MULTI-LAYER DIGITAL VALIDATION OF CANDIDATE SERVICE APPOINTMENT WITH DIGITAL SIGNATURE AND BIO-METRIC AUTHENTICATION APPROACH

Saikat Bose[1], Tripti Arjariya[2], Anirban Goswami[3], Soumit Chowdhury[4]

[1]Department of Computer Science Engineering, Bhabha University, Bhopal, India

[2]Department of Computer Science Engineering, Bhabha University, Bhopal, India

[3]Techno Main Salt Lake, Sec – V, Kolkata-700091, India

[4]Government College of Engineering & Ceramic Technology, Kolkata-700010, India

ABSTRACT

Proposed work promotes a unique data security protocol for validating candidate's service appointment. Process initiated with concealment of private share within the first segment of each region of the e-letter at commission's server. This is governed by hash operations determining circular orientation of private share fragments and their hosted matrix intervals. Signed e-letter downloaded at the posted place is validated through same hash operations and public share. Candidate's on spot taken fingerprint are concealed in two segments for each region of the e-letter adopting similar hiding strategies. The copyright signature of posting place is similarly shielded on fourth segment of each region using hash operations. The certified e-letter is thoroughly validated at commission's server and signatures stored justify authenticity of appointment and proper candidature at the posting place. The superior test results from wider angles establishes the efficacy of the proposed protocol over the existing approaches.

Keywords

Dynamic Authentication, Standard-Deviation Based Encoding, Variable Encoding, Multi-Signature Hiding, Random Signature Dispersing.

1. INTRODUCTION

The increase in transmission of digital data especially under the public wireless domains [1] has really caused effective validation of the digital documents from different perspectives. One of the main feature of such validation utilizes secret embedding of digital signature of the owner within a digital document to confer the ownership claims [2-3]. In addition, signatures are to be encoded securely so that it is not revealed to unauthorized parties and also cannot be destroyed by external attacks.

In this approach, authenticating e-documents related to e-governance system encourages bio-metric features of the client incumbent. Accordingly, Ganesan et al. [4] mentioned secured disperse of multi-signatures in different color intensity components of the e-certificate. The utility of multi-phase validations based authentication of the ownership signature restores copyright documents by restricting various attacks [5-6]. Effectiveness of multi-phase technique can be classified as: **a) Composite**- All secret watermarks combine into one which can be hidden. **b) Successive**-Encoding successive watermarks in place of previous marks, **c) Segmented**- To avoid interference non-overlapping regions are used for encoding. Successive technique imparts better security [7], but both composite and successive types are vulnerable to cropping attack including watermark interferences. Amongst all, the segmented pattern provides good robustness with recovery of at least one signature amidst various attacks. Also, interference is not a problem due to non-overlapping or segmented nature of signature encoding [8].

DOI: 10.5121/ijcnc.2022.14506

So, considering all these critical aspects, this proposed scheme actually tries segmented hiding of multi-signatures in dynamic pattern. The objective is to achieve secure authentication in wireless domain, thus resisting illegal access and loss of signal strengths due to external interferences [8]. Hence, sustaining security and robustness in wireless transmissions using dynamic casting of signatures is the primary goal.

So, in view of such e-document validations, the current existing works have mostly tried watermarking approaches for achieving ownership claims as well as content authentications. However, these works can be further improved with digital signature concept and this can be mainly implemented through visual cryptography. Apart from that, watermark embedding by utilizing the hash values derived from sensitive e-document data should take care of the data integrity issues in a better manner. So, considering the effectiveness of these practices, this proposed work efficiently amalgamates both visual cryptography and watermarking while also employs dynamic embedding of watermarks that is based on hash values computed from e-document data. Hence, this work actually addresses all the critical data security issues by combining all these well recognised solutions to mainly validate the e-document from different angles.

Nowadays and eventually due to the lock down phase, people in significant numbers seek health care at hospitals, medical facilities, holistic groups and physicians practice in online mode. This creates a new set of challenges for the staff members. So recent technological advancement has led to development of online scheduling software to ease a part of physical interactions for both patients and administrative staffs. In addition to this, e-appointment can be implemented as the primary step for recruitment in organization, admission in institutions and in many other areas. Basically, online scheduling system is based on web-based applications and enables secured and convenient booking technique. However, due to immense advancement of technology, most of the time appointment of one person is mishandled by an intruder especially for situations where appointment is issued form some centralized authority and the posting is applicable for the local office. Hence, this practice actually leads to a fraudulent e-appointment generation which injects some misleading or wrong information and this is utilized for bad intension. Apart from that, actual candidature of such appointment may be in question with unauthorized person joining the service. So, obviously there is a necessity of verifying the authenticity of the e-appointment and the proper person joining the service at the actual posting place.

Additionally, if this e-appointment validation can be done digitally in an authentic manner, the staff responsible will spend less time in managing appointments and can use their free time for more urgent and vital tasks. In turn, the clients will save time for calling the office and booking an appointment in the middle of their busy schedule.

So, considering all these critical aspects, this proposed scheme now precisely focuses on a unique data security solution for validating e-appointment related issues online with its key features considered as:

1. Confirming legality of the e-appointment from both client and owner's perspectives to ensure proper validation. This is mainly achieved by concealing copyright signatures of both client and owner on the same e-appointment based on some authentic hash values found from the critical sensitive data. The idea here is to confirm the multi-phase validation of e-appointment, authenticity of the concern candidate and also the applicable place of posting. Further, the authentic candidate's service joining proof in proper posting place is also recorded in the same e-appointment letter and hence whole this appointment procedure is actually validated with a single e-document.
2. Additionally, all the critical data security issues like authenticity, integrity, confidentiality and non-repudiations are thoroughly complied with this self-defined protocol for total online validation of the appointment.
3. Apart from that, the proposed work implements some novel data hiding and digital signature concepts for color images. In this context combination of spatial and transformation based data hiding concepts are adopted with variable threshold range based secret data encoding on concern pixel bytes. This idea clearly strengthens the data hiding scenarios with much more enhanced data hiding imperceptibility and robustness over the existing ideas.

So, now to focus on this exhaustive study of e-appointment validation, the current paper is presented as follows. Section 2 gives a brief study of existing related works while section 3 summarizes some of the major enhancements addressed in this proposed work in contrast to the existing ideas. Then section 4 highlights the critical workflow of the client server authentication process and after that signature share generation and decoding algorithm given in section 5. After that signature hiding and extraction process

is focused in section 6 whereas experimental results and comparative study presented in section 7. Finally, section 8 gives the conclusion of this work and then relevant references are followed afterwards.

2. EXISTING APPROACHES

The combination of visual cryptography and watermarking [32] has been a unique proposition for digital and digitized document preservation and authentication. Mohananthini et al. [9] mentioned better performance with the use of LL2 sub-bands of DWT. More secure bit encoding techniques in transform domain concepts is proposed by Bhatnagar et al. [10] where multi-signature bits are encoded in segmented Discrete Cosine Transform (DCT) blocks [23] by utilizing the threshold value of block energy. In another algorithm Inamdar et al. [11] proposed multiple invisible watermarks to protect ownership of tampered image, i.e. by extracting invisible watermark appropriate ownership can be ratified.

In DWT domain, Natarajan et al. [12] utilized LL2 sub-bands of DWT for multi-signature concealment. In addition, Babaei et al [13] segmented fabrication of multiple signatures in wavelet transformed blocks and Thanki et al. [14] targeted HH3 and HH4 coefficients for the same. In another algorithm, Mohananthini et al. [16] mentioned both embedding and extraction technique for medical images using multi-resolution analysis of wavelet transform. An extension has also been proposed by Mohananthini et al. [17] where three watermarks are embedded into different channels (R, G and B) of a colour image. Chowdhury et al. [21] has worked upon a concept of validating an e-document online form from both the issuer and incumbent perspectives. To add, Chowdhury et al. [28] has complied all the major data security issues during hiding of signatures controlled by hash information.

Hence, this literature review reflects that the transform domain based data hiding concepts are more comprehensive. Further, the segmented data hiding scenario in transform domain and secret data encoding in combination with variable signature dispersing clearly strengthens the authenticity and robustness under the wireless domain.

So, considering all these novelties, the next section further highlights some of the major enhancements addressed in his proposed concept over the current existing ideas related to e-document validations [19].

3. UP-GRADATION OVER THE EXISTING APPROACHES

Proposed idea promotes a unique data security solution for validating the appointment of a candidate in online mode with some novel client-server authentication rules and innovative data hiding approaches. The concept mainly focuses on different possible frauds related to an e-appointment and also their effective handling. Hence, this work suggests a mutually trustable client-server data authentication protocol and here major advancements are as follows.

1. Confirming authenticity of the whole appointment event by validating e-appointment, appropriate candidature and candidate's joining at the applicable place of posting. This is reliably achieved at both the client and server end by secretly casting the respective signatures of both the client and owner on the same communicated e-document. Moreover, this signature embedding is dynamic and is dependent on some sensitive data related to the appointment. This dual dynamism basically enhances the authenticity a great deal by adding extra security and robustness while this dynamic signature casting is governed by self -defined hash operations involving sensitive data of e-appointment.
2. This novel e-appointment validation protocol also complies all the major data security issues like authenticity, integrity, confidentiality and non-repudiations for both the client and owner's perspectives and this practice is rarely addressed in the existing e-document validation approaches. Since, this work needs proper validation in both the client and owner's end, so this compliance of all the critical data security issues strengthens this idea even more.
3. Additionally, this work also applies novel data hiding techniques where combination of spatial and transform data encoding policies is adopted on different pixel bytes of a sub image block for better security. Further, variable threshold computation range based data encoding polices on different pixel bytes of a sub image block improves the robustness a great deal due to variable data hiding policies on different pixel bytes. Apart from that, region wise casting of multi-copy signature in cover image also boosts the robustness greatly as shown in Figure 1 & 2 respectively.

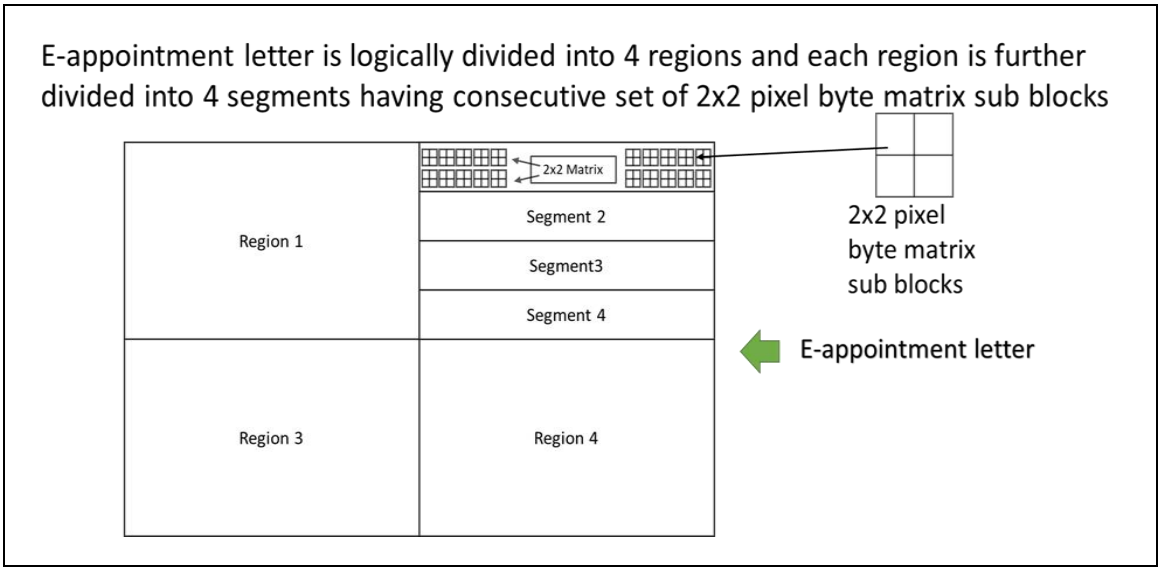


Figure 1. Region wise partitioning of the e-appointment cover image

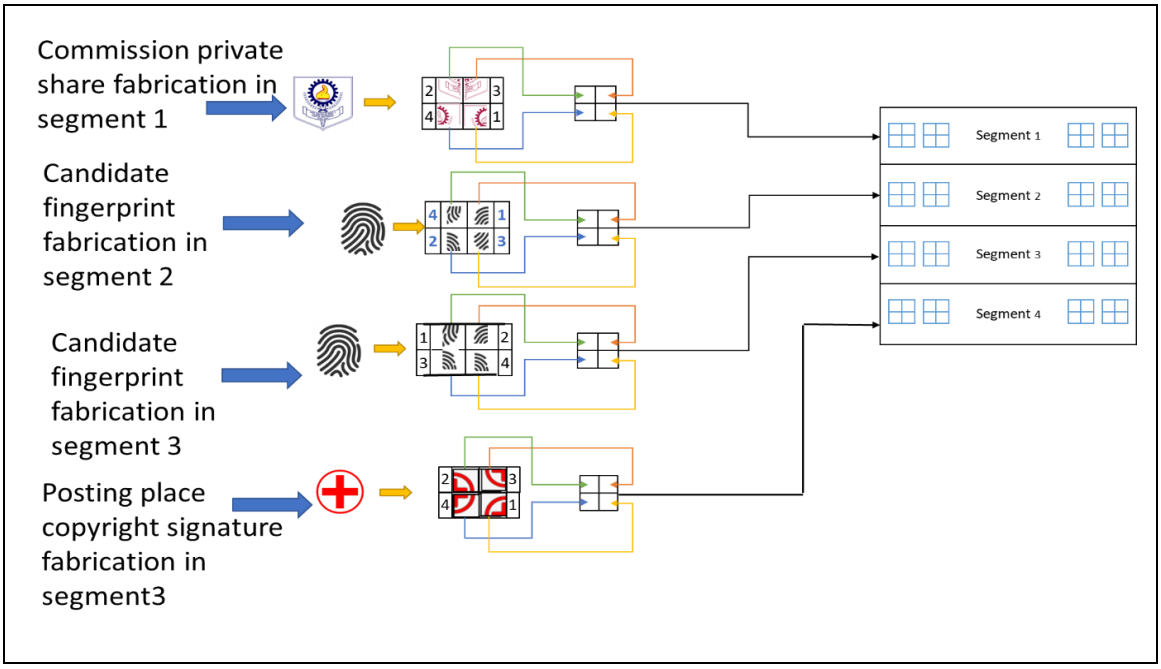


Figure 2. Segment wise signature embedding within the e-appointment cover image

Hence, designing of reliable data security protocol with handling of all the critical data security issues is the main motivation for this work while imparting dynamical authentication. This manifests the proposed idea in wireless domain.

4. WORKFLOW OF THE CLIENT SERVER AUTHENTICATION PROCESS

Step 1: The candidate visits the commission's office for collection of appointment letter, the candidate's fingerprint is collected and stored in the database. Further, the e-appointment letter is generated with attributes like employee Id, name, post/designation, order number, order date and place of posting etc.

Step 2: The private share of commission's watermark is concealed within the e-appointment letter in segment-1 based on the hash values H1 and H2, generated form employee Id (E) and order no. (O) respectively, using the following equations.

$$H1 = [\sum_{i=1}^{i=L} i \times ASCII(E_i) + \sum_{i=1}^{i=M} i \times ASCII(O_i)] \text{ Mod } 4 + 1 \quad (1)$$

$$H2 = [\sum_{i=1}^{i=L} i \times ASCII(E_i) - \sum_{i=1}^{i=M} i \times ASCII(O_i)] \text{ Mod } 4 + 1 \quad (2)$$

Where, *L* is the length of *E* and *M* is the length of *O*.

Step 3: The database at the commission's office consists of the following items:

Employee Id, name, order no, date of order, designation, contact number, place of posting, candidate's fingerprint image, e-appointment letter with commission's private share embedded within it, copyright logo of place of posting.

Step 4: When the candidate approaches his office of posting for joining, first of all his personal data (i.e. employee Id, name, designation, order no, date, etc.) is fed to the system manually from the printed appointment letter of the candidate. Here, only the employee Id is sent to the commission's office server and the e-appointment letter embedded with commission's private share is downloaded at the candidate's office.

Step 5: Based on these data exactly same hash values of H1 & H2 is derived at the candidate's office. Further, with the help of these hash values and the public share of the commission's watermark, the visual signature watermark of the commission will be detected and validated.

Step 6: Now, the candidate's fingerprint is taken on-spot and is embedded in segment-2 within the same copy of downloaded e-appointment letter. This is done on the basis of two hash values H3 & H4 generated from name (*N*) and designation (*D*) respectively, using the following equations.

$$H3 = [\sum_{i=1}^{i=L} i \times ASCII(N_i) + \sum_{i=1}^{i=M} i \times ASCII(D_i)] \text{ Mod } 4 + 1 \quad (3)$$

$$H4 = [\sum_{i=1}^{i=L} i \times ASCII(N_i) - \sum_{i=1}^{i=M} i \times ASCII(D_i)] \text{ Mod } 4 + 1 \quad (4)$$

Where, *L* is the length of *N* and *M* is the length of *D*.

Step 7: Next, the same fingerprint is also embedded within this downloaded e-appointment letter in segment-3 based on two separate sets of hash values H5 and H6 generated form order no, (*O*) and date of joining (*J*) respectively.

$$H5 = [\sum_{i=1}^{i=L} i \times ASCII(O_i) + \sum_{i=1}^{i=M} i \times ASCII(J_i)] \text{ Mod } 4 + 1 \quad (5)$$

$$H6 = [\sum_{i=1}^{i=L} i \times ASCII(O_i) - \sum_{i=1}^{i=M} i \times ASCII(J_i)] \text{ Mod } 4 + 1 \quad (6)$$

Where, *L* is the length of *O* and *M* is the length of *J*.

Step 8: Further, the copyright logo of the candidate's office is also embedded within this same e-appointment letter in segment-4 based on two hash values H7 & H8 generated form place of posting (*P*) and date of joining (*J*) respectively, using the following equations, using the following equations.

$$H7 = [\sum_{i=1}^{i=L} i \times ASCII(P_i) + \sum_{i=1}^{i=M} i \times ASCII(J_i)] \text{ Mod } 4 + 1 \quad (7)$$

$$H8 = [\sum_{i=1}^{i=L} i \times ASCII(P_i) - \sum_{i=1}^{i=M} i \times ASCII(J_i)] \text{ Mod } 4 + 1 \quad (8)$$

Where, *L* is the length of *P* and *M* is the length of *J*.

Step 9: Finally, this e-appointment letter along with employee Id and date of joining are transmitted to the commission's server for verification.

Step 10: On receiving this authenticated e-appointment letter at the commission's server end, the hash values are again computed based on the same critical data from the server database. Hence the

commission's server will be able to extract those same signatures from the respective segments for overall validation of this e-appointment letter, concerned candidature and also the office of posting as applicable.

The pictorial representation of this whole client-server authentication process is shown in Figure 3.

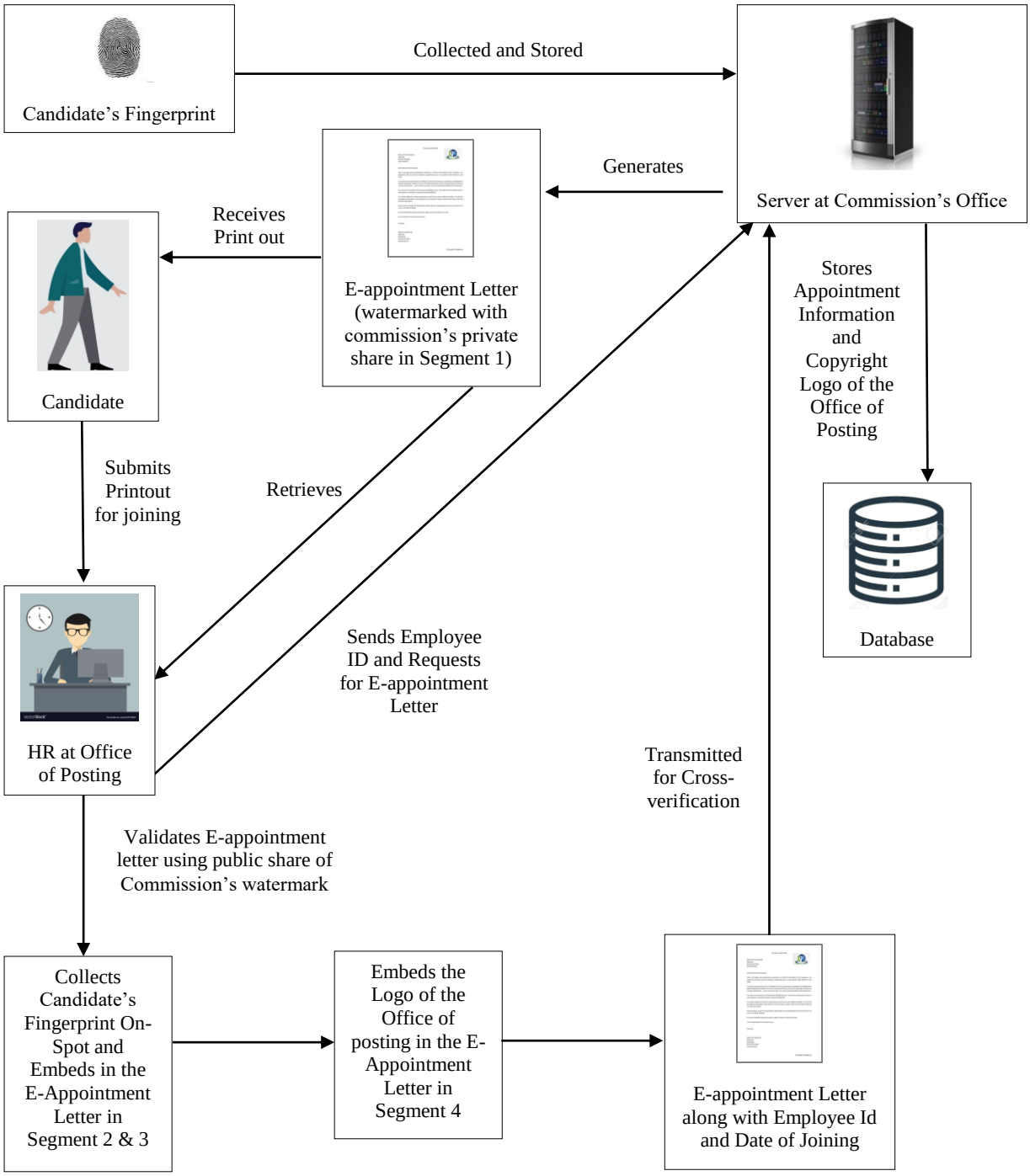


Figure 3. The workflow of the whole client server authentication process

5. FORMATION AND DECODING OF SIGNATURE SHARE

In the algorithm, two intensity values are formed from each RGB value i.e. P_N where N-> {1, 2,..., N} of the original signature image. Further, each of these two derived intensity values are written at the same pixel position 'pos' for the two concerned share images. In this context, let R[pos], G[pos], and B[pos] denotes the intensity values respectively at pixel position 'pos'. The conversion of intensity values is done by arithmetic operations and TV_r, TV_g, and TB_b are used as predefined threshold values

for the respective planes at index 'pos'. The possible set of {TV_r, TV_g, TB_b} can be {126, 52, 52}, {48, 121,46}, {45,45,121} and {126,125,126} respectively.

P_r, P_g and P_b are used for storing the intermediate values in the process of deriving the two intensity values at pixel position $P_N$where N-> {1,2,...,N}. In addition, Q_r, Q_g, and Q_b are also used for storing an alternate set related to R, G, and B components respectively at the same pixel position 'pos'. Individual generated values at index 'pos' for the secret (S_E) and private (P_R) share can be represented as S_E≡{E1[pos]$_r$, E1[pos]$_g$, E1[pos]$_b$} and P_R≡{E2[pos]$_r$, E2[pos]$_g$, E2[pos]$_b$} respectively. The transformation operation depends on the intensity index u∈{r, g, b} at pixel position 'pos'.

Moreover, merging the transformed value sets of {E1[pos]$_u$} and {E2[pos]$_u$}, where u∈{r, g, b}, as obtained for secret and private share at pixel position 'pos',the original set will be recovered. Likewise, repeating the process for both the shares will recover the original signature image. The algorithmic representation is as follows:

5.1 Signature Share Generation

```
For pos=1 to N
  Do
Pr←R[pos] mod 9 + (pos) Mod 11 + TVr ;
    Pg←G[pos] mod 10 + (pos) Mod 13 + TVg ;
    Pb←B[pos] mod 12 + (pos) Mod 15 + TVb ;
    Qr←R[pos]-Pr ;
    Qg←G[pos]-Pg ;
    Qb←B[pos]-Pb ;
     If(Qr<0) Then   E1[pos]r←R[pos];
                     E2[pos]r←0;
              Else   E1[pos]r←Pr ;
                     E2[pos]r←Qr;
     If(Qg<0) Then   E1[pos]g←G[pos];
                     E2[pos]g←0;
              Else   E1[pos]g←Pg ;
                     E2[pos]g←Qg;
     If(Qb<0) Then   E1[pos]b←B[pos];
                     E2[pos]b←0;
              Else   E1[pos]b←Pb ;
                     E2[pos]b←Qb;
    pos←pos+1;
 End Loop
```

5.2 Signature Recovery by Decrypting Signature Shares

```
For pos=1 to N
 Do
    R[pos] ← E1[pos]r+E2[pos]r ;
    G[pos] ← E1[pos]g+E2[pos]g;
    B[pos] ← E1[pos]b+E2[pos]b ;
    pos←pos+1;
 End Loop.
```

6. SIGNATURE EMBEDDING & DETECTION PROCEDURE

The cover image of the letter is broken into four areas, each of which is further divided into four segments, total 16 segments. Initially, the current letter image segment is separated into a sequence of 2x2 non-overlapping sub-block matrices of pixel bytes. The forward pixel byte transform is applied to the 1st, 2nd, and 4th elements of the matrix to create signature bits on each sub-matrix first, while the 3rd element is kept intact for spatial encoding.

Now, one signature bit is spatially encoded on the 3rd matrix element directly, while one signature bit is embedded on the positive values of those three modified matrix elements. Finally, the bit-coded 1st, 2nd and 4th elements of the matrix are reverse transformed to yield the final signature bit. The receiver applies the same forward transform to the 1st, 2nd and 4th matrix elements in order to extract the hidden signature bits from the concern modified matrix element, while the 3rd matrix element's hidden bit is recovered immediately. The retrieved 4 bits from each matrix element are then stacked or packed in correct sequences to produce the concerned signature fragment, which will be used for later merging and signature generation.

6.1 Sub Image Block Matrix Transformation

Let sub matrix of a region is Z_{bn}=[ei], where ei ϵ{0,1,..,255} is the pixel byte value for matrix element index i ϵ{1,2,3,4} and bn ϵ{1,..,N} is the matrix number. For signature bit encoding, the forward and reverse transformation of Z_{bn} is given as-

Forward Transform

$$Z_{bn} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \tag{9}$$

$$Z_{bn(forward)} = \begin{bmatrix} A_1 = \frac{a+c}{2} & A_2 = b - d \\ A_3 = \frac{a-c}{2} & A_4 = d \end{bmatrix} \tag{10}$$

Reverse Transform

$$Z_{bn(reverse)} = \begin{bmatrix} a = A_1 + A_3 & b = A_2 + A_4 \\ c = A_1 - A_3 & d = A_4 \end{bmatrix} \tag{11}$$

Now signature bit encoding on transformed matrix components are step wise demonstrated as follows-

$$Z_{bn} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$\downarrow \text{ Forward Transform}$$

$$Z_{bn}{}' = \begin{bmatrix} A_1 = \frac{a+c}{2} & A_2 = b - d \\ A_3 = \frac{a-c}{2} & A_4 = d \end{bmatrix}$$

$$= \begin{bmatrix} A_1 = X_1 + \frac{r}{2} & A_2 = \pm(X_2) \\ A_3 = \pm\left(X_3 + \frac{r}{2}\right) & A_4 = X_4 = d \end{bmatrix} \quad \text{where, } r \in \{0, 1\}$$

Signature bit insertion in the resulting sub-matrix $Z_t{}'$,

$$Zbn// = \begin{bmatrix} A_1' = (X_1 \pm \alpha_1) + \frac{r}{2} & A_2' = \pm(X_2 \pm \alpha_2) \\ A_3' = \pm\left((X_3 \pm \alpha_3) + \frac{r}{2}\right) & A_4' = (X_4 \pm \alpha_4) \end{bmatrix} \quad \text{where, } r \in \{0, 1\}$$

$$Z_{bn}{}'' = \begin{bmatrix} A_1' = (C_1) + \frac{r}{2} & A_2' = \pm(C_2) \\ A_3' = \pm\left((C_3) + \frac{r}{2}\right) & A_4' = (C_4) \end{bmatrix} \quad \text{where } Ci = Xi \pm \alpha_i \text{ for } i=1, 2, 3, 4$$

Reverse Transformation

$$Z_{bn}^{///} = \begin{bmatrix} A_1^{//} = A_1^{/} + A_3^{/} & A_2^{//} = A_2^{/} + A_4^{/} \\ A_3^{//} = A_1^{/} - A_3^{/} & A_4^{//} = A_4^{/} \end{bmatrix} \quad (12)$$

The transformed matrix $Z_{bn}^{/}$= [Ai] is obtained from Z_{bn} by applying the transformation procedure in (11), with each Ai representing the transformed or non-transformed matrix element at element index i = 1, 2, 3, 4. On the positive integer part of each transformed component as well as the non-transformed fourth element of $Z_{bn}^{/}$, one signature bit is now coded. The generated matrix $Z_{bn}^{//}$ is then reverse transformed using the matrix transformation method to produce the final bit embedded matrix $Z_{bn}^{///}$. Similarly, the $Z_{bn}^{/}$ matrix is forward transformed at the receiver side using the matrix transformation rule to produce the transformed matrix $Z_{bn}^{//}$. Each embedded bit bi is now detected from the appropriate positive integer part of each transformed matrix element, as well as the non-transformed fourth matrix element.

$C_i \leftarrow FUN1(X_i, b_i)$: Start
If($b_i = 0$) Then [If ((X_i Mod 2) = 0) Then $C_i \leftarrow X_i$;
Else $C_i \leftarrow (X_i - (X_i \text{ Mod } 2))$;
]
If(bi=1) Then [If((X_i Mod 2)=0) Then $C_i \leftarrow (X_i+1)$;
Else $C_i \leftarrow X_i$;
]
Return C_i;
End
$Mid_i \leftarrow FUN2(X_i, p)$: Start
If((X_i Mod p)=0) ? [Low $\leftarrow X_i$; : Low $\leftarrow (X_i - (X_i \text{ Mod } p))$;]
Upp$\leftarrow$Low+p;
If(Upp>256) ? [$Mid_i \leftarrow$ 254; : $Mid_i \leftarrow$(Low+Upp)/2;] (13)
Return Mid_i;
End

Two functions FUN1(X_i, b_i) and FUN2(X_i, p) are defined to code the bit $b_i \in \{0,1\}$ on corresponding transformed positive integer component of X_i, for $i \in \{1,2,3,4\}$. 'FUN2' directly returns the concerned coded value $C_i \in \{0,\pm1..,\pm255\}$, whereas 'FUN2' returns the positive threshold reference point Mid_i $\in \{0,1,..,255\}$ in between the lowest (Low) and upper (Upp) multiple number of 'p' with regard to X_i. This point is then used for threshold value based bit coding with suitable signs, and the following is the step-by-step process for bit casting.

6.2 Signature Bit Insertion Algorithm

Input: One colour e-document and four colour copyright signatures.

Output: Authenticated e-document image hosts four copies of each of the four copyright signatures.

Method: For all regions or segments, the particular matrix Z_{bn} is first forward transformed and one single copyright signature bit is embedded on the positive integer part (X_i) of each transformed component of Z_{bn} or directly on the spatial value. Now this bit coded matrix $Z_{bn}^{//}$ is reverse transformed for obtaining the final bit coded output matrix $Z_{bn}^{///}$. Further, if the matrix interval for the specific e-document image segment is considered as 'intv', then the signature bit hiding procedure in Z_{bn} can be expressed as follows.

For matrix number bn=1 to N
Do
Step 1: Apply forward transform on Z_{bn} as per the matrix transformation rule to obtain the corresponding transformed matrix $Z_{bn}^{/}$

Step 2: Track the concern positive integer part X_i from each of the transformed component of $Z_{bn}{}^{/}$ and also from its non-transformed fourth element spatial value with i ϵ {1, 2, 3, 4}.

Step 3: Read a set of four signature bits $b_i \epsilon \{0, 1\}$ for i=1, 2, 3, 4.

Step 4: Encode the particular signature bit $b_i \epsilon \{0, 1\}$ on the corresponding X_i value to obtain the respective coded value C_i as -

$Mid_1 \leftarrow FUN2(X_1, 4);$
IF ($b_1 = 1$) Then $C_1 \leftarrow Mid_1+1;$
ELSE $C_1 \leftarrow Mid_1-1;$
$Mid_2 \leftarrow FUN2(X_2, 6);$
IF ($b_2 = 1$) Then $C_2 \leftarrow Mid_2+1;$
ELSE $C_2 \leftarrow Mid_2-1;$
$Mid_3 \leftarrow FUN2(X_3, 8);$
IF ($b_3 = 1$) Then $C_3 \leftarrow Mid_3+1;$
ELSE $C_3 \leftarrow Mid_3-1;$
$C_4 \leftarrow FUN1(X_4, b_4);$ (14)

Step 5: Now the bit coded matrix $Z_{bn}{}^{//}$ is reverse transformed as per the matrix transformation rule (12) while keeping the bit coded fourth element value as non-transformed to obtain the final output matrix $Z_{bn}{}^{///}$.

Step 6: If required, perform some delicate adjustments on the respective elements of Z_{bn} to maintain the final output matrix elements of $Z_{bn}{}^{///}$ in spatial domain.

Step 7: bn ← bn + intv;
End Loop

6.3 Signature Bit Detection Algorithm

Input: Authenticated e-document image which hosts four copies of each of the four signatures.

Output: Best copy of each of the four secret copyright signatures sensed from the cover e-document image.

Method: For all regions or segments, the particular signature bit coded sub matrix $Z_{bn}{}^{///}$ is forward transformed to obtain the transformed matrix $Z_{bn}{}^{//}$ and one secret bit (bi) is then sensed from the concern integer part (C_i) of each transformed component of $Z_{bn}{}^{//}$ or from the concern bit coded spatial value as well, with $i \epsilon \{1,2,3,4\}$. Now, these four sensed bits are further clustered in exact sequences to generate the particular signature image. If the matrix interval for the concern image segment is 'intv' just like the signature bit embedding algorithm, then bit detection algorithm is step wise given as follows.

For matrix number bn=1 to N

Do

Step 1: Apply forward transformation on the received bit coded matrix $Z_{bn}{}^{///}$ as per the matrix transformation rule (11) to obtain the transformed matrix $Z_{bn}{}^{//}$.

Step 2: Track the corresponding bit coded positive integer part C_i from each of the transformed component of $Z_{bn}{}^{//}$ and also from its non-transformed fourth element, with i=1, 2, 3, 4.

Step 3: The single encoded bit bi from each of the corresponding C_i of $Z_{bn}{}^{//}$ for i=1,2,3,4 is now detected as

$Mid_1 \leftarrow FUN2(C_1,4);$
IF ($C_1 >= Mid_1$) Then $b_1 \leftarrow 1;$
ELSE $b_1 \leftarrow 0;$
$Mid_2 \leftarrow FUN2(C_2,6);$
IF ($C_2 >= Mid_2$) Then $b_2 \leftarrow 1;$
ELSE $b_2 \leftarrow 0;$
$Mid_3 \leftarrow FUN2(C_3,8);$

IF (C_3>=Mid_3) Then $b_3 \leftarrow 1$;
ELSE $b_3 \leftarrow 0$;
IF ((C_4 Mod 2) = 0) Then $b_4 \leftarrow 1$; (15)
ELSE $b_4 \leftarrow 0$;

Step 4: Now arrange all these detected bits form the respective matrix elements in proper sequences and then write these chunks of four bits in exact orders within the output image to generate the concern signature image.

Step 5: bn ← bn + intv;
End Loop

7. EXPERIMENTAL RESULT ANALYSIS & COMPARATVE STUDY

This proposed scheme is extensively tested with color cover images of size 512 x 512 and the signature images of size 32x32 or 64x64. Critically, all these images are taken in PPM format and the signature embedding and extraction algorithm implemented through C language under the LINUX platform while the simulation results related to image similarity traced through MATLAB software (R2018a) [20, 24]. The effectiveness of this scheme further judged from different angles in terms of data hiding imperceptibility and robustness with common standard image similarity parameters like Peak Signal to Noise Ratio [i.e PSNR with its unit in decibel (dB)], Structural Similarity Index Measurement [i.e SSIM with its value ranges between –1(mostly dissimilar) to +1(exactly similar))] and Correlation Coefficient [i.e CC with its value ranges between – 1(mostly dissimilar) to +1(exactly similar)] [10-17]. In this aspect, at first Table 1 reflects identical visual qualities of the original and signature casted watermarked e-document images with good PSNR, SSIM and CC values while Table 2 shows the signatures and respective shares used for embedding. Hence, Table 1 clearly highlights that the shown watermarked images are mostly free form any visual or statistical attacks while they reflect superb data hiding imperceptibility as well.

Table 1. Visual representation of original and watermarked image with similarity parameter values

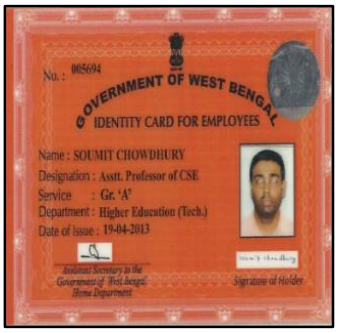
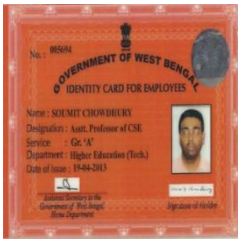
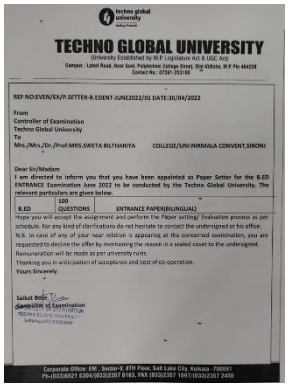
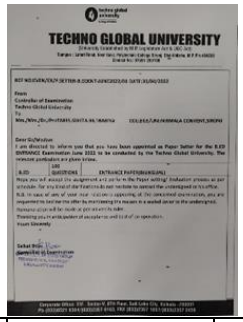
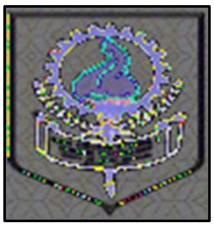
<table>
<tr><th>Original Cover Image</th><th colspan="3">Watermarked Image</th></tr>
<tr><td rowspan="2"> 
</td><td colspan="3">  </td></tr>
<tr><td>PSNR</td><td>NCC</td><td>SSIM</td></tr>
<tr><td>ID Card</td><td>41.24</td><td>0.9934</td><td>0.9961</td></tr>
<tr><td rowspan="2"> 
</td><td colspan="3">  </td></tr>
<tr><td>PSNR</td><td>NCC</td><td>SSIM</td></tr>
<tr><td>Appointment Letter</td><td>40.94</td><td>0.9978</td><td>0.9943</td></tr>
</table>

Table 2. Signature images along with respective signature share used for embedding purpose

			
Private share of Commission	Fingerprint of Candidate	Fingerprint of Candidate	Copyright Signature of posting place

In addition to these above mentioned image similarity parameters, a detail histogram analysis is also shown in Table 3 and Table 4 to further judge the data hiding imperceptibility. In this context, Table 3 visualizes almost identical general histograms whereas Table 4 reflects mostly similar Red (R)-Green (G)-Blue (B) component or R-G-B plane histograms for both the original and watermarked images. So, in view of such good results of histogram analysis for both general and R-G-B histograms, it can be said that the proposed data hiding technique mostly resists any kind of visual or statistical attacks and shows very good data hiding invisibility. This is mainly due to the fact that maximum deviation of any pixel byte falls between ±(4-6) which is not high as compare to transform domain data hiding concept.

Table 3. General Histogram Analysis for Cover and Watermarked Image

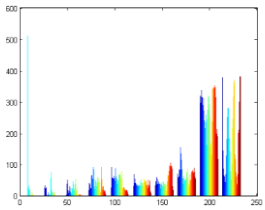
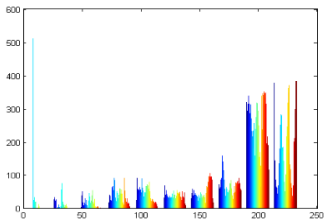
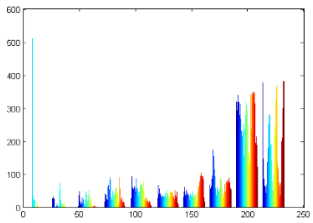
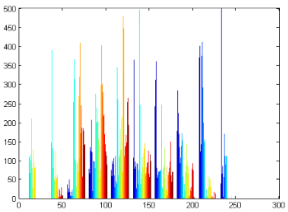
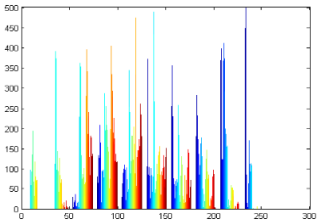
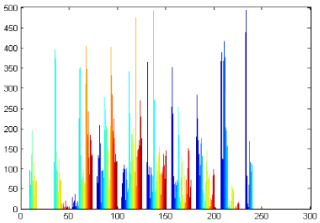
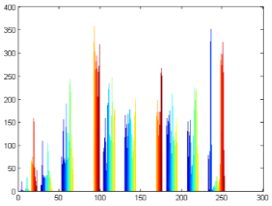
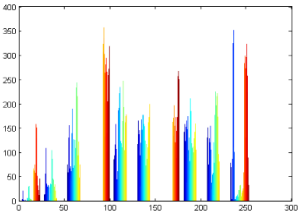
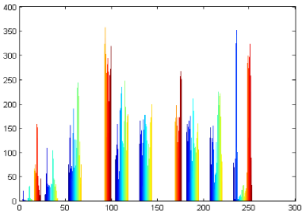
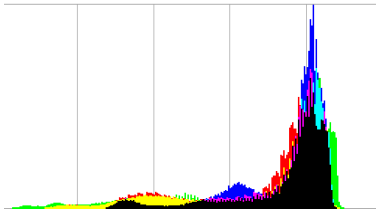
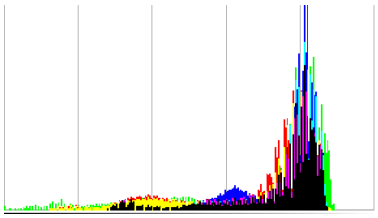
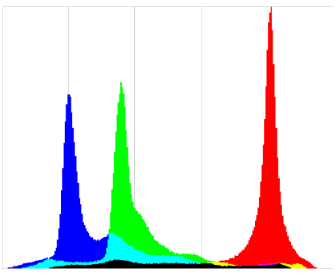
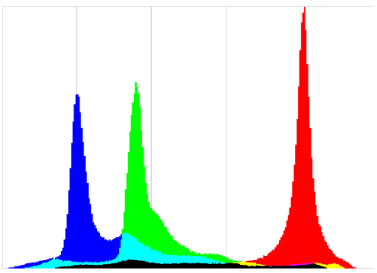
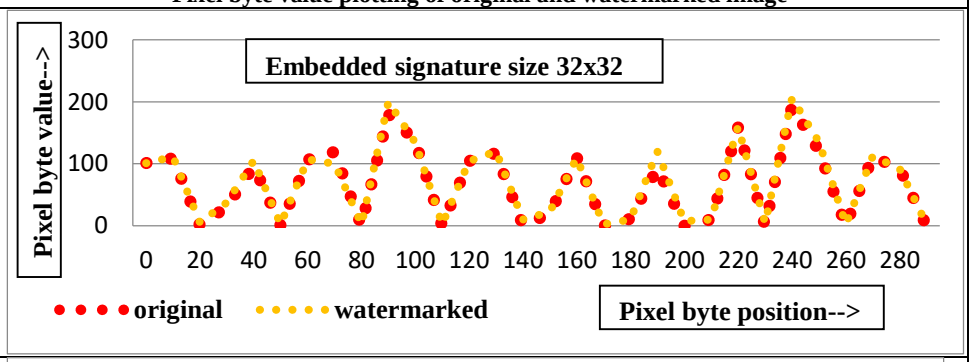
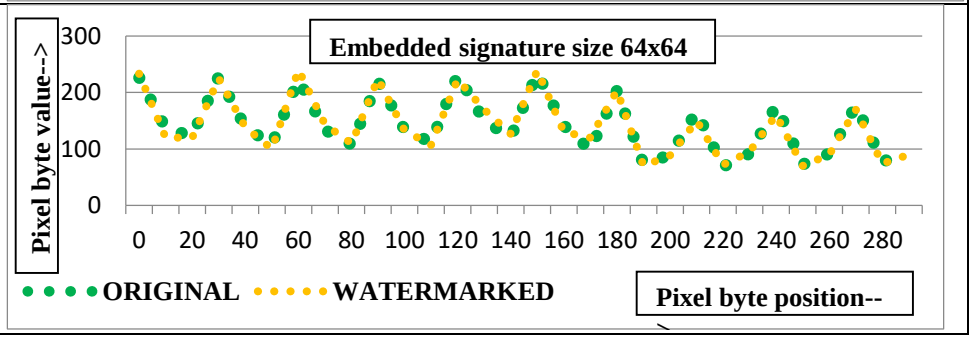
Cover Image	**Bit Sequence of Authenticated image with Secret Data (32x32)**	**Bit Sequence of Authenticated image with Secret Data (64x64)**
 **ID Card**		
 **Appointment Letter #1**		
 **Appointment Letter #2**		

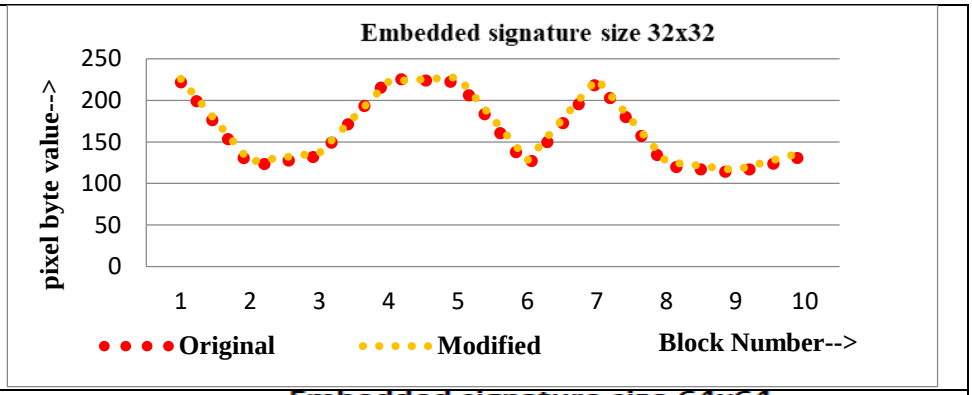
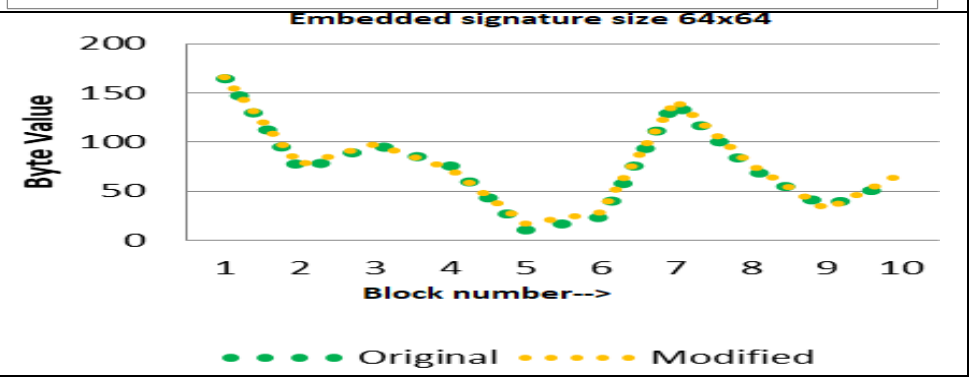
Table 4. R-G-B Plane or R-G-B Component Histogram Analysis for Cover and Watermarked Image

Cover Image	Bit Sequence of Authenticated image with Secret Data (32x32)	Bit Sequence of Authenticated image with Secret Data (64x64)
 Appointment Letter #1		
 Appointment Letter #2		

Apart from using these common standard methods, the noise injection due to signature embedding within the watermarked image is further evaluated through pixel byte value deviations line graph as reflected in Table 5. Here in case (a) and (b) respective pixel byte position values are plotted for the original and watermarked images considering certain periodical interval of pixel byte positions. Additionally, another line graph pairs in (c) and (d) is also shown by taking into account the average of respective block pixel byte values for both the original and watermarked image.

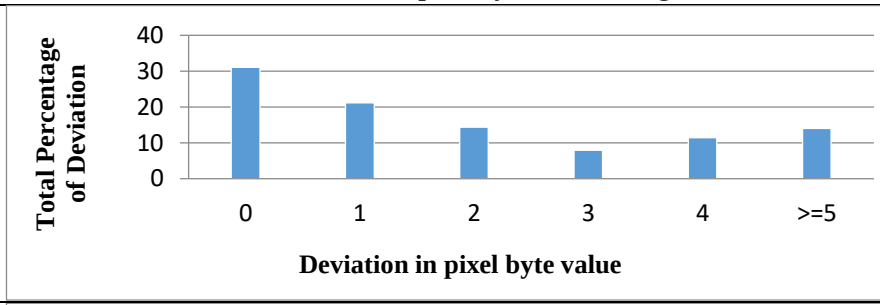
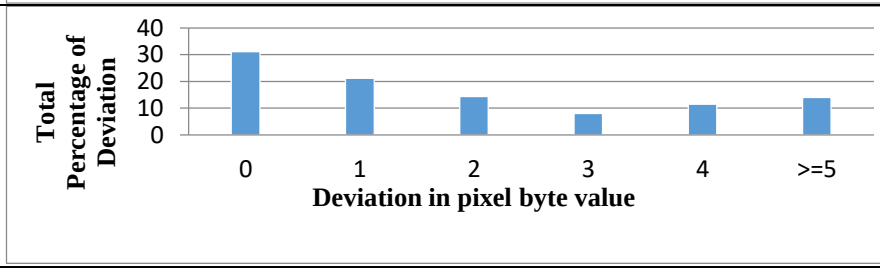
Table 5. Deviation of pixel bytes for both the original and watermarked image

Cover image used	Pixel byte value plotting of original and watermarked image
(a) ID-Card	
(b) Appointment Letter #1	

(c) ID-Card	
(d) Appointment Letter #1	

Critically, all such line graph pairs for the original and watermarked images does not deviate that much from each other and hence indicating very little distortion between the original and watermarked image. To highlight this lesser deviation scenario even more, Table 6 represents a bar chart reflecting the total number of pixel byte deviation % for the respective deviation value as traced between the original and watermarked image.

Table 6. Total % of different levels of pixel byte value changes for original and watermarked image

Cover Image	Estimation of different levels of pixel byte value changes in terms of %
ID-Card (embedded signature size 32x32)	
Appointment letter #1 (embedded signature size 64x64)	

Further assessment on data hiding invisibility is also explored by way of an exhaustive comparative study with the existing concepts where the proposed work highlights significant enhancements from different angles especially 1-3% minimum growth of PSNR under much higher data pay load hiding. This comparison is shown in Table 7 where the proposed idea mostly reflects 2-3 times higher pay load embedding and superior PSNR for colour cover and signature images both in contrast to the other works.

Table 7. Comparison of data hiding imperceptibility with the existing approaches

Existing works	Signature hiding category	Signature type used	Signature copies embedded	Pay load capacity	PSNR (dB)	SSIM
Nasir et al.[2], 2009	Segmented	Binary	04	4,096 bits	39.0627(max.)	
Behnia et al.[3], 2010	Segmented	Grey scale	03	6,144 bytes	30.11	
Bhatnagar et al.[10], 2013	Segmented	Grey scale	09	5,120 bytes	33.8506(max.)	
Babaei et al.[13], 2014	Segmented	Binary	04	4,096 bits	28.44 (max.)	
Karthik et al. [15], 2015	Composite	Binary	03	3,072 bits	40.76	
Thanki et al., [14], 2015	Successive	Grey scale	02	320 bytes	30.79	
Mohantini et al., [18], 2016	Segmented	Color	02	13,824 bytes	38.0639(max.)	
Sadh et al.[22], 2016	Segmented	Binary	08	8, 192 bits	38.9060	
Chowdhury et al.[21], 2017	Segmented	color	04	12,288 bytes	40.4091(max.)	
Kumar et al.[25], 2018	Segmented	Binary	02	10, 240 bytes	40.97 (max.)	0.9994(max.)
Chowdhury et al.[28], 2019	Segmented	Color	16	30,000 bytes	39.0547 (avg.)	
Chowdhury et al.[27], 2020	Segmented	Color	08	13,824 bytes	38.75 (avg.)	
Alias et al.[29], 2020	Segmented	Binary	02	Not Reported	Not Reported	0.9157 (avg.)
Proposed work	**Segmented**	**Color**	**16**	**49,152 bytes**	**41.897 (avg.)**	**0.9948(avg.)**

To proceed further with the successful implementation of this scheme, the hidden signature extraction or recovery aspects is now focused where at first Table 8 reflects exact identical signature recovery by merging the respective public share and the extracted private share of the concern signature. Critically all these attack related tests were carried out on the watermarked ID-Card image and after extraction of attack affected signatures form the attacked watermarked image, they were matched with their respective original form to judge the concern quality. If due to attack affects signature bit coded altered pixel byte value stays within the applicable valid range, then the correct signature bit will be sensed form that particular pixel byte value. Further, this proposed idea also adopts multi-copy signature embedding which actually promotes quality wise best signature copy sensing from all those attacks affected extracted signature copies. Hence, this proposed algorithm aims to serve strong robustness that is reasonable recovery of signatures under various attacks and this is clearly judged from the following tables of 9, 10 and11. Among these, Table 9 shows the matching CC value for each of the best signature copy recovered against the corresponding attack. After that, Table 10 presents the average CC value of all the four best recovered signatures against a particular attack and this value looks superior in contrast to the other related works showing the similar scenario. Finally, at last Table 11 highlights a comparison where the proposed concept visualizes cent percent good quality ($CC \geq 0.7$) signature recovery against numerous attacks and this scenario is either at par or much better in contrast to the other related works.

Table 8. Regeneration or reframing of commission signature by merging its public and private share

		
(a) Private share generated form Commission signature	(b) Public share generated form Commission signature	Regeneration of commission signature after merging (b) (public share) and (a) private share)

Table 9. CC value of best recovered signature copy traced under different attacks

Applied attacks with their respective parameter values	**CC value for each of the best recovered signature copy as observed under different attacks and recovered from different regions of the cover e-document image**			
	Signature-1	**Signature-2**	**Signature-3**	**Signature-4**
File format change (JP2 or JPEG 2000, Q=98%)	0.8788	0.8530	0.8864	0.7466
Vertical Flip – 180^0 and then back to the normal form	0.9918	0.9954	0.9913	0.9912
Horizontal Flip – 180^0 and then back to normal form	0.9956	0.9948	0.9945	0.9945
Blurring (Blur Radius – 5, Max Delta – 2)	0.9211	0.9065	0.9123	0.9014
Gaussian Filter (Filter - 3*3 & Sigma – 0.9)	0.8079	0.7667	0.8344	0.7923
Gamma Correction (1.15)	0.7879	0.8088	0.8217	0.7399
Circular Average Attack (radious 0.5)	0.9113	0.9321	0.8512	0.8334
HSV Noise attack (Hue–4, Saturation–4, Variance– 4)	0.7145	0.7445	0.6366	0.6188
Normalization	0.9655	0.9978	0.9956	0.9844
File format change .ppm to .png and back to .ppm	0.9910	0.9988	0.9934	0.9941

Table 10. Average CC value comparison for detected signatures with the existing works under attacks

Applied attack names	**Proposed work (average CC of best detected signatures)**	**Existing Works**	
		Average CC of best signatures	**Respective works/approaches**
Salt & Pepper Noise	0.9817 (used with 5%)	0.9417	Mohananthini et al., [18], 2016 (used 3%, embedded 2 signatures)
		0.7577	Chowdhury et al.[21], 2017 (5%, 4 signatures)
		0.963	Chowdhury et al.[27], 2020 (5% with 4 best signatures)
		0.8676	Chowdhury et al.[28], 2019 (5%, 4 best signatures)
		0.9845	Shen et al.[31], 2021 (1%, 2 best signatures)
		0.9704	Kumar et al.[25], 2018 (1%, 2 signatures)
Gaussian Noise	0.8015 (used with 2%)	0.7563	Chowdhury et al.[21], 2017 (2%, 4 signatures)
		0.517	Chowdhury et al.[28], 2019 (1 %, 4 best signatures)
Median Filtering	0.9945 (for 3x3 blocks)	0.9716	Kumar et al.[25], 2018 (2x2, 2 signatures)
		0.96	Liu et al.[26], 2019 (3x3, 3 signatures)
		0.9586	Shen et al.[31], 2021 (3x3, 2 signatures)
		0.9929	Singh et al.[30], 2021 (3x3, 2 signatures)
Wiener Filtering	0.9981 (for 3x3 blocks)	0.7910	Mohananthini et al.[18], 2016 (3x3, 2 signatures)
		0.9997	Chowdhury et al.[27], 2020 (3x3, 4 best signatures)

Cropping	0.9998(75% cut)	0.9935	Shen et al.[31], 2021 (25% cut, 2 signatures)
		0.863	Alias et al.[29], 2020 (column crop 25%, 2 signatures)
		0.5933	Liu et al.[26], 2019 (37% in Y direction, 3 signatures)
		0.3487	Mohananthini et al.[18], 2016 (2 signatures)
Translation	0.9979 (used 0.4,-0.4)	0.9999	Chowdhury et al.[27], 2020 (0.4, -0.4, with 4 best signatures)
		0.9472	Mohananthini et al.[18], 2016 (2 signatures)
Sharpening	0.9712 (used with 5%)	0.9678	Chowdhury et al.[21], 2017 (2% & 3%, 4 signatures)
		0.8932	Chowdhury et al.[28], 2019 (3%, 4 best signatures)
		0.9516	Mohananthini et al. [18], 2016 (2 signatures)
Smoothing	0.9984(used with 30%)	0.9531	Chowdhury et al.[27], 2020 (30%, 4 best signatures)
		0.9918	Chowdhury et al.[28], 2019 (30%, 4 best signatures)
Brightness & Contrast change	0.75874 (used with B–5, C–5)	0.4534	Chowdhury et al.[28], 2019 (B-5 & C-5, best 4 signatures taken)
RGB value Change in Gimp	0.6815 (used as Hue:R-10, G-10, B-10)	0.3777	Chowdhury et al.[28], 2019 (Hue: R-5, G-5, B-5, best 4 signatures taken)
RGB Change in Irfan view	0.9718 (R-5, G-5, B-5)	0.6216	Chowdhury et al.[28], 2019 (R-5, G-5, B-5, best 4 signatures taken)

Table 11. Comparison of the percentage of signature recovery with CC value > 0.7

Attack Name	**[18], 2016 (2 sign)**	**[21], 2017 (4 sign)**	**[25], 2018 (2 sign)**	**[28], 2019 (4 sign)**	**[26], 2019 (3 sign)**	**[29], 2020 (2 sign)**	**[30], 2021 (2 sign)**	**[31], 2021 (2 sign)**	**This work (4 sign)**
Salt & Pepper Noise (5%)	02 (100%)	03 (75%)	02 (100%)	04 (100%)	NA	02 100(%)	02 100(%)	02 100(%)	04 (100%)
Gaussian Noise (2%)	02 (100%)	03 (75%)	02 (100%)	0 (0%)	03 (100%)	02 (100%)	02 (100%)	02 (100%)	04 (100%)
Median Filtering (3x3)	02 (100%)	04 (100%)	02 (100%)	04 (100%)	03 (100%)	02 (100%)	02 (100%)	02 (100%)	04 (100%)
Wiener Filtering (3x3)	02 (100%)	04 (100%)	NA	04 (100%)	NA	NA	NA	NA	04 (100%)
Crop(up to 75% cut)	0 (0%)	04 (100%)	02 (100%)	04 (100%)	0 (0%)	02 (100%)	NA	02 (100%)	04 (100 %)
Row-Column alter 60(R), 60(C)	0 (0%)	04 (100%)	NA	04 (100%)	NA	NA	NA	NA	04 (100%)
Translation [0.4, -.04]	02 (100%)	04 (100%)	NA	04 (100%)	03 (100%)	NA	NA	NA	04 (100%)
Sharpening (up to 5%)	02 (100%)	04 (100%)	NA	04 (100%)	NA	NA	02 (100%)	NA	04 (100%)
Smoothing (up to 30%)	02 (100%)	04 (100%)	NA	04 (100%)	NA	NA	NA	NA	04 (100%)
Speckle Noise (5%)	02 (100%)	01 (25%)	02 (100%)	0 (0%)	NA	02 (100%)	02 (100%)	02 (100%)	02 (50%)
Brightness & Contrast change (B-5, C-5)	NA	02(50%)	NA	0 (0%)	NA	NA	NA	NA	04 (100%)

RGB value Change in Irfanview(R-5, G-5, B-5)	NA	03 (75%)	NA	01 (25%)	NA	NA	NA	NA	04 (100%)
Gaussian Filter (Filter - 3*3 & Sigma – 0.9)	NA	01 (25%)	NA	NA	NA	02 (100%)	02 (100%)	NA	04 (100%)
Gamma Correction (up to 1.15)	NA	02 (50%)	NA	NA	NA	NA	NA	02 (100%)	04 (100%)

8. CONCLUSION

This idea thoroughly justified a unique data security protocol for validating the whole appointment process of a candidate in online mode to resist the different frauds related to e-appointment scenarios. The work clearly shows significant enhancements on current approaches regarding online validation of such precious e-documents while also promoting some inventive data security solutions and here the major contributions are as follows.

1. The appointment of a candidate is validated from different angles by judging the authenticity of e-appointment, the appropriate candidature at proper place of posting and all the associated sensitive data. Hence all components of the appointment are validated and this is achieved by concealing respective signatures of both client and owner dynamically on the same communicated e-document at the concern end. Further, this dynamical signature casting is based on some self-defined hash operations which ultimately leads to some innovative data hiding strategies. So, this whole appointment validation concept truly raises a novel client-server data authentication protocol.
2. In contrast to the existing works this proposed protocol thoroughly complies all the critical data security issues like authentication, confidentiality, integrity and non-repudiations from both the client and owner's perspectives.
3. Additionally, this proposed work also establishes a typical data hiding concept by combining both spatial and transformed data encoding techniques within the same sub image block pixel byte matrix. Importantly, this idea has shown much more effectiveness with at least 10% improvement of test results from different angles over the current existing approaches both in terms of data hiding imperceptibility and robustness.

So, with these vital attainments the proposed idea can be promoted as a possible solution for e-appointment fraud cases where the whole appointment can be validated including service joining of a candidate at the proper place. Also, this work should suit the wireless domain applications with such strong data security solutions. However, this work can be further extended for implementation of automations and handling of different geometrical attacks.

CONFLICT OF INTEREST

The authors declare no conflict of interest

ACKNOWLEDGEMENTS

The author(s) expresses their deep sense of gratitude towards all the faculty and staff members of the Department of Computer Science Engineering, Bhabha University, Bhopal, India for their kind cooperation and support in connection of carrying out this research work.

References

[1] Tsui, T., Zhang, Xiao-Ping., Androutsos, D.: Color image watermarking using multidimensional fourier transformation. IEEE Transactions on Information Forensics and Security. 3(1), 16-28 (2008). doi: 10.1109/TIFS.2007.916275.

[2] Nasir, I., Weng, Y., Jiang, J., Ipson, S.: Multiple spatial watermarking technique in color images. Signal Image & Video Processing (SiViP). 4(2), 145–154 (2009). doi: 10.1007/s11760-009-0106-7.

[3] Behnia, S., Teshnehlab, M., Ayubi, P.: Multiple watermarking scheme based on improved chaotic maps. Communication in Nonlinear Science and Numerical Simulation, 15(9), 2469-2478 (2010). doi:10.1016/j.cnsns.2009.09.042.

[4] Ganesan, K., Guptha, T. K.: Multiple binary images watermarking in spatial and frequency domains. Signal & Image Processing: An International Journal. 1(2), 148-159 (2010).

[5] Ghoshal, N., Mandal J. K.: Discrete fourier transform based multimedia color image authentication for wireless communication. In Proceeding of 2nd IEEE International Conference, WIRELESS VIATE. (2011). doi:10.1109/WIRELESSVITAE.2011.5940849. ISBN: 978-1-4577-0787-2.

[6] Radharani, S., Valarmathi, M. L.: Multiple watermarking scheme for image authentication and copyright protection using wavelet based texture properties and visual cryptography. International Journal of Computer Application (IJCA). 23(3), 29-36 (2012).

[7] Zhang, Li., Yan, X., Li, H., Chen, M.: A dynamic multiple watermarking algorithm based on DWT and HVS. International Journal of Communications, Network & System Sciences. 5, 490-495 (2012). doi:10.4236/ijcns.2012.58059.

[8] Natarajan, N., Govindarajan, Y., Vivek, R.: Comparison of successive and segmented watermarking techniques for color images. In Proceedings of national conference on emerging trends in information & communication technology (NCETICT 2013, Chennai). International Journal of Computer Applications (IJCA). 13-16 (2013).

[9] Mohananthini, N., Yamuna G.: Multiple successive watermarking scheme based on wavelet transform. International Journal of Emerging Trends & Technology in Computer Science. 2(2), 416-420 (2013).

[10] Bhatnagar, G., Wu, Q. M. J.: A new robust and efficient multiple watermarking scheme. Multimedia Tools & Appl.. 74(19), 8421-8444 (2013). doi:10.1007/s11042-013-1681-8.

[11] Inamdar, V., Rege, P. P.: Dual watermarking technique with multiple biometric watermarks. Sadhana, Indian Academy of Sc.(1), 3–26 (2014). doi:10.1007/s12046-013-0208-3.

[12] Natarajan, M., Govindarajan, Y.: Performance comparison of single and multiple water-marking techniques. International Journal of Computer Network and Information Security., 7, 28-34 (2014). doi: 10.5815 / ijcnis.2014. 07. 04.

[13] Babaei, M., Ng, K., Babei, H., Niknajeh, H. G.: Robust multi watermarking scheme for multiple digital input images in DWT domain. International Journal of Computer and Information Technology. 3(4), 834-840 (2014).

[14] Thanki, R. M., Borisagar, K. R.: Compressive sensing based multiple watermarking technique for biometric template protection. International Journal of Image Graphics and Signal Processing. 1, 53-60 (2015). doi: 10.5815/ijigsp.2015.01.07.

[15] Karthik, K., Rangaswamy, M. A. D.: A novel three-tier protection for digital images using blind watermarking scheme. International Journal of Advance Trends in Computer Science and Engineering. 4(1), 15–19 (2015). http://warse.org/pdfs/2015/icacet2015sp03.pdf.

[16] Mohananthini, N., Yamuna, G.: Image fusion process for multiple watermarking schemes against attacks. Journal of Network Communications and Emerging Technologies. 1(2), 1-8 (April, 2015).

[17] Mohananthini, N., Yamuna, G.: A study of DWT-SVD based multiple watermarking scheme for medical images. International Journal of Network Security. 17(5), 558-568 (Sept., 2015).

[18] Mohananthini, N., Yamuna, G.: Comparison of multiple watermarking techniques using genetic algorithms. Journal of Electrical Systems & Information Technology. 3, 68-80 (2016). doi: 10.1016/j.jesit.2015.11.009.

[19] Al-Haj, A., & Farfoura, M.: "Providing Security for E-Government Document Images Using Digital Watermarking in the Frequency Domain", In the Proceedings of 5th International Conference on Information Management (ICIM), IEEE, pp. 77–81, (2019).

[20] Matlab: http://in.mathworks.com/help/images/index.htm (2016).

[21] Chowdhury, S., Mukherjee, R., Ghoshal, N.: Dynamic authentication protocol using multiple signatures. Wireless Personal Communications. 93(3), 1-32 (2017). doi:10.1007/s11277-017-4066-x.

[22] Sadh R., Mishra N., Sharma S.: Dual plane multiple spatial watermarking with self-encryption. Sadhana, Indian Academy of Sciences. 41(1), 1-14 (2016). https://www.ias.ac.in/article/fulltext/sadh/041/01/0001-

0014

[23] Thanki, R. M., Borisagar, K. R.: Combined DCT–CS Theory Based Digital Watermarking Technique for Color Images. In Proceedings of National Conference on Emerging Trends in Information & Communication Technology (NCETICT 2013, Chennai). International Journal of Computer Applications (IJCA). 17-23 (2013).

[24] Matlab:http://codinlab.blogspot.in/2013/10/image-comparison-in-matlab-matrix.html. (2016).

[25] Kumar, C., Singh A.K., Kumar, P., Singh, R., Singh, S.: SPIHT-based multiple image watermarking in NSCT domain. Wiley Online. Special issue paper, 1-9 (2018). DOI: 10.1002/cpe.4912. https://doi.org/10.1002/cpe.4912

[26] Liu, J., Li J., Ma, J., Sadiq, N., Bhatti, U. A., Ai, Y.: A Robust Multi-Watermarking Algorithm for Medical Images Based on DTCWT-DCT and Henon Map. Applied Sciences. 9, 700, 1-23 (2019). doi:10.3390/app9040700.

[27] Chowdhury, S., Mistry, S., Goswami, A., Pal, D., Ghoshal, N.: Multi Data Driven validation of E-Document Using Concern Authentic Multi-Signature Combinations. In Proceedings of International Conference on Frontiers in Computing and Systems. Advances in Intelligent Systems and Computing (COMSYS 2020). vol 1255, 731-743 (2020). Online ISBN:978-981-15-7834-2. Springer, Singapore. Doi: https://doi.org/10.1007/978-981-15-7834-2_68.

[28] Chowdhury, S., Mistry, S., Ghoshal, N.: Multi-Phase digital authentication of e-certificate with secure concealment of multiple secret copyright signatures. Int. J. of Innovative Technology and Exploring Engineering 8(10), 3365–3380 (2019). DOI: 10.35940/ijitee.J1231.0881019.

[29] Alias, N., Ernawan, F.: Multiple watermarking technique using optimal threshold. Indonesian Journal of Electrical Engineering and Computer Science. 18(1), 368-376 (2020). ISSN: 2502-4752, DOI: 10.11591/ijeecs.v18.i1.pp368-376.

[30] Singh, A.K., Thakur, S., Jolfaei, A., Srivastava G.: Joint Encryption and Compression-Based Watermarking Technique for Security of Digital Documents. ACM Transactions on Internet Technology. 2(21), 1-20 (2021). https://doi.org/10.1145/3414474.

Authors

Mr. Saikat Bose is a M.Tech in Computer Science (Embedded System) from MAKAUT in the year 2006. He had worked as Assistant Professor in Techno India for 12 years. Currently he is working as Controller of Examination in Techno Global University, Sironj.

Dr.Tripti Arjariya had done Ph.D (Computer Science) and has a teaching experience of 16 years. She has 8 patent, 59 Research Papers etc. Currently she is working as professor in Bhabha University, Bhopal.

Dr. Anirban Goswami is currently working as Asst. Professor and Asst. Registrar in Techno Main Salt Lake (An Engineering College under Maulana Abul Kalam Azad University of Technology), Kolkata, West Bengal, India. He has more than 22 years of teaching experience. He had contributed in more than 10 graduate level projects and has 15 international conference and 6 international journal publications.

Dr. Soumit Chowdhury is presently working in the position of Assistant Professor of Computer Science & Engineering, in the Govt. College of Engineering & Ceramic Technology, Kolkata, India. He has more than 16 years of teaching experience in different engineering colleges and has published 16 research papers in different National, International Journals as well as Conferences. Dr. Chowdhury has also successfully supervised one UGC funded research project as a Principal Investigator and did his Ph. D. in Engineering from University of Kalyani, West Bengal, India.