**Verification of the E-Certificates to check the validation of the Online Scholarship Process**

**A Project Report**

***Submitted in partial fulfilment of the***

***requirements of the award of the degree***

***of***

**Bachelor of Technology**

**In**

**Computer Science and Engineering**

***under supervision of***

**Dr. Soumit Choudhury**

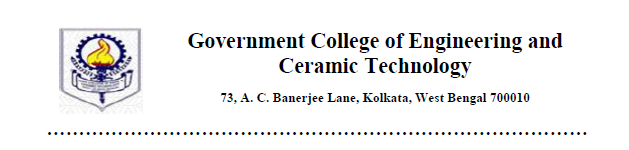
***by***

**Koustav Mondal (GCECTB-R19-3015)**

**Bickram Adhikary (GCECTB-R19-3012)**

**Sourin Kundu (GCECTB-R19-3032)**

**Soumil Biswas (GCECTB-R19-3030)**



**BONAFIDE CERTIFICATE**

Certified that this literature survey report titled Verification of the E-Certificates to check the validation of the Online Scholarship Process is the realistic work carried out by Koustav Mondal (GCECTB-R19-3015), Bickram Adhikary (GCECTB-R19-3012), Sourin Kundu (GCECTB-R19-3032) and Soumil Biswas (GCECTB-R19-3030), who will carry out the project work under my / our supervision

*…………………………………..*

**Dr. Soumit Chowdhury**

**SUPERVISOR**

Assistant Professor

Department of Computer Science and Engineering

Government College of Engineering and

Ceramic Technology

Kolkata-700010

*………………………………….. …………………………………………*

**Dr. K. Saha Roy External Examiner**

**HEAD OF THE DEPARTMENT**

Assistant Professor & Head

Department of Computer Science and Engineering

Government College of Engineering and

Ceramic Technology

Kolkata-700010

**Acknowledgement**

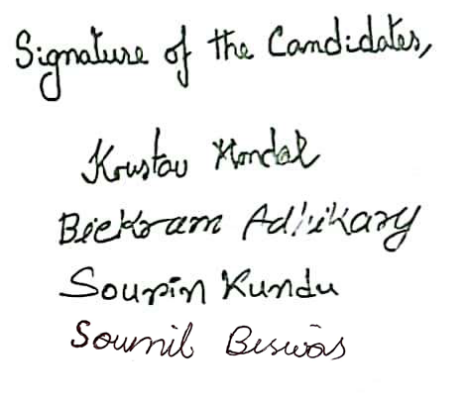
Through this acknowledgement, we are express our sincere gratitude to all those people who have been associated with this Project and have helped with it and made it a worthwhile experience. On this great occasion of accomplishment of our project on E-Validation of cheque application. We would also like to expand our deepest gratitude to all those who have directly and indirectly guided us in this project.

Foremost, we would like to express our sincere gratitude to our guide, Professor Dr. Soumit Choudhury, for his encouragement, patience, guidance, insightful comments, helpful information, practical advice, endless ideas, support and understanding that have always helped us to accomplish this project. His immense knowledge, in-depth experience and professional expertise has enabled us to complete this project successfully. His suggestions were invaluable, which enabled us to overcome the difficulties we encountered during the project.

We would also be thankful to H.O.D.(CSE) Mrs. Dr. Kalpana Saha (Roy) of Govt. College of Engineering & Ceramic Technology for providing all the required facilities in completion of this project. We are also grateful to our college for giving us the opportunity to work with them and providing us the necessary resources for the project.

Finally, as one of the team members, I would like to appreciate all my group members for their support and coordination, I hope we will achieve more in our future endeavors.

Thanks for all your encouragement!

With Gratitude,

Koustav Mondal (GCECTB-R19-3015)

Bickram Adhikary (GCECTB-R19-3012)

Sourin Kundu (GCECTB-R19-3032)

Soumil Biswas (GCECTB-R19-3030)

**Abstract**

The proposed concept mainly focuses on digital verification of e-certificates to validate the Online Scholarship Process and secure encryption techniques for better confidentiality of the data. The target here is to address all the major data security issues like authentication, confidentiality, integrity, and non-repudiation of data while making sure the ease of access to make sure the verification process is smooth enough for realistic and widespread usage.

The Protocol begins with the Candidate Physically appearing in the Scholarship Processing Agency and providing the public share of the Candidate’s information. The Scholarship Processing Person first uses the Candidate’s Roll No. and University/ Institution Name to Fetch an OTP from the Institution Server, which arrives in the Candidate’s Mobile Device. Upon supplying the OTP to the Server, the digital Grade Card is available for download. The Above inputs that have been supplied are also used to create 2 hash values, which unlock the private share of the Grade Card, with the Private share of the Institution’s encrypted logo. This logo, when superimposed with the public share of the Institution’s logo, decrypts the Actual logo of the Institution. This stage verifies whether the Candidate is a legitimate student of said Institution.

The next stages involve a 2-step biometric verification of the Candidate that has appeared before the Scholarship Processing agency. The Candidate’s Year of Passing, DGPA, Fingerprint and Voice Sample are all taken by the Processing Person and supplied to the server, who matches the input with the respective entries in the database. If there is a match, the biometric authenticity of the Candidate is verified.

Once the Verification process is complete, the Scholarship Processing Person performs the transfer of the Scholarship Amount to the Candidate’s bank account. An SMS is sent to the Candidate’s Mobile Device, containing the Transaction ID and Amount of this Online transaction. Finally, the candidate is asked to provide a fingerprint of the left thumb as proof of a successful transaction of the designated scholarship amount.

**Introduction**

With the advent of the computer and subsequently internet networking at the turn of the 21st Century, human society has observed a technological shift and a streak of exponential growth never before seen in History. The lives of people in every and all aspects has seen dramatic changes, and have for the most part, become easier and more convenient, due to the introduction of the computer networks in our day-to-day lives. One such sector that has been revolutionized due to digitization is the enrollment for the production of temporary and permanent documents for every member of the population. From Identification Cards, Social and Financial Security Documents and even Testaments or Academic Documents, people now mostly opt to fill up and enroll for all these documents online. In this project, our aim scope is limited to the Online Scholarship Enrollment Process for Students.

To maintain such a system where students can apply for Scholarships without much difficulty, an intricate system of multi-layered verification, validation, fragmentation and authentication is put in place to make sure the process is smooth and above all, secure.

There has been significant research in the field of validation and verification of documents online, but not much for the purpose of Scholarship application. This endeavor seeks to change that. The purpose of this project is to observe the current Scholarship Application procedure that is in place, and how we can improve on this system using the present advancements in digital document verification research. The primary target of this project is to counter some of the preliminary vulnerabilities of the system that are as follows.

1. Forgery of Candidate’s Data (Name, Roll No., DGPA, Year of Passing, etc.), by the Legitimate Candidate or some other third party.
2. Unauthorized person posing as the Candidate to receive The Scholarship money.
3. Forgery/ tampering on the part of the Scholarship Processing Person/ Agency to fraud the Candidate in question.
4. Attempt to hide evidence of receipt of Scholarship money, for the purpose of reclaiming said Amount.
5. The Scholarship Agency not transferring/ transferring the wrong amount to the Candidate, on accident or with malicious intent.

**Literature Review**

Despite the rapid advancements in cryptography and other Data security sciences, not much progress has been made in terms of assisting the Scholarship Application Procedure for students, and no known research documents have been made towards this area. Therefore, the Team has made the decision to look to other areas of research, learn from their procedures and appropriately apply them to make a safe, secure and Cohesive protocol to assist Students to further their education.

The Basis of the project is laid in the system in Place by the National Scholarship Portal (NSP), with the Focus on improving any security vulnerabilities that are present in the current model. The existing model has made headway by implementing an all-online process of application which greatly increases the reach and accessibility of the Scholarship schemes.

A Poignant approach in this context, introduced by Kamta et al, incorporates a method which use the biometric details of the owner including facial characters, retinal scan, palatal patterns, fingerprints to verify the legitimacy of the document’s owner and DNA to be inserted in a smart card which is provided to the owner for identification purpose. Sixteen possible categories are therefore created based on the biometric details of the owner. Each of these sixteen possible categories is a string containing ‘y’ and ‘n’, a central database is used to store the biometric identifier string corresponding to each user. An NDFA with five possible states and having input symbols for each state, is used to match the recalculated string and the recaptured biometric details during the verification process. The authenticity of the owner is verified if the NDFA accepts the string. However, the drawback of this scheme is that it fails to determine the impact of external noise incorporated in the smart card, also it is not focused on how biometric data can be used for template generation. This method is also very infrastructure heavy, and on top of that most of the above biometric information is difficult to record and verify on a large scale.

Among the recent approaches in the field of e-document authentications, the idea of biometric watermarking was implemented by Anitha et al [1], in order to verify the relation between the owner and the corresponding details that appears on the document. Regarding this, the Biometric details which is basically the iris image of the user is captured and converted to a live template in order to obtain a bit code image. This bit code image is then periodically duplicated to be of same size of the cover image. Thereafter, both of these images are partitioned into blocks having equal size. After performing an XOR operation of the bit code image blocks, the watermark bits are obtained. The LSBs of the cover image blocks are encoded by a hash value for each block from a set of inputs interconnected to the image particulars. This model can be used to detect largescale tampering of the document but the drawback is that when it comes to distinguish the sensitive tampering from the external noise attacks, it fails, because for noise and small-scale tampering it is not validated. Therefore, this model needs to be less strict in its implementation, and used with a more lenient version of Biometric verification to ensure a level of security that can feasibly be applied for its purpose.

More works on transform domain watermarking continued in recent times as Hubli et al. [10] used an idea where watermark bits are produced from singular values of SVD block generated from the concern quantized blocks of the cheque image. However, these watermark bits are encoded on the quantized LL sub band components of the DWT blocks existing on the specific portions of the actual cheque image.

Among the very recent approaches on e-document authentications, Hasan et al [3] implemented the idea of segmented multi watermarking which divides the cover image into three separate regions of variable intensity namely R, G, B components in order to enhance the security and for better robustness of digital documents. The components namely R, G, B are therefore embedded into the components of the watermark image namely RW, GW, BW by converting the R, G, B components of the cover image into transformation domain using DWT. Therefore, LH1, LL2, LL3 these three levels along with the watermarks are inserted into LL3. Afterwards, in order to obtain the watermarked image of the digital document the RRW, GGW, BBW are combined together.

**Enhancement proposed on existing works**

The current Scholarship Application Workflow as written in the National Scholarship Portal Standard Operating Procedure (NSP SOP) involves Registering with the NSP, with the Registration, application and Scholarship Transaction all taking place online. Registration in the NSP requires the Aadhar Card or the Bonafide Student Certificate from the Institute. However, neither the Registration Process nor any of the Documents it requires have Biometric Authentication measures in place, and all such documented information is vulnerable to tampering and alteration.

The proposed protocol begins at the Institute level, where the candidate is registered for the first time in this process. The institute is required to have, aside from the prerequisite documented proof of identification, geographical address and family tree identification, two distinct samples of biometric data for each student. These two samples being their fingerprint, as well as their voice recording of a secret spoken password.

This data, along with the other important data which may be at risk of tampering, is hidden in invisible segment of the Candidate’s Grade Card via multi-layered invisible watermarking. These hidden watermarks will be checked for verification.

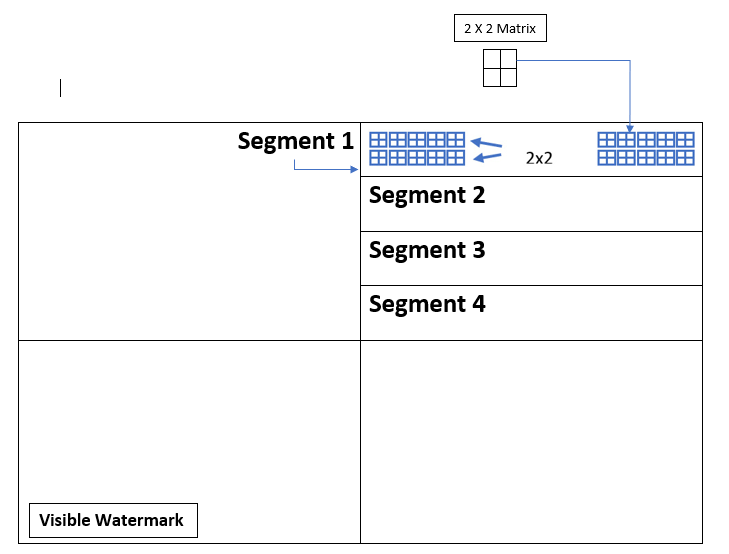
When a Candidate wishes to apply for a Scholarship scheme, they will need to contact a Scholarship Processing Agency in Person to provide the necessary documents and information for verification, or follow through the Procedure themselves (provided they have proper equipment to record the required biometric data). The main part of this phase protocol is to ensure the Institute and Biometric verification of the Candidate to deal with any cases of Data Forgery, Tampering or Identity Theft.

Upon successful verification of the Candidate, the designated scholarship amount will be transferred by the Scholarship Agency to the Candidate’s linked active Bank account via Online Bank Transfer. To further ensure integrity, the Transaction Id and Amount shall be communicated to the Candidate via SMS as proof of a successful transaction. The Candidate is also required to put a Biometric sign. on the Grade Card as proof of a successful reception of payment. In the event the Candidate doesn’t receive the payment for any reason (accidental or not), the Candidate can utilize the Transaction Information to trace back if and where a transaction fraud may have occurred or not.

**Protocol**

The e-scholarship verification process consists of secret embedding of stored institute and biometric information of the Candidate and using this to validate the authenticity of the Candidate at the server end.

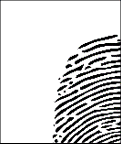
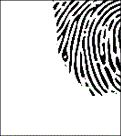
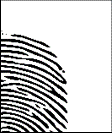
The fabrication of the information is done based on two hash values derived from different information from the Candidate’s Grade Card, and the OTP sent to their Mobile Device. The Grade Card is divided into 4 regions and each region is further divided into 4 segments. In Each segment, a different part of the Candidate’s validation information is stored via invisible image steganography. For each segment we generate different hash values (Matrix Interval, Starting Fragment Index). Matrix interval means how many 2x2 matrix will be skipped between two fragment bits containing matrix and starting fragment index determines the index in the matrix from where hiding fragment bits will start.



A visible watermarking at the lower section of the Grade Card for authentication of the Candidate will also be added. This watermarking is already Standardized, and as such will not be discussed in this project.

**Image Fragmentation**

|  |  |
| --- | --- |
|  |  |
|  |  |



4

3

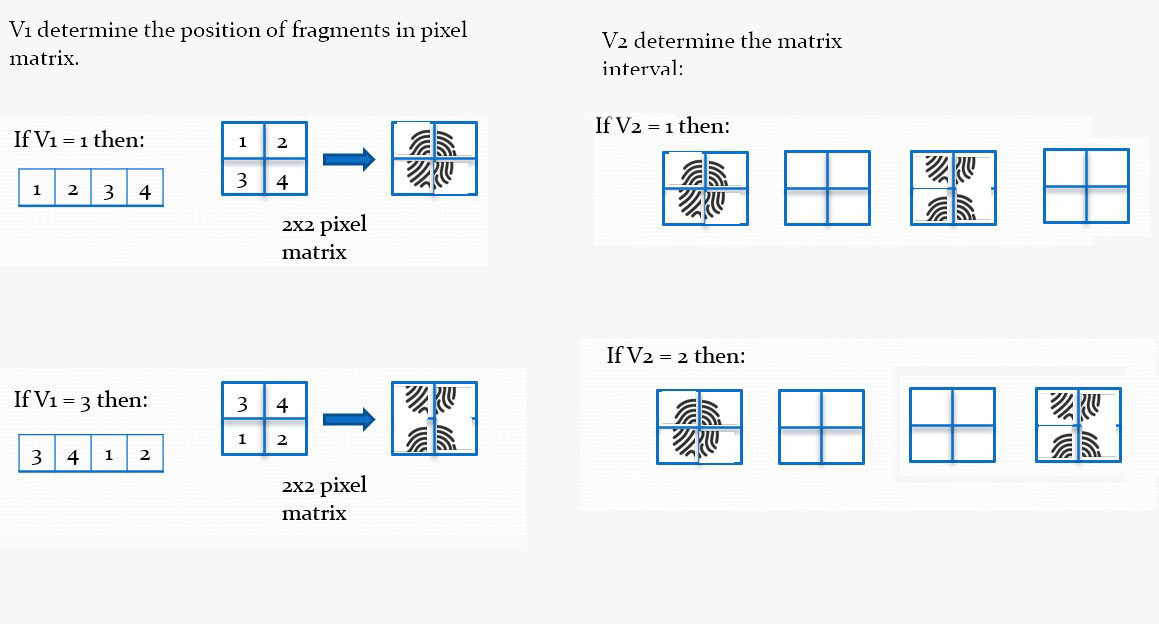
2

1

V1

Hash

V2



The Institute Logo, Candidate’s fingerprint as well as their Voice Spectrogram are all embedded into Segments 1, 2 and 3 respectively via Image Fragmentation. These validations are decrypted using the hash values generated for each stage of the verification process.

Thus, with this protocol, we are able to achieve multi-layered verification of the Candidate’s authenticity for the Scholarship Application Process.

**Stage 1 (University Verification)**

At first, university server embeds private share (Roll no., University name, hash value) of its signature into the 1st segment of the digital grade card. F (Roll no., University name) -> Hash value, H1(starting fragment index), H2(Matrix interval) … H1, H2 belongs to n + 1 (n belongs to 0,1,2,3….).

1. Scholarship processing person supplies candidate’s roll no. for verifying the existence of the student’s data in the university server.
2. Now, after checking the student’s existence university server sends an OTP to the candidate.
3. After supplying the OTP to the university server, the digital grade card is downloaded to the scholarship processing person.
4. At this moment, public share of the university’s signature along with Roll no., University name is injected in the system by the scholarship processing person and, after merging of the detected private share with the supplied public share the university’s signature will be formed.

**Stage 2 (Biometric Verification – Phase 1)**

The university server embeds private share (Year of Passing, DGPA, hash value) of the Candidate’s biometric information (fingerprint) into the 2nd segment of the digital grade card. F (Year of Passing, DGPA) -> Hash value, H3(starting fragment index), H4(Matrix interval) … H3, H4 belongs to n + 1 (n belongs to 0,1,2,3….).

1. Scholarship Processing Person supplies Candidate’s Year of Passing and DGPA for verifying the existence of the student’s biometric data in the university server.
2. The Scholarship Processing Person asks the Candidate to provide a fingerprint sample of their right Thumb on the spot.
3. At this moment, public share of the Candidate’s biometric signature (fingerprint) along with Year of Passing and DGPA is injected in the system by the scholarship processing person. The Supplied public share is then matched with the Private share stored in the University’s database.
4. If the public and private share match, the biometric authenticity of the Candidate is verified. (Phase 1)

**Stage 3 (Biometric Verification – Phase 2)**

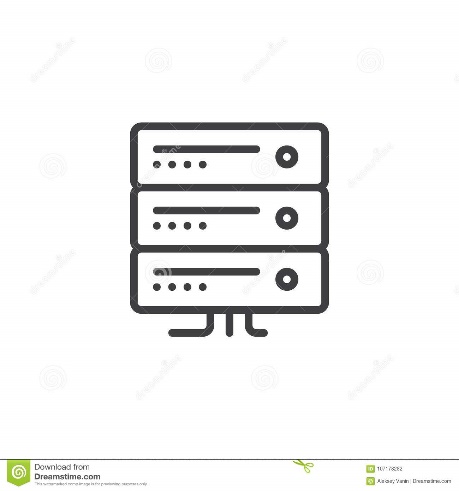
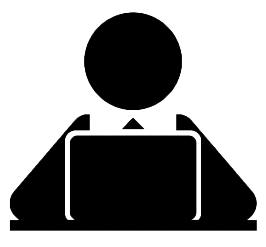
The university server embeds private share (Year of Passing, DGPA, hash value) of the Candidate’s biometric information (Voice) into the 3rd segment of the digital grade card. F (Year of Passing, DGPA) -> Hash value, H5(starting fragment index), H6(Matrix interval) … H5, H6 belongs to n + 1 (n belongs to 0,1,2,3….).

Every student is given a specific and unique word to say whenever they are asked to provide their voice sample. This ensures a 2-layer authentication via Voice signature as well as a spoken secret password. The student is to remember this password for future reference at all times.

1. Scholarship Processing Person supplies Candidate’s Year of Passing and DGPA for verifying the existence of the student’s biometric data in the university server.
2. The Scholarship Processing Person asks the Candidate to provide their voice sample. The Candidate is to provide the secret password to the voice recording equipment.
3. At this moment, public share of the Candidate’s biometric signature (voice) along with Year of Passing and DGPA is injected in the system by the scholarship processing person. The Supplied public share is then matched with the Private share stored in the University’s database.
4. If the public and private share match, the biometric authenticity of the Candidate is verified. (Phase 2)

**Stage 4 (Transaction Verification) – End of Verification Process**

1. Once the Candidate’s authentication procedure is completed, the Scholarship Processing Person embeds private share (Transaction ID, Transaction Amount, hash value) of the Money Transaction in the 4th segment of the digital grade card. F (Transaction ID, Transaction Amount) -> Hash value, H7(starting fragment index), H8(Matrix interval) … H7, H8 belongs to n + 1 (n belongs to 0,1,2,3….).
2. The Scholarship Processing Person sends an SMS or communication, containing the Transaction ID and the Amount transferred in this Transaction.
3. The Scholarship Processing Person asks the Candidate to provide a fingerprint sample of their left Thumb on the spot, as proof of the scholarship application Procedure being completed.



Institution Server

**3**

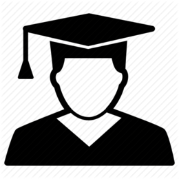
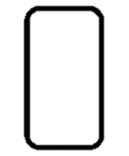
**1**

Roll No., College Name

Scholarship Processing Person (SPP)

OTP

Public Share



Candidate

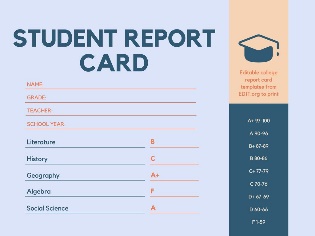
Report Card

Mobile of Candidate

**4**

Hash H1, H2 from OTP, Roll No., College Name

**2**





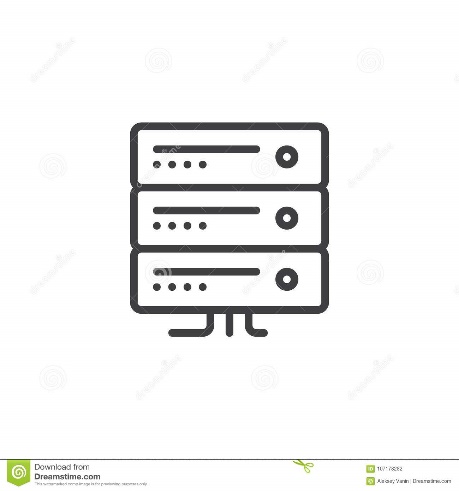
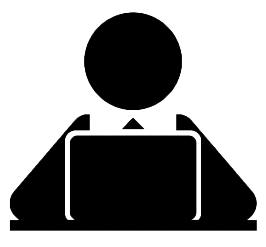
Putting both Overlays together





Private Share of Report Card

Proper University Logo Establishing Institution Verification



Institution Server

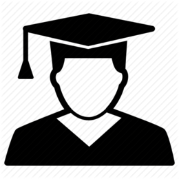
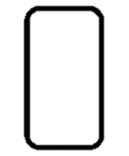
**5**

Year of Passing, DGPA

Scholarship Processing Person (SPP)

OTP

Public Share



Candidate

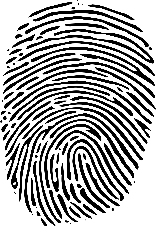
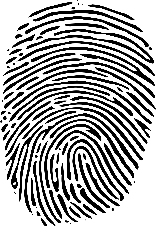
Mobile of Candidate

Verification Failed

**6**

**7**

Hash H3, H4



Putting both Overlays together

Public Share of Fingerprint

Match?

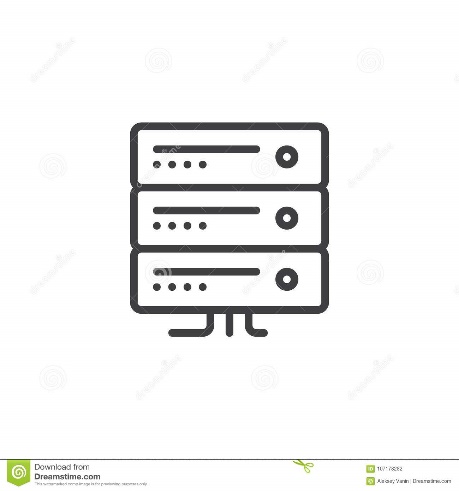
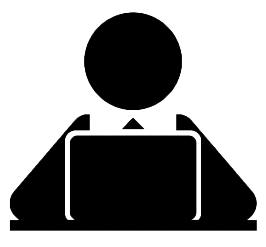
Private Share of Fingerprint

No

Yes

Biometric Verified

**8**



Institution Server

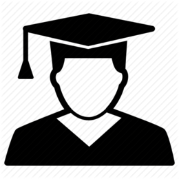
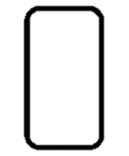
**9**

Year of Passing, DGPA

Scholarship Processing Person (SPP)

OTP

Public Share



Candidate

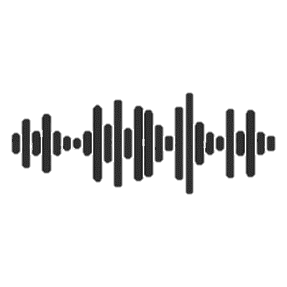
Mobile of Candidate

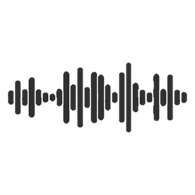
Verification Failed

**10**

**11**

Hash H5, H6





Putting both Overlays together

Public Share of Voice

No

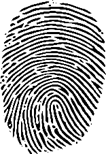
Match?

Private Share of Voice

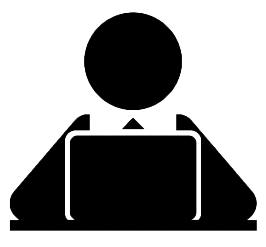
Yes

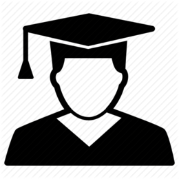
Biometric Verified

**12**



Fingerprint of Left Hand



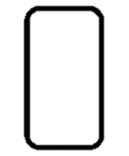


**15**

Scholarship Processing Person (SPP)

Candidate

Transaction ID, Transaction amount



**13**

**14**

Hash H7, H8

SMS

Mobile of Candidate

Transaction ID, Transaction amount

**16**



Putting both Overlays together

Transaction Receipt Public Share

No

Match?

Yes

Transaction Verified

Transaction not Verified

**Share Generation Algorithm**

The basic premise for a share generation algorithm is to consider each pixel of an image and shift the bits left or right by a specified magnitude to produce one share and then produce a complimentary share such that when fused together, they can recreate the original image.

Example:

For an image 1000 x 1000 pixels; we generate shares E1 and E2 (which will also have the same dimensions) by generating a pair of encrypted pixels for each respective pixel position ‘ps’. For each pixel ps we derive the intensity values of Red (R), Blue (B) and Green (G) and encrypt them for Share E1 using a function of the nature:

E1r= R[ps] mod 8 + (ps) mod 11 + Vr…………………………………………...(1)

E1g= G[ps] mod 16 + (ps) mod 13 + Vg…………………………………………(2)

E1b= B[ps] mod 24 + (ps) mod 15 + Vb…………………………………………(3)

Where R[ps], G[ps], and B[ps] denoting the red, green and blue intensity values in the actual signature image at pixel position ‘ps’. Further, Vr, Vg and Vb are used as some predefined threshold values in the encryption operation for the respective intensities at pixel index ‘ps’.

To make a complimentary share E2, we use the function:

E2r=R[ps]-E1r…………………………………………………........................(4)

E2g=G[ps]-E1g……………………………………………………………………...(5)

E2b=B[ps]-E1b………………………………………………………………………(6)

We repeat this process for each pixel in the original image, ultimately generating two unrecognizable images, which only when put together can yield the original image using the function:

E1r[ps]+E2r[ps]=R[ps]…………………………………………………………(7)

E1g[ps]+E2g[ps]=G[ps]………………………………………………………..(8)

E1b[ps]+E2b[ps]=B[ps]………………………………………………………..(9)

**Data Hiding Algorithm**

The Data to be hidden (College Logo, biometrics, etc.) will be embedded in a base image (in this case, the Report Card/ Mark Sheet of the Candidate). Below is a prototype algorithm for the encryption method to be used.

**Encryption:**

Data to be Embedded: 1001.

We take each element of this value to be hidden in each cell of the 2x2 matrix of the base image. (Here, R, G & B are colour intensity values of the base image)

|  |  |
| --- | --- |
| a1(1) | a2(0) |
| a3(0) | a4(1) |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | R1 | G1 | B1 | R2 | G2 | B2 |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | R12 | G12 | B12 | R22 | G22 | B22 |  |  | |  |
|  |  |

Let The cell in question have the values:

|  |  |
| --- | --- |
| R1 | G1 |
| R12 | G12 |

|  |  |
| --- | --- |
| 7(a1) | 13(a2) |
| 9(a3) | 11(a4) |

We use the following equations to transform a1, a2, a3, a4 to A1’, A2’, A3’ and A4’. Then we keep aside the negative signs from the values.

A1’ = a1-a4 A2’ = (a3+a2)/2

|  |  |
| --- | --- |
| 4(A1’) | 11(A2’) |
| 2(A3’) | 11(A4’) |

A3’ = (a3-a2)/2 A4’ = a4

|  |  |
| --- | --- |
| -4(A1’) | 11(A2’) |
| -2(A3’) | 11(A4’) |

For each cell, consider x & y (multiples of 4) such that x <= A1’ < y for all cells. Transform A1’, A2’, A3’ & A4’ to R1, R2, R3 & R4 using the equation: R= (x + y)/2

|  |  |
| --- | --- |
| 4 → (4->4->8) | 11 → (8 → 11 → 12) |
| 2 → (0 → 2 → 4) | 11 → (8—>11-->12) |

|  |  |
| --- | --- |
| R1=6 | R2=10 |
| R3=2 | R4=10 |

Hide the encryption data 1001 into the matrix, one bit at a time, such that: (Also include the Negative signs back in)  
if Bit = 1:

R = R+1

Else if Bit = 0:

R = R-1

Then use the inverse equations to get the Final Embedded matrix:

a1 = A1’+A4’ a2 = A2’-A3’

a3 = A2’+A3’ a4 = A4’

|  |  |
| --- | --- |
| -7 | 9 |
| -1 | 11 |

|  |  |
| --- | --- |
| 4 | 10 |
| 8 | 11 |

**Decryption:**

Received Image matrix:

|  |  |
| --- | --- |
| 4 | 10 |
| 8 | 11 |

Decoding ==>

C1 = a1-a4 C2 = (a3+a2)/2

C3 = (a3-a2)/2 C4 = a4

|  |  |
| --- | --- |
| -7 (4 → 7 → 8) | 9 (8 → 9 → 12) |
| -1 (0 →1 → 4) | 11 (8→1→12) |

Compute R1, R2, R3, R4 the same way as before (using (x+y)/2):

|  |  |
| --- | --- |
| R1 = 6 | R2 = 10 |
| R3 = 2 | R4 = 10 |

Use the following loop to extract the embedded message (Taking absolute Values)

If Ci >= Ri:

print 1

else:

print 0

extracted -- > 1001

Data Hiding Deviation:

“The deviation in color values of the carrier image due to embedding a hidden message inside it.”

A high degree of deviation can significantly change the colors of the image thereby arousing suspicion of tampering.

final watermarked bit embedded matrix-->

|  |  |
| --- | --- |
| 4 | 10 |
| 8 | 11 |

Initial matrix →

|  |  |
| --- | --- |
| 7(a1) | 13(a2) |
| 9(a3) | 11(a4) |

Difference between final and initial values of each cell D(i) in the matrix

D1=3 D2 =3 D3 = 1 D4 = 0

Avg = d1+d2+d3+d4 / 4 = 7/4 = 1.75

Deviation % = 0-255 🡪 1.75/255 \* 100 % = 0.68% deviation

This level of deviation is not identifiable by human vision and can fly under the radar as unsuspicious.

**Quantitative experimental data for fingerprint matching:**

We are observing two different parameters for this representative observation, the university logo and a fingerprint image. Each of these images were embedded in their respective segments (segment 1 for logo, segment 2 for fingerprint) in all four regions of the report card cover image. Sample 1 is the original image that was embedded and sample 2 are the images that were extracted from the cover image after steganography.

logo.png thumb-56x56.png

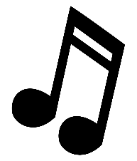
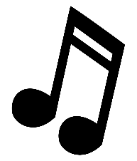
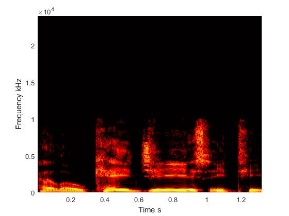
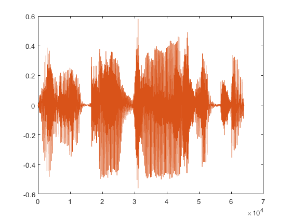
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sample 1** | **Sample 2** | **PSNR** | **SSIM** | **MSE** | **CC** |
| logo | secret-reg-1-seg-1 | 24.9297 | 0.78927 | 208.981 | 0.980873 |
| logo | secret-reg-2-seg-1 | 24.9473 | 0.81138 | 208.135 | 0.981861 |
| logo | secret-reg-3-seg-1 | 24.0767 | 0.77994 | 254.335 | 0.976143 |
| logo | secret-reg-4-seg-1 | 23.7401 | 0.77387 | 274.837 | 0.973726 |
| thumb-56x56 | secret-reg-1-seg-2 | 23.8869 | 0.92716 | 265.700 | 0.989641 |
| thumb-56x56 | secret-reg-2-seg-2 | 24.3109 | 0.93306 | 240.983 | 0.990038 |
| thumb-56x56 | secret-reg-3-seg-2 | 24.4796 | 0.93803 | 231.806 | 0.990946 |
| thumb-56x56 | secret-reg-4-seg-2 | 24.3182 | 0.93246 | 240.581 | 0.989830 |

**Voice Recognition Algorithm**

* First, we convert the Audio file into a visible graphical representative

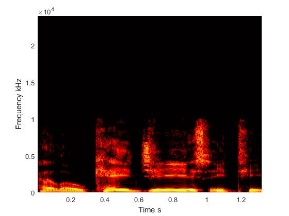
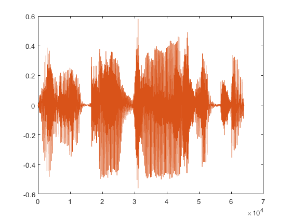
format. Our current options include a basic audio plot, a spectrogram, and a

histogram.



Reference audio file

Target audio file



* Then we attempt to retrieve four different image comparison values: PSNR (Peak Signal to Noise Ratio), SSIM (Structural Similarity index), MSE (Mean Squared Error) and CC (2D Correlation Coefficient) in order to get a clearer and quantitative comparison of the given images.

A = imread('Peter GCECT.tif');

B = imread('Peter KGECT.tif');

[peaksnr, snr] = psnr(B, A);

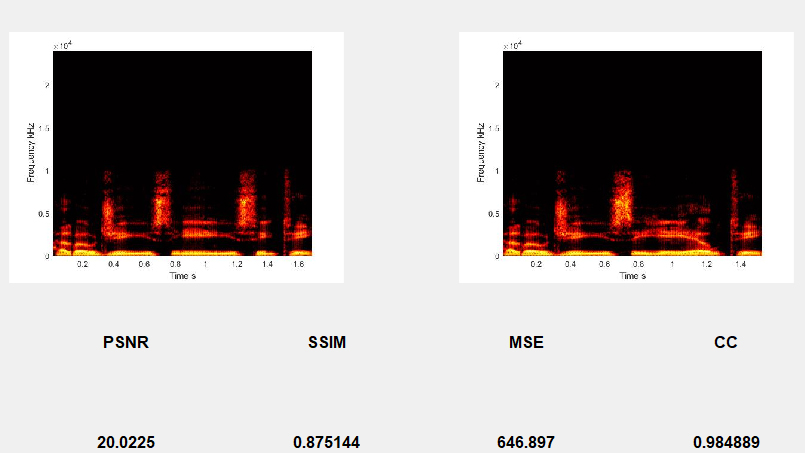
[ssimval, ssimmap] = ssim(B, A);

err = immse(B, A);

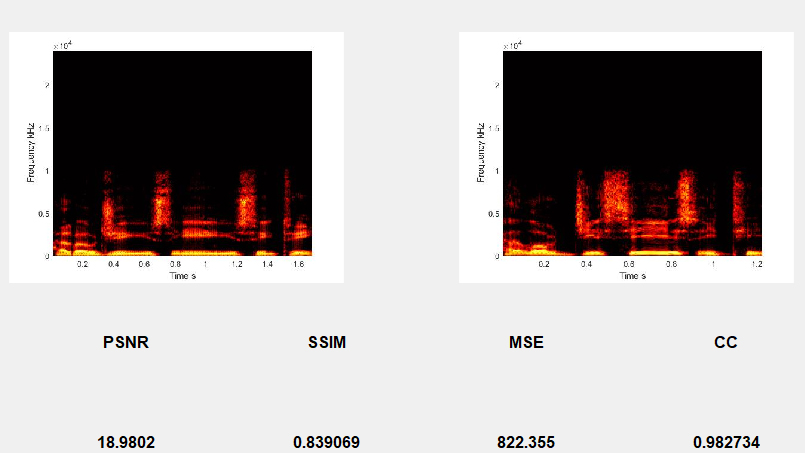
c = corr2(A, B);

* If the comparison values are in an acceptable range (factoring in for external noise sources), the target audio is verified, otherwise it is flagged for mismatch and the system may request for a re-take.

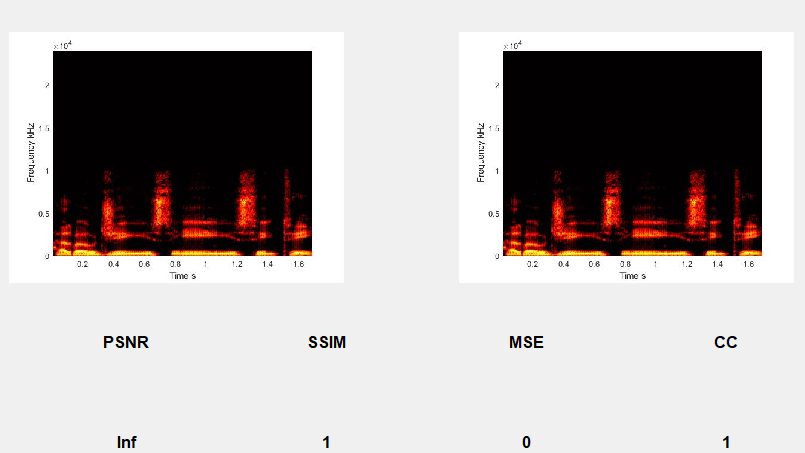
**Case 1 (Same Phrase, different voice):**



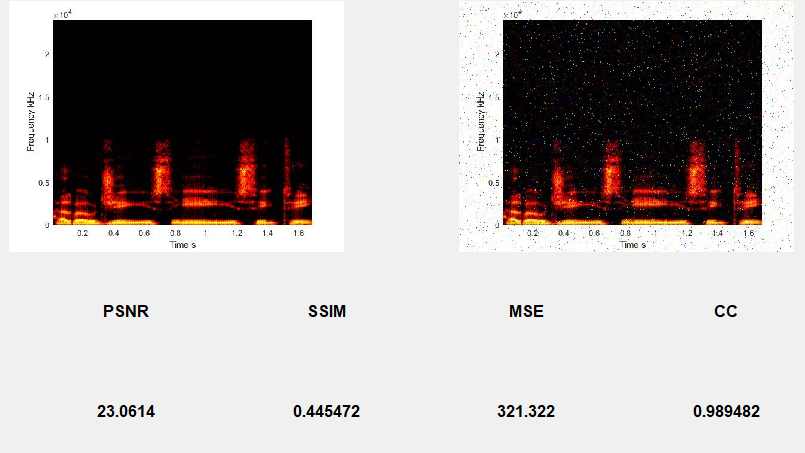
**Case 2 (Different Phrase, Same voice):**



**Case 3 (Same Phrase, Same voice):**



**Case 4 (Same Phrase, Same voice, with added noise):**



**Experimental Values for Different Comparisons:**

We are using two different synthesized voices (Voice1 and Voice2) using three different words (“Hello GCECT.”, “Hello GCELT.” And “Hello KGECT.”) providing for six different voice tacks to permutate with. Noisy versions of voice files were also added in between the mix to have greater observational diversity and simulate conditions closer to practical testing. Voice1 and Voice2 are also selected to be closely similar to one another to simulate practical infringement attempts and therefore comparative values may appear closer than normal for the two different voices.

Below are some notable experimental results on comparing different Values.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sample 1** | **Sample 2** | **PSNR** | **SSIM** | **MSE** | **CC** |
| Voice1 “GCECT” | Voice2 “GCECT” | 12.1635 | 0.66866 | 3951.2 | 0.590765 |
| Voice1 “GCECT” | Voice2 “GCELT” | 12.6271 | 0.69067 | 923.245 | 0.980802 |
| Voice1 “GCECT” | Voice1 “GCECT” | Inf | 1 | 0 | 1 |
| Voice1 “GCECT” | Voice1 “GCECT” 2% noise | 20.4354 | 0.58444 | 588.225 | 0.962638 |
| Voice1 “GCECT” | Voice1 “GCECT” 5% noise | 16.4483 | 0.42218 | 1473.15 | 0.909408 |
| Voice1 “GCECT” 2% noise | Voice1 “GCECT” 5% noise | 15.0376 | 0.38078 | 2038.55 | 0.875282 |
| Voice1 “GCECT” | Voice1 “KGECT” | 12.906 | 0.70620 | 3330.24 | 0.635514 |
| Voice2 “GCECT” | Voice2 “KGECT” | 12.9844 | 0.69567 | 3270.69 | 0.642318 |
| Voice1 “GCECT” 2% noise | Voice1 “GCECT” 9% noise | 13.0954 | 0.32995 | 3188.14 | 0.813395 |

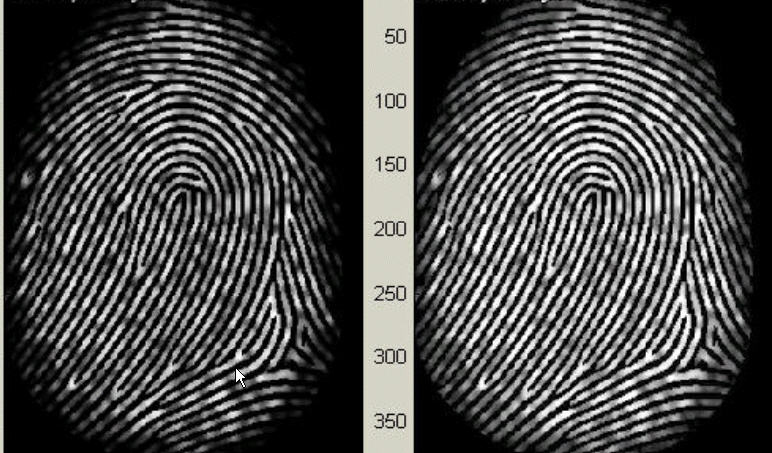
**Fingerprint Recognition Algorithm**

The procedure makes use of the tried and tested minutiae-based Fingerprint Identification System, which extracts minutia features (ridges, grooves, bifurcations and terminations) from a fingerprint and compares them to the sample database to identify the person to whom the fingerprint belongs.

**Step 1 – Histogram Equalization:**

First, we enhance the target fingerprint using Histogram-equalization. Histogram equalization is to expand the pixel value distribution of an image so as to increase the perceptional information. The visualization effect is enhanced as shown in the figure below.

|  |  |
| --- | --- |
|  |  |
| Original histogram of a fingerprint image | Histogram after the Histogram Equalization |

The right side of the following figure [Figure 3.1.1.3] is the output after the histogram equalization.

Histogram Enhancement. Original Image (Left). Enhanced image (Right)

**Step 2 – Fourier Transform:**

The target image is divided into small processing blocks (32 by 32 pixels) and perform the Fourier transform according to:

     (1)

for u = 0, 1, 2, ..., 31 and v = 0, 1, 2, ..., 31.

In order to enhance a specific block by its dominant frequencies, we multiply the FFT of the block by its magnitude a set of times. Where the magnitude of the original FFT = abs(F(u,v)) = |F(u,v)|.

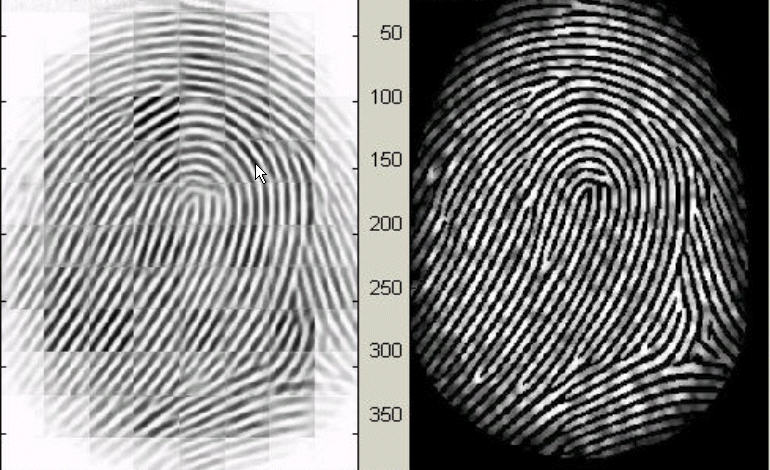
Get the enhanced block according to

  (2) ,

where F-1(F(u,v)) is done by:

    (3)

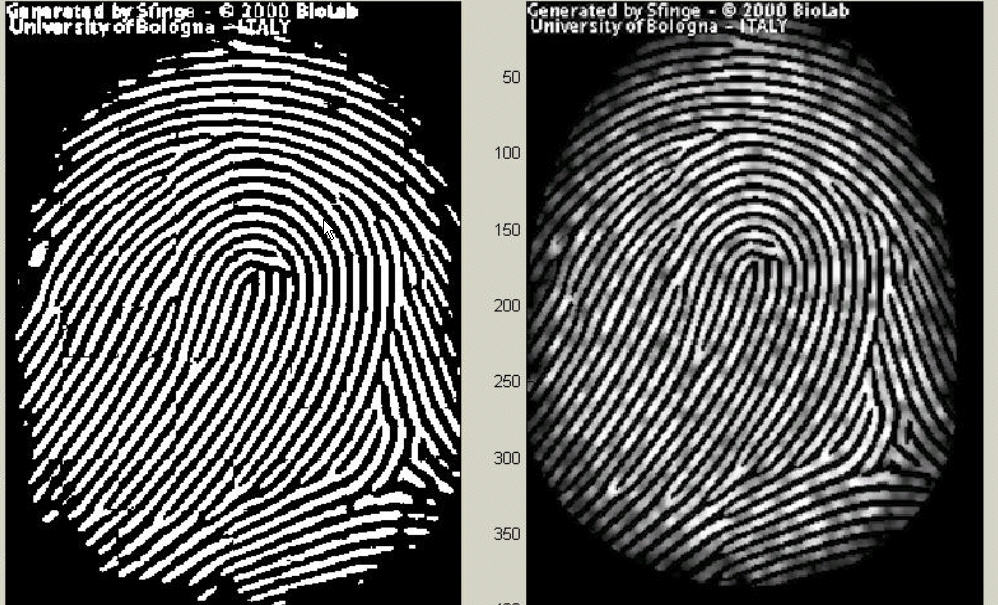
for x = 0, 1, 2, ..., 31 and y = 0, 1, 2, ..., 31.

The k in formula (2) is an experimentally determined constant, which we choose k=0.45 to calculate. While having a higher "k" improves the appearance of the ridges, filling up small holes in ridges, having too high a "k" can result in false joining of ridges. Thus, a termination might become a bifurcation. The figure below presents the image after FFT enhancement.

Fingerprint enhancement by FFT  
Enhanced image (left), Original image (right)

**Step 3 – Binarization:**

Fingerprint Image Binarization is to transform the 8-bit gray fingerprint image to a 1-bit image with 0-value for ridges and 1-value for furrows. After the operation, ridges in the fingerprint are highlighted with black colour while furrows are white.



Fingerprint image after adaptive binarization  
Binarized image(left), Enhanced Gray image(right)

**Step 4 – Image Segmentation:**

In general, only a Region of Interest (ROI) is useful to be recognized for each fingerprint image. To extract the ROI, a two-step method is used. The first step is Block direction estimation and direction variety check, while the second is intrigued from some Morphological methods.

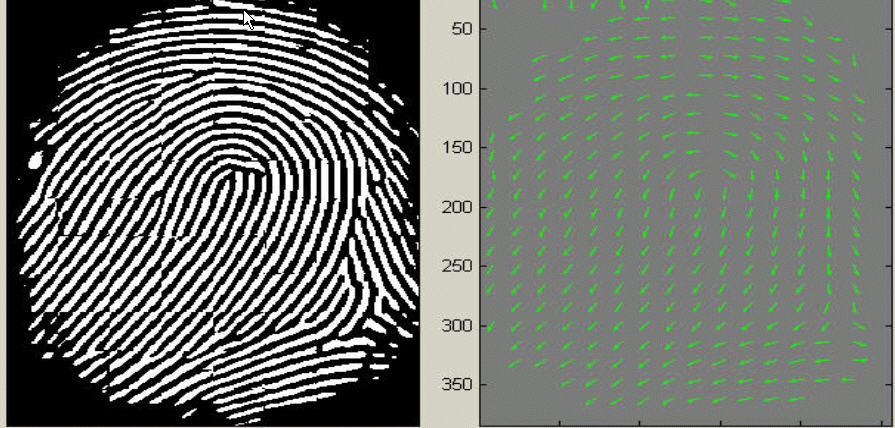
1. **Block direction estimation**

Estimate the block direction for each block of the fingerprint image with WxW in size(W is 16 pixels by default).

After finished with the estimation of each block direction, those blocks without significant information on ridges and furrows are discarded.

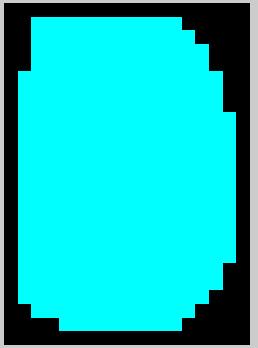
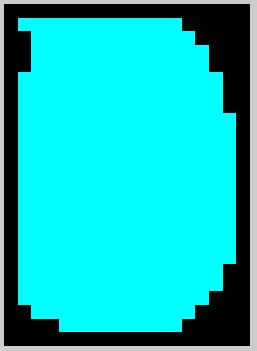
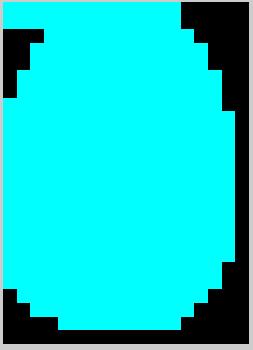
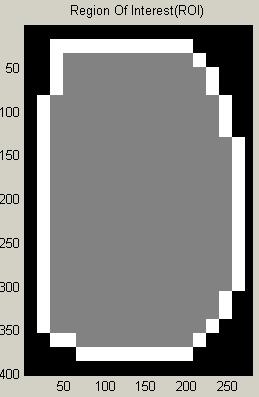
For each block, if its certainty level E is below a threshold, then the block is regarded as a background block.

The direction map is shown in the following diagram. We assume there is only one fingerprint in each image.



Direction map.   
Binarized fingerprint (left), Direction map (right)

1. **ROI extraction by Morphological operations**

Two Morphological operations called ‘OPEN’ and ‘CLOSE’ are adopted. The ‘OPEN’ operation can expand images and remove peaks introduced by background noise. The ‘CLOSE’ operation can shrink images and eliminate small cavities.

Original Image Area After CLOSE operation After OPEN operation ROI + Bound

The final image shows the interest fingerprint image area and its bound. The bound is the subtraction of the closed area from the opened area. Then the algorithm throws away those leftmost, rightmost, uppermost and bottommost blocks out of the bound so as to get the tightly bounded region just containing the bound and inner area.

**Step 5 – Minutiae Extraction:**

**Part 1: Fingerprint Ridge Thinning**

Ridge Thinning is to eliminate the redundant pixels of ridges till the ridges are just one pixel wide. For this purpose, the built-in Morphological thinning function

(bwmorph(o1,'thin',Inf));

in MATLAB used. The thinned ridge map is then filtered by other three Morphological operations to remove some H breaks, isolated points and spikes.

**Part 2: Minutia Marking**

After the fingerprint ridge thinning, marking minutia points is relatively easy. But it is still not a trivial task as most literatures declared because at least one special case evokes my caution during the minutia marking stage.

Error handling methods need to be implemented to ensure the triple counting branch error does not evoke. For this, check routine requiring that none of the neighbours of a branch are branches is added. Also, the average inter-ridge width D is estimated at this stage.

0

0

1

1

1

0

0

1

0

1

0

0

0

1

0

0

0

0

1

0

1

0

1

0

0

1

0

Bifurcation Termination Triple counting branch

Together with the minutia marking, all thinned ridges in the fingerprint image are labelled with a unique ID for further operation. The labelling operation is realized by using the Morphological operation: bwlabel.

.

**Step 6 – Minutia Postprocessing**

**Part 1: False Minutia Removal**

The pre-processing stage does not totally heal the fingerprint image. For example, false ridge breaks due to insufficient amount of ink and ridge cross-connections due to over inking are not totally eliminated. Actually, all the earlier stages themselves occasionally introduce some artifacts which later lead to spurious minutia. These false minutiae will significantly affect the accuracy of matching if they are simply regarded as genuine minutia. So, some mechanisms of removing false minutia are essential to keep the fingerprint verification system effective.

Seven types of false minutia are specified in following diagrams:

m1 m2 m3 m4

m5 m6 m7

False Minutia Structures. m1 is a spike piercing into a valley. In the m2 case a spike falsely connects two ridges. m3 has two near bifurcations located in the same ridge. The two ridge broken points in the m4 case have nearly the same orientation and a short distance. m5 is alike the m4 case with the exception that one part of the broken ridge is so short that another termination is generated. m6 extends the m4 case but with the extra property that a third ridge is found in the middle of the two parts of the broken ridge. m7 has only one short ridge found in the threshold window.

Several error-handling conditions are used which trigger when any one of these abnormal Structures are seen. This ensures False Minutia structures do not get passed on for matching purposes in the next step. It is also essential to remember to not overuse the conditional error-handling so as to not remove genuine minutiae at this stage.

**Part 2: Unify terminations and bifurcations**

Since various data acquisition conditions such as impression pressure can easily change one type of minutia into the other, most researchers adopt the unification representation for both termination and bifurcation. So, each minutia is completely characterized by the following parameters at last: 1) x-coordinate, 2) y-coordinate, and 3) orientation.

**Step 7 – Minutia Matching**

Given two set of minutiae of two fingerprint images, the minutia match algorithm determines whether the two minutia sets are from the same finger or not.

An alignment-based match algorithm partially derived from the Lin Hong’s "Automatic Personal Identification Using Fingerprints" is used in this project. It includes two consecutive stages: one is alignment stage and the second is match stage.

1. Alignment stage. Given two fingerprint images to be matched, choose any one minutia from each image, calculate the similarity of the two ridges associated with the two referenced minutia points. If the similarity is larger than a threshold, transform each set of minutia to a new coordination system whose origin is at the referenced point and whose x-axis is coincident with the direction of the referenced point.
2. Match stage: After we get two set of transformed minutia points, we use the elastic match algorithm to count the matched minutia pairs by assuming two minutiae having nearly the same position and direction are identical.

**Quantitative experimental data for fingerprint matching:**

Each unique fingerprint is given a number (101, 102, etc.) and each sub-version as denoted after an underscore (101\_1, 101\_2, etc.) is the same fingerprint but scanned in a different position. The minutiae match system is designed specifically to detect fingerprints even when the scans may not be pinpoint accurate as they are difficult to achieve in practical conditions, but it can only cover so much for scanning imperfections (see image 101\_2) and therefore is showcased to display what an improper fingerprint scan can cause. There is a substantial number of fingerprint samples available for testing but we have kept this observational sample to a minimum for display constraints.

101\_1 101\_2 101\_3

102\_1 103\_1 103\_3

|  |  |  |
| --- | --- | --- |
| **Fingerprint 1** | **Fingerprint 2** | **% Match** |
| 101\_1 | 101\_1 2%noise | 29.1667 |
| 101\_1 | 101\_1 5%noise | 29.1667 |
| 101\_1 | 101\_1 9%noise | 29.1667 |
| 101\_1 | 101\_2 | 29.1667 |
| 101\_1 | 101\_3 | 25 |
| 101\_1 2%noise | 101\_1 5%noise | 56.5217 |
| 101\_1 5%noise | 101\_1 9%noise | 70.3704 |
| 101\_3 | 101\_3 2% noise | 39.1304 |
| 101\_3 | 101\_3 5%noise | 39.1304 |
| 101\_3 2% noise | 101\_3 5%noise | 63.6364 |
| 101\_1 2%noise | 101\_3 5%noise | 43.4783 |
| 101\_3 | 101\_2 | 26.087 |
| 101\_1 | 102\_1 | 20.456 |
| 101\_3 | 103\_1 | 25 |

The Minutiae based SIFT system not only is heavily resistant to noisy pictures but is also surprisingly well suited to work with noisy pictures compared to noiseless ones as well.

**FUTURE SCOPE OF WORK**

* Design of improved and more suitable voice sampling system as part of biometric authentication.
* Design of suitable thumb impression gathering hardware as part of biometric authentication.
* Testing the effectiveness of data hiding algorithm for judging data hiding imperceptibility and robustness.
* Further modification of Data hiding Algorithm to embed and retrieve images of higher resolution.
* Optimising Audio Authentication system to distinguish between Similar and different audio with even higher fidelity, especially under noisy conditions.
* Alternatively, upgrade the fingerprint SIFT system to take lower-resolution fingerprint images as input and work with it properly.
* Design of a comprehensive Client – server program to embed, retrieve and compare steganographic data in Cover documents.

**References**

* + - 1. “National Scholarship Portal (NSP) Standard Operating Procedures”, Version 1.0, July 2019, NSP Team, NIC DBT Mission, Central Ministries of the Onboarded schemes
      2. Mishra, K. N. (2016) “AAdhar based smartcard system for security management in South Asia”, In the Proceedings of International Conference on Control, Computing, Communication and Materials (ICCCCM), pp. 1–6.
      3. Anitha, V., & Velusamy, R. L. (2012) “Authentication of digital documents using secret key biometric watermarking”, International journal of communication network security, Vol. 1, Issue 4, pp. 5–11.
      4. S. Hubli and A. S. Nayak, “Watermarking technique for tamper detection of cheque image in CTS,” International Journal on Recent & Innovation Trends in Computer & Communications, vol. 5, no. 1, pp. 281-284, January, 2017.
      5. Hasan, H. R. (2018) “Copyright Protection for Digital Certificate using Blind Watermarking Technique”, Kurdistan Journal of Applied Research, Vol. 3, Issue 1, pp. 75–79.
      6. Lin Hong. "Automatic Personal Identification Using Fingerprints", Ph.D. Thesis, 1998.
      7. L.C. Jain, U.Halici, I. Hayashi, S.B. Lee and S.Tsutsui. Intelligent biometric techniques in fingerprint and face recognition. 1999, the CRC Press.
      8. D.Maio and D. Maltoni. Direct gray-scale minutiae detection in fingerprints. IEEE Trans. Pattern Anal. And Machine Intell., 19(1):27-40, 1997.
      9. Arkadip Roy, “Online Validation of E-documents with Multi-Signature Driven Certifications”