Multi-Phase Digital Authentication of e-Certificate with Secure Concealment of Multiple Secret Copyright Signatures

Soumit Chowdhury, Sontu Mistry, Nabin Ghoshal

Abstract*: The work suggests a unique data security protocol for trusted online validation of e-documents like university certificates to confirm its credibility on different aspects. The idea reliably validates such e-documents from both the issuing authority and incumbent perspectives by strongly complying the security challenges like authentication, confidentiality, integrity and non-repudiations. At the very beginning, the parent institute physically issues the client copyright signature to the incumbent and stores this signature and biometric fingerprint of the incumbent on the server database. Additionally, the server secretly fabricates ownership signatures of parent institute and concern officer both within the e-document and this certified e-document is kept on the server database. Importantly, these signature fabrications are governed by self-defined hash computations on incumbent registration and certificate number respectively. Next, the server transmits this signed e-document to the client after a successful login by the client. Now client conceals shared copyright signature and taken thumb impression of the incumbent separately within this received e-document. Critically, these client-side signature castings are employed through self-defined hash computations on the incumbent name and obtained marks respectively. Finally, this authenticated e-document is validated at the server end by sensing all authentic signatures from it through those same identical hash operations. For stronger authenticity each signature is concealed by tracing its valid or authentic circular orientation of fragment sequences and embedding locations both derived from respective hash operations. Also, each signature is dispersed in non-overlapping manners on each separate region of the e-document promoting better signature recovery. Additional robustness is further injected with variable encoding of signature bits on different transformed pixel byte components of the e-Certificate image. Overall, the scheme confirms significant performance enhancements over exiting approaches with exhaustive simulation results on image data hiding aspects and their standardized comparisons

***Index Terms*: e-Certificate Authentication, Hash-Based Validation, Multi-Signature Fabrication, Variable Encoding**

Revised Manuscript Received on August 05, 2019

Soumit Chowdhury, Department of Computer Science and Engineering, Government College of Engineering & Ceramic Technology, Kolkata, India. (*Corresponding Author)

Sontu Mistry, Department of Computer Science and Engineering, Government College of Engineering & Ceramic Technology, Kolkata, India.

Nabin Ghoshal, Department of Engineering & Technological Studies (DETS), University of Kalyani, West Bengal, India.

I. INTRODUCTION

Rapid growth of digital data communication in recent time has urged the need for validation cum authentication of such digital documents in order to ensure trusted data transmission. In this aspect secret fabrication of some copyright signature on the concern e-document is the traditional practice to achieve ownership claims. This idea is mainly implemented through digital watermarking concepts where presence of such secretly fabricated signatures will remain unknown to the unauthorized recipients. Further, all these secretly embedded signatures also required to be protected from different external image processing attacks. Hence these approaches are quite useful for authenticating vital digital documents existing in the form of images such as e-certificates. Importantly this practice will be quite useful for online validation of such e-documents which are needed for the purpose of third-party verification. So, to emphasis this issue the proposed work designs a unique data security protocol for validation cum authentication of such e-documents and the main objective of this scheme are-

1. Achieving ownership claims for such e-documents from both the issuing authority and the candidate perspectives.
2. Data validations for the e-certificate using hash value-based signature fabrication concept which is performed on all the critical e-certificate data.
3. Complying critical data security issues like authentication, confidentiality, integrity, Non-repudiations.
4. Incorporation of secure data hiding techniques for signature fabrications using variable encoding of secret signature bits.

The vital issue here is that most of the existing works have actually focused such e-document authentications only by utilizing the idea of ownership claims. However, a digital document validation is a bigger issue where the authenticity of the whole document is important and, in this aspect, the existing works in this domain are highlighted further.

To depict the utility of these proposed concepts the paper is organized as follows- next sec. II discusses the existing works, followed by enhancements in sec. III.

Further sec IV states the data validation protocol, while sec. V focuses on signature bit encoding and decoding algorithm. Then, sec. VI highlights the simulation results and comparisons, with the existing works. Finally, sec-VII gives the conclusion followed by references are listed at the end.

II. RELATED WORKS

Among the recent approaches on e-document authentications, Anitha et al. [1] implemented the idea of biometric watermarking for verifying the relation between the owner and the details on the document. Biometric details(iris image) of the user is captured and converted to a live template to obtain a bit code image which is periodically duplicated to be of same size of the cover image. Both the cover and the bit code images are partitioned into same-sized blocks. The watermark bits are generated from an XOR operation of the bit code image blocks and a hash value for each block from a set of inputs interconnected to the image particulars which is then encoded into the LSBs of the cover image blocks. Largescale tampering of the document can be detected using this model but it fails in distinguishing the sensitive tampering from external noise attacks as it is not validated for noise and small-scale tampering.

Kamta [2] introduced a method to verify the document owner's legitimacy by using biometric details of the owner which include fingerprints, retinal scan, facial characteristics, palatal patterns and DNA to be inserted in a smart card provided to the owner for identification. Based on the owner's biometric details, sixteen possible categories are created, each of which is a string containing 'y' & 'n' and the biometric identifier string corresponding to each user is stored in a central database. During the verification, the recaptured biometric details and the recalculated string is matched using a NDFA having five possible states and input symbols for each state. If the string is accepted by NDFA then the authenticity of the owner is verified. This scheme fails to determine the impact of external noise incorporated in the smart card and no focus on template generation from the biometric data.

Further, very recently Hasan [3] has offered a segmented multi watermarking scheme for better security and robustness of digital documents by dividing the cover image into three regions of different intensity namely R,G,B components. R ,G and B components are embedded into the RW, GW and BW components of the watermark image by converting the R,G,B of the cover image into transform domain using DWT. Three levels LH1,LL2,LL3 and the watermarks are inserted into LL3.Lastly the RRW,GGW,BBW are combined together to get the watermarked image of the digital document.

In view of such e-document validations, the multi-signature fabrication aspect will come in very handy while establishing ownership claims for achieving multi-purpose authentication. Apart from that these multi signature-based authentications known as multi-watermarking also provides more secure and trustable authentications. Vitally these multi watermarking concept are broadly categorized as – (a) Composite – All watermarks are combined to a single one to be embedded. (b) Successive – One watermark is codded on top of the other embedded watermark, (c) Segmented – Different watermarks are embedded on separate non-overlapping portions. Among these multi watermarking concepts both composite and successive ones are secure to a reasonable extent, but the segmented type is observed to have good robustness. So, on the basis of this experience this proposed authentication concept can be better implemented through segmented multi-signature scenarios. Interestingly, this multi-signature hiding implies both multi-copy signature coding as well as multiple different signature embedding approaches and this aspect some segmented multi-watermarking ideas are as follows.

Nasir et al. [4] has proposed the approach of one non-blind method where multiple encrypted fragments of a binary copyright image dispersed in their respective copies. This fragment hiding was thoroughly executed on different regions of the blue components of the host color image using spatial encoding mechanisms.

Behnia et al. [5] showed a more upgraded work by using chaotic map-based technique, that reflected the hiding of different binary watermarks onto the concern Red, Green, and Blue channel, in which both the data embedding positions and secret data bits were securely encrypted.

Further, more sophisticated works on multi-watermarking is carried out in the frequency domain for better security and robustness. Among these works, Bhatnagar et al. [6] coded multi-watermarks on non-overlapping DCT blocks where the threshold value of block energy is utilized in secret data coding. To achieve better robustness, recent transform domain works are more focusing on Discrete Wavelet Transformed (DWT) coefficients to encode the secret data.

Interestingly Babaei et al. [7] has reflected segmented multi-watermarking on non-overlapping uniform wavelet block.

Natarajan et al [8] suggested a watermarking technique, where two binary watermarks were embedded one after the other on the grayscale source image in the LL2 sub-band of the DWT using the additive, multiplicative & hybrid coding. This method shows better security for the "single watermark approach" most noticeably for the "hybrid coding" but with some effect on the hidden image quality.

Thanki et al [9] suggested a powerful two-level watermarking in which multi-purpose DWT is used on the host fingerprint image and higher recurrence values are selected for watermarking. One level DWT is applied on the face and iris image. On the basis of Compressive Sensing (CS) theory scanty quantification data is obtained using transform values. This acquired data, playing the role of a secure watermark is placed on the HH3 and HH4 values of host fingerprint for iris and face watermark pictures.

Using selective DWT values in embedding Singh et al [10] proposed a robust multiple watermarking process for medical images. This technique depends on reliable spread-spectrum method where false noise orders are constructed with respect to each watermarking bit. These orders are placed in the chosen DWT values column wise within the sub-band. This scheme is found to be comparatively better in terms of activeness and imperceptibility. Mohananthini et al [11] developed a multiple watermarking process based on DWT for both medical and color images. The two watermarks are combined resulting in a single watermark and the extricated watermarks are taken out from the modified image.

Mohananthini et al [12] on comparing the performances of the multiple successive and segmented message hiding techniques on the host color image found that the LL2 sub-band of the 2 level DWT is identified for watermark insertions. The second watermark is added on the intermediate watermarked image produced after the first watermark whereas in case of segmented approach two watermarks are embedded on the LL2 sub bands - on the even and odd number of rows respectively for the host image.

Natarajan et al [13] developed a multiple watermarking method based on distinct wavelet transmute for the interpretation of indistinguishable nature and activeness. Watermarks are inserted into sub bands via genetic algorithms.

In view of these existing approaches it is obvious that most of the multi-watermarking-based concepts have focused secure data hiding and its robustness scenarios. Also, the digital authentication part is critically achieved with watermarking perspective rather than designing some trusted data security protocol. Hence, by considering these issues the proposed approach aims to develop a secure client-server subscriber authentication protocol to validate the issued e-Certificate to the candidate. So, for building such an application the specific improvements on existing ideas are now discussed as follows.

III. ENHANCEMENT OVER EXISTING APPROACHES

In contrast to the current approaches for digital authentication of e-documents, this proposed work categorically focusing on a secure data security protocol for validating the whole digital document. In this context the proposed protocol addresses both way ownership claims as well as the data validation scenarios for the e-Certificate. The critical factor here is that this proposed protocol encourages on spot validation of the e-Certificate from client perspectives with a definite aim to satisfy the non-repudiation and data integrity issues.

Apart from addressing the necessary data security properties this proposed approach also utilises a novel authentication criterion with circular orientation of hidden signature fragments. Since, this circular orientation is dynamically decided based on starting fragment index computed through the secure hash operation, so this concept serves a new horizon in the image authenticity scenarios.

In addition of developing such a secure data authentication protocol this approach also injects some specific improvements on data hiding techniques to achieve most trustable digital authentications. This is mainly achieved through variable encoding of secret signature bits on different transformed pixel byte components. Further, this secret bit embedding is also based on variable threshold range driven bit encoding scenarios for better imperceptibility and robustness. Apart from robust data hiding for secret signature fabrication this proposed work also believes in multi-copy signature fabrication which ultimately helps in better signature recovery under attacks. Since this work is implemented for both color signature and host images, so achieving better data hiding imperceptibility under higher data payload is also one of the improvements over the existing data hiding practices.

So, considering all these critical issues this proposed approach actually incorporates significant enhancements on various aspects over the existing works and the concern details in this regard are now discussed from the next section onwards.

In order to implement the data validation and ownership aspects, different copyright signatures of both the issuer and the concern candidate is secretly fabricated on the e-Certificate document. In this context, multiple copies of four different signatures are casted on that e-document by utilizing the hash values derived from the authentic certificate data. Importantly the proposed signature fabrication concept is visualized through Fig. 1, where each of four equally divided regions of the host image is further partitioned into four equal non-overlapping segments (P1, P2, P3, P4). Critically each of these segments will host the concern signature based on the hash value derived from the respective authentic data. To materialize this idea each signature on the concern segment is fabricated depending upon the circular orientation of the signature fragments and also the concern matrix interval of such signature data casting. For convenience here each secret signature bit is embedded on each pixel byte element of a 2x2 sub image bock matrix. Importantly, each of these four signatures are fabricated by deriving hash values determining the starting signature fragment index and the concern data matrix interval found from the particular certificate data. This idea is clearly pictorially demonstrated in Fig.1 with multi-copy hosting of each signature on different regions of the e-Certificate such that same signature casting orientation for a particular segment is repeated for all regions. This discussed signature bit hiding concept is categorically focused for region-2 of the e-Certificate in Fig. 1 as a sample. In this elaborated demonstration of region-2, a sample 2x2 sub-block matrix is shown with elements [A_{11}, B_{11}, C_{11}, D_{11}]. Here Segment-1 hosts the University's Copyright Signature (U_Sign) with its circular fragment orientation started with fragment index = 4, which is derived from the hash operation on Candidate's Registration Number (R_No).

Hence the first matrix element A_{11} hosts the bit for the 4th fragment of the U_Sign. Similarly, the 2nd element (B_{11}), 3rd element (C_{11}) and 4th element (D_{11}) of the sub block matrix host the signature bit for fragment 1, 2 and 3 of U_Sign respectively. In addition of this signature fragment orientation another hash value is derived from same R_No, which will determine this secret data fabrication matrix interval in segment-1. Further, by adopting this similar idea other concern signatures are also fabricated in the respective segments of region-2. In this aspect the Issuing person Signature (A_Sign), Candidate's on spot Thumb impression (C_Thumb) and Candidate's copyright Signature (C_Sign) fabricated on segment-2, 3, 4 respectively. Vitally each of these signature fabrications are also done with their concern hash values determining the circular orientation of signature fragments and the data matrix interval for secret data casting. So, to promote strong validation cum authentication, this A_Sign, C_Thumb and C_Sign are further secretly fabricated based on their concern hash values derived from Certificate Number (C_No), Candidate's Name (C_Name) and obtained marks data (C_Marks) respectively.

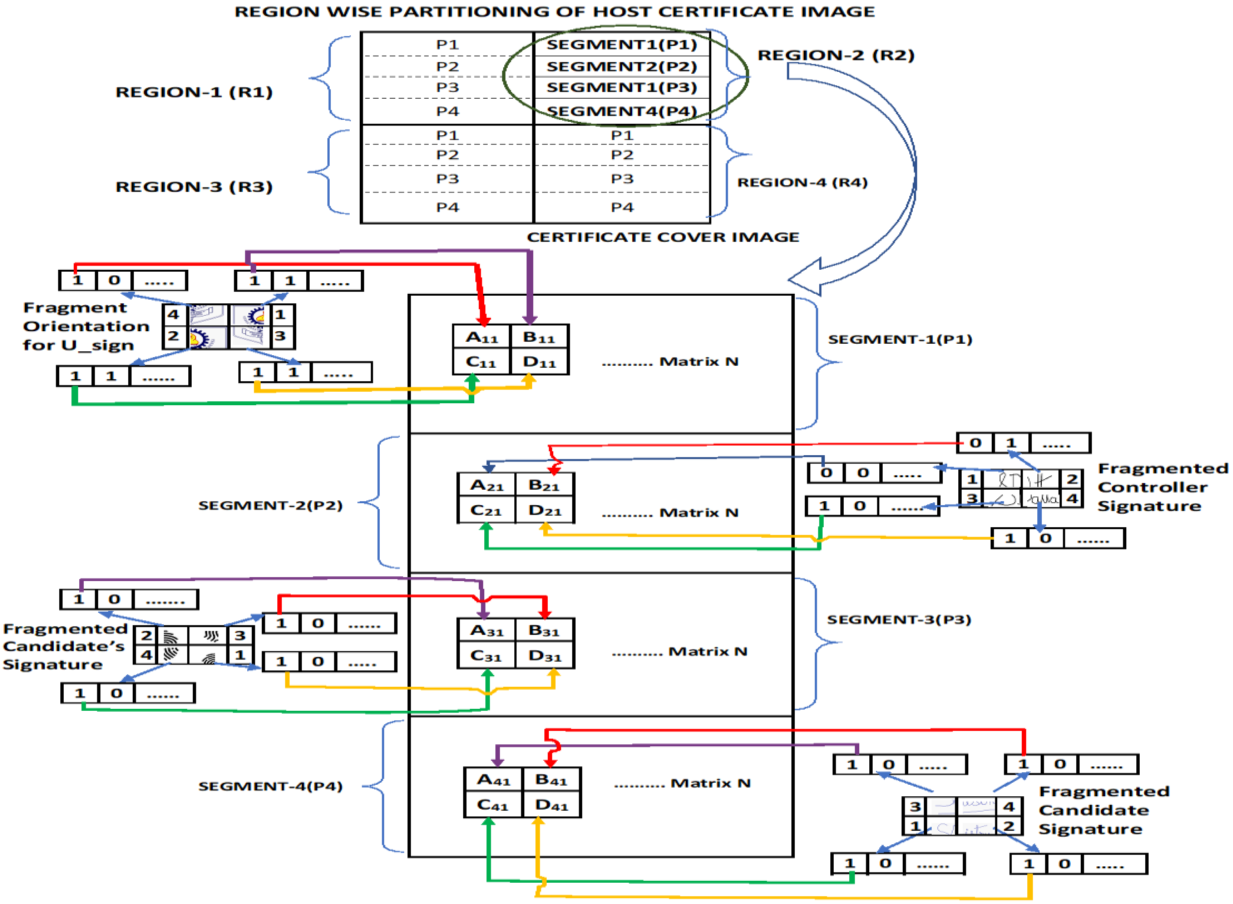


Fig. 1: Signature Bit Orientation Mechanism

IV. PROPOSED DATA AUTHENTICATION PROTOCOL

The authentication process is first initiated by the server with secret fabrication of university copyright signature and the issuing person's signature as images within the concern digital certificate on non-overlapping portions. Critically these two signature fabrications are based on the hash value derived from the incumbent's or the candidate's registration number and the particular certificate number. Importantly, one copy of each of these signatures are fabricated on each of the four equally segmented separate regions of the digital certificate to promote signature recovery under different attacks. In this aspect university copyright signature is fabricated in segment-1 of each region while issuing person's signature is embedded in segment-2 of each region. Now, this signature fabricated digital document is issued to the particular candidate for its' subsequent validation from the client-side. To ensure the candidate's ownership the thumb impression of the candidate is taken on spot and signature provided by the university to the candidate are secretly embedded on the same digital certificate in segment-3 and segment-4 of each region based on the hash value found from the candidate's name and the grade value awarded. Further, all these signatures fabricated authenticated digital certificate is transmitted to the server for its final phase of validation. Since server database keeps all those ownership signatures and candidate record, so the server-side validates all those detected signatures sensed from the digital certificate by utilizing those same hash operations as used during the signature embedding process. For confirming the authentication, the best-detected copy of each signature found from each region of the digital certificate is matched with its' original form stored in the database. In this context, a certain threshold value of each signature needs to be complied to finalize the total authentication process. This whole idea of the authentication is stepwise highlighted as below for a better understanding of the client-server validation protocol.

Step1: University secretly embeds its copyright signature on the first segment of each region of the concern digital document based on the hash value found on student's registration number (R_No). This signature embedding is visualized in Fig. 2 where the hash values determining the circular embedding of signature fragment orientations and also the matrix interval [$H_{12} \in \{1,2,3\}$] of that signature data embedding for this first segment. Further these two-hash values computation on R_No, determining the starting fragment index [$H_{11} \in \{1,2,3,4\}$] for the circular orientation of signature fragments and the matrix interval of signature data embedding is reflected through the following equations (1) and (2), where r_i is the $i^{th} \in \{1,2,\ldots n\}$ digit in the roll number.

$$\mathbf{H_{11} = [(R\_No + \textstyle\sum_{i=1}^{n} r_i)\ Mod\ 4] + 1} \qquad (1)$$

$$\mathbf{H_{12} = [(reverse\ of\ R\_No + \textstyle\sum_{i=1}^{n} r_i)\ \ Mod\ 3] + 1} \qquad (2)$$

Step2: University secretly embeds issuing person's proprietary signature on the second segment of each region of the same digital document based on the hash value generated on the particular certificate number (C_No). This signature embedding is also reflected in Fig. 2 where the computed hash values determining the circular embedding of signature fragment orientations and also the matrix interval [$H_{22} \in \{1,2,3\}$] of that signature data embedding for this second segment. Further these two hash value computations on C_No determining the starting fragment index [$H_{21} \in \{1,2,3,4\}$] for the circular orientation of signature fragments and matrix interval (H_{22}) of signature data embedding is reflected through the following equations (3), (4), where d_i is the i^{th} digit [$i \in \{1,2,\ldots n\}$] of C_No.

$$\mathbf{H_{21} = [\ (C\_No + \textstyle\sum_{i=1}^{n} d_i)\ Mod\ 4\ ] + 1} \qquad (3)$$

$$\mathbf{H_{22} = [\ (reverse\ of\ C\_No + \textstyle\sum_{i=1}^{n} d_i)\ \ Mod\ 3\ ] + 1} \qquad (4)$$

Let, **I** is the original e-Certificate and $\mathbf{I_1}$ is the signature codded e-Certificate with embedding of U_Sign and A_Sign in Segment 1 and 2 of each region of the e-Certificate respectively. Now if each four signature fragments of U_Sign and A_Sign are stored in the array $L[q]\,[j]_{q = 1\ to\ 2,\ j = 1\ to\ 4}$ then this signature fabricated e-Certificate denoted as I_1 is given by

$$I_1 = F\ (I,\ L[q][j]_{\ q=1\ to\ 2,\ j = 1\ to\ 4},\ H_{11},\ H_{12},\ H_{21},\ H_{22})$$

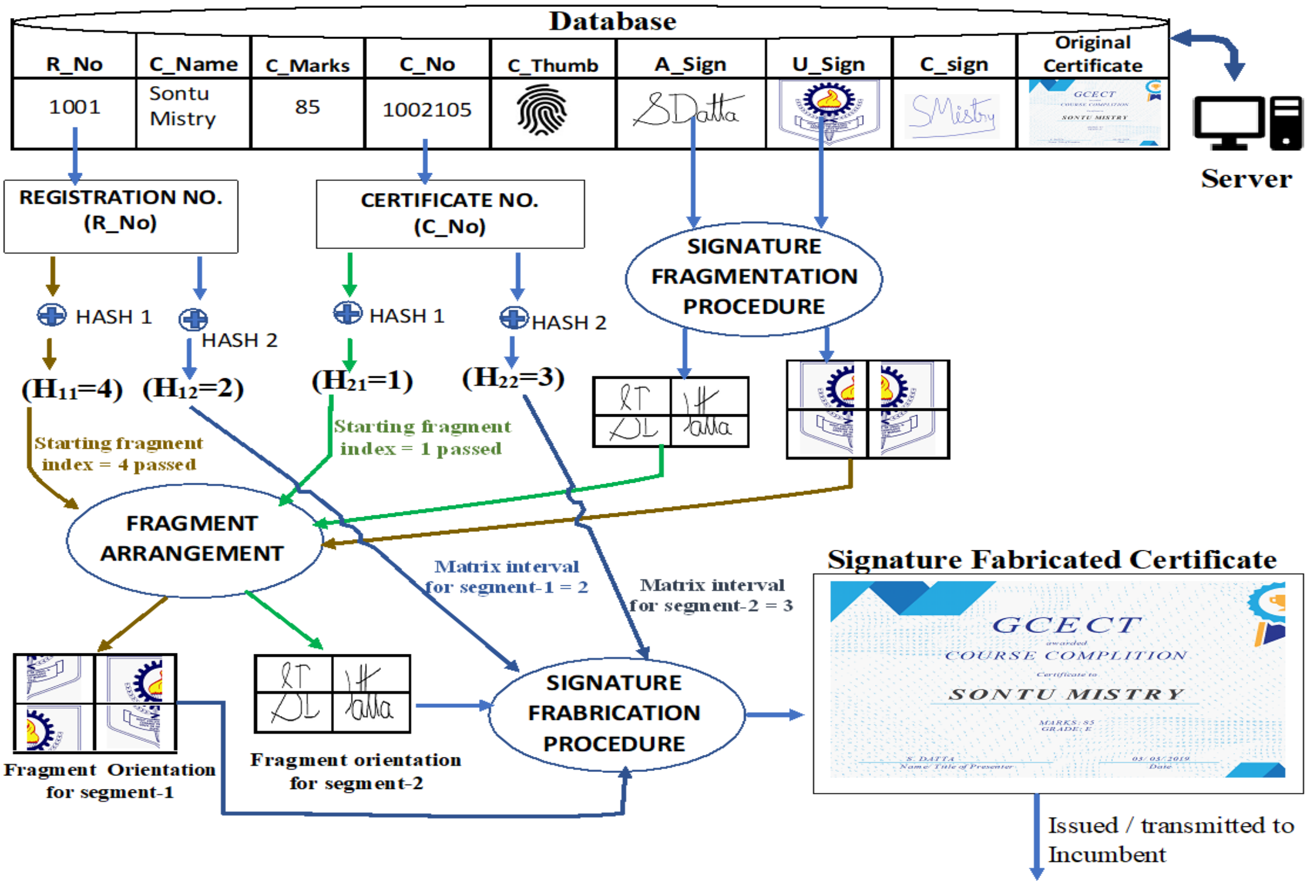

Database
R_No
C_Name
C_Marks
C_No
C_Thumb
A_Sign
U_Sign
C_sign
Original Certificate
1001
Sontu Mistry
85
1002105
Server
REGISTRATION NO. (R_No)
CERTIFICATE NO. (C_No)
SIGNATURE FRAGMENTATION PROCEDURE
HASH 1
HASH 2
HASH 1
HASH 2
(H11=4)
(H12=2)
(H21=1)
(H22=3)
Starting fragment index = 4 passed
Starting fragment index = 1 passed
FRAGMENT ARRANGEMENT
Matrix interval for segment-1 = 2
Matrix interval for segment-2 = 3
Signature Fabricated Certificate
GCECT
COURSE COMPLETION
SONTU MISTRY
SIGNATURE FRABRICATION PROCEDURE
Fragment Orientation for segment-1
Fragment orientation for segment-2
Issued / transmitted to Incumbent

Fig. 2: Server-Side Bit Fabrication Procedure

Step 3: This server-side signature embedded authenticated digital document is now issued to the concern candidate.

Step 4: The authorized client login to the server-side database by using the candidate registration number as the login id and the concern applicable password.

Step 5: Server validates client's authorization and conveys the respective acknowledgment to the client.

Step 6: Now the candidate's thumb impression taken on spot (C_Thumb) is embedded on the third segment of each region of I_1. Importantly, this biometric signature embedding is done on the basis of two hash value computations performed on the name of the candidate (C_Name) and this concept is highlighted in Fig. 3. Here, two hash values determining the starting fragment index [$H_{31} \in \{1,2,3,4\}$] for the circular orientation of signature fragments and the particular matrix interval [$H_{32} \in \{1,2,3\}$] of signature data embedding. Critically these hash operations are reflected with the following equations (5), (6), where a_i representing the i^{th} character ASCII value of the name [$i \in \{1, 2, \ldots .n\}$]

$$H_{31} = [(\textstyle\sum_{i=1}^{n} a_i * 2^{i}) \text{ Mod } 4] + 1 \qquad (5)$$

$$H_{32} = [(\textstyle\sum_{i=1}^{n} a_i * 2^{n-i+1}) \text{ Mod } 3] + 1 \qquad (6)$$

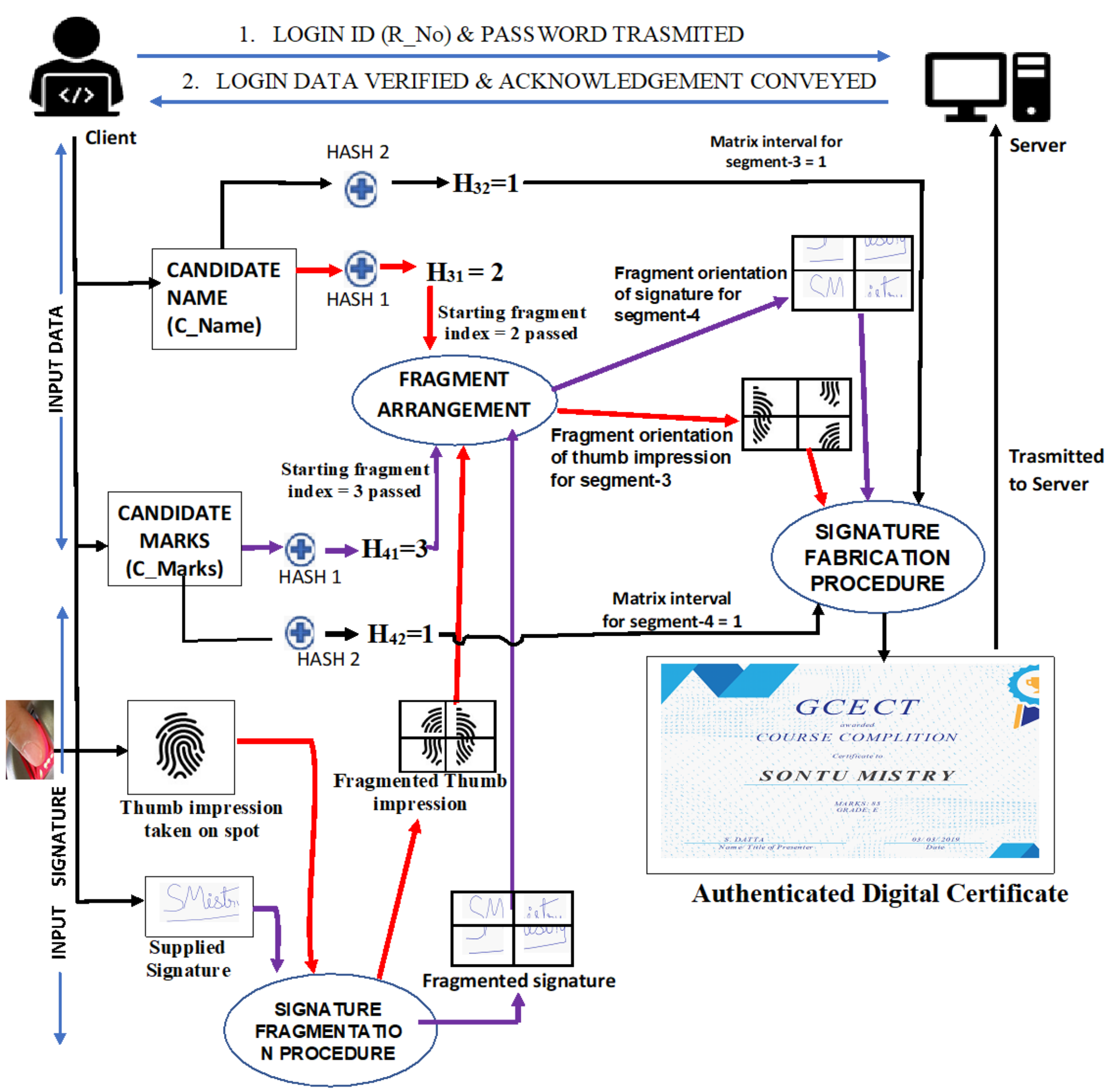

1. LOGIN ID (R_No) & PASSWORD TRASMITED
2. LOGIN DATA VERIFIED & ACKNOWLEDGEMENT CONVEYED
Client
Server
INPUT DATA
INPUT SIGNATURE
HASH 2
H_{32}=1
Matrix interval for segment-3 = 1
CANDIDATE NAME (C_Name)
HASH 1
H_{31} = 2
Starting fragment index = 2 passed
Fragment orientation of signature for segment-4
FRAGMENT ARRANGEMENT
Fragment orientation of thumb impression for segment-3
Starting fragment index = 3 passed
CANDIDATE MARKS (C_Marks)
HASH 1
H_{41}=3
HASH 2
H_{42}=1
Matrix interval for segment-4 = 1
SIGNATURE FABRICATION PROCEDURE
Trasmitted to Server
Thumb impression taken on spot
Fragmented Thumb impression
Supplied Signature
Fragmented signature
SIGNATURE FRAGMENTATION PROCEDURE
GCECT
COURSE COMPLITION
SONTU MISTRY
Authenticated Digital Certificate

Fig. 3: Client-Side Bit Fabrication Procedure

Step 7: Now the copyright signature (C_Sign) of the candidate is secretly fabricated onto the fourth segment of each of region of I_1 resulting the authenticated e-Certificate I_2. This signature fabrication is performed based upon two hash values derived from the obtained numeric grade (C_Marks) of the candidate as reflected in Fig 3. These two hash values will determine the starting fragment index [$H_{41} \in \{1,2,3,4\}$] of the circular orientation of signature fragments and the particular matrix interval [$H_{42} \in \{1,2,3\}$] of signature fragment data embedding on the concern segment. Critically these hash operations are reflected through the following equations of (7), (8). In this aspect, if the integer part of C_Marks is represented by v_1 and its fraction part is denoted as v_2 then the hash operations are

$$H_{41} = [(v_1 + v_2 + digit\ sum(v_1))] \text{ Mod } 4 + 1 \qquad (7)$$

$$H_{42} = [(\text{reverse}(v_1) + v_2 + \text{digit sum}(v_1))]\text{Mod } 3 + 1 \qquad (8)$$

Let us assume that the four signature fragments of each signature version C_Thumb and C_Sign are stored in the 2-D array $L[q]\,[j]_{q = 1 \text{ to } 2,\ j = 1 \text{ to } 4}$ then these signature fabricated e-Certificate I_2 is obtained through the expression –

$$I_2 = F\,(I_1,\ L[j]_{\,q=1 \text{ to } 2,\ j = 1 \text{ to } 4},\ H_{31},\ H_{32},\ H_{41},\ H_{42})$$

Step 8: Now this digitally authenticated e-Certificate (I_2) is transmitted to the server for its subsequent validation

Step 9: Server computes those same hash values H_{11} & H_{12} by adopting Eq. (1) & (2) and utilizing the same registration number (R_No) of the candidate fetched from server database. Similarly, other same hash value sets like (H_{21}, H_{22}), (H_{31}, H_{32}) and (H_{41}, H_{42}) are computed by the server through Eq. (3, 4), (5, 6) and (7, 8) with utilization of the same C_No, C_Name and C_Marks data respectively as fetched from server.

Step 10: At this stage, the server utilizes those concern hash values applicable for the concern segment and detects the respective signatures from the particular segment of the e-Certificate. So, by tracking the data matrix intervals like H_{12}, H_{22}, H_{32} and H_{42} through those derived hash values the server extracts the concern signature fragments of U_Sign, A_Sign, C_Thumb and C_Sign respectively. Critically, such fragments of U_Sign, A_Sign, C_Thumb and C_Sign are detected from the concern segments 1, 2, 3 and 4 of each region respectively.

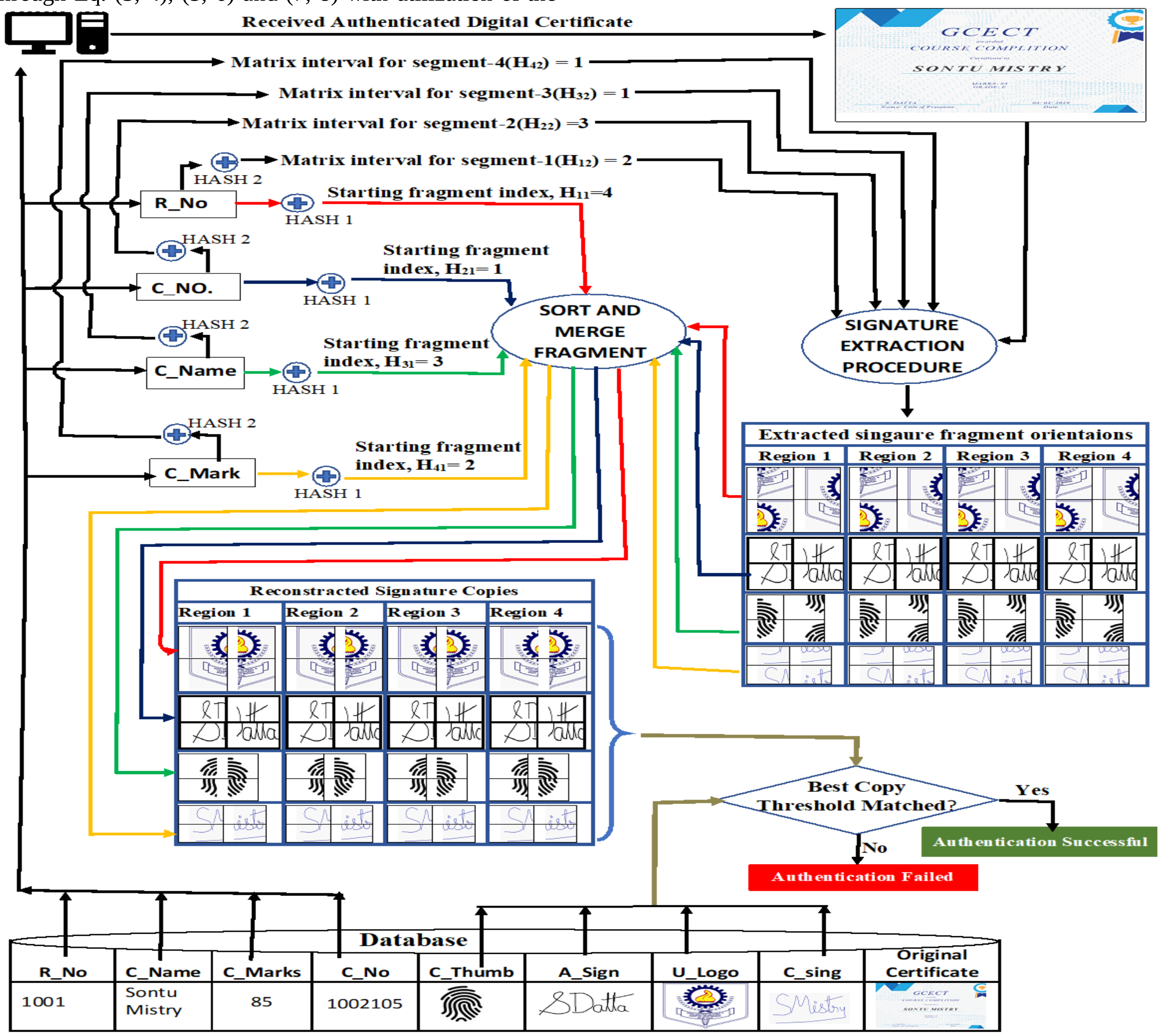

Received Authenticated Digital Certificate
GCECT
COURSE COMPLETION
SONTU MISTRY
Matrix interval for segment-4(H42) = 1
Matrix interval for segment-3(H32) = 1
Matrix interval for segment-2(H22) =3
Matrix interval for segment-1(H12) = 2
HASH 2
R_No
Starting fragment index, H11=4
HASH 1
HASH 2
C_NO.
Starting fragment index, H21= 1
HASH 1
HASH 2
C_Name
Starting fragment index, H31= 3
HASH 1
HASH 2
C_Mark
Starting fragment index, H41= 2
HASH 1
SORT AND MERGE FRAGMENT
SIGNATURE EXTRACTION PROCEDURE
Extracted singaure fragment orientaions
Region 1
Region 2
Region 3
Region 4
Reconstracted Signature Copies
Region 1
Region 2
Region 3
Region 4
Best Copy Threshold Matched?
Yes
No
Authentication Successful
Authentication Failed
Database
R_No
C_Name
C_Marks
C_No
C_Thumb
A_Sign
U_Logo
C_sing
Original Certificate
1001
Sontu Mistry
85
1002105

Fig. 4: Server-side Authentication Procedure

Step 11: At this stage, each of the four extracted signature fragments found from the concern segment of the particular region is merged based on the respective starting fragment index derived as hash value. So, by following this method the concern signatures U_Sign, A_Sign, C_Thumb and C_Sign are reconstructed by utilizing the starting fragment index hash values H_{11}, H_{21}, H_{31} and H_{41} respectively. Hence, with this idea four copies of each of the signature is recovered from different regions of the authenticated e-Certificate. Further, all these reconstructed signature copies are matched with the original signature copy stored at the server database to track the best-detected copy for each signature.

Now if at least one of the signature copies for each signature category satisfies a predefined threshold value of matching then server conforms the total validation of the e-Certificate. The step-wise mathematical discussion of this final data validation and authentication procedure is highlighted as follows.

Let us assume, N[reg][sig][part] stores the region-wise four decomposed signatures for each signature orientation type. Hence the array index reg ϵ {1, 2, 3, 4} denoting the concern region number while sig ϵ {1, 2, 3, 4} is used for storing each signature copy related to a specific orientation and part ϵ { 1, 2, 3, 4} is for the 4 decomposed part of each signature. Further Sort_Merge operation is done to get the MARGED[reg][sig] matrix which stores the reconstructed signature images of each region. Then each signature stored in different regions are compared with the signature image stored in STORE[sig] array, which was fetched from the server's database. If signatures of MARGED[reg][sig] and signatures of STORE[sig] matches with some predefined threshold value then a success message is sent to the client, else a failure message is generated.

```
$\text{STORE[sig]}_{\text{sig = 1 to 4}}$ = [U_Sign, A_Sign, C_Thumb, C_Sign];
$\text{N[reg][sig][part]}_{\text{reg= 1 to 4, sig = 1 to 4, part= 1 to 4}} = F^{-1} (I_2, H_{12}, H_{22}, H_{32}, H_{42})$;
$\text{MARGED[reg][sig]}_{\text{reg = 1 to 4, sig =1 to 4}}$ = Sort_Merge ($\text{N[reg][sig][part]}_{\text{reg=1 to 4, sig= 1 to 4, part =1 to 4}}, H_{11}, H_{21}, H_{31}, H_{41}$);
  for reg = 1 to 4
      for sig = 1 to 4
          If (MERGED[reg][sig] = = STORE[sig])
              Count[sig] ← Count[sig] + 1;
          Else
              Continue;
If (Count[1] && Count[2] &&Count[3] && Count[4]==1)
          Send("Successful Authentication");
Else
          Send("Authentication Fail");
End;
```

V. SIGNATURE BIT FABRICATION AND DETECTION

The cover image is logically partitioned into four equal regions and each region is further divided into four equal segments as shown in Fig. 1. Now, the concern segment of the certificate image is initially divided into consecutive series of 2x2 non-overlapping sub-block matrices of pixel bytes. Now one single bit is fabricated on each pixel byte element of such 2x2 sub-block matrix. For this purpose, the pixel bytes of the submatrix is transformed and single signature bit is encoded on each such transformed component. Further, these bit coded pixel byte elements are reverse transformed to obtain the final signature bit fabricated matrix. The receiver performs the forward transform on this received bit fabricated matrix and detects the hidden bit from the concern transform pixel byte element of the submatrix. To implement such signature bit encoding in this present context the 1st, 2nd and 4th matrix elements are transformed as shown through matrix operation (10). Interestingly here the 3rd element is kept intact for spatial encoding of a single signature bit on it to optimize the data hiding imperceptibility and robustness issues. Next, the bit-encoded 1st, 2nd and 4th elements of the matrix are reverse transformed to produce the ultimate signature bit fabricated matrix. For extraction purpose the 1st, 2nd and 4th matrix elements are forward transformed and their hidden bits are extracted from the respective transformed components. Here the bit coded on the third matrix element is directly decoded. Now these detected bits from the concern matrix elements are packed in proper sequences to form the respective fragments.

A. *Signature Fragment Bit Insertion Algorithm*

START INDEX CALCULATION

Let, Sub-block matrix number = bn and a variable named as index ϵ {0, 1, 2 , 3}is computed as -

Index=(bn + $\sum_{j=1}^{k} D_k$ + Next Multiple of 4 w.r.t bn) Mod4 +1 (9)

where D_k represents the respective digits of the concern matrix number bn, with k ϵ {0, 1, …, 7}

Block Transformation Procedure

Let a submatrix block of a region is **M_{bn}= [a, b, c , d]**, where{a, b, c, d} ϵ{0,1,.,255} is the pixel byte values and bn ϵ{1,..,N} is the concern matrix number. The transformations adopted for all the four regions or the whole host image is given as -

Forward Transform

$$M_{bn}' = \begin{array}{|c|c|} \hline X_1 = a-c & X_2 = b-c \\ \hline X_3 = c & X_4 = d-c \\ \hline \end{array} \qquad (10)$$

Reverse Transform

$$M_{bn} = \begin{array}{|c|c|} \hline a = X_1 + X_3 & b = X_2 + X_3 \\ \hline c = X_3 & d = X_3 + X_4 \\ \hline \end{array} \qquad (11)$$

Here M_{bn}' = $[X_i]$ is the transformed matrix. X_i denotes transformed elements at concern index i ϵ{1,2,3,4}. Now one signature bit is coded on each transformed component of M_{bn}' using matrix operation (10), which yields the matrix M_{bn}''. Then matrix M_{bn}'' is further reverse transformed using the formula as shown in matrix operation (11) to produce the final bit casted matrix M_{bn}'''.

To execute the signature bit encoding on concern element, two-bit coding functions FUN1(X_i, Φ_i) and FUN2(X_i, b) are used where both functions operate on X_i and given as follows

P_i←**FUN1(X_i, Φ_i):**

```
Start
  If($\Phi_i$==1) Then [
    If (($X_i$ Mod 3) == 0) Then $P_i \leftarrow X_i$;
    Else      Pi ← ($X_i$ – ($X_i$ Mod 3));
  ]
  If($\Phi_i$==0) Then
  [ If (($X_i$ Mod 3) ==0) Then $P_i \leftarrow$ ($X_i$+1);
    Else              $P_i \leftarrow X_i$;
  ]
    Return $P_i$;
End
```

/* for hiding bit=1, X_i will be converted to P_i as multiple of 3, whereas for hiding bit=0, X_i will be converted to

Rf_i←FUN2(X_i, b):

```
Start
  If(($X_i$ Mod b)==0) Then(L←$X_i$);
  Else      L ← ($X_i$ – ($X_i$ Mod b));
  U ← L+ b;
  If(U>256) Then $Rf_i$ ← 254;
  Else          $Rf_i$ ←(L+U)/2;
  Return $Rf_i$;
End
```

/* threshold reference range point Rf_i is found by computing the mid-point of upper (U) and lower (L) multiple number of b w.r.t Xi . Now for coding bit=1, The coded value $C_i \leftarrow Rf_i$ +1; while for coding bit=0, The coded value

Here, FUN1 takes the concern transform value X_i and the particular bit Φ_i to be coded on X_i, while the FUN1 returns the respective bit codded value as P_i. Next FUN2 takes the transformed value X_i and the particular multiple b ϵ {4,6,8} which to be considered while determining the threshold reference point Rf_i with respect to X_i. Critically, this FUN2 tracks the upper multiple (U) and lower multiple (L) number of b with respect to X_i and finds their mid-value as the threshold reference point (Rf_i). Next this Rf_i is returned from FUN2 and is utilized for bit coding on X_i. To understand this bit hiding concept the whole algorithm of bit hiding on concern matrix elements are step-wise discussed as follows -

Input: A color cover image and four-color signature images.

Output: Authenticated cover image hosts four signatures.

Method: At first the concern segments of the host image is partitioned into consecutive sets of 2x2 sub-block matrices of pixel bytes as M_{bn}. Further, each M_{bn} is forward transformed according to matrix operation (10) resulting the transformed matrix M_{bn}'. Then single signature bit is encoded on each transformed matrix component X_i of matrix M_{bn}' to produce the concern bit coded matrix element C_i in M_{bn}''. Now reverse transform as per matrix operation (11) will produce the final signature bit fabricated matrix M_{bn}'''. Since the receiver also operates on this M_{bn}''' so the receiver first performs forward transform as per matrix operation (10) on this M_{bn}''' to track those bit codded matrix elements. Further, those respective hidden bits are extracted from the concern transform matrix element. To discuss this bit hiding algorithm let, the found matrix interval for the concern image segment is t_r and the steps of coding are-

For matrix number t =1 to L
Do
Step1: Perform forward transform on M_{bn} as per matrix operation (10).
Step2: Read chunk of four fragment bits $\Phi_i \epsilon \{0,1\}$ for i=1,2..4.
step3: Compute the value of index as per Eq. (9) for M_{bn}.
Step4: Code each $\Phi_i \epsilon \{0,1\}$ on the concern transformed value X_i of M_{bn}' to obtain the respective coded value C_i as

```
If (index == 0) Then
 [  $C_1$ = FUN1($X_1$, $\Phi_1$);
Rf$_2$ = FUN2($X_2$,4);
If ($\Phi_2$ ==1) Then $C_2 \leftarrow Rf_2$+1;
Else              $C_2 \leftarrow Rf_2$-1;
Rf$_3$ = FUN2($X_3$,6);
If ($\Phi_3$ == 1) Then $C_3 \leftarrow Rf_3$+1;
Else              $C_3 \leftarrow Rf_3$-1;
Rf$_4$ = FUN2($X_4$,8);
If ($\Phi_4$ == 1) Then   $C_4 \leftarrow Rf_4$+1;
Else              $C_4 \leftarrow Rf_4$-1;
 ]
If (index == 1) Then
[  $C_1$ = FUN1($X_1$, $\Phi_1$);
    Rf$_2$ = FUN2($X_2$,6);
    If ($\Phi_2$ == 1) Then $C_2 \leftarrow Rf_2$+1;
    Else          $C_2 \leftarrow Rf_2$-1;
    Rf$_3$ = FUN2($X_3$,8);
    If ($\Phi_3$ == 1) Then $C_3 \leftarrow Rf_3$+1;
    Else          $C_3 \leftarrow Rf_3$-1;
    Rf$_4$ = FUN2($X_4$,4);
    If ($\Phi_4$ == 1) Then  $C_4 \leftarrow Rf_4$+1;
    Else          $C_4 \leftarrow Rf_4$-1;
 ]
If (index == 2) Then
[  $C_1$ = FUN1($X_1$, $\Phi_1$);
    Rf$_2$ = FUN2($X_2$,8);
    If ($\Phi_2$ == 1) Then $C_2 \leftarrow Rf_2$+1;
    Else        $C_2 \leftarrow Rf_2$-1;
    Rf$_3$ = FUN2($X_3$,4);
    If ($\Phi_3$ == 1) Then $C_3 \leftarrow Rf_3$+1;
    Else            $C_3 \leftarrow Rf_3$-1;
    Rf$_4$ = FUN2($X_4$,6);
    If ($\Phi_4$ == 1) Then $C_4 \leftarrow Rf_4$+1;
    Else            $C_4 \leftarrow Rf_4$-1;
 ]
```

```
If (index == 3) Then
 [  $C_1 = FUN1(X_1, \Phi_1)$;
    $Rf_2 = FUN2(X_2,8)$;
    If ($\Phi_2 == 1$) Then $C_2 \leftarrow Rf_2+1$;
    Else                $C_2 \leftarrow Rf_2-1$;
    $Rf_3 = FUN2(X_3,6)$;
    If ($\Phi_3 == 1$) Then $C_3 \leftarrow Rf_3+1$;
    Else                $C_3 \leftarrow Rf_3-1$;
    $Rf_4 = FUN2(X_4,4)$;
    If ($\Phi_4 == 1$) Then $C_4 \leftarrow Rf_4+1$;
    Else                $C_4 \leftarrow Rf_4-1$;
 ]
```

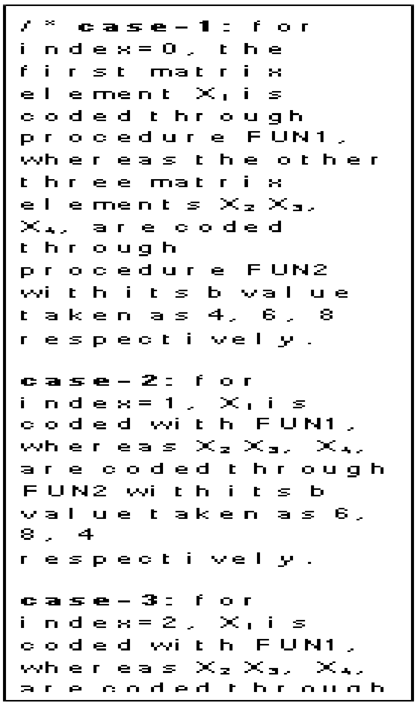
Step5: Collect all these bit coded values of C_i in matrix M_{bn}''.

Step6: Apply reverse transform on M_{bn}'' as per matrix operation (11) to produce the final bit fabricated matrix M_{bn}'''.

Step7: If needed perform minor adjustments on M_{bn}'' to keep the final bit fabricated elements of M_{bn}''' in spatial domain.

Step8: $t \leftarrow t + t_r$;

End Loop



```
/* case-1: for
index=0, the
first matrix
element X1 is
coded through
procedure FUN1,
whereas the other
three matrix
elements X2 X3,
X4, are coded
through
procedure FUN2
with its b value
taken as 4, 6, 8
respectively.

case-2: for
index=1, X1 is
coded with FUN1,
whereas X2 X3, X4,
are coded through
FUN2 with its b
value taken as 6,
8, 4
respectively.

case-3: for
index=2, X1 is
coded with FUN1,
whereas X2 X3, X4,
are coded through
```

B. Signature Fragment Bit Extraction Algorithm

Input: Authenticated cover image hosts hidden signatures.

Output: Four copies of each signature sensed from the cover.

Method: For all regions signature coded sub matrices M_{bn}''' is forward transformed to obtain M_{bn}'' and one secret bit is sensed from bit fabricated transformed matrix component X_i of M_{bn}''. These detected bits then packed in proper sequences to form those four signatures and just as coding the extraction of bit Φ_i from concern matrix element i ϵ {1,2,3,4}. let, the found matrix interval for the concern image segment is t_r as mentioned previously, then the step wise bit encoding on M_{bn}' is as follows

For matrix number t = 1 to L

Do

Step1: Read the currently tracked matrix elements of M_{bn}''' and apply forward transform on them as per matrix operation (10) to produce the transformed matrix M_{bn}'' with bit coded matrix elements C_i , for element index values i = 1,2,3,4.

Step2: Compute the value of the variable index as per Eq. (9) for the current matrix number 'bn'.

```
If (index == 0) Then
[  If (($C_1$ Mod 3) == 0) Then $\Phi_1$= 1
   Else                       $\Phi_1$= 0;
   $Rf_2 = FUN2(X_2,4)$;
   If (C2>=Rf2) Then $\Phi_2$ = 1;
   Else              $\Phi_2$= 0;
   $Rf_3 = FUN2(X_3,6)$;
   If (C3>=Rf3) Then $\Phi_3$ = 1;
   Else              $\Phi_3$ = 0;
   $Rf_4 = FUN2(X_4,8)$;
   If (C4>=Rf4) Then $\Phi_4$ = 1;
   Else              $\Phi_4$ = 0;
]
If (index == 1) Then
[  If (($C_1$ Mod 3) == 0) Then $\Phi_1$= 1
   Else                       $\Phi_1$= 0;
   $Rf_2 = FUN2(X_2,6)$;
   If (C2>=Rf2) Then $\Phi_2$ = 1;
   Else              $\Phi_2$= 0;
   $Rf_3 = FUN2(X_3,8)$;
   If (C3>=Rf3) Then $\Phi_3$ = 1;
   Else              $\Phi_3$ = 0;
   $Rf_4 = FUN2(X_4,4)$;
   If (C4>=Rf4) Then $\Phi_4$ = 1;
   Else              $\Phi_4$ = 0;
]
If (index == 2) Then
[  If (($C_1$ Mod 3) == 0) Then $\Phi_1$= 1
   Else                       $\Phi_1$= 0;
   $Rf_2 = FUN2(X_2,8)$;
   If (C2>=Rf2) Then $\Phi_2$ = 1;
   Else              $\Phi_2$= 0;
   $Rf_3 = FUN2(X_3,4)$;
   If (C3>=Rf3) Then $\Phi_3$ = 1;
   Else              $\Phi_3$ = 0;
   $Rf_4 = FUN2(X_4,6)$;
   If (C4>=Rf4) Then $\Phi_4$ = 1;
   Else              $\Phi_4$ = 0;
]
If (index == 3) Then
```

```
[   If (($C_1$ Mod 3) == 0) Then $\Phi_1$= 1
    Else                    $\Phi_1$= 0;
    $Rf_2$ = FUN2($X_2$,8);
    If (C2>=Rf2) Then $\Phi_2$ = 1;
    Else                $\Phi_2$= 0;
    $Rf_3$ = FUN2($X_3$,6);
    If (C3>=Rf3) Then $\Phi_3$ = 1;
    Else             $\Phi_3$ = 0;
    $Rf_4$ = FUN2($X_4$,4);
    If (C4>=Rf4) Then $\Phi_4$ = 1;
    Else                $\Phi_4$ = 0;
]
Step3: Append these sensed bits in exact sequences.
Step4: t←t+$t_r$;
    End Loop
```

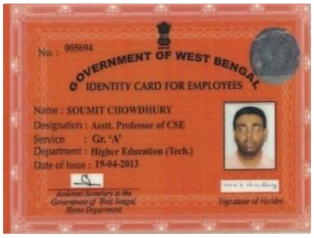
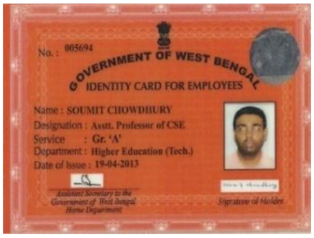
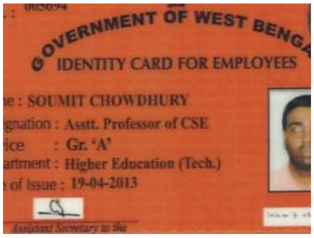
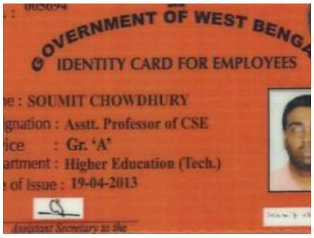
VI. SIMULATION RESULT AND COMPARISONS

The proposed signature fabrication scheme is tested on different colored e-Certificates and I-CARD images of size 512x512 with four color signature images of size 25x25. Importantly all these images are taken in PPM format as reflected in TABLE 1. Critically, the signature encoding and decoding operations are performed through C programming under LINUX environment while the simulation results related to data hiding invisibility and robustness are mainly evaluated through MATLAB (2018a), GIMP (2.10) and IrfanView (4.52). To show the effectiveness of this scheme the concern simulation results are discussed as follows.

A. Signature Fabrication Imperceptibility

Since the scheme mainly adopts signature hiding concepts so, the imperceptibility of data hiding is thoroughly focused here to promote the strength of this algorithm. In this context **TABLE I** reflects identical visual qualities for the signature fabricated e-Certificates. Hence, this data-hiding algorithm is quite capable of resisting all kinds of visual and statistical attacks. Further, **TABLE II** also justifies this good data hiding imperceptibility with mostly identical histograms for both the original and signature fabricated image documents. Apart from such visual quality judgements this hiding imperceptibility is also thoroughly quantified in **TABLE III** reflecting good similarities for both the original and signature fabricated images. In this regard the standard image comparison parameters like Pick Signal to Noise Ratio (PSNR), Structural Similarity Index Matrix (SSIM) and Correlation Coefficient (CC) are adopted to emphasize the image similarity aspects with their higher values. Here PSNR is used to indicate the overall noise injection during data hiding whereas SSIM focuses on local structural similarities and CC value adopts the block mean aspect of comparisons for the concern images [9, 11, 12]. In addition of such quantifiable evaluation the respective pixel byte value-based comparisons are also considered in this simulation result analysis to practically observe the differences between the original and signature fabricated image. Importantly this graphical analysis is shown through **Fig. 5** where very little differences are visualized between the concern pixel bytes for both the original and its signature fabricated image. Ultimately, this imperceptibility scenario is further compared with the current existing approaches in **TABLE IV** where the proposed scheme clearly confirms superior data hiding imperceptibility under much higher data payload embedding. Overall all these evaluations on hiding imperceptibility and its comparisons from different angles shown in Table IV truly ensuring enhancements on present data hiding concepts.

Table I. Visual Quality of Original and Signature Fabricated Image

Original Image	Fabricated image	Enlarged original image	Enlarged Fabricated image
 No. : 005694 GOVERNMENT OF WEST BENGAL IDENTITY CARD FOR EMPLOYEES Name : SOUMIT CHOWDHURY Designation : Asstt. Professor of CSE Service : Gr. 'A' Department : Higher Education (Tech.) Date of Issue : 19-04-2013 Assistant Secretary to the Government of West Bengal Home Department Signature of Holder	 No. : 005694 GOVERNMENT OF WEST BENGAL IDENTITY CARD FOR EMPLOYEES Name : SOUMIT CHOWDHURY Designation : Asstt. Professor of CSE Service : Gr. 'A' Department : Higher Education (Tech.) Date of Issue : 19-04-2013 Assistant Secretary to the Government of West Bengal Home Department Signature of Holder	 GOVERNMENT OF WEST BENGA IDENTITY CARD FOR EMPLOYEES ne : SOUMIT CHOWDHURY gnation : Asstt. Professor of CSE ice : Gr. 'A' artment : Higher Education (Tech.) of Issue : 19-04-2013 Assistant Secretary to the	 GOVERNMENT OF WEST BENGA IDENTITY CARD FOR EMPLOYEES ne : SOUMIT CHOWDHURY gnation : Asstt. Professor of CSE ice : Gr. 'A' artment : Higher Education (Tech.) of Issue : 19-04-2013 Assistant Secretary to the
A. I-CARD	*E. SIGNATURE FABRICATED I-CARD*	*I. MAGNIFIED I-CARD*	*M. MAGNIFIED SIGNATURE FABRICATED I-CARD*
GCECT awarded COURSE COMPLETION Certificate to SONTU MISTRY MARKS: 85 S. DATTA Name Title of Presenter 03/03/2019 Date	GCECT awarded COURSE COMPLETION Certificate to SONTU MISTRY MARKS: 85 S. DATTA Name Title of Presenter 03/03/2019 Date	GCECT awarded COURSE COMPLETION Certificate to SONTU MISTRY MARKS: 85 GRADE: E S. DATTA Name Title of Presenter 03/03/2019 Date	GCECT awarded COURSE COMPLETION Certificate to SONTU MISTRY MARKS: 85 GRADE: E S. DATTA Name Title of Presenter 03/03/2019 Date
B. CERTIFICATE-1	*F. SIGNATURE FABRICATED CERTIFICATE-1*	*J. MAGNIFIED CERTIFICATE-1*	*N. MAGNIFIED SIGNATURE FABRICATED CERTIFICATE-1*

DOI: 10.35940/ijitee.J1231.0881019

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

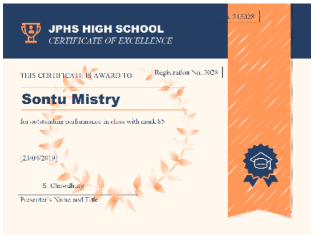
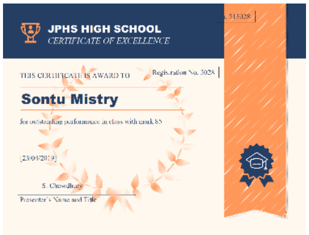
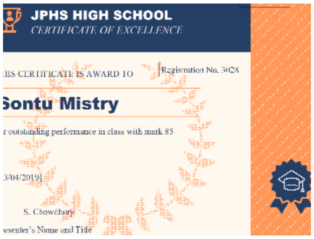
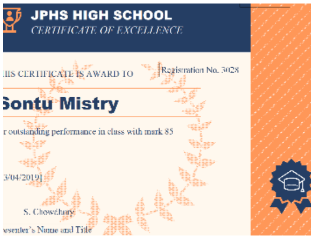
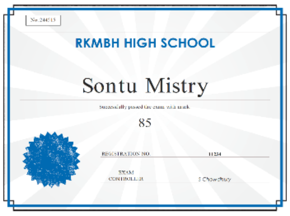
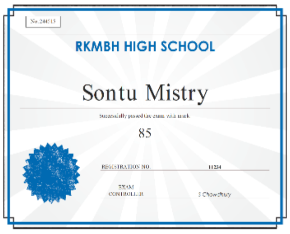
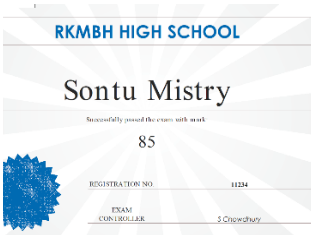
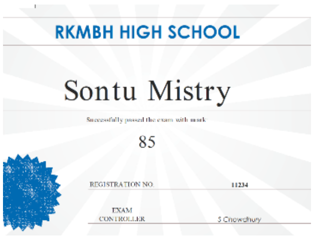
Original Image	Fabricated image	Enlarged original image	Enlarged Fabricated image
 JPHS HIGH SCHOOL CERTIFICATE OF EXCELLENCE THIS CERTIFICATE IS AWARD TO Registration No. 3028 Sontu Mistry for outstanding performance in class with mark 85 [23/04/2019] S. Chowdhury Presenter's Name and Title	 JPHS HIGH SCHOOL CERTIFICATE OF EXCELLENCE THIS CERTIFICATE IS AWARD TO Registration No. 3028 Sontu Mistry for outstanding performance in class with mark 85 [23/04/2019] S. Chowdhury Presenter's Name and Title	 JPHS HIGH SCHOOL CERTIFICATE OF EXCELLENCE IIS CERTIFICATE IS AWARD TO Registration No. 3028 Sontu Mistry r outstanding performance in class with mark 85 3/04/2019] S. Chowdhury esenter's Name and Title	 JPHS HIGH SCHOOL CERTIFICATE OF EXCELLENCE IIS CERTIFICATE IS AWARD TO Registration No. 3028 Sontu Mistry r outstanding performance in class with mark 85 3/04/2019] S. Chowdhury esenter's Name and Title
C. CERTIFICATE-2	*G. SIGNATURE FABRICATED CERTIFICATE-2*	*K. MAGNIFIED CERTIFICATE-2*	*O. MAGNIFIED SIGNATURE FABRICATED CERTIFICATE-2*
 RKMBH HIGH SCHOOL Sontu Mistry Successfully passed the exam with mark 85 REGISTRATION NO 11234 EXAM CONTROLLER S Chowdhury	 RKMBH HIGH SCHOOL Sontu Mistry Successfully passed the exam with mark 85 REGISTRATION NO 11234 EXAM CONTROLLER S Chowdhury	 RKMBH HIGH SCHOOL Sontu Mistry Successfully passed the exam with mark 85 REGISTRATION NO 11234 EXAM CONTROLLER S Chowdhury	 RKMBH HIGH SCHOOL Sontu Mistry Successfully passed the exam with mark 85 REGISTRATION NO 11234 EXAM CONTROLLER S Chowdhury
D. CERTIFICATE-3	*H. SIGNATURE FABRICATED CERTIFICATE-3*	*L. MAGNIFIED CERTIFICATE-3*	*P. MAGNIFIED SIGNATURE FABRICATED CERTIFICATE-3*
Signature Images Used for Fabrication			
	S Chowdury	S Mistry	
Q. UNIVERSITY'S COPYRIGHT SIGNATURE	*R. ISSUING PERSION'S PROPRIETARY SIGNATURE*	*S. CANDIDATE'S PROPRIETARY SIGNATURE*	*T. CANDIDATE'S THUMB IMPRESSION*

Table II. General Histogram and RGB Histogram

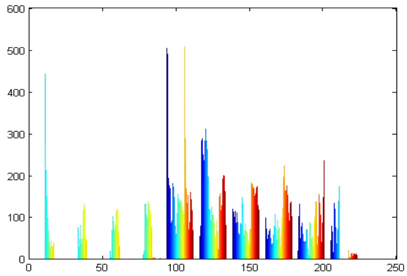
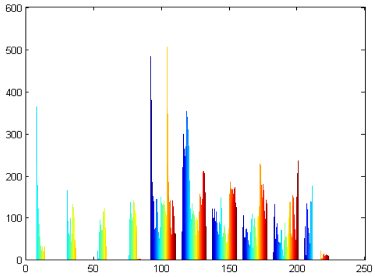
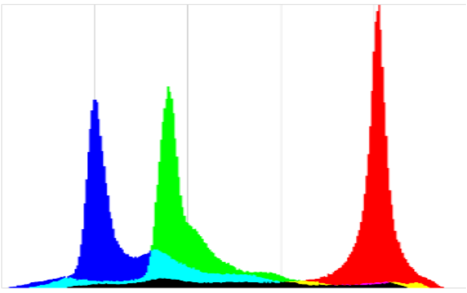
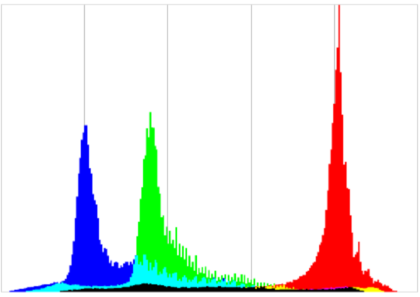
Histogram Category	Original I-Card Image	Fabricated I-Card
General Histogram		
RGB Histogram		

Table III. Signature Fabrication Imperceptibility

Cover Image	Fabricated Image		
I-CARD	PSNR(db)	SSIM	CC
	38.9731	**0.9897**	**0.9957**
CERTIFICATE-1	PSNR(db)	SSIM	CC
	39.0981	**0.9756**	**0.9952**
CERTIFICATE-2	PSNR(db)	SSIM	CC

	39.1197	**0.9824**	**0.9972**
CERTIFICATE-3	PSNR(db)	SSIM	CC
	38.9554	**0.9612**	**0.9927**

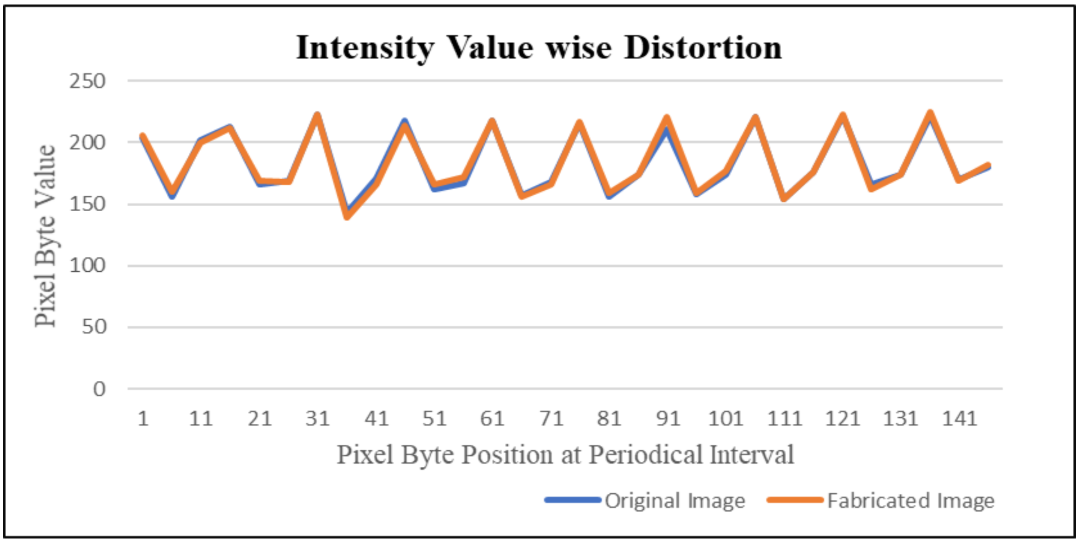


Fig.5: Pixel Byte Deviation Pattern for I-CARD

Table IV. Comparisons Of Signature Fabrication Imperceptibility With Other Existing Approaches

Works / Approach	**Signature Copies**	**Signature Image Type**	**Dispersing Capacity**	**PSNR (db)**
[5] Segmented	03	Grey scale	6144 bytes	30.11
[4] Segmented	16	Binary	4,096 bits	39.0627 (max.)
[6] Segmented	09	Grey Scale	5,120 bytes	33.8506 (max)
[7] Segmented	04	Binary	4,096 bits	28.44 (max)
[9] Successive	02	Grey Scale	320 bytes	30.79
[12] Segmented	02	Color	13,824 bytes	38.0639 (max.)
[14] Segmented	08	Binary	8,192 bits	38.9060
Proposed Approach	**16**	**Color**	**30,000 bytes**	**39.0547 (avg.)**

B. Performance against Attacks

For evaluating the robustness of this scheme various attacks are applied on the signature fabricated e-Certificate and the quality of the four best extracted signatures are examined to judge the attack impact. Since attacks normally alters the pixel byte values of the signature coded e-Certificate image so possible alteration of hidden data bits on the concern pixel byte values. Hence, significant amount of destruction is possible for extracted signatures and in this aspect the best copy of each extracted signature is identified by judging the similarity between the extracted signature and its original form. This signature quality evaluation is first reflected in **TABLE V** which clearly shows better extraction of extracted signatures under different image processing attacks. In this aspect the CC value of the four best extracted signatures are reflected in Table V for each attack and they are compared with the existing works reflecting better signature extraction. Further, this proposed scheme is also tested under some additional attacks and these results are shown in **TABLE VI** with CC value of the four best detected signatures. Critically all these attack testing covered in Table V and Table VI are applied on the authenticated I-CARD image as already visualized in Table I. Importantly all such attack performance shown in Table V, VI basically highlighting good signature recovery with higher CC value of four extracted signatures. Further, this better signature recovery scenario is graphically visualized with **Fig. 7** focusing the best extracted signature CC value under each attack covered in Table V and VI. Vitally, this superior signature extraction is mainly possible due to variable threshold range driven signature bit encoding on different pixel bytes resulting variable attack impact on different pixel bytes. Hence, this scheme clearly promotes good signature recovery through TABLE V, VI and Fig. 7. This fact is truly justified in Fig. 7 which actually indicates the CC value of the best sensed signature rarely falls below 0.6. Apart from this the bar chart shown in **Fig. 6** definitely reflects excellent recovery of the number of signatures under various attacks based on the threshold CC value > 0.7. Here Fig. 6 highlights a comparison for the number of signature recoveries in contrast to the existing approaches on the basis of extracted signature CC values > 0.7 against specific attacks.

Table V. Performance Comparisons Against Attack With Existing Approaches

Attack name	Applied in works or approaches	Attack Parameter	CC values of the extracted signatures			
			Sign-1	Sign-2	Sign-3	Sign-4
Salt & Pepper Noise	[8]	5%	0.76	0.42	NA	NA
	[12]	3%	0.8856	0.9978	NA	NA
	[15]	5%	0.9187	0.8495	0.7676	0.4953
	This proposed work	**5%**	**0.8702**	**0.8605**	**0.8069**	**0.9331**
Median Filtering	[6]	13x13	0.9670	0.9384	0.9807	NA
	[8]	3x3	0.93	0.97	NA	NA
	[11]	3x3	0.9011	0.9240	NA	NA
	[12]	3x3	0.9993	1	NA	NA
	[15]	3x3	1	1	1	0.9998
	This proposed work	**3x3**	**1**	**1**	**0.9999**	**1**
Winner Filter	[12]	3x3	0.8142	0.7679	NA	NA
	[15]	3x3	1	1	1	0.9999
	This proposed work	**3x3**	**1**	**1**	**1**	**1**
Cropping	[6]	2.5% area left	0.9763	0.8304	0.9627	NA
	[8]	Not given	0.65	0.85	NA	NA
	[11]	Not given	0.6851	0.6562	NA	NA
	[12]	Not given	0.3374	0.3600	NA	NA
	[15]	60x60 block cut	1	1	1	0.9999
	This proposed work	**60x60 block cut**	**0.9837**	**1**	**1**	**1**
Row(R) and Column (C) Manipulations	[6]	20(R), 20(C)	0.9876	0.7332	0.9898	NA
	[11]	Not given	0.6866	0.6279	NA	NA
	[12]	Not given	0.6686	0.6705	NA	NA
	This proposed work	**60(R), 60(C)**	**0.9947**	**0.9959**	**0.9157**	**0.9329**
Translation	[8]	Not given	0.35	0.99	NA	NA
	[11]	Not given	0.7055	0.8141	NA	NA
	[12]	Not given	0.9586	0.9359	NA	NA
	[15]	[0.4,-0.4]	1	1	1	1
	This proposed work	**[0.4, -0.4]**	**1**	**1**	**1**	**1**
Sharpening	[8]	Not given	0.92	0.99	NA	NA
	[12]	Not given	0.9078	0.9655	NA	NA
	This proposed work	**3%**	**0.9331**	**0.8827**	**0.8144**	**0.9421**
Smoothing	[8]	Not given	0.98	1	NA	NA
	[12]	Not given	1	1	NA	NA
	[15]	30 %	1	0.9959	0.9993	0.9999
	This proposed work	**30%**	**0.9999**	**0.9999**	**0.9716**	**0.9959**

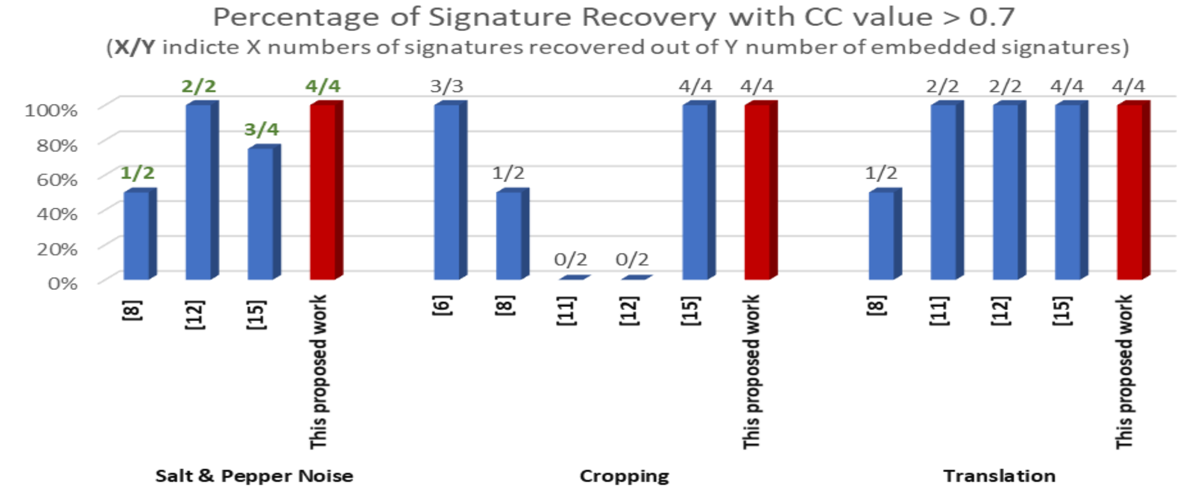


Fig. 6: Comparison Of Signature Recovery Based On CC Threshhold Value > 0.7 Under Different Attacks

Table VI. Performance Against Some Additional Attacks

Applied Attacks	Attack Parameter	Extracted Logo Images			
		Watermark 1	Watermark 2	Watermark 3	Watermark 4
Gaussian Noise	(Variance of 1%)	0.4894	0.4416	0.4792	0.6579
Speckle Noise	(Density of 5%)	0.3835	0.2858	0.4637	0.5455
JPEG Compression	(Quality 98%)	0.5143	0.4950	0.5592	0.7324
Flip	(Vertically- 180)	1	1	1	1
Normalize	NA	1	1	1	1
Brightness & Contrast	(Brightness – 5 & Contrast – 5)	0.4818	0.3454	0.3624	0.6241
RGB Value Change in Irfanview	(R-5, G-5, B-5)	0.5481	0.5310	0.7118	0.6956
RGB Value Change in Gimp	(only Hue: R-5, G-5, B-5)	0.3069	0.2263	0.3586	0.6192

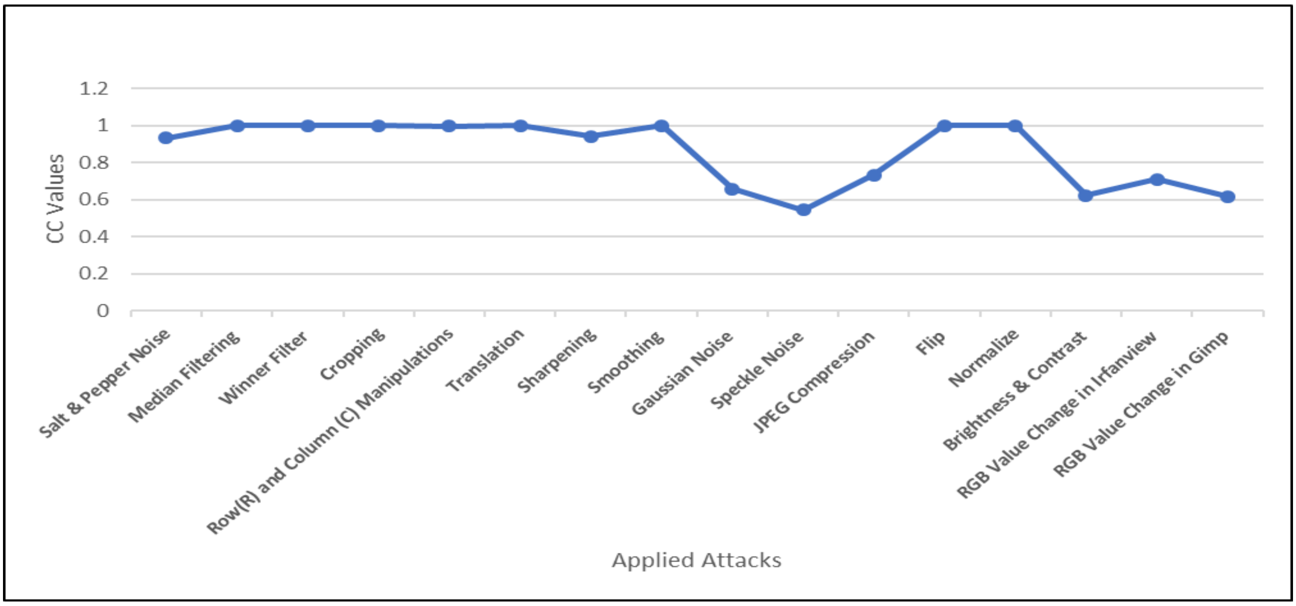


Fig. 7: Best Detected Signatures With Maximum CC Value Under Attacks

VII. CONCLUSION

This proposed approach establishes a unique and strong data security protocol for trusted online validation of e-documents like university certificates issued to the concern incumbent. To achieve this goal the major research contributions made in this work are as follows.

- Strongly complying all the critical data security issues like authentication, confidentiality, integrity and non-repudiations as a whole related to secret and authentic data transmissions.
- Implementation of new authentication criteria like valid circular sequencing of signature fragments, and is formed on the basis of authentic start fragment index of that circular combination.
- Enhanced robustness and imperceptibility related to data hiding and is mainly achieved through the novel idea of variable encoding of signature bits on different transformed pixel byte components.

So, with the help of these improved and advanced features this proposed approach clearly achieves more trustable validation of e-Certificates from various angles or perspectives. Further, as claimed this scheme also reflects significant performance elevations on data hiding issues with at least 0.3% growth of PSNR values on an average under minimum two times of data payload embedding. Apart from that, the scheme shows very good signature recovery under attacks with best detected signature CC value rarely falls below 0.6 in the worst-case attack performance. Additionally, this work also highlights a greater number of signature recoveries in good forms or qualities as compare to the other existing approaches with CC value > 0.7 under some specific attacks.

Hence, this proposed scheme clearly ensures advancement on both data security protocol aspects and data hiding techniques and hence superior validation of e-documents. However, this proposed concept or study can be further extended to cover robustness against some typical geometrical attacks and malicious tampering related issues on digital e-Certificate images

REFERENCES

1. V. Anitha, R. Leela Velusamy, "Authentication of Digital Documents Using Secret Key Biometric Watermarking", International Journal of Communication Network Security, Vol 1, Issue 4, 2012. ISSN: 2231 – 1882.
2. K. N. Mishra, "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**, **2016**, **E. ISBN:** 978-1-4673-9084-2. **DOI:** 10.1109/ICCCCM.2016.7918256
3. H. R. Hasan, "Copyright Protection for Digital Certificate using Blind Watermarking Technique", Kurdistan Journal of Applied Research, Vol **3**, Issue **1**, pp: **75-79**, **June 2018**. ISSN: 2411-7706.
4. I. Nasir, Y. Weng, J. Jiang, S. Ipson, (2009). "Multiple spatial watermarking technique in color images", Signal Image & Video Processing (SiViP), Vol. **4,** Issue. **2**, pp. **145–154**. doi: 10.1007/s11760-009-0106-7.
5. S. Behnia, M. Teshnehlab, P. Ayubi, "Multiple watermarking scheme based on improved chaotic maps", Communication in Nonlinear Science and Numerical Simulation, Vol. **15**, Issue. **9**, pp. **2469-78**. **2010**, doi:10.1016/j.cnsns.2009.09.042
6. G. Bhatnagar, Q. M. J. Wu, "A new robust and efficient multiple watermarking scheme", Multimedia Tools & Application, Vol. **74**, Issue. **19**, pp. **8421-8444**, **2013**, doi:10.1007/s11042-013-1681-8.
7. M. Babaei, K. Ng, H. Babei, H. G. Niknajeh, "Robust multi watermarking scheme for multiple digital input images in DWT domain" International Journal of Computer and Information Technology, Vol. **3**, Issue. **4**, pp. **834-840**, **2014**
8. M. Natarajan, Y. Govindarajan, "Performance comparison of single and multiple watermarking techniques", International Journal of Computer Network and Information Security, vol. **6**, Issue. **7**, pp **28-34**, **2014**. DOI: 10.5815/ijcnis.2014.07.04
9. R.M. Thanki, K.R. Borisagar, "Compressive Sensing Based Multiple Watermarking Technique for Biometric Template Protection", International Journal of Image Graphics and Signal Processing, vol. 7, Issue. **1**, pp **53-60**, **2015**. DOI: 10.5815/ijigsp.2015.01.07.
10. A.K. Singh, B. Kumar, M. Dave, A. Mohan, "Multiple watermarking on medical images using selective DWT coefficients", Journal of Medical Imaging and Health Informatics, vol. **5**, Issue. **3**, pp. **607-614**, **2015**. DOI: https://doi.org/10.1166/jmihi.2015.1432.
11. N. Mohananthini, G. Yamuna, "Image fusion process for multiple watermarking schemes against attacks", Journal of Network Communications and Emerging Technologies, vol. **1**, Issue. **2**, pp. **1–8**, **2015**. ISSN: 2395-5317.
12. N. Mohananthini, G. Yamuna, "Comparison of multiple watermarking techniques using genetic algorithms", Journal of Electrical Systems & Information Technology, vol. **3**, issue **1**, pp.**68–80**, **2016**, DOI: https://doi.org/10.1016/j.jesit.2015.11.009
13. M. Natarajan, Y. Govindarajan, "Performance optimization of multiple watermarking using genetic algorithms", International Journal of Enterprise Network Management, vol. 7, Issue. **3**, pp. **237-249**, **2016**, DOI: https://doi.org/10.1504/IJENM.2016.078970.
14. R. Sadh, N. Mishra, S. Sharma, "Dual plane multiple spatial watermarking with self encryption", Sadhana, Indian Academy of Sciences, Vol. **4**, Issue. **1**, pp. **1-14**, **2016**
15. S. Chowdhury, R. Mukherjee, N. Ghoshal, "Dynamic authentication protocol using multiple signatures". Wireless Personal Communications, Vol. **93**, Issue. **3**, pp. **1-32**, **2017**, doi:10.1007/s11277-017-4066-x.

AUTHORS PROFILE

Mr. Soumit Chowdhury presently serving in the position of Assistant Professor of Computer Science & Engineering, in the Govt. College of Engineering & Ceramic Technology, Kolkata, India. He has more than 13 years of teaching experience in different engineering colleges in West Bengal. He has also published 12 research papers in various National, International Journals and Conferences. Further, Mr. Chowdhury has successfully supervised one UGC funded research project as Principal Investigator and presently acting as co-supervisor in another sponsored research project funded by Department of Higher Education, Science and Technology and Biotechnology, Government of West Bengal. has also guided 5 MTech projects till now. Current research area of Mr. Chowdhury includes Cryptography, Steganography/Watermarking, Coding Theory etc.

Mr. Sontu Mistry is currently pursuing his bachelor in Computer Science & Engineering from Govt. College of Engineering & Ceramic Technology, Kolkata, India. He passed his Xth class exam from Jatragachi Pronabananda High School, Kolkata in the year 2014 and completed his XIIth class education from Ramakrishna Mission Boys' Home High School in the year 2016. Apart from his regular studies Mr. Mistry has also undergone an internship program in Oil and Natural Gas Corporation and has significantly contributed in a web development project. His current area of interest mainly lies on Cryptography, Steganography, Watermarking, Coding theory, Image processing and Artificial intelligence.

Dr. Nabin Ghoshal attached with the Department of Engineering & Technological Studies (DETS), University of Kalyani, West Bengal, India. His research areas are Steganography, Watermarking, Data Security, Bio-metric steganography, Visual Cryptography, Visual Cryptography through Steganography, Copyright protection and authentication (Audio & Video). He received Bachelor degree in Mathematics (Honours) from the University of Calcutta in 1994. He got Master in Computer Applications (MCA) from the University of North Bengal in 1998 and also obtained M. Tech. degree in Computer Science and Engineering from the University of Kalyani in 2005 respectively. He received his Ph.D. degree in Computer Science & Engineering from the University of Kalyani in 2011. He has 53 research papers in various international journals and national and international conferences.