3rd National Conference on Enhancement in Biomedical Engineering and Healthcare
Organised by Department of Biomedical Engineering,
Adhiyamaan College of Engineering, Hosur, Tamil Nadu, India

Contactless Biometric Fingerprint and Signature Identification and Verification

Dr. D. Thilagavathy[1], N. Deepasri[2], P. Gahana[3], S. Nivethasree[4], M. Varshini[5]

[1]Professor, Department of IT, Adhiyamaan College of Engineering (Autonomous), Dr. M. G. R. Nagar, Hosur, Tamil Nadu, India

[2-5]UG Student, Department of IT, Adhiyamaan College of Engineering (Autonomous), Dr. M. G. R. Nagar, Hosur, Tamil Nadu, India

ABSTRACT

To query the biometric and fingerprint and signature identification, the database communicates with a single secure server as if the entire database is stored in it. In CSP, outsourced encrypted biometric and fingerprint and signature identification are stored in a distributed manner, whereas the secure server manages the query processing on such a distributed database. The desired data will be distributed and stored in secure servers which increases the verification of accessing data. It stores data in a particular cloud server from which the server distributes them based on availability and performance. It increases the security of the verification process by comparing the details stored. Study on signature and finger knuckle patterns has attracted increasing attention for the automated biometric signature identification. Signature and finger knuckle pattern is essentially a biometric identifier and the usage or availability of 2D knuckles and key limitations to avail biometric identifiers. So the proposal since proposes 2D signature and finger knuckle collection of data, which was gathered from various sources using a photometric imaging stereo approach. This paper investigates on 2D information from signature and finger knuckle patterns and introduces a new feature descriptor to extract discriminative features for accurate signature and finger knuckle matching. An individuality model for the proposed feature descriptor is also presented. Expected experimental analysis by consuming state of the art technology on the signature and finger pattern executes and validates the efficiency of the proposal. This process is verified from the obtained results, using the state of the art technique, signature and fingerprint collection patterns on available datasets that are distributed.

Keywords : Service Oriented Architecture (SOA), State-of- the-Art, Support Vector Machine (SVM), Deep Neural Network (DNN), Knuckle Patterns.

I. INTRODUCTION

Biometric technologies offer enormous potential to meet a range of security requirements for the automated and efficient recognition of humans. Among various biometric identifiers, the fingerprint is probably the most widely deployed biometrics for e-governance, e-business and a range of law-enforcement applications. Other biometric identifiers such as the face, iris, palm print, or vascular pattern shave also established their usefulness for a range of applications. The usefulness of biometric identifiers depends on the nature of application requirements including the accuracy, efficiency and importantly the user convenience. Several challenges have emerged with the biometric recognition deployments using fingerprints. The degradation in finger-print matching accuracy due to frequent skin deformations, residual dirt, sweat, moisture and/or scars, is well-known while a large number of manual laborers and elderly population also suffer from fingerprints with less than acceptable quality for the identification. The NIST report submitted for the US Congress stated that about 2% of the population does not have usable fingerprints. Similar conclusions have also been reported in a large-scale proof of concept study from UIDAI which stated that about 1.9% of subjects cannot be reliably authenticated by using their fingerprints. The finger knuckle patterns can be simultaneously imaged during the fingerprint identification and are less susceptible to damages during daily life activities. The finger knuckle patterns can be more conveniently imaged from a distance, unlike fingerprints, as the major creases and curved patterns are easily visible with naked eyes. In summary, there are reasonable arguments to indicate that the addition of finger knuckle patterns for biometric recognition could address some of the limitations with the usage of only fingerprints. Therefore, many more enterprises and individuals have moved their data, such as personal data and large archive system, into the cloud every day. The cloud has become a necessity for many of us for individual, enterprise, and government use. The cloud aims to reduce costs and helps the users focus on their core business instead of being impeded by IT obstacles. The major available technique in cloud computing is data virtualization. Cloud computing holds the proposals from Service Oriented Architecture (SOA) which help users to overcome issues into various processes that were combined to intimate an optimized result.

II. RELATED WORK

K. Getgen: An approach to probabilistic risk assessment of electrical system grounding is proposed. The method uses all significant factors that affect the risk of electrocution at substations and takes into account their probabilistic nature. The approach implements an accurate statistical description of IEC479-1 fibrillation and body impedance data, and it uses detailed computer simulations of the modeled grounding system to provide safety level distributions that take into account the individual's presence at a site as a random variable. Variation in the power system fault level is accounted for, and extensive data of actual system fault clearance time are included. It is proposed that the probabilistic risk assessment is utilized as a second stage of the grounding system assessment when the first-stage deterministic analysis requires expensive or impractical mitigation. Implementation of the second stage probabilistic risk assessment yields a measure of individual risk. This is then benchmarked against industry-accepted "as low as reasonably practicable" values to determine whether an investment in mitigation is required. To illustrate the applicability of the proposed approach, the probabilistic risk assessment is applied to a practical case study of a transmission substation.

C. Gentry: In this paper, a new architecture for accelerating homomorphic function evaluation on FPGA is proposed. The architecture is based on a parallel cached NTT algorithm with an overall time complexity $O(\sqrt{N} \log \sqrt{N})$. The architecture has been implemented on Xilinx Virtex 7 XC7V1140T FPGA that achieves a 60% utilization ratio. The implementation performs a 32-bit 2^{16}-point NTT algorithm in 23.8 μs which is a 2x speedup over the state of the art architectures. The architecture has been evaluated by computing a block of each of the AES and SIMON-64/128 on the LTV and YASHE schemes. The proposed architecture can evaluate the AES circuit using the LTV scheme in 4 minutes while processing 2048 blocks in parallel. This leads to an amortized performance of 117 ms/block, which is the fastest performance reported to the best of our knowledge.

R. A. Popa: OpenEHR is an open standard specification for developing a flexible electronic health record (EHR) management system. It defines the standard service models and APIs and offers a whole lifetime data storage method to the patient's record. As an important OpenEHR system component, EHRServer plays the role of back-end services repository for data storage and query. It complies with the OpenEHR specifications and adopts the MySQL database. However, level EHRServer has many limitations. For example, its official requirement stresses that one organization cannot access the EHR owned by other organizations. The original EHRServer database is in plaintext format. It can lead to the risk of electronic record leakage. Encryption is one common protection method, but the level EHRServer APIs do not support encrypted data queries. That restricts building EHRServer on the cloud. What's more, the inconvenience of information sharing among different organizations may also hinder the extension of OpenEHR coverage to more domains and countries. To solve the above open problems, in this paper, we explore two approaches that guarantee the security and flexibility of sharing EHR on the cloud and thus propose a new architecture called Crypt-EHRServer. Firstly, we use attribute-based encryption to realize flexible EHR access authority for different authorized organizations. Secondly, we learn from an efficient ciphertext query model, CryptDB, and adopt their onion encryption approach to support standard SQL queries on the encrypted EHR. The result of our work could provide a flexible, scalable and secure EHR system. Crypt-EHRServer will benefit OpenEHR's widespread adoption in the world, and will also arouse people's awareness about incorporating security criteria into the design of electronic health records management systems.

M. F. Kaashoek: Data mining is a powerful new technique to discover knowledge within a large amount of data. A number of theoretical and practical clarifications to query processing have been proposed under various scenarios. With the recent popularity of cloud computing, data owners now have the opportunity to outsource not only their data but also data processing functionalities to the cloud. Because of data security and personal privacy concerns, sensitive data (e.g., medical records) should be encrypted before being outsourced to a cloud, and the cloud should perform query processing tasks on the encrypted data only. These tasks are termed as Privacy-Preserving Query Processing (PPQP) over encrypted data. These protocols protect the confidentiality of the stored data, user queries, and data access patterns from cloud service providers and other unauthorized users. Several queries were considered in an attempt to create a well-defined scope. These queries included the k-Nearest Neighbor (kNN) query, advanced analytical query, and correlated range query. This paper presents protocols utilize additive cryptography-based privacy-preserving data mining technique at different stages of query processing to achieve the best performance all computations can be done on the encrypted data.

N. Zeldovich: With the rapid increase of Internet users, network security becomes very essential. Cryptography plays a major role in network security. However, cryptographic systems consume considerable amounts of resources, like memory, CPU time, encryption and decryption time. In this paper, we compared the most common block cipher modes of operation on AES according to the recommendations of the National Institute of Standards and Technology (NIST). The comparison is done in terms of encryption time, decryption time, and throughput with variable data packet sizes. The results of the comparison are summarized and our observations are highlighted to help to make an informative decision when choosing the mode of operations for different applications with symmetric-key ciphers.

III. PROBLEM AND MODEL DESCRIPTION

To address this security problem, there have been many proposed solutions: using homomorphic linear regression to analyze the fingerprint and as well as the signature verification of a trusted coprocessor. However, they are either incomplete or infeasible (with low efficiency). In this paper, we propose a novel system architecture called RPA Region Proposal Algorithm, which is based on re-designing the processor architecture to support arbitrary computation. Our design tightly couples the original data with the collection of information that has been stored in the database or in the dataset that has been proposed architecture. With our method, the comparison can be attained with better accuracy and the compared result has been optimized with accuracy. Our main contributions are as follows: To the best of our knowledge, it is the first to use processor architectural design to successfully protect remote operation on signature as well as the fingerprint knuckle patterns database against any honest-but-curious administrator.

This paper addresses the key limitations of levelly available finger knuckle identification technologies by developing a 2D finger knuckle feature extraction and matching model that can simultaneously recover extended finger knuckle features from finger knuckle images reconstructed from a single 2D imaging sensor. Simultaneous availability of information from the finger knuckle images not only offers significantly improved matching accuracy but can also ensure automated detection of sensor-level spoof attacks using printed knuckle images. Any direct application of known or popular feature descriptors, e.g. those designed for other biometric identifiers such as palm or fingerprint, is expected to offer limited performance. Instead, specialized feature extractors should be designed to recover the most discriminative information from the 2D finger knuckle patterns which is largely embedded in curves and creases with varying thickness. Some of the successful attempts in recovering fingerprints using photometric stereo require reconstruction or the integration of source information,

i.e. surface normal. The reconstruction process is generally complex, e.g. popular method used in requires FFT and IFFT which are known for their complexity, and are known to introduce errors in the reconstructed depth images. These errors are introduced as it is difficult to

find closed-form solutions for the integration, i.e., inerrability problem and mainly results from the discontinuities around irregular ridge valley boundaries during the re-construction. Therefore, any direct usage of source information from the surface normal vector scan not only enhances matching accuracy for knuckle images but can also help to reduce the complexity and is therefore highly desirable. The introduction of new finger knuckle modality also raises a fundamental question on the (theoretical) upper limit on the performance from this biometric modality. Therefore, the uniqueness of knuckle patterns needs to be established to answer some of such fundamental questions relating to finger knuckle patterns.

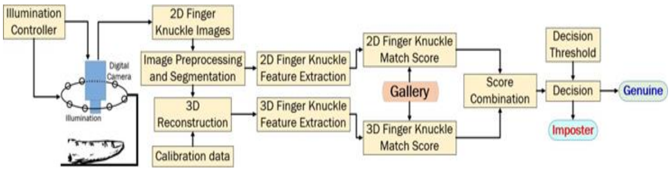
IV. SYSTEM IMPLEMENTATION

Finger Print Acquisition:

The concerned person's fingerprints have been stored and analyzed with the matching patterns and have been moved on to the storage for verification. To access that storage, the proper authentication policies have been needed. After acquiring the details, several fingerprint information can be gathered and manipulated to match and analyze the sequential patterns that have been already stored.

Upload and View File Details:

Each user who can access the cloud storage can upload their desired data to the cloud storage server. The entire data will be in an encrypted format in the cloud server. The admin i.e.: the cloud owner can view the file details such as size, location and as well as user can retrieve their data from the cloud server.



Verify Secret Key:

The cloud owner verifies the secret key provided by the user to access the data. The user maintains data privacy by using the honey encryption algorithm. Hence incase of an attack of data the breacher can't access the user data.

Verify Trapdoor and Unlinkability:

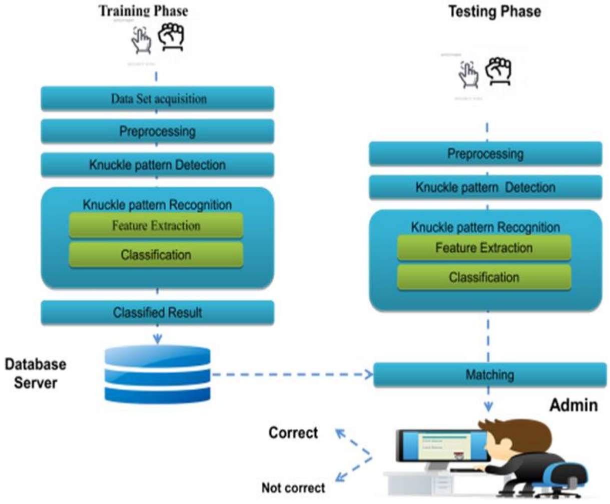
It has been done by the cloud owner i.e.: the server to gain knowledge about the tracker or the attacker. After knowing the attacker details the cloud owner can block or make unavailable status to the attacker for accessing the data of the user. The data of the user has been stored with a quiet higher security level.

View Request and Send Response:

The cloud server transfers the user data into secure nodes to make the security of the user data. The data has been stored in multiple secure nodes so that the gain zero knowledge about the user data. If the user sends the request to the server to retrieve the stored data, the server accesses the secure node and provides the data to the user.

View Attacker:

The cloud owner can view and block the attacker who tries to breach the data that has been stored in the secure node. The tracking of the attacker can be done based on identifying the IP or MAC address of the attacker. So that the data breacher can't access the data that has been stored in the secure node.



V. EXPERIMENTAL RESULT AND EXPECTED OUTCOMES

In the comparative work naive Bayes, the SVM algorithm is used to classify and the data set, and it also used the K-means clustering algorithm for prediction of air quality. Thus Air quality prediction system successfully diagnoses the data and predicts the Air quality. The results thus obtained shows that the K- Means clustering algorithm provides 86.58% of accuracy with minimum time.

Dataset Description

This data is a cleaner version of both 2D finger knuckle patterns and signature which provides a perfect asset. Datasets are gathered, stored and compared with the collection of datasets and matches the fingerprint knuckle patterns and signatures that are currently provided. Each data pacifies various stages of signature and fingerprint pattern information.

The dataset contains the following features:

1. ptn_code: Pattern code. A code is given to each pattern that recorded the data.
2. sampling date: The date when the data was recorded.
3. state: It represents the states whose fingerprint and fingerprint knuckle pattern quality of data is measured.
4. type: The type of pattern which specifies the measurement of each pattern.
5. SVM: Comparison done by support vector machine.
6. DNN: Patterns are deeply analyzed and processed.

Precision

In the field of information retrieval, precision is the fraction of retrieved patterns that are relevant to the query: For example, for a signature search on a set of patterns, precision is the number of correct results divided by the number of all returned results. Precision takes all retrieved fingerprint patterns or signature patterns into account, but it can also be evaluated at a given cut-off rank, considering only the topmost results returned by the system. This measure is called precision at n or P@n.

Precision is used with recall, the percent of all relevant patterns that are returned by the search. The two measures are sometimes used together in the process to provide a single measurement for a system.

Note that the meaning and usage of "precision" in the field of information retrieval differs from the definition of accuracy and precision within other branches of science and technology.

Recall

In information retrieval, recall is the fraction of the relevant patterns that are successfully retrieved. For example, for a fingerprint search on a set of datasets, recall is the number of correct results divided by the number of results that should have been returned.

In binary classification, recall is called sensitivity. It can be viewed as the probability that a relevant pattern is retrieved by the query.

It is trivial to achieve a recall of 100% by returning all patterns in response to any query. Therefore, recall alone is not enough but one needs to measure the number of non- relevant knuckle patterns also, for example by also computing the Precision.

Precision recall and F-Measure are then defined as

$$Preceision = tp/(tp + fp)$$

$$Recall = tp/(tp + fn)$$

$$\boldsymbol{Recall} = 2*[(\text{Precision}*\text{Recall})/\ (\text{Precision} + \text{Recall})]$$

Accuracy Rate

The below figure shows the Accuracy rate having value 96 % with the SVM (Support Vector Machine) Algorithm and DNN.

$$Accuracy = tp + tn/(tp + tn + fp + fn)$$

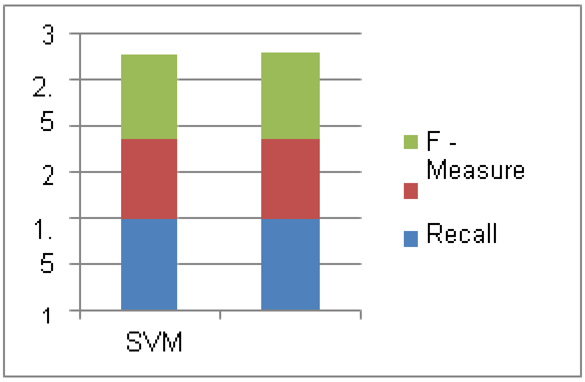
Whereas,
P – Precision R- Recall

F- (F-Measure) A - Accuracy

The below table represents the results of SVM and DNN in the signature pattern and fingerprint knuckle pattern and the accuracy obtained.

Methods	P	R	F	ACCURACY
SVM	0.98	0.895	0.92	92.98%,
DNN	0.95	0.896	0.94	92.66%,

The below graph provides the accuracy levels that have been obtained by considering precision, recall, and f-measure values, which concludes the accuracy in predicting the 2D signature verification and fingerprint knuckle patterns.



VI. CONCLUSION AND FUTURE WORK

Levelly available online finger knuckle identification systems only incorporate discriminative 2D information for user identification. This paper has investigated the development of a 2D finger knuckle identification system and also introduced a 2D finger knuckle image database, for the first time in the literature, for further research. Any direct application of existing 2D feature descriptors, like those developed for the 2D palmprint or 2D fingerprint identification, is not expected to recover most discriminative features from the 2D finger knuckle patterns. Therefore, the development of specialized feature descriptors is critical to realize the full potential from 2D finger knuckle biometrics. The feature descriptor introduced in this proposal addresses such objective and has shown to offer outperforming results. One of the fundamental questions relating to any new bio-metric modality relates to its uniqueness, or individuality of the finger knuckle biometrics, which has not yet been studied in the literature. This paper has attempted to address this problem by developing the individuality model for 2D finger knuckle patterns using the best performing feature descriptor.

Despite the advantages of the 2D finger knuckle identification, the deployment of a 2D finger knuckle identification system is more complex than that of a 2D finger knuckle identification system. Such an increase in complexity, over 2D systems, is largely due to the reconstruction or acquisition of 2D finger knuckle images. Among the existing 2D imaging technologies such as laser scanning, multi-view stereo, and structured lighting, our proposed new system adopted the photometric stereo approach due to its low cost, high-quality imaging, and simple deployment. This approach only requires a single fixed camera with at least three light sources, while more light sources may enhance the reconstruction accuracy. The key limitation of such an approach lies in its sensitivity towards the ambient illumination. Therefore, efforts are required to appropriately position the camera, select and fix the illuminators, which reduce the adverse influence from ambient illumination during the imaging. Such shortcomings are however worthy of the tradeoff of more accurate recognition and anti-spoofing performance, as also indicated from our results in the paper.

Our work or attempt to systematically evaluate the potential from 2D finger knuckle patterns for the biometric identification has achieved promising results. A lot more work, however, needs to be done to realize the full potential of this biometric identifier. Recovery of non-pixel-wise features or those based on the singularity of patterns, such as the minutiae features employed for matching fingerprints, is expected to be more effective (for higher accuracy and efficiency) than pixel-wise features and should be pursued in further extension of this work. Our attempts to achieve further performance improvement by incorporating popular deep learning-based methods were not effective and their performance is limited by the size of training data which is the key challenge for 2D finger knuckle data employed in this work. The individuality model presented in this paper has made assumptions on the mutual independence of match scores and has been justified as such a model can provide a theoretical upper limit on the performance expected from the 2D finger knuckle pat-terns. Incorporating interdependence of features, or the scores during the feature extraction process can provide more realistic estimates on the individuality and is suggested in the further extension of this work.

VII. REFERENCES

[1]. R. Billions, "Authorship of clinical trial documents," Medical Writing, vol. 25, pp. 33 – 35, 2016.

[2]. “Information Technology - Biometric Data Interchange Formats - Part 7: Signature/Sign Time Series Data,” ISO/IEC Standard 19794-7:2014, ISO/IEC JTC1, 2014.

[3]. "Information Technology - Biometric Performance Testing and Reporting - Part 3: modality-specific Testing," ISO/IEC TR Standard 19795- 3:2007, ISO/IEC JTC1, 2007.

[4]. “Information Technology - Biometric Presentation Attack Detection - Part 3: Testing and Reporting,” ISO/IEC Standard 30107-3, ISO/IEC JTC1, 2017

[5]. G. Dyer, B. Found, and D. Rogers, “Best practice manual for the forensic examination of handwriting,” European Network of Forensic Science Institutes (ENFSI), pp. 1–40, 2015

[6]. J. E. Douglas and C. Munn, “Modus operandi and the signature aspects of violent crime,” in Crime classification manual, 1992, pp. 259–268.

[7]. S. A. Slyter, Forensic signature examination. Charles C Thomas Publisher, 1995

[8]. G. Dyer, B. Found, and D. Rogers, “Visual attention and expertise for forensic signature analysis,” Journal of Forensic Sciences, vol. 51, no. 6, pp. 1397–1404, 2006

[9]. M. Diaz, M. A. Ferrer, D. Impedovo, M. I. Malik, G. Pirlo, and R. Plamondon, "A prospective analysis of handwritten signature technology," ACM Computing Surveys (CSUR), vol. 51, no. 6, pp. 1–39, 2019

[10]. L. G. Hafemann, R. Sabourin, and L. S. Oliveira, “Offline handwritten signature verification - literature review,” in Seventh Int. Conf. on Image Processing Theory, Tools and Applications (IPTA), Nov 2017, pp. 1–8.

[11]. M. I. Malik, M. Liwicki, L. Alewijnse, W. Ohyama, M. Blumenstein, and B. Found, "Signature Verification and Writer Identification Competitions for On- and Offline Skilled Forgeries (SigWiComp2013)," in 12th Int. Conf. on Document Analysis and Recognition, 2013, pp. 1477–1483.

[12]. M. I. Malik, S. Ahmed, A. Marcelli, U. Pal et al., “ICDAR2015 competition on signature verification and writer identification for on- and off-line skilled forgeries

(SigWIcomp2015)," in Int. Conf. on Document Analysis and Recognition (ICDAR), 2015, pp. 1186–1190.

[13]. H. Suwanwiwat et al., "Competition on thai student signatures and name components recognition and verification (TSNCRV2018)," in 16th Int. Conf. on Frontiers in Handwriting Recog. (ICFHR), 2018, pp. 500–505.

[14]. S.-H. Cha and S. N. Srihari, "Writer identification: Statistical analysis and dichotomizer," in Advances in Pattern Recognition, F. J. Ferri, J. M. Inesta, A. Amin, and P. Pudil, Eds. Springer Berlin Heidelberg, 2000, pp. 123-132.

[15]. S. N. Srihari, Aihua Xu, and M. K. Kalera, "Learning strategies and classification methods for off-line signature verification," in 9th Int. Workshop on Frontiers in Handwriting Recog., Oct 2004, pp. 161–166.

Cite this article as :

Dr. D. Thilagavathy, N. Deepasri, P. Gahana, S. Nivethasree, M. Varshini, "Contactless Biometric Fingerprint and Signature Identification and Verification", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 5 Issue 5, pp. 189-197, March-April 2020. Journal URL : http://ijsrst.com/EBHIT027