Novel Web Service Based Fingerprint Identification Using Steganography and Xml Mining

Praseetha V M[1], Ayush Dattagupta[1], Suma R[2], S. Vadivel[1]

[1] Department of Computer Science, BITS Pilani,
International Academic City, Dubai, UAE.
[2] Department of Computer Science, SJCET, Choondacherry,
Pala, Kottayam

praseethasunil@gmail.com

Abstract. Fingerprint recognition has been considered as the most popular and reliable system for web based person authentication. Fingerprints have unique patterns that can be used to distinguish one fingerprint from another. The fingerprint pattern can be used to enhance the security of existing authentication system by adding a layer of biometric security. In this paper we propose a novel algorithm that is able to distinguish the pattern of one fingerprint from the pattern of another fingerprint using XML mining. But the valuable fingerprint data of a user is at risk as it can be hacked during web based authentication and the data can be easily compromised. Therefore we further enhance the security by extracting the fingerprint features into an xml file and embed the same into an image file using steganography. The encoded file can be used for safe transmission of fingerprints across the web for bio metric authentication. Our proposed system uses a novel method in which xml mining is applied at the server side to make the fingerprint identification faster.

1. Introduction

Automatic personal identification is very important as our day to day life is getting digitized. Two categories of traditional personal identification are there: they are token based and knowledge based [1]. In the token based approach a person is identified based on what he/she has (physical key, ID card, passport, Badges, etc.) and in knowledge based approach a person is identified based on what he/she knows (ID number, password, PINs, etc.). However both these approaches have certain limitations. In the token based approach, the token can be easily stolen, lost, shared or can be duplicated. In knowledge based approach, the knowledge can be guessed, shared or forgotten. Biometric authentication/ identification systems overcome the above mentioned limitations and are widely accepted. Biometric based approaches are considered as the most promising option for identifying individuals. Among the various approaches fingerprint recognition is one of the oldest and most popular technique for recognizing people [2].

Fingerprint recognition is used in many areas like access control [3], law enforcement, forensic science to aid criminal investigation [4], biometric smart cards etc. The popularity is mainly because of the uniqueness of fingerprint images, the availability of inexpensive fingerprint readers and the fact that criminals often leave their fingerprints at crime scenes. A fingerprint is a unique pattern of ridges and valleys on a finger. There are different stages in a fingerprint recognition system as shown in figure 1. They are mainly fingerprint acquisition, feature extraction, and matching. The traditional method for acquiring fingerprint was by using ink and paper. But now, many modern techniques are there to get an image of the fingerprint. They include optical, capacitive, ultrasound and thermal fingerprint readers.

Fingerprint matching is very challenging since two images acquired at different time exactly under same conditions need not be exactly the same. The difficulty in matching is due to several reasons [5]. The translation and rotation of the fingerprint images, application of a poor feature extraction algorithm, displaced, false and missing minutiae and the non linear deformations of the images are some of the reasons. To overcome these variations a powerful matching algorithm is needed. So the matching algorithm should be invariant to translation and rotation of the images. It should return the correct result while comparing fingerprints from the same finger even the feature extractor has missed some features or even when the fingerprint images are affected by non linear distortions.
The fingerprint matching algorithm can generally be classified into three different classes.

- Correlation based matching algorithms [6] [7]which use superimpose two fingerprint images to find the correlation among pixels for different displacement and rotation.
- Minutiae based matching algorithms [8] [9]which use the extracted minutiae of two fingerprints to find the matching pairs of minutiae.
- Non minutiae based matching algorithms [10] [11] which use the orientation, shape or frequency of ridges to perform matching between two fingerprints.

Among the three classes minutiae based algorithms are the most common and minutiae based matching is considered as a point pattern matching problem.

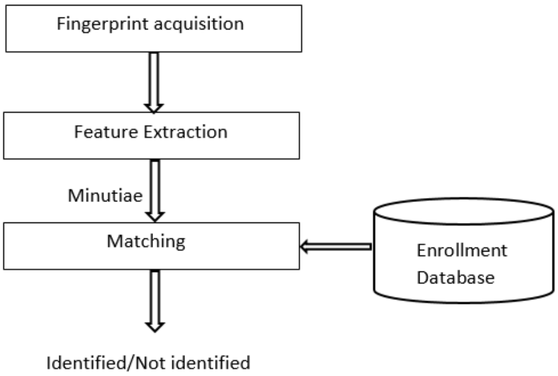


Figure 1. Different stages in fingerprint recognition

Our goal is to develop a soap enabled web service to perform authentication of a person using fingerprint. Towards this at the client end the finger print features are extracted, converted the features as an XML file and embedded the XML file into an image as part of improved security using steganography. The resultant image is sent in the form of a SOAP request to a web service. The hosted web service will extract the XML finger print data from the image and do the matching using XML data mining. In this paper we propose a secure, fast and accurate model for fingerprint verification.

The organization of this paper is as follows. Section 2 describes about the related works in this area, Section 3 explains the proposed model, Section 4 is about the extraction of features from a fingerprint image and creating the XML file using the minutiae triplets. Section 5 explains the technique of steganography to hide the fingerprint features. Section 6 explains the process of XML mining and fingerprint matching. In section 7 the results are discussed and section 8 is the conclusion and future scope of this work.

2. Related works

2.1. Transmission of Biometric Data

Lot of risk factors are there when biometric data is transmitted over communication channels. In the papers [12] [13] [14], the authors have mentioned about data hiding techniques using which biometric data are made hidden within another media. In [12], the authors use watermarking to hide the minutiae of fingerprint in a face or synthetic fingerprint. A random cover image is used to hide the biometric data in [15]. Before hiding the authors encrypt the biometric data using a key and then by using error correcting code the encrypted data is encoded. Finally the encoded biometric data is embedded bit by bit using the sign of discrete cosine transform. In [16] the authors describe about multimodal biometric system employing both fingerprint and face information using watermarking techniques. They tested two different scenarios where in the first scenario they used a fingerprint image as a cover work and hide facial features into it. In the second scenario they hide fingerprint features into a facial image. By comparing the two scenarios the authors have found that hiding fingerprint features in a facial image is better than hiding facial features in a fingerprint image in terms of the verification accuracy of the watermarked image.

2.2. Fingerprint Recognition

Fingerprint recognition can be considered as a complex pattern recognition problem. The design of accurate feature extraction and matching algorithms is a very complicated and challenging task. Researchers have proposed many methods for fingerprint identification.

A fingerprint recognition system which uses Fast Fourier Transform and Gabor filters is explained in [17]. In this method two fundamental types of minutiae, endpoints and bifurcations, are extracted and these extracted features are used to perform fingerprint recognition. A new method for automatically identifying rare features in fingerprints based on combining level 1 features and minutia-based triangular descriptors is described in [18]. A fingerprint feature that is rare has higher discriminatory power when it is identified in a print (latent or otherwise), and multiple rare features in a single print can increase discriminatory power dramatically. The authors observed that some rare 9-point feature was found within every fingerprint that was tested and some of these rare 9-point features occurred only once in 1000 fingerprints. A robust damaged fingerprint recognition algorithm, with simpler recognition process Convolution Neural Network (CNN) of deep learning is explained in [19].

A method based on local minutia topology which generated by local minutia around the core point is proposed in [20]. The topological relationship is built on the extracted minutiae and the core point. The authors found that the proposed model has high computational efficiency and a significant improvement on robustness. Wang Yuan et al. [21] proposed a novel approach for minutiae filtering in fingerprint images. They use directionally selective steerable wedge filters to discriminate between minutiae and non-minutiae regions with reasonable accuracy.

3. Proposed Model

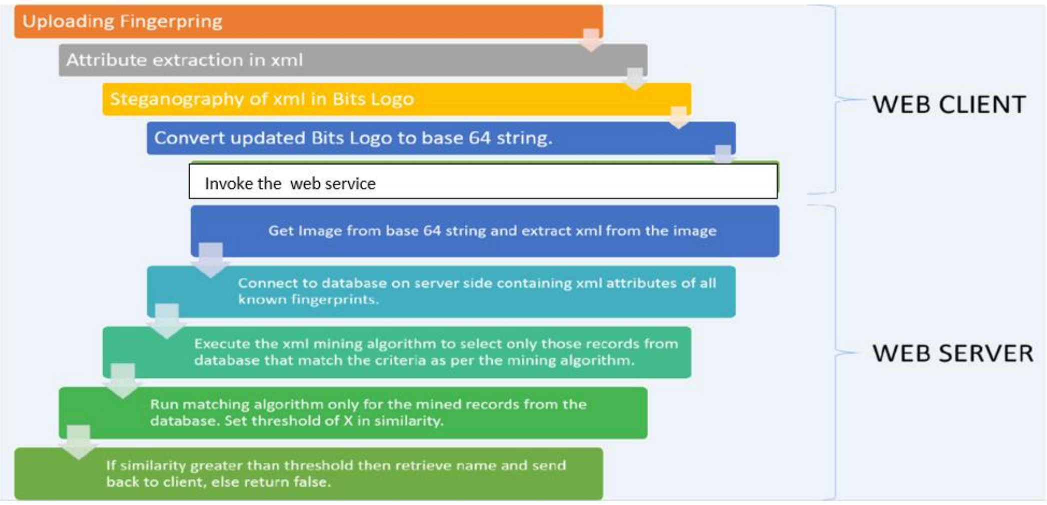

Uploading Fingerpring
Attribute extraction in xml
Steganography of xml in Bits Logo
Convert updated Bits Logo to base 64 string.
Invoke the web service
Get Image from base 64 string and extract xml from the image
Connect to database on server side containing xml attributes of all known fingerprints.
Execute the xml mining algorithm to select only those records from database that match the criteria as per the mining algorithm.
Run matching algorithm only for the mined records from the database. Set threshold of X in similarity.
If similarity greater than threshold then retrieve name and send back to client, else return false.
WEB CLIENT
WEB SERVER

Figure 2. Proposed Web service model

Service Oriented Architecture (SOA) is a platform independent design which give emphasis to reusability and interoperability. Regardless of the platform, the services provide a common way of interaction [22]. Web services provide services which are easily accessible [23] over a network and they are considered as common means to exchange data and information over the network. The client program will extract the minutiae of the fingerprint image to be identified and these minutiae are then embedded in a host image as an xml file. Thus the features are protected using steganography and then the host image with embedded fingerprint features are send to the web server by invoking a SOAP enabled web service where the identification is taking place.

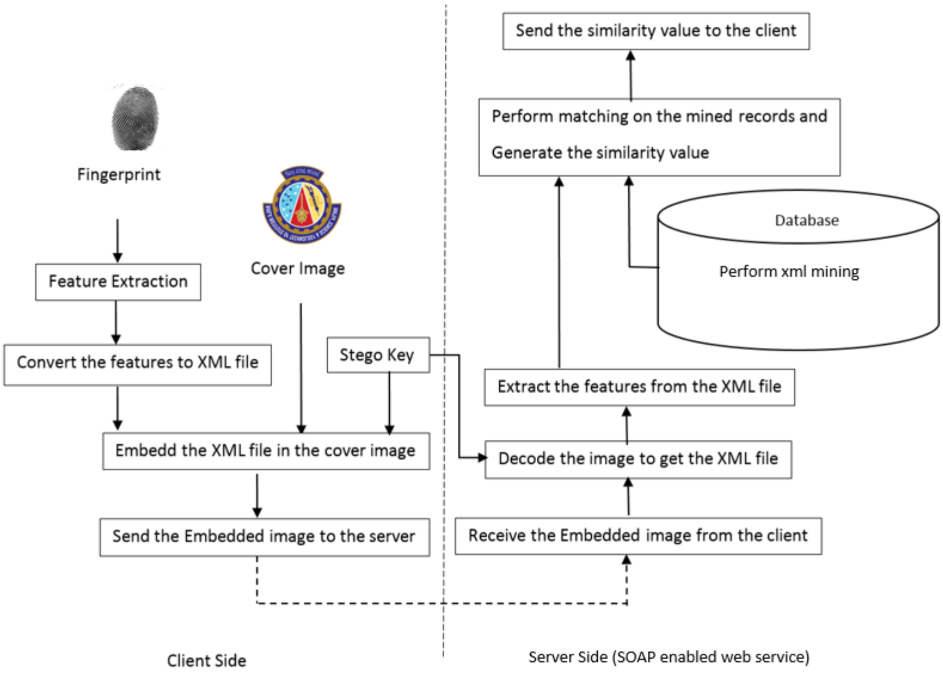

Fingerprint
Feature Extraction
Convert the features to XML file
Cover Image
Stego Key
Embedd the XML file in the cover image
Send the Embedded image to the server
Client Side
Send the similarity value to the client
Perform matching on the mined records and Generate the similarity value
Database
Perform xml mining
Extract the features from the XML file
Decode the image to get the XML file
Receive the Embedded image from the client
Server Side (SOAP enabled web service)

Figure 3. Client and server side operations of the proposed model

The client program will extract the minutiae of the fingerprint image to be identified and these minutiae are then embedded in a host image as an xml file. Thus the features are protected using steganography and then the host image with embedded fingerprint features are send to the web server by invoking a SOAP enabled web service where the identification is taking place. On the server an xml mining algorithm is executed to filter out the fingerprints from the database which contain the xml files corresponding to each fingerprint and to make the identification process easier. We have used a faster matching algorithm based on minutiae triplets known as the M3gl algorithm [24]. The result of the identification is then send back to the client.

4. Feature Extraction and XML file Generation

The three main categories of techniques used for fingerprint recognition are the minutiae-based (feature-based) matching, the pattern-based (or image-based) matching, and correlation-based matching [25]. Among the three, minutiae based technique is widely used as it is computationally inexpensive. The minutiae-based technique utilizes the rich local features of a fingerprint like ridge ending, bifurcation, crossover, island, lake etc. Figure 4. shows some of the important features that we need to extract from a fingerprint image in order to make an accurate recognition.

Here, we are considering the features like ridge ending, bifurcation and short ridge or independent ridge. The extracted fingerprint features are stored as (x,y,θ) where x and y give the coordinate of a particular feature and θ gives the angle of orientation of the feature. The extracted minutia data is converted to xml using xml serialization and some modifications to the framework classes to support xml formats. The modification have been made to the original framework itself and the changes can be observed in the Mtriplet extractor class of the framework.

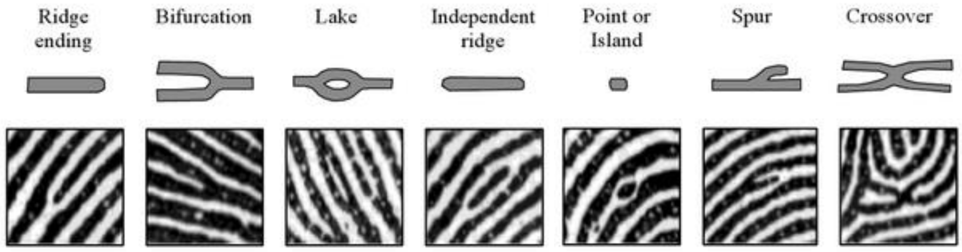


Figure 4. Fingerprint features

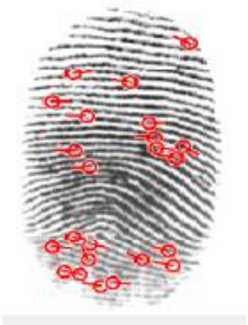
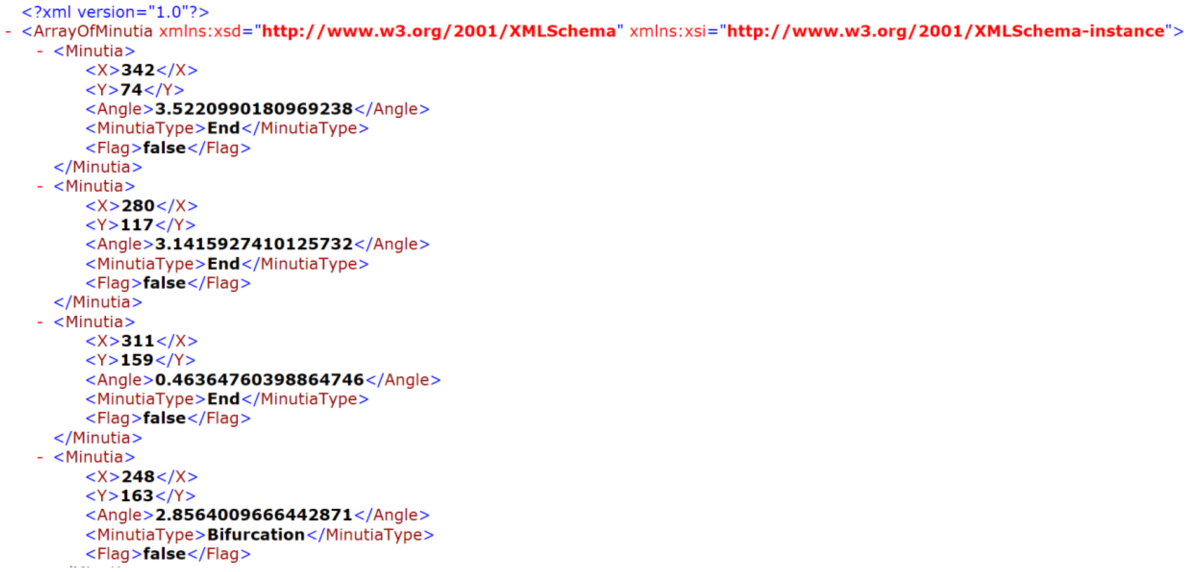


Figure 5. Extracted minutiae



```
  <?xml version="1.0"?>
- <ArrayOfMinutia xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  - <Minutia>
        <X>342</X>
        <Y>74</Y>
        <Angle>3.5220990180969238</Angle>
        <MinutiaType>End</MinutiaType>
        <Flag>false</Flag>
    </Minutia>
  - <Minutia>
        <X>280</X>
        <Y>117</Y>
        <Angle>3.1415927410125732</Angle>
        <MinutiaType>End</MinutiaType>
        <Flag>false</Flag>
    </Minutia>
  - <Minutia>
        <X>311</X>
        <Y>159</Y>
        <Angle>0.46364760398864746</Angle>
        <MinutiaType>End</MinutiaType>
        <Flag>false</Flag>
    </Minutia>
  - <Minutia>
        <X>248</X>
        <Y>163</Y>
        <Angle>2.8564009666442871</Angle>
        <MinutiaType>Bifurcation</MinutiaType>
        <Flag>false</Flag>
```

Figure 6. XML file created with the extracted minutiae of finger print

5. Steganography for hiding minutiae

Lot of security risks are there while transmitting the sensitive fingerprint minutiae over the internet. The following figure shows the various security risks [26] that can occur from fingerprint image sensing to fingerprint matching.

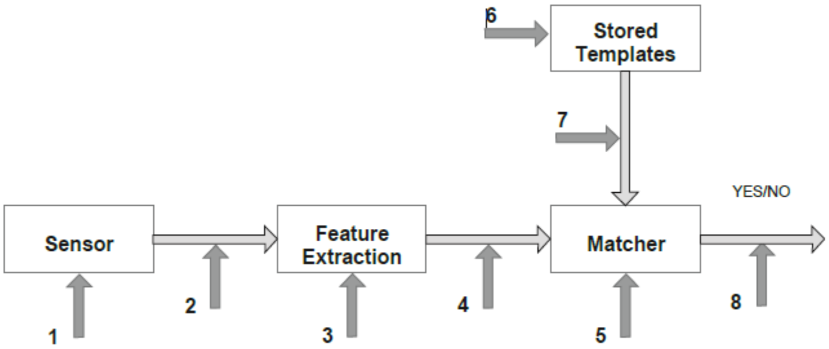


Figure 7. Security risks at various stages of fingerprint verification

1. Fake Biometrics at sensor: A reproduction of biometric feature is present such as face mask, a fake finger or a fake signature.
2. Resubmitting digitalized feature: In this type of attack a previously stored feature is resubmitted such as presenting an earlier recorded copy of fingerprint.
3. Overriding the biometric extraction program: A Trojan horse is used, the Trojan produces preselected features by the intruder.
4. Tampering with the extracted features: Changing the extracted features while it is being sent to the matcher.
5. Corrupting the matcher: Using Trojan horse, matcher is corrupted i.e. it selects the data which is preselected by the intruder.
6. Tampering with the database: As the database is spread over a number of server an intruder tries to modify one or more template, which results in authorization of a fraud data.
7. Attacking the data sent to matcher from the database: The stored data is communicated to matcher which can be intercepted and modified.
8. Overriding the final decision: Overriding the final yes/no result.

Our application primary focuses on enhancing security at point 4 of attack. In most verification systems the first three steps occur on the client side device which includes getting the fingerprint and extracting the features. Then these features are sent via the internet to a web service or a server that does the matching making this point of transmission of data from client to server most vulnerable. Therefore our program enhances the security at this level. This is done by the following methods:

- The extracted features are converted to xml format. This makes the data less readable and also creates the possibility of performing xml encryption of the features.
- The extracted xml is further secured by using a process of steganography.
- The steganography images are converted to base64 string and there can be an encryption at this level too.

Steganography is the method of hiding important data in an unrelated piece of information [27]. The security of biometric data can further be ensured by using steganography. Three basic types of steganography techniques are Pure Steganography, Secret key Steganography and Public key Steganography. Among the three different techniques pure steganography is the one used in most of the applications since it avoids the need to share the stego key between the communication parties.

The pure Steganography can be defined as the quadruple (C, M, D, and E) [28] where:
C: the set of possible covers,
M: the set of secret massage with $|C| \geq |M|$,
E: $C \times M \rightarrow C$ the embedding function,
D: $C \rightarrow M$ of the extraction function with the property that $D(E(c,m))=m$ for all $m \in M$ and $c \in C$

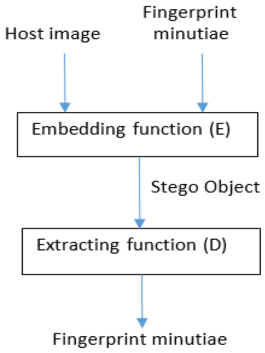


Figure 8. Steganography applied for fingerprint minutiae

We have used pure steganography to hide the fingerprint minutiae. The technique used to implement steganography here is LSB replacement logic. We hide the fingerprint minutiae in the image by hiding a bit of the minutiae in every least significant bit of every byte. We can hide three bits per pixel as there are 3 bytes for every pixel in a color image. The reverse process is done at the receiving end. The LSB is removed from every byte of the image until an ending byte is found and appended to the text file to get the original fingerprint minutiae.

```
For each pixel in the image
  If the whole XML file is not embedded
    Clear the LSB of R, G, B values
    Get the character to be embedded and convert it to integer
    Hide the 8 bits of the character in the
    LSBs of the RGB values of consecutive pixels
Add 8 consecutive zeros to indicate the end of text
```

Figure 9. Algorithm for pure steganography

The encoded images are converted to Base 64 strings. The base 64 strings are sent to a soap web service that computes the similarity between 0 and 1, where 0 means completely different and 1 means completely same.

6. Xml Mining and Fingerprint Matching

On the server side the database contains the XML files corresponding to the extracted features of each fingerprint. These XML files are grouped into three different classes based on the number of bifurcations and number of ridge endings. There are finite group of Minuta based finger print features which can be formed into definite number of groups based on the presence or absence of some features.

XML mining is a form of semi structured data mining which uses trees to identify schema and mine based on different techniques. The current application uses structure based/ schema based xml mining techniques for static xml documents, as the pattern of the fingerprint xml is fixed. Our algorithm compares the schema of the incoming xml file with the schema of the xml files in the database. This comparison is done with the tree structure of the xml document. Then the files whose schema matches with the schema of the incoming file are selected. Then we apply a matching algorithm on these mined files to get the exact match of the fingerprint.

The matching technique uses the M3gl algorithm proposed in [24]. The algorithm is based on minutiae triplet similarity measure. m_1, m_2 and m_3 are three minutiae arranged clockwise. d_i is the Euclidean distance between the minutiae other than m_i. α_i is the angle required to rotate the direction of a minutiae to coincide with the vectors associated with the minutiae and β_i is the angle required to rotate the direction of the minutiae to coincide with the other minutiae.

ach figure should have a brief caption describing it and, if necessary, a key to interpret the various lines and symbols on the figure.

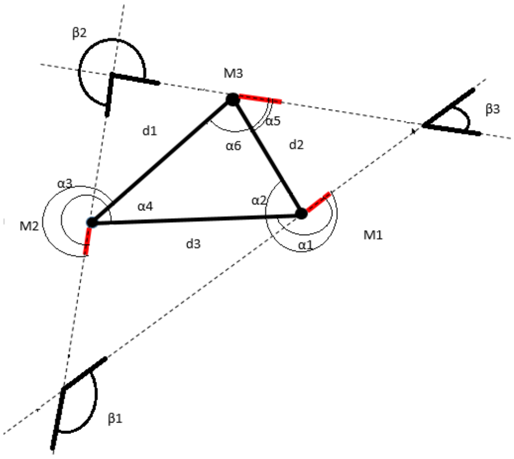


Figure 10. Components of m-triplets feature representation

For finding the m-triplets for a given minutiae set M, for each minutiae m in M its nearest c minutiae are found out. By including m and two of its nearest minutiae all possible m-triplets are computed discarding duplicates. After computing the m-triplets local minutiae matching is done to find similar m-triplets and then to find the local matching minutiae pairs of the query and template fingerprints. Then global minutiae matching is done in which every minutiae pair is considered as a reference pair for fingerprint rotation. A query minutiae transformation for each reference pair is done in the global minutiae matching. Finally the similarity score is computed as $n^2/|X||Y|$ where n is the number of matching minutiae pairs and X and Y are the template and query fingerprint minutiae.

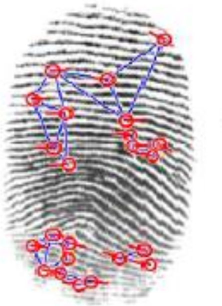
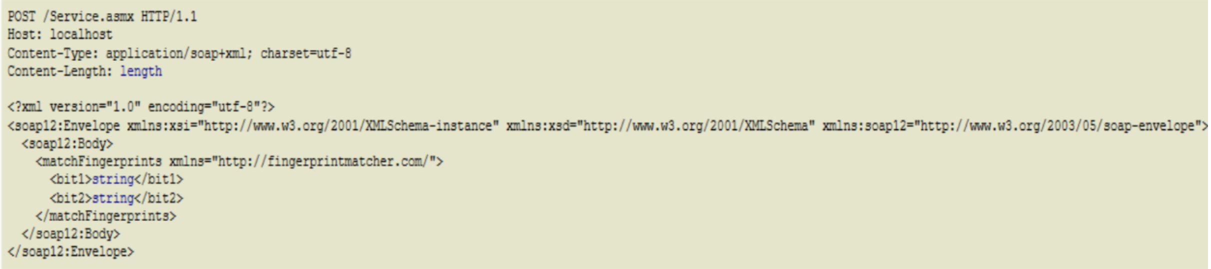


Figure 11. Extracted triplets

7. Results

We have successfully implemented a model by which we can transmit and verify fingerprints in a secure, faster and accurate way.

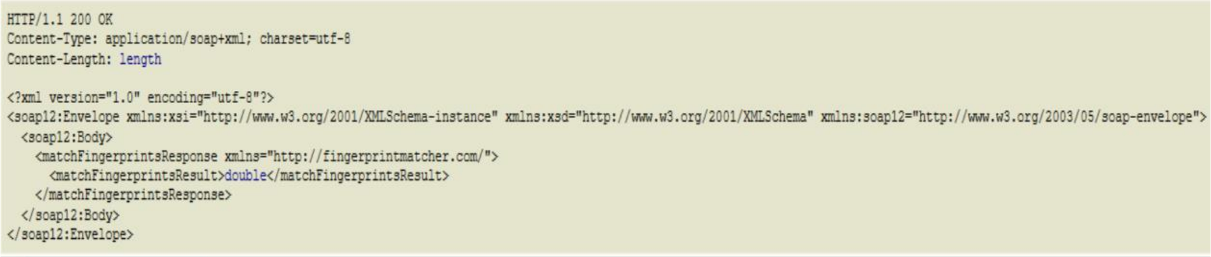


```
POST /Service.asmx HTTP/1.1
Host: localhost
Content-Type: application/soap+xml; charset=utf-8
Content-Length: length

<?xml version="1.0" encoding="utf-8"?>
<soap12:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap12="http://www.w3.org/2003/05/soap-envelope">
  <soap12:Body>
    <matchFingerprints xmlns="http://fingerprintmatcher.com/">
      <bit1>string</bit1>
      <bit2>string</bit2>
    </matchFingerprints>
  </soap12:Body>
</soap12:Envelope>
```

Figure 12. Sample SOAP request

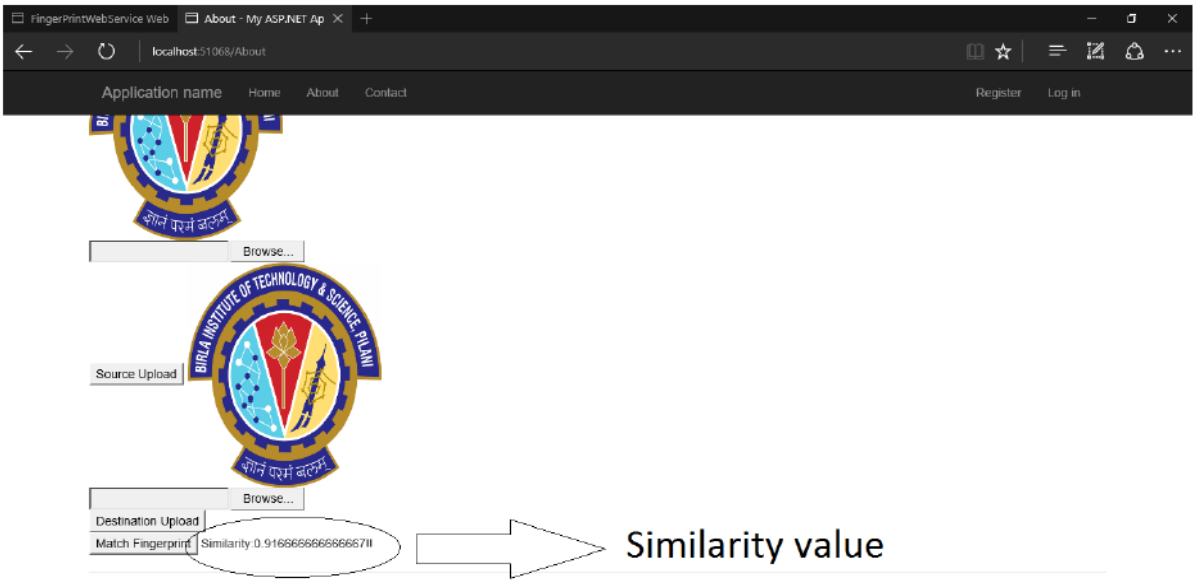
Using the extracted minutiae, we created an XML file and this XML file is embedded in an image for transferring the minutiae securely. The SOAP web methods and the HTTP request and response are shown in the below figures. The server calculates the similarity value by matching with a template fingerprint and the similarity value is returned to the client.



```
HTTP/1.1 200 OK
Content-Type: application/soap+xml; charset=utf-8
Content-Length: length

<?xml version="1.0" encoding="utf-8"?>
<soap12:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap12="http://www.w3.org/2003/05/soap-envelope">
  <soap12:Body>
    <matchFingerprintsResponse xmlns="http://fingerprintmatcher.com/">
      <matchFingerprintsResult>double</matchFingerprintsResult>
    </matchFingerprintsResponse>
  </soap12:Body>
</soap12:Envelope>
```

Figure 13. Sample SOAP response



Similarity:0.9166666666666667II

Figure 14. Final similarity of two different fingerprints of the same person

Our experiment compared the performance of fingerprint identification without xml mining and with xml mining. It is observed that the time required for the fingerprint identification can be reduced considerably if xml based mining is used.

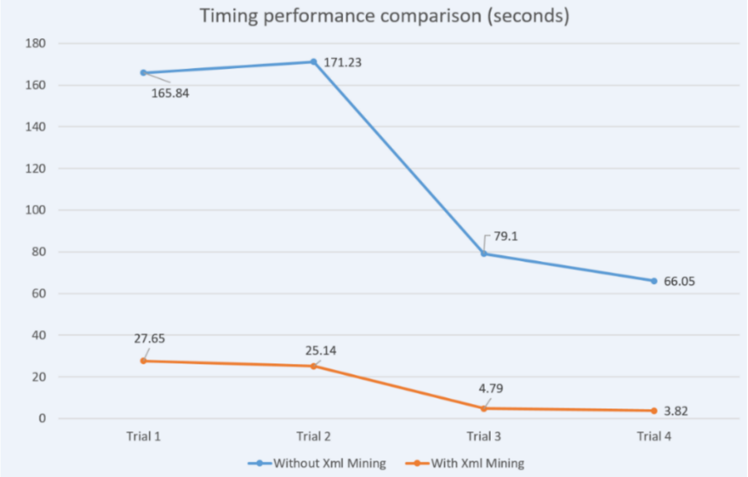


Figure 15. Performance comparison

8. Conclusion and Future Scope

The implementation of the proposed mechanism will ensure end to end security between a client side web application and a server based RPC web service. Converting the features in xml format is a very good technique as it gives programmers the independence to use it in multiple ways and makes transmission very easy and lightweight as xml format for data transmission is used in web and cloud based applications extensively. It is a very fast and very secure method for comparing two fingerprints on an online platform and is easy to use and understand.

The data can be encrypted twice before it is send to the service for computation. Double encryption means double protection. Xml encryption can be performed at the extraction level and the extracted xml can be encrypted using a Hash Key technique. The base 64 strings can also be encrypted using AES or RSA or other such encryption algorithms adding another layer of security to the data just before it is passed to the web service. The framework can be extended so that instead of comparing two fingerprints the fingerprint can be uploaded and can be compared with a list of fingerprints already stored in the database in base 64 encrypted format. The Graphical user interface of the web application can be improved. The security implementation may be extended to other biometric methods of verification like iris scanning, palm recognition etc.

9. References

[1] Jayaraman, in *Digital Image Processing*, Tata Mc Graw Hill, pp. 434-435.

[2] A. Babich, "Biometric Authentication. Types of biometric identifiers," Haaga-Helia University of Applied Sciences, 2012.

[3] Priyanka, "Fingerprint recognition techniques and its applications," in *International Conference on Advances in Engineering and Technology Research (ICAETR)*, Unnao, 2014.

[4] M. Saini and A. K. Kapoor, "Biometrics in Forensic Identification: Applications and Challenges," *Journal of Forensic Medicine*, 2016.

[5] W. Sheng, G. Howells, M. Fairhurst and F. Deravi, "A Mementic Fingerprint Matching Algorithm," *IEEE Transactions of Information Forensics and Security*, vol. 2, no. 3, pp. 402-412, 2007.

[6] T. Hatano, T. Adachi, S. Shigematsu, H. Morimura, S. Onishi , Y. Okazaki and H. Kyuragi, "A fingerprint verification algorithm using the differential matching rate," in *Proceedings of the 16th International Conference on Pattern Recognition*, Quebec City, Quebec, Canada, 2002.

[7] A. LindosoLuis, L. Entrena, J. Liu-Jimenez and E. San Millan, "Correlation-Based Fingerprint Matching with Orientation Field Alignment," in *International Conference on Biometrics*, 2007.

[8] X. Jiang and W.-Y. Yau, "Fingerprint minutiae matching based on the local and global structures," in *Proceedings of 15th International Conference on Pattern Recognition*, Barcelona, Spain, 2000.

[9] X. Luo, J. Tian and Y. Wu, "A minutiae matching algorithm in fingerprint verification," in *Proceedings of 15th International Conference on Pattern Recognition*, Barcelona, Spain, 2000.

[10] J. ChengYang and D. Sun Park, "A fingerprint verification algorithm using tessellated invariant moment features," *Neurocomputing*, vol. 71, no. 10-12, pp. 1939-1946, 2008.

[11] L. Nanni and A. Lumini, "Descriptors for image-based fingerprint matchers," *Expert Systems with Applications*, vol. 36, no. 10, pp. 12414-12422, 2009.

[12] A. K. Jain and U. Uludag, "Hiding Fingerprint Minutiae in Images," in *Third Workshop on Automatic Identification Advanced Technologies (AutoID)*, Tarrytown, New York. USA, 2002.

[13] A. K. Jain and U. Uludag , "Hiding a Face in a Fingerprint Image," in *16th International Conference on Pattern Recognition*, Canada, 2002.

[14] A. Jain and U. Uludag, "Hiding biometric data," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, no. 11, pp. 1494 - 1498, 2003.

[15] N. Agrawal and M. Savvides, "Biometric data hiding: A 3 factor authentication approach to verify identity with a single image using steganography, encryption and matching," in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, Miami Beach Florida, 2009.

[16] Y. Chung, D. Moon, K. Moon and S. Pan, "Hiding Biometric Data for Secure Transmission," in *International Conference on Knowledge-Based and Intelligent Information and Engineering Systems*, 2005.

[17] G. Aguilar, G. Sanchez, K. Toscano, M. Salinas, M. Nakano and H. Perez, "Fingerprint Recognition," in *Second International Conference on Internet Monitoring and Protection ICIMP 2007*, San Jose, CA, USA , 2007.

[18] I. Munagani , M. S. Hsiao and L. Abbott, "On the Uniqueness of Fingerprints via Mining of Statistically Rare Features," in *IEEE International Symposium on Technologies for Homeland Security (HST)*, Waltham, MA, USA, 2015.

[19] W. Yani, W. Zhendong, Z. Jianwu and C. Hongli, "A Robust Damaged Fingerprint Identification Algorithm Based on Deep Learning," in *Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), IEEE*, Xi'an, China , 2016.

[20] S. Bei , L. Wusheng , D. Liebo and L. Qin, "A fingerprint identification algorithm based on local minutiae topological property," in *IEEE International Conference on Data Science in Cyberspace (DSC)*, Changsha, China , 2016.

[21] W. Yuan , Y. Lixiu and Z. Fuqiang, "A Real Time Fingerprint Recognition System Based On Novel Fingerprint Matching Strategy," in *8th International Conference on Electronic Measurement and Instruments, ICEMI '07.* , Xi'an, China, 2007.

[22] S. Kumari and S. K. Rath, "Performance comparison of SOAP and REST based Web Services for Enterprise Application Integration," in *International Conference onAdvances in Computing, Communications and Informatics (ICACCI)*, Kochi, 2015.

[23] S. G. C. Isaac and V. U. Devi, "Efficient Querying and SOAP Based Streaming of Multimedia Content Using WEB Services," in *International Conference on Intelligent Computing Applications (ICICA)*, Coimbatore, 2014.

[24] M. A. Medina-Perez, M. Garcia-Borroto, A. E. Gutierrez-Rodriguez and L. Altamirano-Robles, "Improving Fingerprint Verification Using Minutiae Triplets," *Sensors*, pp. 3418-3437, 2012.

[25] J. F. Lim and R. K. Y. Chin, "Enhancing Fingerprint Recognition Using Minutiae-Based and Image-Based Matching Techniques," in *1st International Conference on Artificial Intelligence, Modelling and Simulation (AIMS)*, Kota Kinabalu, 2013.

[26] TanishaAggarwal and C. K. Verma, "Fake Fingerprint Detection Methods," *IJITKM*, no. Special Issue, pp. 61-69, 2014.

[27] C. Whitelam, N. Osia and T. Bourlai, "Securing Multimodal Biometric Data through Watermarking and Steganography," in *IEEE International Conference on Technologies for Homeland Security (HST)*, Waltham, MA, 2013.

[28] Z. K. AL-Ani, H. O.Alanazi , A. Zaidan and B. Zaidan, "Overview: Main Fundamentals for Steganography," *Journal Of Computing*, vol. 2, no. 3, pp. 158-165, 2010.