skin of a finger, biometric ID is broadly used as proof in criminal examinations. A biometric framework is essentially an example acknowledgment framework that perceives an individual in view of an element vector made from a specific physiological or social characteristic moved by the person. The component vector is habitually kept in a data set whenever it has been extricated. Regardless of whether the last option is simpler to integrate into specific applications, a biometric framework in light of physiological boundaries is much of the time more dependable than one in view of social elements. The biometric framework can then work in one of two modes: confirmation or ID. While recognizable proof involves contrasting the acquired biometric information with layouts relating to all clients in the data set, check simply includes contrasting the expressed character with those formats. This implies that character and confirmation are two separate worries that should be managed independently.

3. EXISTING SYSTEM

The discrete wavelet change (DWT) is a typical technique for separating highlights, distinguishing edges, and recognizing objects. DWT is utilized for multi-goal examination with areas in the recurrence and time spaces. DWT is a useful answer for unique finger impression recognizable proof since it gets a powerful pace of recurrence parts. As far as computational time, DWT can give more exactness, power, adaptability, and effortlessness when contrasted with elective procedures.The visual sign is changed into moved and area exactness as far as area in the two-layered DWT (2D-DWT) approach, bringing about scaled duplicates of the essential wavelet to deliver DWT groups. DWT might dismantle pictures into sub-groups like low (LL), low-high (LH), high-low (HL), and high (HH). The low sub-band contains itemized data about the picture, the low-high sub-band contains flat data about the picture, the high-low sub-band contains vertical data about the picture, and the high sub-band has inclining information about the picture. Since it needs gathering a greater region to investigate.
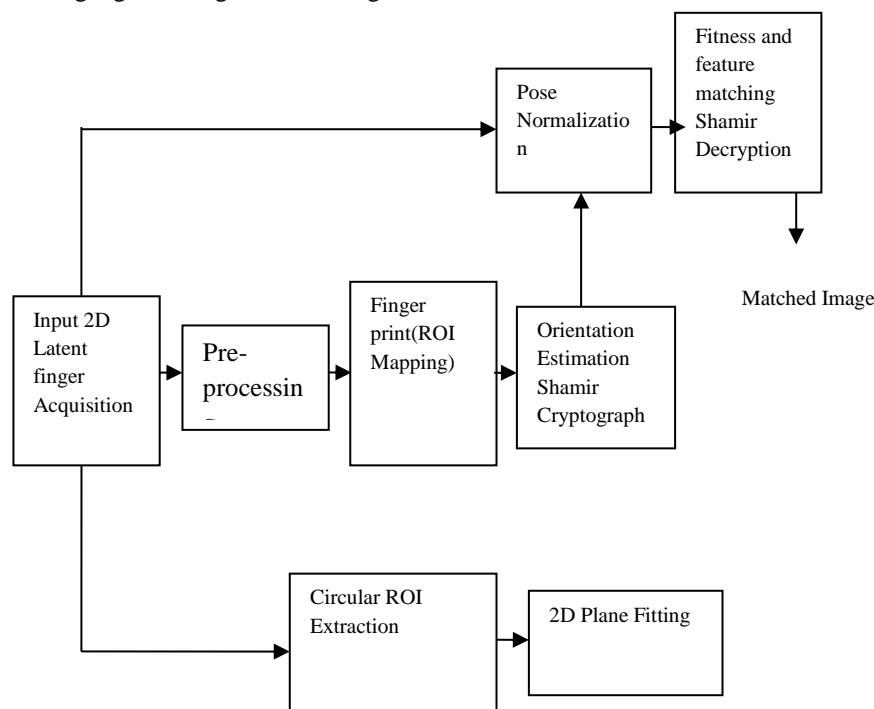
4. PROPOSED SYSTEM

The proposed system is involved the helpful blocks finger impression picture informational index, act changed reach and power pictures, and areas of premium (profit from starting capital venture) for finger estimation and finger impression incorporate extraction. This procedure, which relies upon the unmistakable verification of interfinger centers, may be found comprehensively. It should be focused on that since there is no get over between fingers in the position amended finger pictures, the interfinger centers can be definitively recognized. The fragment that follows gives a short summary of the part extraction methods of reasoning used in this work. A security-further developed

INTERNATIONAL JOURNAL OF PROGRESSIVE
RESEARCH IN ENGINEERING MANAGEMENT
AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 05, May 2023, pp : 452-459

e-ISSN :
2583-1062

Impact
Factor :
5.725

game plan free cushioned vault-set up novel finger impression cryptosystem based regarding coordinate polar (P) trifling subtleties structures was recommended. Two fingerprints are connected utilizing worldwide details matching calculations in view of their details. Every P small details structure is changed prior to being encoded into the fluffy vault to further develop security. The encoding approach utilizes a two-level secure sketch of a fluffy vault and Shamir's mystery sharing instrument. can be gathered when contrasted with ordinary techniques This makes it considerably more great for use in biometric ID frameworks. In spite of the way that it requires particular equipment to work, it could be basically integrated into different gadgets or frameworks. It has no open discernment issues since it is generally typically connected with endorsed admittance. Truly agreeable and equipped for working with any Inert unique mark arrangements. Time to figure is short. When contrasted with ordinary strategies, the Locale of Interest Idle finger impression acknowledgment qualities might be procured. This makes it considerably more great for use in biometric ID frameworks. Notwithstanding the way that it requires particular equipment to work, it could be essentially integrated into different gadgets or frameworks

4.1 MANAGER OF PRE-PROCESSING

This module is utilized to preprocess finger position variety pictures to find the finger in the recorded finger pictures. Since the force and reach pictures of the finger were caught almost at the same time, they were enlisted and related pixel by pixel. As a result, we pair the power picture and find the finger utilizing Otsu's edge. To improve these parallel pictures, morphological open administrators are used to eliminate separated uproarious spots. At long last, the arrangement of pixels comparing to the finger is viewed as the main associated part in the subsequent twofold picture. To lay out the finger community, we at first attempted an interfinger approach. Unique mark Planning: This step is separated into many segments, starting with distinguishing various fingerprints for every person and getting done with the use of a fundamental low pass channel to diminish commotion from photographs. Then, at that point, to accelerate the following phase of handling, resize all unique finger impression pictures to a similar size.

4.2 2-D FINGER GEOMETRY MAPPING

This application extricates 2-D finger calculation data from pairs finger power pictures. The finger math qualities utilized in this work are finger lengths and widths, finger edge, finger region, and finger broadness. Connecting estimations from every one of the four fingers yields an element vector. The Euclidean distance is utilized to compute the matching score between two component vectors from a matched sets of fingers. Due to impediment at the finger limits in the proposed pose standardization approach, the finger (finger) math qualities lose huge data. The heft of the finger at its limits isn't apparent to the scanner when turned about the hub, bringing about critical loss of data during stance remedy. Subsequently, the position changed power and reach pictures for fingers can recuperate a negligible part of the district of interest. Changing over variety pictures to grayscale: The age of grayscale pictures is the focal point of this stage. Grayscale pictures are made utilizing a variety to dim converter and are then prepared for the following phase of handling.

4.3 2-D FINGER PRINT ANALYZER

In this module, 2-D fingerprints made from range pictures of the finger (locale between finger valleys and the edge) give exceptionally recognizing characteristics to individual ID. The profundity and bend of finger lines and kinks in the 2-D unique finger impression are for the most part neighborhood surface elements. In this examination, we utilize the Surface Code 2-D finger impression portrayal from our earlier work. This straightforward portrayal depends on the calculation of the shape file at every area on the finger surface. In view of the worth of the structure record, every information point might be arranged into one of the nine surface sorts. From that point onward, the surface classification file is paired encoded with four pieces to make a Surface Code portrayal. The normalization The Hamming distance is utilized to ascertain the closeness of two component networks (Surface Codes). The method involved with social occasion conventional unique finger impression information, coordinating it, and making an interpretation of it into advanced finger impression pictures that are prepared for handling is known as finger impression securing. A smartcard has an assortment of haphazardly chosen client explicit refuse particulars credits, and just a negligible portion of this assortment is utilized at every procurement. To deliver a fixed-length hardened highlight, the waste details assortment is blended in with the format set. The proposed solidifying technique is imperceptible to the chart based unique matching calculation, which goes about as though the first format and inquiry credits are utilized. Our discoveries show that biometric solidifying diminishes mistake rates to 0% while recognizing certified and faker populaces by significant degrees.

4.4 FINGER PRINT EXTRACTION AND POSE ANALYZER

This module gathers and jelly 2-D finger presents in a data set of without contact finger photographs; we fostered our own data set utilizing an economically accessible 2-D digitizer. The image catching innovation utilized in this study is

equivalent to that portrayed in. Members in our establishment's information assortment method were generally understudies who consented to contribute biometric data. The information base currently contains 1140 right finger photographs (2-D and similar 2-D) taken from 114 individuals. To add significant stance changes into the data set, subjects were encouraged to offer their finger in five unmistakable positions. Unique finger impression Upgrade: The picture is further developed utilizing the histogram adjustment strategy at this step. The picture will be cleaner and less complex to peruse by applying picture improvement, a fruitful methodology for helping picture subtleties, and the picture will have a decent element that gives significant information for the accompanying step. In Shamir's Mystery Sharing Plan, a mystery esteem 'S' is broken into 'n' parts, and at least 'k' parts are expected to remake the mystery, where k is the quantity of parts. Individual offers are inadequate all alone and can't be utilized to remake the mystery. Secret sharing is a strategy for spreading confidential among a gathering, every one of whom is given a portion of the mystery. Shamir's Edge Plan alludes to a Mystery Sharing Calculation. <=n. Unique mark Element Extraction: This stage permits the highlights to be removed. To deliver the ideal characteristics for every person, three degrees of 2D-DWT are utilized. 2D-DWT is a successful strategy for removing credits that are significant in arriving at an official choice. The applied procedure blended highlights (right thumb elements and left thumb highlights) in this stage to fabricate a half and half method of successful factual strategy to extricate the viable elements for every individual.

5. CONCLUSION

For genuine esteemed finger impression coordinating, we proposed an original element dimensionality decrease procedure. In view of their small details, two fingerprints are associated utilizing worldwide particulars matching calculations. To fortify security, every P small details structure is altered prior to being encoded into the fluffy vault. As far as execution, our proposed technique beats existing component extraction calculations. Our relative exploration shows that our proposed highlight dimensionality decrease procedure beats the DWT technique as far as minimized highlight vector execution as far as acknowledgment rate and ROC. Subsequently, the P strategy is quicker than the DCT technique, which requires an assortment of channels at different points and frequencies. The essential benefit of our proposed highlight dimensionality decrease method is that it requires genuinely esteemed activities. The District of Interest Idle unique finger impression acknowledgment highlights might be acquired when contrasted with standard methodology. Thus, it is much more appropriate for use in biometric distinguishing proof frameworks. There are two levels of security in this framework: the client secret word and the biometric capability. In the event that the client's finger impression is lifted, he might decide to utilize a similar finger impression however with an alternate secret word.

6. FUTURE ENHANCEMENT

While the proposed approach for certified unique mark matching utilizing a clever component dimensionality decrease method seems promising, there are a few roads for future work that could additionally work on its viability and pertinence. Right off the bat, the methodology could be tried and approved involving a bigger dataset to evaluate its exhibition in genuine situations. This could include testing the methodology with fingerprints got from a more extensive scope of people with various segment and physiological qualities. Also, the methodology could be reached out to incorporate other biometric modalities, for example, facial acknowledgment or iris acknowledgment to upgrade the exactness and security of the framework. Thirdly, the methodology could be enhanced for cell phones with restricted computational assets to work on its convenience and availability. This could include investigating lightweight calculations or lessening the intricacy of existing calculations to empower them to run productively on cell phones. At last, the proposed approach could be incorporated with existing security frameworks, for example, access control frameworks or cell phone security frameworks to upgrade their general security and exactness. All in all, the proposed approach for veritable finger impression matching utilizing a clever component dimensionality decrease strategy offers a promising answer for biometric distinguishing proof frameworks. Be that as it may, further innovative work is important to completely understand its true capacity and work on its viability in genuine situations.

7. RESULT
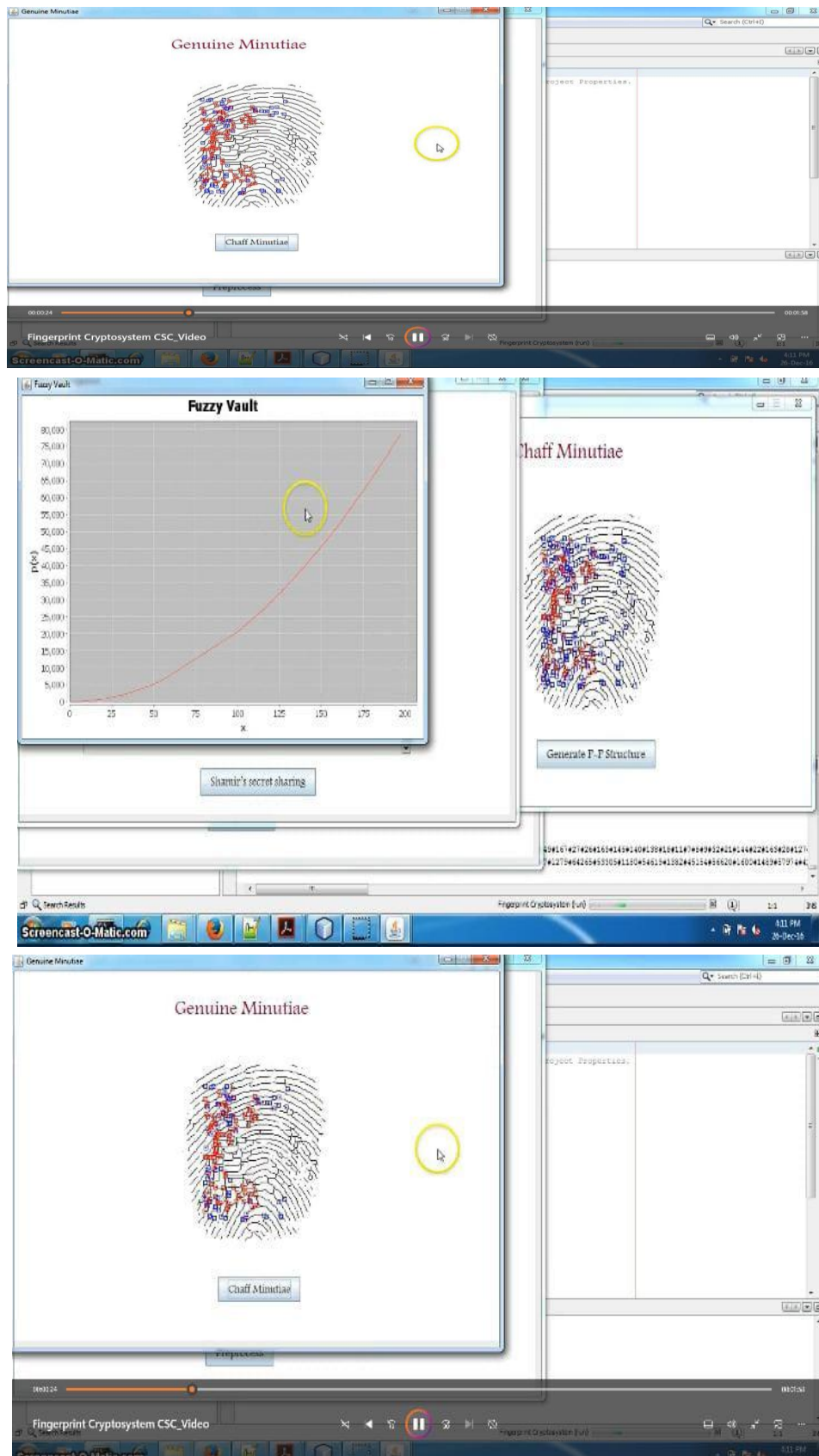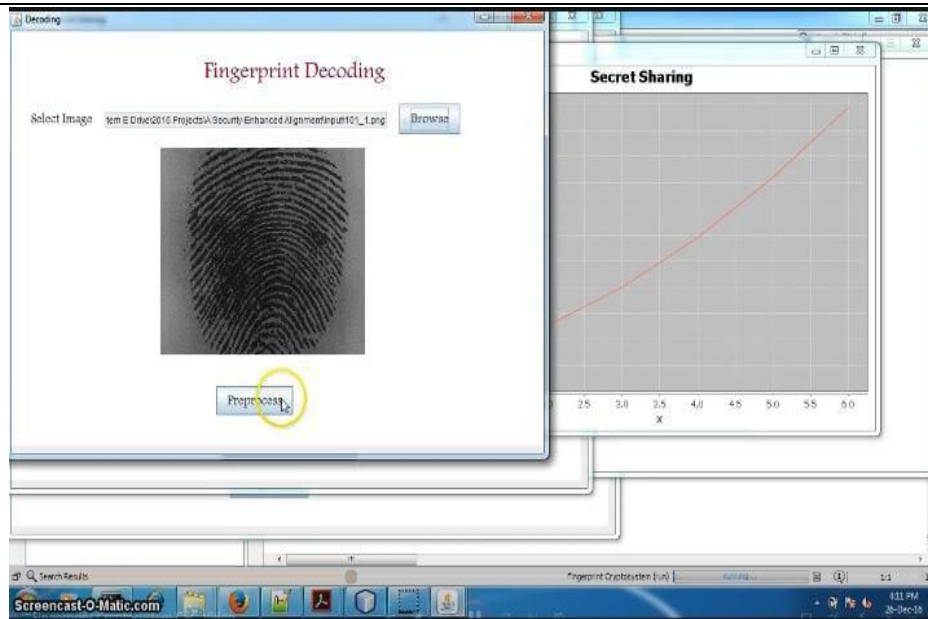
8. REFERENCES

[1] Maio, A. Fingerbook of Unique finger impression Acknowledgment, second Release, Springer-Verlag, 2021. K. Jain and S. Prabhakar.

[2] S. "Biometric Acknowledgment: Security and Protection Concerns," Prabhakar, S. Pankanti, and A. K. Jain, IEEE Security and Protection, Walk/April 2020, pp.33-42.

[3] A. L. Hong, K. Jain, and Y. Kulkarni, "A multimodal biometric framework incorporating unique finger impression, face, and discourse," Second Global Gathering on AVBPA (Washington D.C., USA), Walk 2021, pp. 182-187.

[4] A. K. Jain, A. Ross, and S. Prabhkar, "A Prologue to Biometric Acknowledgment," IEEE Exchanges on Circuits and Frameworks for Video Innovation, Vl. 14, pp. 4-20, 2021.

[5] S. Ribaric and I. Fratric, "A Biometric Distinguishing Proof Framework In view of Eigen Finger and Eigen Finger Highlights," IEEE Exchanges on Example Examination and Machine Knowledge, Vol. 27 (11), 2020, pp. 1698-1709.

[6] A. Jain, L. Hong and S. Pankanti, "Biometricidentification," Communications of the ACM,vol. 43, no. 2, pp. 90-98, 2000.

[7] R. Allen, P.Sankar and S.Prabhakar, "Fingerprint identification technology," Biometric Systems, pp. 22-61, 2005.

[8] J. de Mira, H. Neto, E. Neves, et al., "Biometric-oriented Iris Identification Based on Mathematical Morphology," Journal of Signal Processing Systems, vol. 80, no. 2, pp. 181-195,2015.

[9] S. Romdhani, V. Blanz and T. Vetter, "Face identification by fitting a 3d morphable model using linear shape and texture error functions," in European Conference on Computer Vision, pp. 3-19, 2002.

[10] H. Delfs, H. Knebl, and H. Knebl, "Introduction to cryptography," Berlin etc.: Springer, 2002.