

Original Article

Medical Test Image Authentication With Multi-Ownership Certification and Sensitive Test Data Validation

Saikat Bose¹, Tripti Arjariya², Anirban Goswami³

^{1,2}Department of Computer Science Engineering, Bhabha University, Madhya Pradesh, India.

³IT Department, Techno Main Saltlake, West Bengal, India.

¹Correspondin Author : technoglobalregistrar@gmail.com

Received: 28 November 2023

Revised: 01 March 2024

Accepted: 01 April 2024

Published: 24 April 2024

Abstract - The technique of steganography has been widely used for sensitive data protection. The proposed technique is based on the authentication and validation of patient's health records in a digital environment. This helps in correct diagnosis, subsequent treatment and claim medical insurance. Multi-scale validation for digital medical images is combined with trusted ownership claims. The ownership is complied with the patient's fingerprint, private share of the laboratory logo and pathologist's signature. Each of these components is integrated into each of the four segments of the four regions of a medical image. The security of data is ensured through CIA (Confidentiality, Integrity and Authentication) property and non-repudiations. The embedding pattern is confidential through a hash value-based data set. The first hash value specifies the sub-image block interval, and the second hash value determines the circular orientation of embedded image fragments, both on sub-image block elements. Even though the data and one share can be public, but client side will stage-wise validate the medical image utilizing identical hash operations. The test results like PSNR (Peak signal-to-noise ratio) (41.08 dB) on real-time images emphasise superiority over similar existing algorithms. To conclude, the technique proposes superiorly enhanced features like data hiding imperceptibility and robustness with intrinsic encoding strategies as compared to existing approaches from different perspectives.

Keywords - Digital Signature Validation, Multi-Ownership Certification, Medical Image Authentication, Region Wise Multi-Copy Signature Casting, Variable Encoding.

1. Introduction

E-document transmission in public networks, either wired or wireless, has required extensive data validations [1] or proper user authentications from different levels. Effective hiding of copyright signatures within a particular digital document has established authenticity or ownership claims, including sensitive data for trusted validations [2, 3]. In addition, secure encoding of copyright data has mostly prevented unauthorized access and protects them from various image processing attacks. Related to this domain, the proposed concept promotes a unique authentication technique for medical test images alongside validating some real time authentic data as well [4].

The idea is very useful for reliable medical treatments as well as health insurance claim-related issues. Moreover, this also initiates some E-governance-based health treatment in contrast to some of the existing systems by authenticating the source of the medical image, patient identity and test-related sensitive data. This is achieved through the multi-

watermarking concept [5, 6, 7], which disperses multiple signatures on medical images [4], leading to Multi-phase authentications of the medical image from different angles [8-10, 11]. In addition, significant recovery of different signatures under various attacks is also a key concern, especially in a wireless domain where security and loss of signal strength are the main challenges [12, 13].

The multi-ownership certifications are the way to achieve it, and hence, some of its variations are mentioned here. Multi-signature embedding concepts have been broadly classified as: a) Composite - Watermarks treated as a single component and used for hiding. b) Successive - Replacing previous marks by successive watermarks, i.e. one is added after the other, c) Segmented – these are embedded in non-overlapping manners, and the watermarks are completely independent of each other. [14-16, 11] Although successive and composite technique imparts good security [6], but segmented concept yields better robustness and mostly encourages recovery of at least one signature.



So, considering the benefits of segmented data hiding, the proposed protocol conceals copyright signatures or data on each of the four segments of a particular region of the medical image in a non-overlapping manner. Additionally, this data hiding is dynamically implemented for separate clients based on the related test data to portray stronger authentication and data validation scenarios. The objective is here to resist the illegal access of the hidden copyright data and also their recovery under attacks or even loss of signal strengths, especially in [10-11, 17] wireless domain. This proposed protocol further improves multiple digital signature implementations by way of a visual cryptographic or visual secret-sharing approach. Dynamic casting of such copyright signatures or data controlled by the hash values derived from the sensitive test data makes this protocol strongly reliable.

Maintaining the secrecy and accuracy of the patient's Electronic Health Record (EHR), which is currently the most important factor in the healthcare business, was the driving force for framing the proposed technique. Administrative, physical, and technical precautions may be the most crucial security considerations [18–19, 4]. To frame an electronic health record [19], sensitive legal data has been used in the medical diagnostic centre or hospital environment. However, electronic medical records might not be fully trusted by healthcare persons nowadays. So, the concept of data hashing, encryption and hiding are merged together to protect the patient record.

Therefore, taking into account all of these important factors, our algorithm presents a unique solution for the trusted validation of an electronic medical report or a medical test image with the following particular goals:

- To explore the secure preservation of electronic medical reports through concealing signatures, authenticating with hash values, and facilitating multi-phase validation for medical treatment. This ensures legal compliance and upholds data integrity.
- To verify and validate EHR through CIA properties and non-repudiation and to achieve data integrity through test data-driven hash value-based copyright data hiding and non-repudiation property involving visual cryptography and watermarking and biometric fingerprint of the patient.
- To establish superior data hiding imperceptibility and robustness using novel data-hiding techniques, which include embedding copyright image fragments in circular sequences on the host image sub-block pixel bytes and also variable encoding of those copyright data bits on sub-block pixel bytes. Here, variable encoding reflects the combination of spatial and transform modes of data hiding along with variable threshold reference range-based data encoding. Also, the design of a signature share generation algorithm related to visual cryptography presents a new idea while encrypting a signature image.

The proposed concept is organized into different sections. Section 2 discusses some existing algorithms along with enhancements over the existing approaches. Section 3 demonstrates the proposed authentication process and method in different sub-sections, such as the workflow of the protocol in sub-section 3.1, the Algorithm for Signature share generation and decryption in 3.2 and the Algorithm for Secret data embedding and detection in 3.3. Section 4 demonstrates the experimental results of the algorithm, and section 5 mentions about the Analysis of Experimental results and the limitations. Conclusion and future scope are mentioned in section 6, followed by relevant references and an appendix.

2. Literature Review

Since this particular medical image validation scheme is based on copyright signature watermarking and a visual secret-sharing approach along with hash generations on sensitive data, the following section states some of the existing works in these areas. The idea is to focus on the critical issues of this domain for enhancements inducted in this work.

2.1. Existing Approaches in Image Watermarking

For reliable image authentication as well as ownership validation, the combination of visual cryptography and watermarking has been preferred due to the preservation, authentication and non-repudiation of copyright data [20, 13, 21]. Again, various steganography and cryptographic techniques have been reviewed so far [26]. In addition, the embedding of secret copyright data in the transform domain also served as good authentication and in this aspect, a secret signature has been embedded on DWT components [20]. Then, good performance is shown by encoding the secret data on LL2 sub-bands of Discrete Wavelet Transform (DWT) components [14]. Further, exclusive value is used for DCT-based multiple signature bit embedding [15], while multi-watermarking is adopted in Discrete Cosine Transform-Comprehensive Sensing (DCT-CS) theory [22]. Both visible and invisible watermarks are used for ownership verifications as well as tamper detections, while secret watermark data are cast on DWT components [16]. Also, multi-signature bit concealment is done in DWT coefficients for better robustness [23, 24]. Then, to establish proper protection against attacks, some sub-band coefficients of DWT are utilized for multi-watermark bit embedding [8] and after that three-tier blind multi-watermarking scheme is proposed [9] for better robustness of those watermarks.

Apart from these stated works, multi-watermarking concepts also proved useful for authenticating medical images. In this aspect, multi-watermark hiding on medical images is accomplished by utilizing specific multi-resolution components [10]. An extension of this work reflects the embedding of three different watermarks in RGB planes [17]. Further as advance, multi-watermark concealment on DWT components using a genetic algorithm is also incorporated for

effective hiding of watermarks [11]. In recent trends in medical image authentications, pre-processing of the watermarks with chaotic encryption technology for better watermark security using watermark casting is done with dual-tree complex wavelet transform (DTCWT) and DCT [4]. Additional works in this area have shown e-document validation by casting multi-signatures in the frequency domain [25], while visual cryptography is combined with the multi-watermarking concept in the frequency domain for validation of the e-document [13]. This particular work actually has presented a data security protocol and adopts variable encoding for embedding multiple signature data. Also, the focus is on multi-signature hiding with authentic hash values and addressing critical data security issues for e-document validations. In addition to this, validation of e-document images is demonstrated by combining signature sharing, i.e. visual cryptographic concept and data hiding approach. The idea has validated multiple copyright signatures of respective parties detected from the e-document based on sensitive data.

Using dual color images, digitized data validation with improved robustness and error correction facility is also proposed. Further improvement has protected a digitized document by ensuring the security features of Confidentiality, Integrity, Authenticity and Non-repudiation using Chaotic Visual cryptography based visual authentication. A Novel Approach to the Information Hiding Technique is stated using the ASCII Mapping Based Image Steganography technique [31]. Also, it is seen that an improvement is done with an enhancement in Data Hiding Capacity in Code Based Steganography using Multiple Embedding [32]. In a paper, an encrypted coverless information hiding method is framed that transfers secret images between two different image domains using generative models [33]. A piece of work has shown a new data-hiding approach for image steganography based on human visual properties using adaptive LSB [34]. In another research work, a modified LSB technique is capable of protecting and hiding medical data to solve the crucial authentication issue [35]. In a paper, a secure data-hiding method is conveyed using a hyper-chaotic map and the left-most embedding strategy [36]. The proposed methods have been hybrid, with the DCT frequency domain and encrypted domain together. A high-capacity reversible data-hiding technique is proposed to embed patient data using a new weighted interpolation technique [37]. Generally, steganography will be used to embed the patient's personal information securely in their medical images to enhance confidentiality in case of a distant diagnosis [38]. The security of the medical data has improved to maintain confidentiality and integrity using IoT which is the further advancement in this field. From the above facts, it is evident that the protection of copyright data requires extensive use of transform domain, steganography and visual cryptography. Strong data security protocol to address critical data security issues requires reliable authentications or validations of the e-

documents. Thus, keeping in line, the proposed algorithm highlights appropriate techniques for trusted validation of the medical test image with some major enhancements, as discussed in the subsequent sections.

2.2. Enhancement Over Existing Approaches

The proposed concept focuses on a novel data authentication scenario for trusted validation of medical test images, leading to reliable medical treatment and smooth processing of the health insurance claims for the patient party. The idea is based on a unique data security approach to achieve reliable authentications for each of the associated parties. While framing the protocol, multi-factor authentication is adopted with secure hash functions, signature share generations and data hiding approach. This will help to handle possible frauds, and for that purpose, some major enhancements have been incorporated over the existing concepts. These unique advancements are implemented to meet the gap between the existing approaches and they are illustrated as follows. First to confirm validation of the medical image from both the patient party and diagnostic center. This was mainly achieved with secret casting of medical test related critical findings, patient fingerprint and digital signature of the diagnostic authority within the host medical test image. Since this secret embedding was governed by self-defined hash values compared to [30] as derived from sensitive data, the data integrity issue was also addressed. In this context, two hash values were utilized for the secret data hiding method; one tracked the rotation casting sequence of fragmented signature and the other identified the host image subblock interval for signature datacasting. Hence, this proposed idea strongly complies with CIA and non-repudiation properties, which were rarely focused collectively in any of the existing techniques [31], [32], [33], [34], [35], [36]. Here again, two private shares are used in comparison with previous study of this work to add a multi-layer of security. Secondly, robust data hiding was achieved whenever fragmented signature images were embedded in circular patterns in the host image sub-block pixel byte elements (shown in Figure 1). This practice imparted strong security and authenticity for the hidden signature images in contrast to the current ideas. This was mainly because of the fact that any sensitive tampering or supply of wrong test data would derive the wrong hash value and, hence, wrong signature embedding or extraction. Thirdly, some advanced data-hiding policies were adopted in the presented work to upgrade the security and authenticity of the hidden signatures even more. The use of both spatial and transform-based data hiding patterns in different pixel bytes of a sub-block matrix escalated the security and robustness further. In addition, threshold-referenced point-based data encoding derived from variable and dynamic border ranges for different pixel bytes enhances the robustness a great deal as compared to the existing approaches. Finally, in host image region-wise, multi-copy signature casting, as shown in Figure 2, vastly improved the recovery chances of such signatures under attacks.

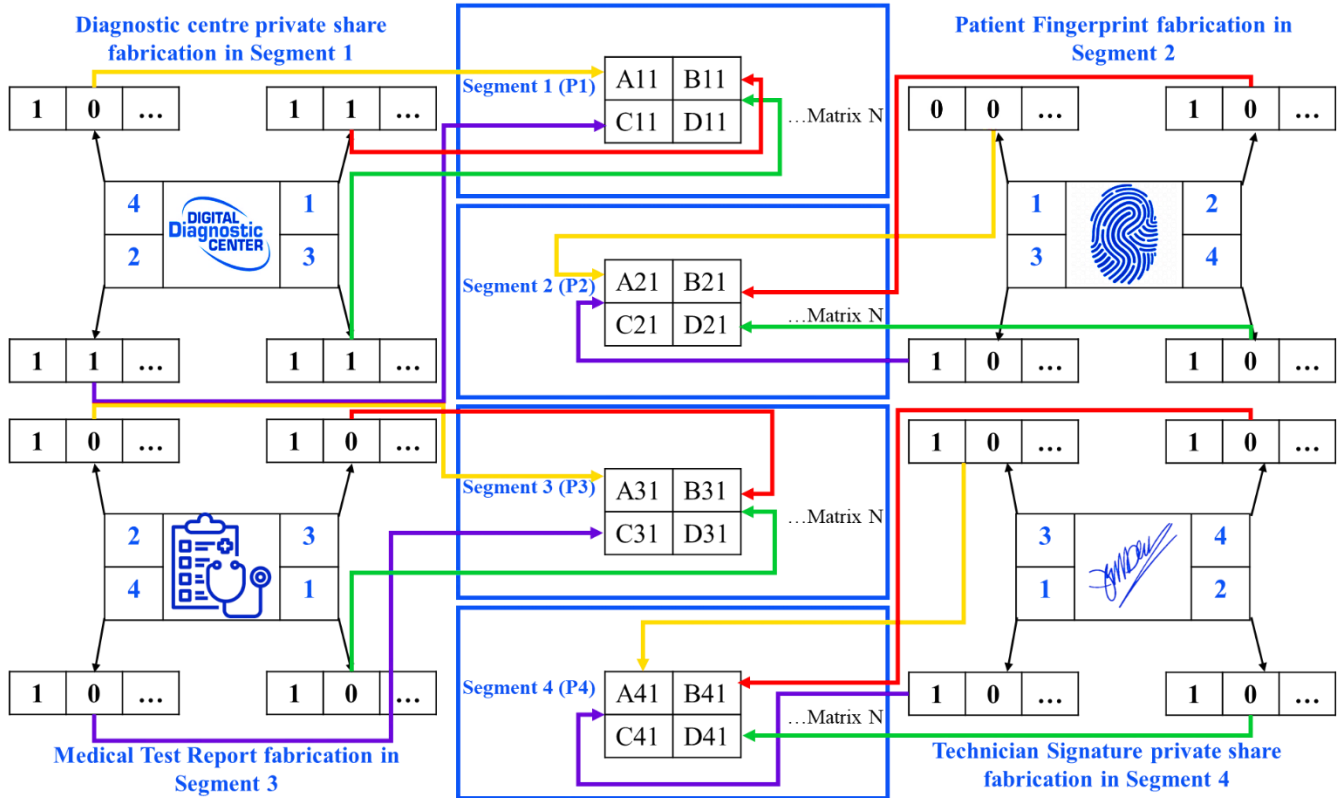
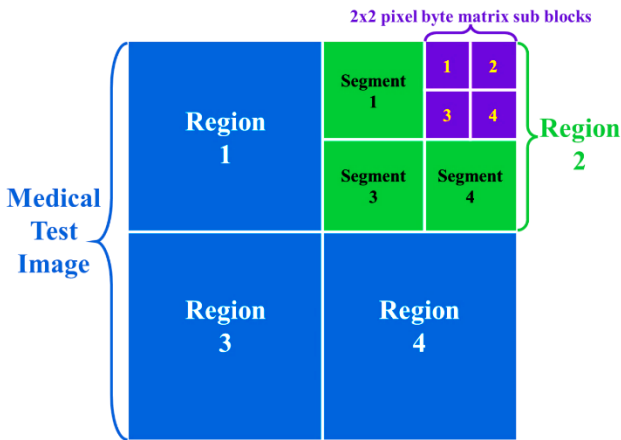


Fig. 1 Embedding within the segmented cover image



Medical test image logically divided into 4 regions and each region is further divided into 4 segments having consecutive set of 2x2 pixel byte matrix sub blocks

Fig. 2 Partitioned cover image

Apart from framing a robust data-hiding algorithm, the proposed work also displayed an exhaustive robustness analysis under attacks for the regenerated share merged signatures. Importantly, this kind of robustness evaluation for the share merged signatures is very rare in existing methods and, in turn, justifies the strength of the proposed algorithm. Hence, this proposed work not only presented a reliable protocol for validation of the medical test image from different angles by addressing all the critical data security issues, but it also enhanced the existing data hiding practices.

This justifies the suitability of the proposed method for wireless domain applications as well.

3. Method

3.1. Workflow of the Protocol for Authentication of Medical Image

The patient visited the diagnostic center to take Imaging tests (Radiology) like X-ray/ MRI/ CT-Scan, etc. The acquired patient's fingerprint was saved for further use. The test report in words and image format was considered. Reliable validation of the image was done by secret embedding of the copyright signatures and authentic data within its non-overlapping portions. The image is first divided into four equal regions, and after that, each region is subdivided into four segments (Figure 2).

Now, to ensure CIA and non-repudiation factors, different forms of digital signatures and authentic, sensitive data were secretly fabricated in each of the four segments belonging to each of the four regions, respectively. The idea also employed a sensitive signature data-sharing concept as a part of visual cryptography for promoting strong ownership claims and digital signature implementations. The workflow of the protocol is mentioned as follows-

Step 1: From the copyright logo of the diagnostic laboratory, two shares (private and public) were generated. The public share was kept open for all. The casting of private

share was done in the first segment of each region of the image used as the cover. Two hash values, $H1_{\#1}$ and $H1_{\#2}$, were computed from the 4-digit Registration Number (RN) of the patient and the 4-digit Branch Code (BC) of the diagnostic center, as shown in Equation 1 and Equation 2.

$$H1_{\#1} = [\sum(RN + BC) + \sum(\text{Digits of RN}) + \sum(\text{Digits of BC})] \text{Mod } 4 + 1 \quad (1)$$

$$H1_{\#2} = [|(RN - BC)| + |(\text{rev}(RN) - \text{rev}(BC))|] \text{Mod } 4 \quad (2)$$

Here, $H1_{\#1}$ represents the interval of matrices chosen for embedding, and $H1_{\#2}$ denotes the starting sequence number of the fragmented private share with circular numerical movement.

Step 2: When a patient approaches the diagnostic center for the tests, he/she has to fill up all the personal details. The centre captured the fingerprint of the patient and generated a patient id as the key attribute. A record was maintained for the patient with the patient's id along with other personal details and a captured fingerprint image. Depending on the tests to be taken by the patient, digital reports were prepared with a report reference number. To ratify that a particular patient had actually gone through the specific test and not anyone else, the 2nd segment of every region of the test image was secretly fabricated with the patient's fingerprint image. This embedding was also achieved with two hash values, $H2_{\#1}$ and $H2_{\#2}$ (similar to the working of $H1_{\#1}$ and $H1_{\#2}$), and they were generated with a 10-digit patient id (P_{id}) and a 10-digit patient contact number (C_{no}). The hash values were mathematically computed as in Equation 3 and Equation 4.

$$H2_{\#1} = [\sum(P_{id} + C_{no}) + \sum(\text{Digits of } P_{id}) + \sum(\text{Digits of } C_{no})] \text{Mod } 4 + 1 \quad (3)$$

$$H2_{\#2} = [|(P_{id} - C_{no})| + |(\text{rev}(P_{id}) - \text{rev}(C_{no}))|] \text{Mod } 4 \quad (4)$$

Step 3: Sometimes, in medical science, it was observed that the hard copy version of the medical report had been tampered with for ill-usage. To resist any tampering, the digital copy of the medical report was casted in the 3rd segment of every region of the test image. It could only be deciphered by an intended person. The embedding was achieved with the help of two hash values, $H3_{\#1}$ and $H3_{\#2}$, respectively (similar to the working of $H1_{\#1}$ and $H1_{\#2}$). The hash values were computed on an 8-digit report reference number (R_{rn}), 8-digit date of the test (Dot) and 10-digit patient id (P_{id}) and the mathematical representations are shown in Equation 5 and Equation 6.

$$H3_{\#1} = [\sum(R_{rn} + D_{ot}) + \sum(\text{Digits of } P_{id}) + \sum(\text{Digits of } C_{no}) + \sum(\text{Digits of } P_{id})] \text{Mod } 4 + 1 \quad (5)$$

$$H3_{\#2} = [|(R_{rn} - D_{ot})| + |(\text{rev}(R_{rn}) - \text{rev}(D_{ot}))| + \text{rev}(P_{id})] \text{Mod } 4 \quad (6)$$

Step 4: The fourth segment of each region of the test image was used to prove that the test had actually been done under the supervision of a specific pathologist. A digitized signature of the attending pathologist was taken, and two shares were generated from it. The private share was embedded, while the public share was open to all concerned. This embedding was achieved with the hash values $H4_{\#1}$ and $H4_{\#2}$ respectively (similar to the working of $H1_{\#1}$ and $H1_{\#2}$). Vitialy, these hash values were derived from the 4-digit pathologist's registration number (D_n) and its 4-digit year of registration (Y_n) by using Equation 7 and Equation 8:

$$H4_{\#1} = [[\sum(D_n + Y_n) + \sum(\text{Digits of } D_n) + \sum(\text{Digits of } Y_n)] \text{Mod } 4 + 1 \quad (7)$$

$$H4_{\#2} = [|(D_n - Y_n)| + |(\text{rev}(D_n) - \text{rev}(Y_n))|] \text{Mod } 4 \quad (8)$$

Step 5: Now, this authenticated medical test image was handed over to the patient party for diagnosis of the disease.

Step 6: On receiving the medical test image from an attending doctor, the respective signatures or authentic data were sensed from the corresponding regions of the medical test image. Hence, the validation of the medical test was done from all aspects and the digital report was supposed to be authentic for the correct diagnosis of the patient. The pictorial representation of the whole process is shown in Figure 3.

3.2. Algorithm for Signature Share Generation and their Decryption

Two intensity values were considered from every pixel intensity at positions $P_s \in \{1, 2, \dots, N\}$. Let R_p , G_p and B_p denote the pixel intensity at position 'P' for the three planes, respectively. Critically, the pixel intensities were computed based on threshold values V_r , V_g and V_b , respectively.

Vitialy, in our algorithm, we chose the threshold sets as $\{123, 56, 58\}$, $\{45, 118, 49\}$, $\{48, 49, 123\}$ and $\{127, 123, 125\}$, respectively. The two intensity values at position P_s where s lies in the range $(1 .. n)$ were generated from two sets (P_r, P_g, P_b) and (Q_r, Q_g, Q_b) , which hold the intermediate values. The index values at 'P' for secret (S_i) and private (P_i) share were $S_i \equiv \{V_1[p]_r, V_1[p]_g, V_1[p]_b\}$ and $P_i \equiv \{V_2[p]_r, V_2[p]_g, V_2[p]_b\}$ respectively. This change in values was based on three planes, R, G, B, at location 'p'. On receiving, the original set was recovered when the user merges the altered values of the two sets $\{V_1[p]_i\}$ and $\{V_2[p]_i\}$, where $i \in \{r, g, b\}$. In the broader perspective, the above process could be repeated for both shares to reform the original signature. The concept is detailed as follows:

3.2.1. Algorithmic Representation of Share Generation

```
For i = 1 .. n
do
```

$$\begin{aligned}
 P_r &\leftarrow R_i \bmod 8 + (P) \bmod 10 + V_r; \\
 P_g &\leftarrow G_i \bmod 9 + (P) \bmod 12 + V_g; \\
 P_b &\leftarrow B_i \bmod 11 + (P) \bmod 14 + V_b; \\
 Q_r &\leftarrow R_i - P_r; \\
 Q_g &\leftarrow G_i - P_g; \\
 Q_b &\leftarrow B_i - P_b;
 \end{aligned}$$

$i \leftarrow i+1;$

End Loop

$$(Q_r < 0) ? [V_1[p]_r \leftarrow R_i, V_2[p]_r \leftarrow 0] : [V_1[p]_r \leftarrow P_r, V_2[p]_r \leftarrow [Q_r]$$

$$(Q_g < 0) ? [V_1[p]_g \leftarrow G_i, V_2[p]_g \leftarrow 0] : [V_1[p]_g \leftarrow P_g, V_2[p]_g \leftarrow [Q_g]$$

$$(Q_b < 0) ? [V_1[p]_b \leftarrow B_i, V_2[p]_b \leftarrow 0] : [V_1[p]_b \leftarrow P_b, V_2[p]_b \leftarrow [Q_b]$$

$i \leftarrow i+1;$

End Loop

3.2.2. Algorithmic representation of share recovery

For $i = 1 \dots n$

do

$$\begin{aligned}
 R[i] &\leftarrow V_1[i]_r + V_2[i]_r; \\
 G[i] &\leftarrow V_1[i]_g + V_2[i]_g; \\
 B[i] &\leftarrow V_1[i]_b + V_2[i]_b;
 \end{aligned}$$

3.3 Algorithm for Secret Data Embedding and Detection

The MRI image of a patient was subdivided into four sections and further into 16 equal segments. Each of the segments was represented as 2x2 non-overlapping blocks. In between 1 to 4, and b_n represents the matrix number from 1 to N. The forward and reverse transformation is represented in Equation 9, Equation 10 and Equation 11 each of these 2x2 blocks, 1st, 2nd and 4th pixels were frequency transformed and the 3rd pixel was retained spatial. One bit was cast directly in the 3rd pixel, and the other three bits were casted only in the positive part of 1st, 2nd & 4th transformed pixels.

Then, 1st, 2nd and 4th elements were reverse transformed to yield an authenticated bit. The sensitive bits were extracted correctly from the transformed pixels at the 1st, 2nd and 4th positions and also from the 3rd position by the receiver. The retrieved bits were then arranged accordingly to regenerate a fragment of the signature, and similar such fragments were later combined for the full signature generation.

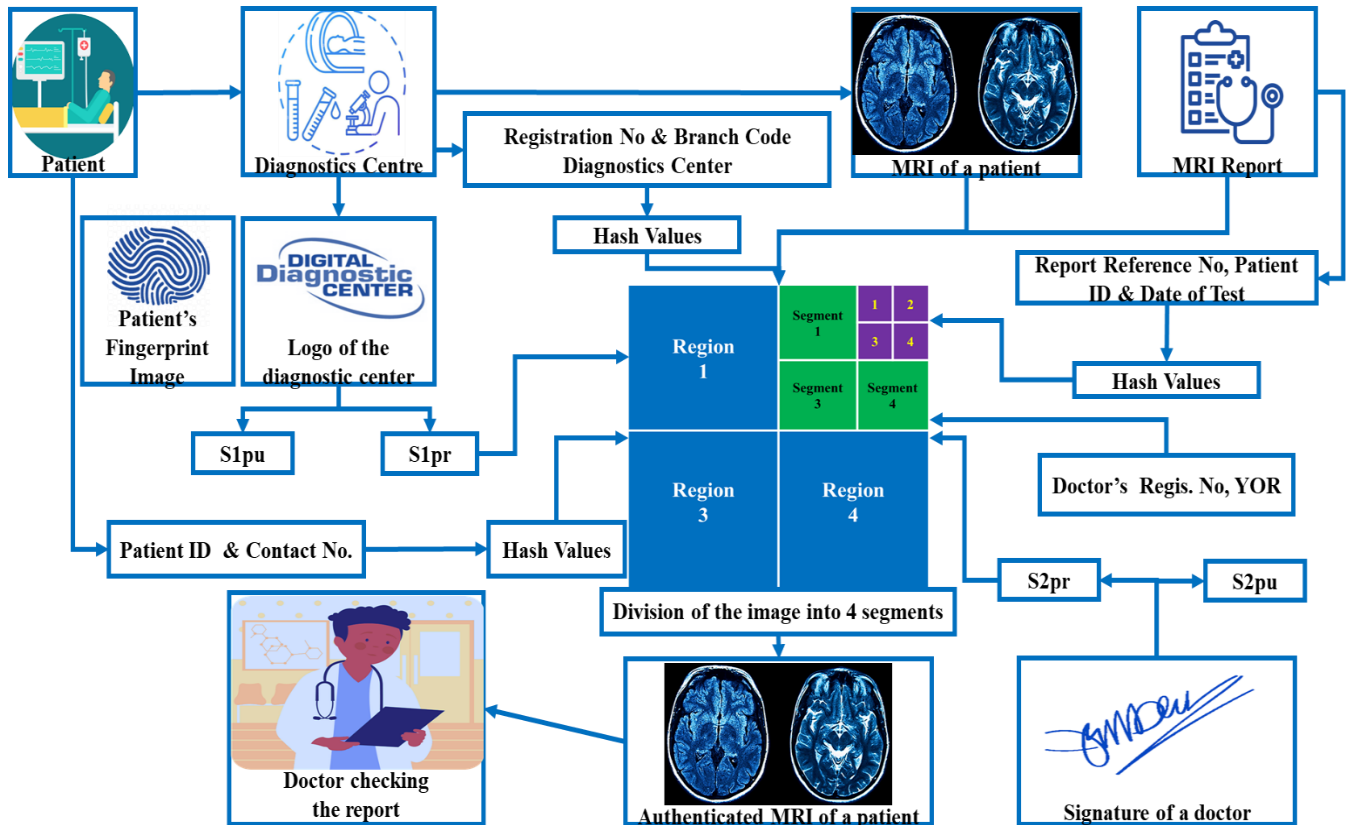


Fig. 3 The workflow of the Digital Medical Test document authentication process

3.3.1. Transformation of Block Matrix

Let the submatrix of an image be $I_{bn} = [M_i]$, where the range is from 0 to 255, i is the index, I_{bn} can be any value

Initial Matrix: $I_{bn} = \begin{bmatrix} x & y \\ z & w \end{bmatrix}$ (9)

$$I_{bn}^{//} \text{ (forward)} = \begin{bmatrix} X_1 = \frac{x+y}{2} & X_2 = z - w \\ X_3 = \frac{x-y}{2} & X_4 = w \end{bmatrix}$$
 (10)

$$I_{bn}^{///} \text{ (reverse)} = \begin{bmatrix} x' = X_1 + X_3 & y' = X_2 + X_4 \\ z' = X_1 - X_3 & w' = X_4 \end{bmatrix}$$
 (11)

X_i represents the elements at positions 1, 2, 3 and 4. The encoding is transformed components is elaborated as

$$I_{bn} = \begin{bmatrix} x & y \\ z & w \end{bmatrix}$$

Forward Transform

$$I_{bn}' = \begin{bmatrix} X_1 = \frac{x+y}{2} & X_2 = z - w \\ X_3 = \frac{x-y}{2} & X_4 = w \end{bmatrix}$$

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

Now, bit insertion in the resulting sub-matrix B_i' ,

$$I_{bn}^{//} = \begin{bmatrix} X_1' = (A_1 \pm \alpha_1) + \frac{r}{2} & X_2' = \pm(A_2 \pm \alpha_2) \\ X_3' = \pm((A_3 \pm \alpha_3) + \frac{r}{2}) & X_4' = (A_4 \pm \alpha_4) \end{bmatrix}$$

where, $r \in \{0, 1\}$

3.3.2. Algorithm for Bit Embedding

Input Medical test images and four types of sensitive authentic data.

Output: Authenticated medical test image.

Method: In each segment, I_{bn} was frequency transformed. One bit was casted either in the (+) ve integer part (X_i) of the transformed coefficient of I_{bn} or directly casted in the spatial value. The bit-encoded matrix $I_{bn}^{//}$ was backwards transformed to generate $I_{bn}^{///}$. The choice of matrix for embedding was 'alt', and the signature bit hiding procedure in I_{bn} is represented algorithmically as:

$$I_{bn}^{//} = \begin{bmatrix} X_1' = (C_1) + \frac{r}{2} & X_2' = \pm(C_2) \\ X_3' = \pm((C_3) + \frac{r}{2}) & X_4' = (C_4) \end{bmatrix}$$

where $C_i = (A_i \pm \alpha_i)$, where i ranges from 1 to 4.

Reverse Transformation

$$I_{bn}^{///} = \begin{bmatrix} X_1^{//} = A_1' + A_3' & X_2^{//} = A_2' + A_4' \\ X_3^{//} = A_1' - A_3' & X_4^{//} = A_4' \end{bmatrix}$$
 (12)

Single bit insertion is done only in the positive part, and the embedded matrix $I_{bn}^{//}$ is reverse transformed to produce the matrix $I_{bn}^{///}$ as shown in Equation 12. Similarly, at the

receiver end, frequency transformation is applied to the $I_{bn}^{///}$ matrix to produce the transformed matrix $I_{bn}^{//}$. The embedded bits are detected properly from the original document.

$CV_i \leftarrow F_1(X_i, B_i)$:

Start

$(B_i = 0) ? ((X_i \text{ Mod } 2) = 0) ? CV_i \leftarrow -X_i : CV_i \leftarrow (X_i - (X_i \text{ Mod } 2)) ;$

$(B_i = 1) ? ((X_i \text{ Mod } 2) = 0) ? CV_i \leftarrow (X_i + 1) : CV_i \leftarrow X_i ;$

Return CV_i ;

End

$Mid_i \leftarrow F_2(X_i, P)$;

Start

$((X_i \text{ Mod } p) = 0) ? Low \leftarrow -X_i : Low \leftarrow (X_i - (X_i \text{ Mod } p)) ;$

$Up \leftarrow -Low + p ;$

$(Up > 256) ? Mid_i \leftarrow 254 :$

$Mid_i \leftarrow (Low + Up) / 2 ;$ Return Mid_i ;

End

(13)

Both $F_1(X_i, B_i)$ and $F_2(X_i, P)$ are utilised to code $B_i \in \{0, 1\}$ from the positive part of X_i , $i \in \{1..4\}$. 'F1' directly returns $CV_i \in \{0, \pm 1, \dots, \pm 255\}$, whereas 'F2' returns the positive threshold reference point $Mid_i \in \{0, 1, \dots, 255\}$. The threshold based bit coding is executed using Mid_i with suitable signs. The stepwise mechanism for casting of bit is given.

Step 1: Forward frequency transform was applied to I_{bn} to obtain I_{bn}' .

Step 2: Only the positive integer portion (X_i) was considered from each of I_{bn}' and also from the spatial value.

Step 3: A combination of four bits represented as B_i was taken.

Step 4: A particular bit out of the set (B_i) was casted specifically in X_i value to generate CV_i , mathematically expressed as in Equation 14:

- 1) $Mid_1 \leftarrow F_2(X_1, 8)$;
 $(B_1 = 1) ? CV_1 \leftarrow Mid_1 + 1$;
 $CV_1 \leftarrow Mid_1 - 1$;
- 2) $Mid_2 \leftarrow F_2(X_2, 4)$;
 $(B_2 = 1) ? CV_2 \leftarrow Mid_2 + 1$;
 $CV_2 \leftarrow Mid_2 - 1$;
- 3) $Mid_3 \leftarrow F_2(X_3, 6)$;
 $(B_3 = 1) ? CV_3 \leftarrow Mid_3 + 1$;
 $CV_3 \leftarrow Mid_3 - 1$;
- 4) $CV_4 \leftarrow F_1(X_4, B_4)$; (14)

Step 5: Further, the three elements of $I_{bn}^{//}$ were backwards transformed except the 4th element to obtain the final matrix $I_{bn}^{///}$.

Step 6: If required, some clinical modifications were performed on specific elements of I_{bn} to keep the elements of $I_{bn}^{///}$ in the correct spatial domain.

Step 7: $B_{In} \leftarrow B_{In} + \text{alt}$;

3.3.3. Algorithm for Bit Extraction

Input: Authenticated medical image.

Output: Four sensitive authentic data.

Method: With respect to all the portions, the matrix $I_{bn}^{///}$ was again frequency-transformed to generate $J_{bn}^{//}$. One bit, i.e. B_i , was traced from the integer part of the coded component, i.e. CV_i of each of $J_{bn}^{//}$ or from the spatial value with i varying between 1 to 4. Further, such extracted bits were grouped in appropriate sequences to regenerate the original image. Choosing the matrices in the manner defined by ‘alt’, the extraction algorithm is stepwise elaborated as:

Step 1: Forward frequency transform was applied on received matrices $I_{bn}^{///}$ to obtain the matrices $J_{bn}^{//}$.

Step 2: Only the positive integer portion (X_i) was considered from each of $J_{bn}^{//}$ and also from the spatial value.

Step 3: Each of the encoded bits was detected from $J_{bn}^{//}$. The formula for the same is shown in Equation 15:

$$\begin{aligned}
 \text{Mid}_1 &\leftarrow F2(CV_1, 8); \\
 (C_1 >= \text{Mid}_1) &? B_1 \leftarrow 1 : B_1 \leftarrow 0; \\
 \text{Mid}_2 &\leftarrow F2(CV_2, 4); \\
 (C_2 >= \text{Mid}_2) &? B_2 \leftarrow 1 : B_2 \leftarrow 0; \\
 \text{Mid}_3 &\leftarrow F2(CV_3, 6); \\
 (C_3 >= \text{Mid}_3) &? B_3 \leftarrow 1 : B_3 \leftarrow 0; \\
 ((C_4 \text{ Mod } 2) = 0) &? B_4 \leftarrow 1 : B_4 \leftarrow 0; \quad (15)
 \end{aligned}$$

Step 4: The detected bits formed the matrix elements in the appropriate format. The matrices were placed in exact orders to reframe the required image.

Step 5: $B_{in} \leftarrow B_{in} + \text{alt}$;

4. Result

4.1. Imperceptibility Aspect of Data Hiding

Extensive testing of the algorithm has been performed with color images (size: 512x512) taken as a cover and the data images (size: 32x32 or 64x64) taken as payload. Only PPM format images had been considered and the casting and detection algorithm had been under LINUX environment. The results were simulated in context to image parameters in MATLAB environment (R2018a) [39, 40]. The viability of the algorithm had been rigorously tested with standard image quality parameters like Peak Signal to Noise Ratio (PSNR), Structural Similarity Index Measurement (SSIM) and Correlation Coefficient (CC) [30].

Figure 4 portrays the visual qualities of the original and authenticated digital images with acceptable levels of PSNR, SIM and CC values. From Figure 4, it is evident that the authenticated images are almost free from any statistical and even visual attacks but not at the helm of degrading image quality. The images from MRI, Endoscopy and X-Ray were taken as the Cover image. Then, comparisons were given based on the Watermarked image created with the values of key parameters like PSNR, CC and SSIM. The PSNR value for the X-ray authenticated image was 42.1631, which was the maximum and minimum SSIM for Endoscopy, which was 0.8121.

Figure 5 reflects signatures and corresponding shares used for embedding. In this figure, the copyright logo of the diagnostic centre, Fingerprint of the patient, Digital medical report and Private share of the doctor’s digitized signature are shown, which were considered for fabrication.


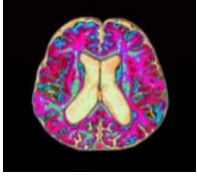
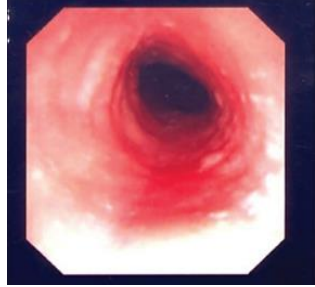
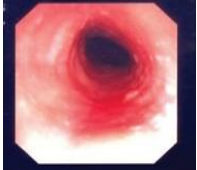
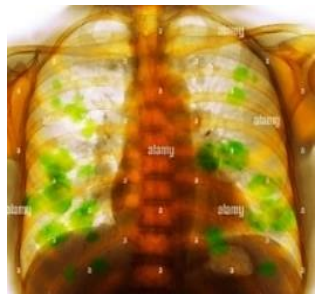
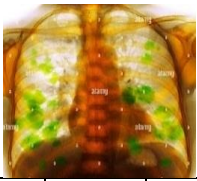
Cover Image	Authenticated Image		
 <p>MRI</p>			
	PSNR	NCC	SSIM
	41.7603	0.9995	0.9926
 <p>Endoscopy</p>			
	PSNR	NCC	SSIM
	38.4965	0.9997	0.8121
 <p>X-Ray</p>			
	PSNR	NCC	SSIM
	42.1631	0.9999	0.997

Fig. 4 Original and watermarked image with equivalent parameter values

			
Copyright Logo of the Diagnostic Centre	Fingerprint of the patient	Digital Medical Report	Private Share of Doctor's Digitized Signature

Fig. 5 Signature images considered for fabrication

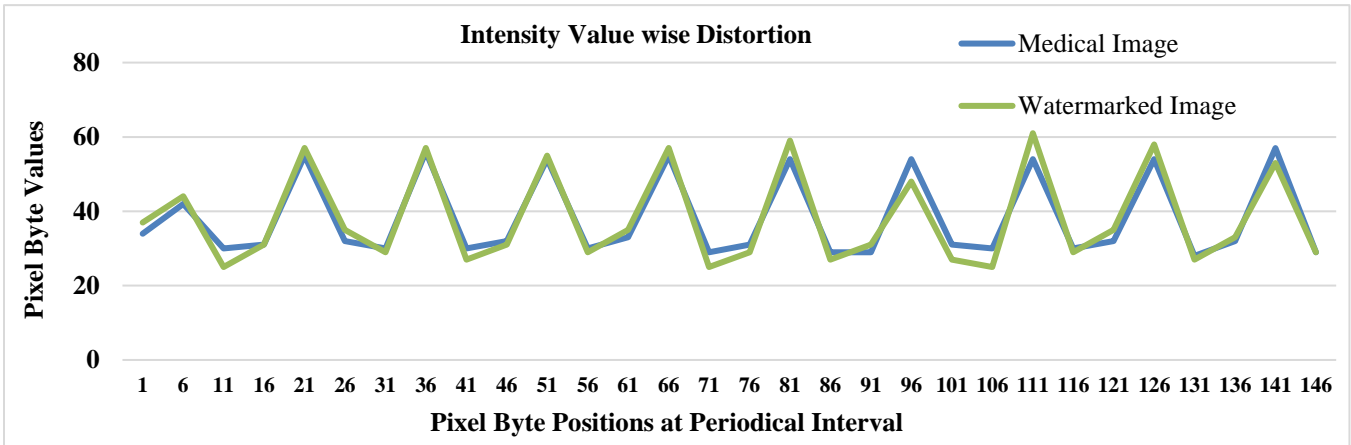


Fig. 6 Change in pixel values of the original and authenticated image

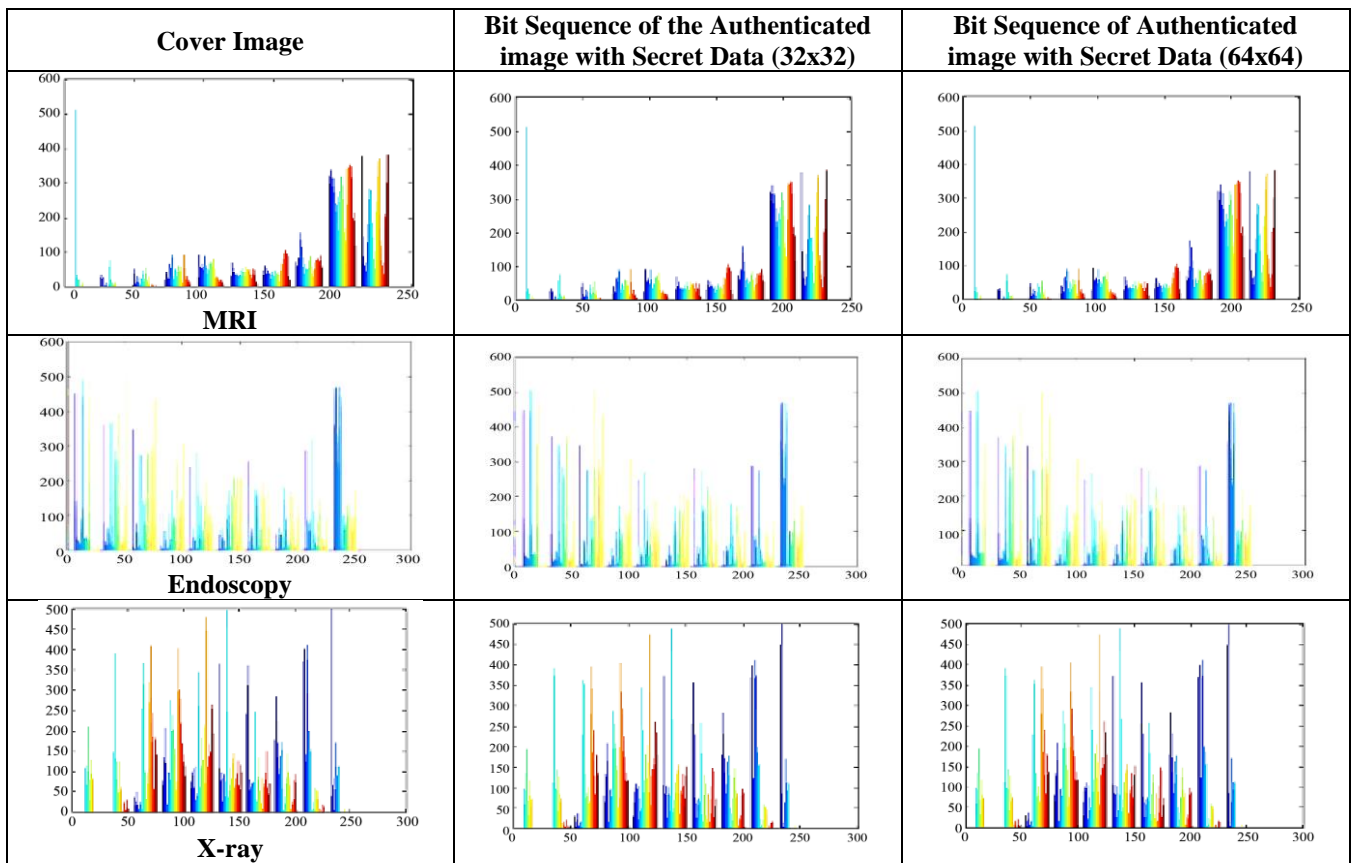


Fig. 7 Histogram analysis for cover and authenticated image

Apart from these methods, the generated noise due to the fabrication of sensitive data is represented through a pixel deviation graph, as shown in Figure 6. In addition to the image quality metrics, a histogram analysis is shown in Figure 7 to justify data imperceptibility. A graphical interpretation has been given with Pixel Byte Positions at Periodical Interval in the X-axis and Pixel Byte Values in the Y-axis. According to histogram analysis, it can be inferred that the proposed algorithm could mostly resist visual or statistical attacks. The reason was that if the maximum deviation of any pixel byte was within the range $\pm (4 - 6)$, the

distortion was quite acceptable in transform domain data hiding practice. Here three different Cover images are given from MRI, Endoscopy and X-ray. In the figure two types of Bit sequence of Authenticated image with Secret Data of 32x32 and 64x64 and their change in pixel value are observed. Critically, the line graph of the authenticated images shows negligible distortion in comparison to the original images measured at periodic intervals. The graphical analysis seemed almost similar in the case of MRI and Endoscopy images, whereas an X-ray image had a very slight variation.

Table 1. Data hiding imperceptibility comparison over existing approaches w.r.t PSNR and SSIM

Existing algorithms	Technique Of data hiding	Type of data	No. of embedded copies	Pay load capacity	PSNR (db)	SSIM
Nasir et al.[2], 2010	Segmented	Binary	04	4,096 bits	39.0627 (max)	
Behnia et al.[3], 2010	Segmented	Grey scale	03	6,144 bytes	30.11	
Babaei et al.[24], 2014	Segmented	Binary	04	4,096 bits	28.44 (max.)	
Bhatnagar et al.[15], 2015	Segmented	Grey scale	09	5,120 bytes	33.8506 (max.)	
Thanki et al. [8], 2015	Successive	Grey scale	02	320 bytes	30.79	
Karthik et al. [9], 2015	Composite	Binary	03	3,072 bits	40.76	
Mohantini et al. [11], 2016	Segmented	Color	02	13,824 bytes	38.0639 (max.)	
Sadh et al.[29], 2016	Segmented	Binary	08	8, 192 bits	38.9060	
Chowdhury et al.[13], 2017	Segmented	Color	04	12,288 bytes	40.4091 (max.)	
Kumar et al.[28], 2018	Segmented	Binary	02	10, 240 bytes	40.97 (max.)	0.9994 (max.)
Previous study of this, 2019	Segmented	Color	16	30,000 bytes	39.0547 (avg.)	
Chowdhury et al.[30], 2020	Segmented	Color	08	13,824 bytes	38.75 (avg.)	
Alias et al.[27], 2020	Segmented	Binary	02	Not Reported	Not Reported	0.9157 (avg.)
Proposed work	Segmented	Color	16	49,762 bytes	41.088 (avg.)	0.9899 (avg.)

The comparison of imperceptibility in data hiding had been done with some existing concepts. A profound enhancement from a different perspective was noticed for our algorithm with a high payload. Table 1 shows a 2-3 times increased volume of payload embedding with escalated PSNR for both cover and authentic images. It also shows that the proposed technique is secure and outperforms almost all

the existing techniques in terms of PSNR. Compared to other techniques having almost similar payloads, the proposed technique performed better than the existing techniques with enhanced payloads. In Figure 8, the PSNR of different existing methods and the proposed algorithm are plotted, and the PSNR of the proposed technique is quite convincing.

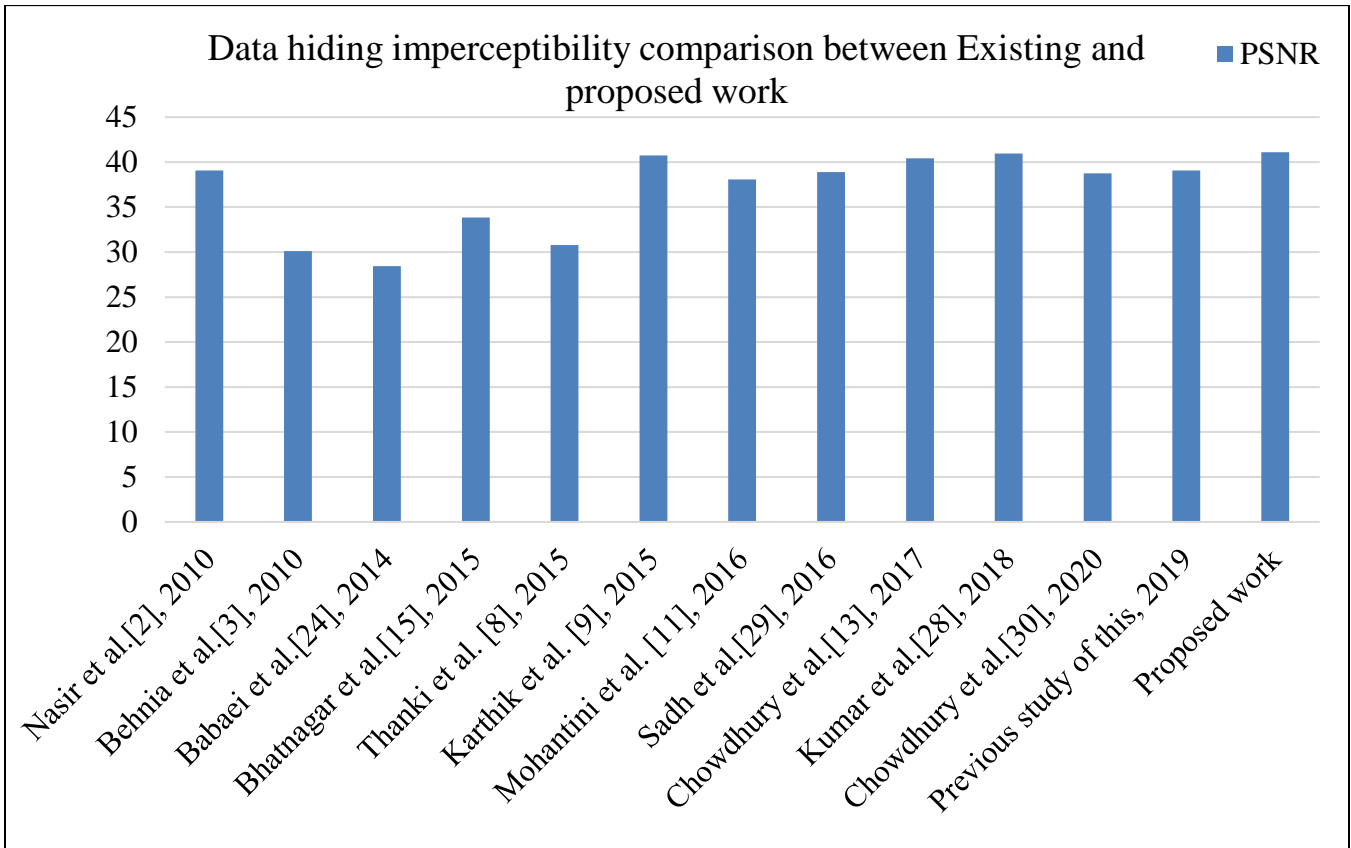


Fig. 8 Data hiding imperceptibility comparison over existing approaches w.r.t PSNR

Table 2. Quality of four best extracted hidden data copies in terms of their CC values under various attacks

ATTACKS APPLIED WITH THEIR RESPECTIVE PARAMETERS	EACH OF THE BEST RECOVERED IMAGE DATA COPY CC VALUE			
	Sensed data-1	Sensed data-2	Sensed data-3	Sensed data-4
File size reduction (Q=98% for JPEG 2000)	0.8762	0.8578	0.8812	0.7401
Flip Vertically at 180 ⁰ and back to the original form	0.9901	0.9910	0.9998	0.9931
Flip horizontally at 180 ⁰ and back to the original form	0.9932	0.9982	0.9930	0.9901
Blur attack (Max Delta – 2, Radius – 5)	0.9235	0.9066	0.9176	0.9071
Gaussian Filtering (Sigma–0.9 & block size- 3*3)	0.8098	0.7610	0.8341	0.7991
Gamma value alteration (1.15)	0.7890	0.8100	0.8271	0.7422
Circular Averaging Attack (radius 0.5)	0.9154	0.9345	0.8587	0.8401
Noise HSV (Hue–4, Saturation–4, Variance– 4)	0.7163	0.7498	0.6398	0.6101
Normalization	0.9687	0.9909	0.9912	0.9931
Alter in file format-.ppm to .png and back to .ppm	0.9991	0.9901	0.9971	0.9891

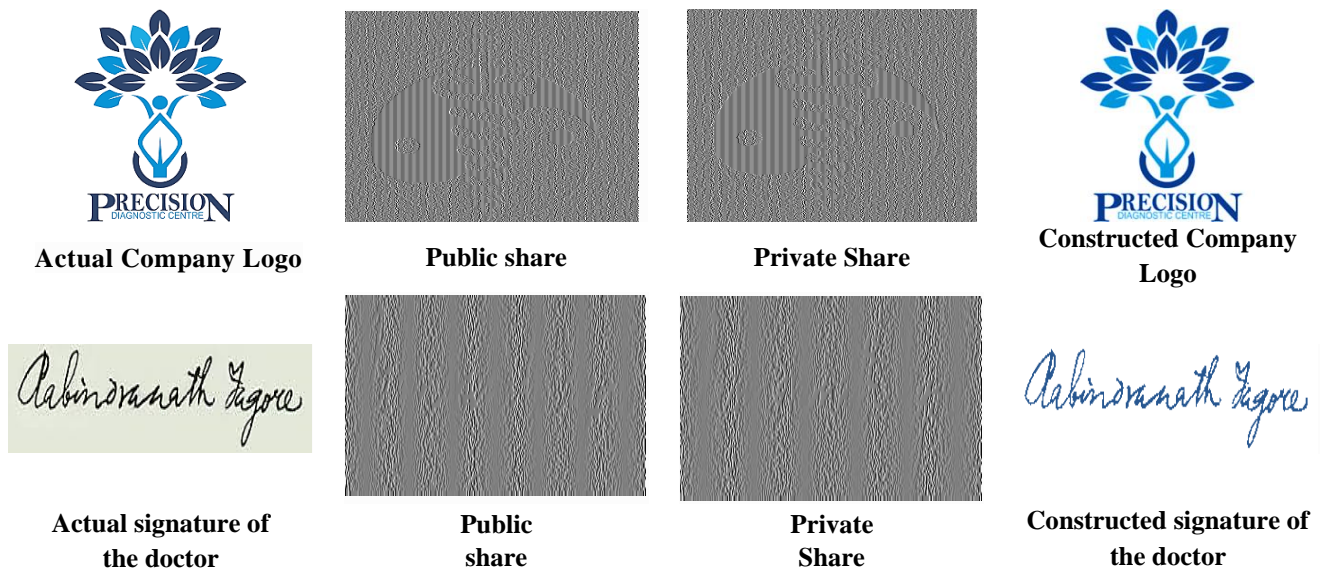


Fig. 9 Sample of share generation

The extraction of hidden sensitive data by merging the public share and the extracted private share is reflected in Figure 9. The figure shows the pattern of shares both for the company Logo and the signature of the attending doctor.

In the first portion of the figure Company logo is constructed with the help of public share and private share. In the second portion signature of the doctor is constructed with the help of public share and private share.

4.2. Robustness Scenario of Data Hiding

Critically, some of the image procession attacks were carried out on the extraction algorithm. Sensitive data extracted from the attack-affected authenticated image was matched with the original version to prove the robustness of the algorithm. The right sensitive bit was detected from the appropriate pixel even if the attack attempted to distort some of the pixel values; the distortion was still within permissible

limits. To add, the proposed concept adopted multi-copy embedding which promoted quality data sensing amongst attacks-affected extracted data. This justified robustness and protection of sensitive data against probable attacks, as mentioned in Tables 2, 3 and 4. In Table 2, the quality of the four best-extracted data copies in terms of their CC values under various attacks is shown. It is observed that in all the cases, the CC values are greater than 0.7.

In Table 3 average CC value was computed from four data copies and compared with similar existing techniques under different attacks. In all the cases, it is found that the proposed work exhibits superior results. Again, in Table 4 comparison of good quality hidden data copy recovery under different attacks with CC value > 0.7 are illustrated with respect to the other existing algorithms. This proves that this algorithm justified enhanced performance as compared to other related works.

Table 3. Average CC value computed from four data copies and compared with similar existing techniques

Attacks Applied	Average CC of four best detected data copies for this proposed algorithm	Existing approaches or works	
		Average CC of sensed signatures	Related algorithms or techniques
Salt & Pepper Noise	0.9789 (used with 5%)	0.8676	Chowdhury et al.[30], 2019 (tracked 4 best signature copies and 5% noise injected)
		0.963	Previous study of this work, 2020 (tracked 4 best signature copies and 5% noise injected)
		0.9704	Kumar et al.[28], 2018 (embedded 2 signatures and 1% noise injected)
		0.7577	Chowdhury et al.[13], 2017 (used 4 signatures and 5% noise injected)
		0.9417	Mohananthini et al. [11], 2016 (used 2 signatures and 3% noise injected)
Gaussian Noise	0.8120 (used with 2%)	0.517	Chowdhury et al.[30], 2019 (4 best signatures detected and 1% noise added)
		0.7563	Chowdhury et al.[13], 2017 (detected 4 signatures and 2% noise used)
Median Filtering	0.9901 (for 3x3 blocks)	0.9929	Singh et al.[21], 2021 (detected 3 signatures and filter block size 3x3)
		0.96	Liu et al.[4], 2019 (detected 3 signatures and filter block size 3x3)
		0.9716	Kumar et al.[28], 2018 (detected 2 signatures and filter block size 2x2)
Wiener Filtering	0.9912 (for 3x3 blocks)	0.9997	Previous study of this work, 2020 (detected 4 best signatures and filter block size 3x3)
		0.7910	Mohananthini et al.[11], 2016 (embedded 2 signatures and filter block size 3x3)
Cropping	0.9998 (75% cut, i.e. 25% left)	0.3487	Mohananthini et al.[11], 2016 (embedded 2 signatures)
		0.5933	Liu et al.[4], 2019 (embedded 3 signatures and cropping used 37% in Y direction)
		0.863	Alias et al.[27], 2020 (embedded 2 signatures and column cropping used as 25%)
Translation	0.9879 (used 0.4,-0.4)	0.9472	Mohananthini et al.[11], 2016 (embedded 2 signatures and translation amount not given)
		0.9999	Previous study of this, 2020 (detected 4 best signatures and translation applied as 0.4, -0.4)
Sharpness	0.9812 (applied 5%)	0.9516	Mohananthini et al. [11], 2016 (embedded 2 signatures and sharpness amount not given)
		0.8932	Chowdhury et al.[30], 2019 (detected 4 best signatures and translation applied 3%)
		0.9678	Chowdhury et al.[13], 2017 (embedded 4 signatures and translation applied 2% and 3%)
Smoothing	0.9910 (used with 30%)	0.9918	Chowdhury et al.[30], 2019 (detected 4 best signatures and 30% smoothing applied)
		0.9531	Previous study of this work, 2020 (detected 4 best signatures and 30% smoothing applied)
Contrast and Brightness alter	0.7621 (used with B-5, C-5)	0.4534	Chowdhury et al.[30], 2019 (best 4 detected signatures taken with B=5 & C=5 value used)
Blue-Red-Green pixel byte alter in Gimp	0.6888 (with Hue: B-10, R-10, G-10)	0.3777	Chowdhury et al.[30], 2019 (Hue: B-5, R-5, G-5)
Blue-Red-Green pixel byte alter in Irfan view	0.9812 (B-5, R-5, G-5)	0.6216	Chowdhury et al.[30], 2019 (best 4 detected signatures taken with B-5, R-5, G-5)

Table 4. Comparison of good quality hidden data copy recovery under attacks with CC value > 0.7

Attacks with parameters (either the same or greater than related works)	[11], 2016 (used 2 signs)	[13], 2017 (used 4 signs)	[28], 2018 (used 2 signs)	[30], 2019 (used 4 signs)	[4], 2019 (used 3 signs)	[27], 2020 (used 2 signs)	[21], 2021 (used 2 signs)	Proposed work (used 04 hidden data item)
Salt & Pepper Noise (5%)	02 nos. (i.e 2/2)	03 nos. (i.e 3/4)	02 nos. (i.e 2/2)	04 nos. (i.e 4/4)	Not found	02 nos. (i.e 2/2)	02 nos. (i.e 2/2)	04 nos. (i.e 4/4)
Gaussian Noise (2%)	02 nos. (i.e 2/2)	03 nos. (i.e 3/4)	02 nos. (i.e 2/2)	0 nos. (i.e 0/4)	03 nos. (i.e 3/3)	02 nos. (i.e 2/2)	02 nos. (i.e 2/2)	04 nos. (i.e 4/4)
Median Filter (3x3)	02 nos. (i.e 2/2)	04 nos. (i.e 4/4)	02 nos. (i.e 2/2)	04 nos. (i.e 4/4)	03 nos. (i.e 3/3)	02 nos. (i.e 2/2)	02 nos. (i.e 2/2)	04 nos. (i.e 4/4)
Winner Filter (3x3)	02 nos. (i.e 2/2)	04 nos. (i.e 4/4)	Not found	04 nos. (i.e 4/4)	Not found	Not found	Not found	04 nos. (i.e 4/4)
Crop (up to 75% cut)	0 nos. (i.e 0/2)	04 nos. (i.e 4/4)	02 nos. (i.e 2/2)	04 nos. (i.e 4/4)	0 nos. (i.e 0/3)	02 nos. (i.e 2/2)	Not found	04 nos. (i.e 4/4)
Row-Col. alter 60(R), 60(C)	0 nos. (i.e 0/2)	04 nos. (i.e 4/4)	Not found	04 nos. (i.e 4/4)	Not found	Not found	Not found	04 nos. (i.e 4/4)
Translation [0.4, -0.4]	02 nos. (i.e 2/2)	04 nos. (i.e 4/4)	Not found	04 nos. (i.e 4/4)	03 nos. (i.e 3/3)	Not found	Not found	04 nos. (i.e 4/4)
Sharpening (up to 5%)	02 nos. (i.e 2/2)	04 nos. (i.e 4/4)	Not found	04 nos. (i.e 4/4)	Not found	Not found	02 nos. (i.e 2/2)	04 nos. (i.e 4/4)
Smoothness (30% max.)	02 nos. (i.e 2/2)	04 nos. (i.e 4/4)	Not found	04 nos. (i.e 4/4)	Not found	Not found	Not found	04 nos. (i.e 4/4)
Contrast & Brightness alter (C-5, B-5,)	Not found	02 nos. (i.e 2/4)	Not found	0 nos. (i.e 0/4)	Not found	Not found	Not found	04 nos. (i.e 4/4)
Red-Green-Blue pixel byte alter in Irfan-view (B-5, G-5, R-5)	Not found	03 nos. (i.e 3/4)	Not found	01 nos. (i.e 1/4)	Not found	Not found	Not found	04 nos. (i.e 4/4)
Filtering of Gaussian type (Sigma=0.9, block size=3x3)	Not found	01 nos. (i.e 1/4)	Not found	Not found	Not found	02 nos. (i.e 2/2)	02 nos. (i.e 2/2)	04 nos. (i.e 4/4)
Gamma value alter (max. 1.15)	Not found	02 nos. (i.e 2/4)	Not found	Not found	Not found	Not found	Not found	04 nos. (i.e 4/4)

5. Discussion

5.1. Analysis of Experimental Results Related to Data Hiding

The proposed data hiding algorithm aims to variable encoding of secret data bits on different pixel byte elements of the concerned host image subblocks. This is mainly implemented with separate transformation equations and threshold point reference ranges while indulging both transform and spatial domain concepts of bit hiding to enable stronger security and robustness towards imperceptible data hiding. Further, by embedding multiple copies of the same copyright data, excellent recovery of hidden data under several attacks is evident in contrast to the existing ideas. This is actually possible with threshold reference range-based data encoding, which returns the same coded bit if the coded value falls in the applicable range after its alteration due to attacks. Importantly, this effective robustness is also handy while recovering the embedded private share of the signature

and finally reconstructing that signature through its public share. In this regard, the shown experimental results also reflect extensive attack analysis for the respective share merged signatures in contrast to the existing works. Overall, this demonstrated work confirms superiority over the currently existing approaches from different angles with at least a 2-3% rise in PSNR value under high data payload embedding and 100% recovery even after the attack effect with their CC value mostly > 0.8 as seen from Table 1, Table 2, Table 3 and Table 4. The graphical representation of maximum CC values of the detected data (out of four best-sensed data copies) under various attacks is presented in Figure 10, which shows the best-detected data copy CC value rarely falls below 0.6, and this fact justified excellent robustness of the proposed data hiding algorithm. The CC values have been plotted in the Y-axis and the different types of Attacks are plotted in the X-axis. From the graph, it is evident that the value varies between 1.0 and 0.6.

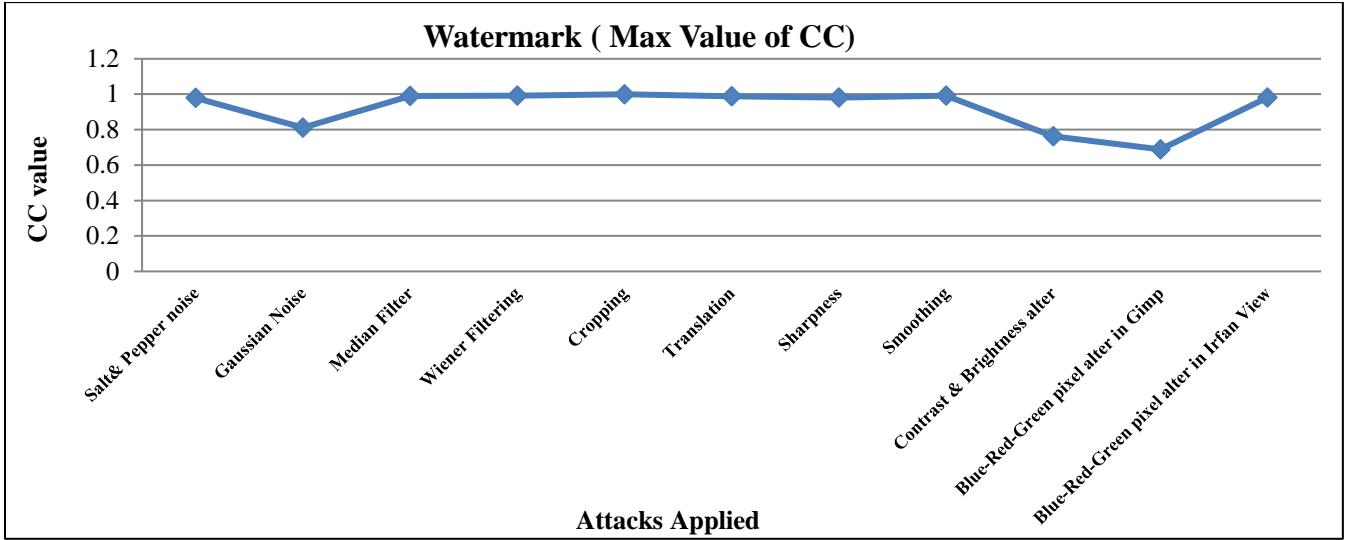


Fig. 10 Highest achieved CC Value of the detected data copy against various attacks

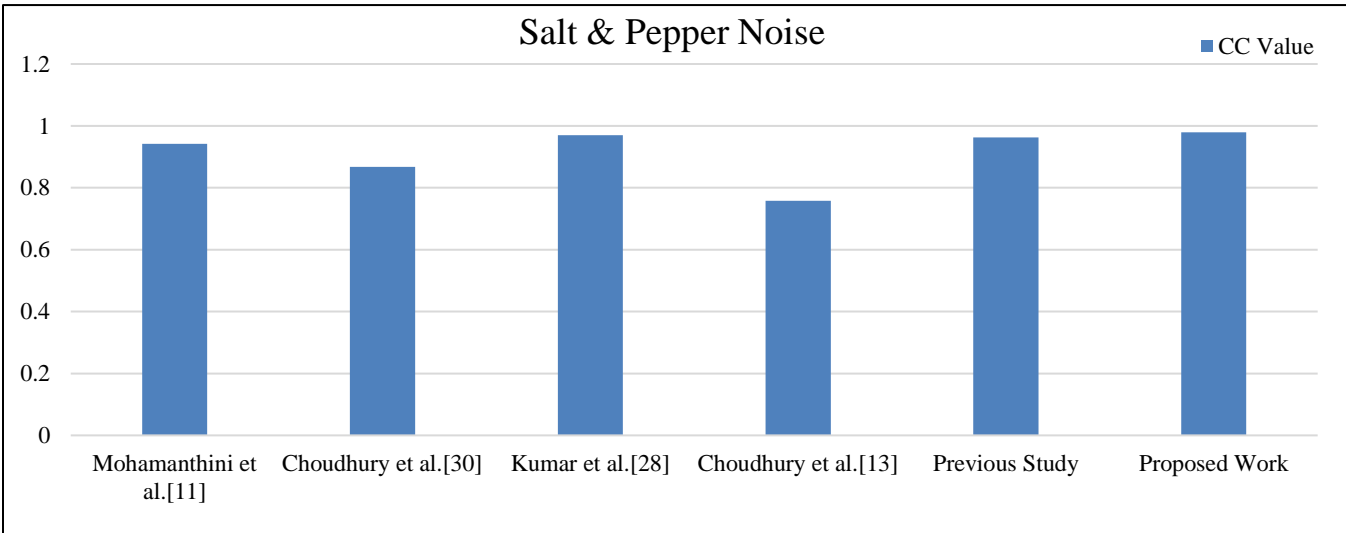


Fig. 11 Comparison of CC value for existing and proposed algorithm against Salt & Pepper Noise Attack

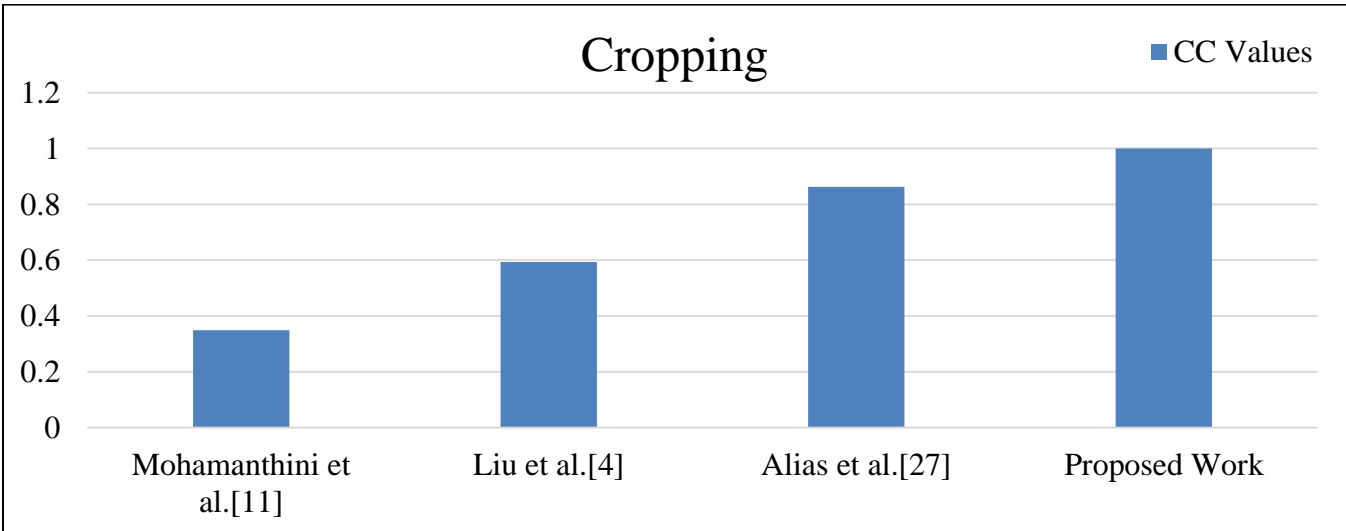


Fig.12 Comparison of CC value for existing and proposed algorithm against Cropping Attack

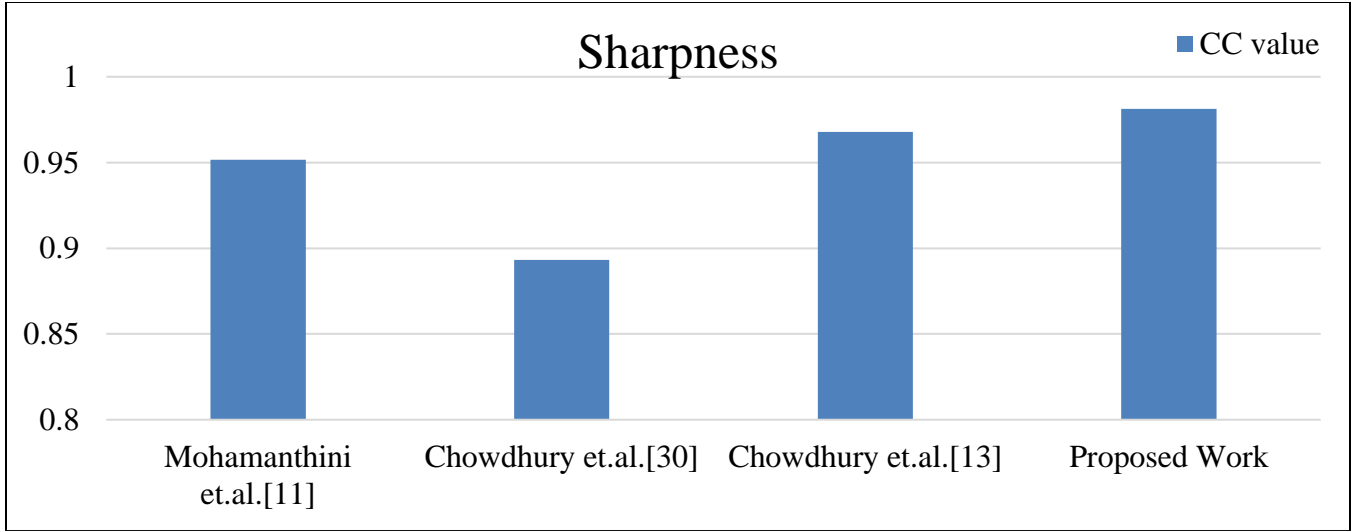


Fig. 13 Comparison of CC value for existing and proposed algorithm against Sharpness Attack

The graphical representation of the best obtained CC value for different algorithms [11],[13],[30] and the proposed one is shown in Figure 11. The proposed algorithm has the highest CC value of 0.9789. In this graphical approach, the obtained CC value for the proposed technique, as calculated, is 0.9998, which is better than the others under the Cropping attack (Figure 12). In Figure 13 it is graphically illustrated about the CC value under Sharpness attack for different algorithms along with the proposed one having the maximum value of 0.9812.

All the findings are given in different tables and figures, which are summarized as follows:

- PSNR, CC and SSIM values of Authenticated Images as constructed from different Cover images.
- Signature images considered for fabrication were shown.
- In addition to the image quality metrics, histogram analysis was shown to justify data imperceptibility.
- The generated noise due to the fabrication of sensitive data was represented through a pixel deviation graph.
- The comparison of imperceptibility in data hiding had been done with some existing concepts.
- The CC value of the retrieved data from attack-affected authenticated images was shown.
- The average CC value of the best four retrieved data which was quite acceptable as compared to other existing algorithms.
- Comparison of good quality hidden data recovery under attacks with CC value > 0.8 .
- The highest achieved CC Value of the detected data copy against various attacks by depicting it graphically.

5.2. Limitations

Although the proposed data-hiding algorithms showed excellent results in terms of data-hiding imperceptibility and

robustness, but there are still certain areas that can be improved here. In this context, the pixel byte distortions due to secret data embedding can be further reduced by introducing noise balancing scenarios or by adjusting the threshold reference range values. In addition, there are further scopes for strengthening the robustness by handling geometrical and compression-related attacks with certain standard frequency domain block transformation techniques.

Apart from these issues, the work can also address the sensitive tampering-related issues on the host medical image by comparing the impact of natural noise and tampering both on the concern extracted watermark image.

6. Conclusion

The proposed algorithm portrayed an exclusive data authentication technique for trusted affirmation of medical test images by addressing most of the possible forgeries. The main objective here was to reliably detect such forgeries as initiated upon the medical image either by the diagnostic centre or patient party or even by the other third party aiming for some personal benefits. This might lead to improper treatment or formal intention or might be used for false medical insurance claims. Hence, some novel data security solutions are raised here to promote a new horizon for online validation of medical test images and the major research contributions are as follows.

1. Medical image validated from both patient as well as test centre related angles using digital signature concept and secret embedding of copyright data within the host medical image involving test centre related authentic components, patient bio-metric fingerprint and diagnosed test data. Additionally, all such copyright information was cast with the help of different trustworthy hash values derived from various test-related

authentic data. Hence, apart from focusing on forgeries this raised idea also comply CIA factors along with the property of non-repudiations.

2. Further, this proposed work also added a new dimension to the image authentication scenario by hiding signature image fragments in circular sequences within the concerned pixel bytes of the host image subblock. The rotative orientation was based on hash values derived from the sensitive authentic data. This idea imparted stronger authenticity and security over the existing approaches.
3. Finally, the proposed work influenced effective data-hiding patterns based on the variable encoding of secret data bits in different pixel byte elements of the host image subblock. In this regard, the observation showed at least 2-3% PSNR rise under high data payload embedding with also 100% signature recovery with CC value > 0.7 under most of the common image processing attacks. Moreover, detailed robustness analysis under attacks for the regenerated share merged signatures is very rare in existing literature, and its excellent results thoroughly justify the strength of this proposed data hiding algorithm as well as the raised share generation algorithm.

Hence, this proposed idea presented a trustable validation scheme for medical images and should help for both doctor treatments and health insurance claim related issues.

References

- [1] Tsz Kin Tsui, Xiao-Ping Zhang, and Dimitrios Androustos, "Color Image Watermarking Using Multidimensional Fourier Transformation," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 16-28, 2008. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [2] Ibrahim Nasir et al., "Multiple Spatial Watermarking Technique in Color Images," *Signal Image & Video Processing (SiViP)*, vol. 4, no. 2, pp. 145-154, 2010. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [3] S. Behnia, M. Teshnehlab, and P. Ayubi, "Multiple Watermarking Scheme Based on Improved Chaotic Maps," *Communication in Nonlinear Science and Numerical Simulation*, vol. 15, no. 9, pp. 2469-2478, 2010. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [4] Jing Liu et al., "A Robust Multi-Watermarking Algorithm for Medical Images Based on DTCWT-DCT and Henon Map," *Applied Sciences*, vol. 9, no. 4, pp. 1-23, 2019. [[Crossref](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [5] K. Ganesan, and Tarun Kumar Guptha, "Multiple Binary Images Watermarking in Spatial and Frequency Domains," *Signal & Image Processing: An International Journal*, vol. 1, no. 2, pp. 148-159, 2010. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [6] Li Zhang et al., "A Dynamic Multiple Watermarking Algorithm based on DWT and HVS," *International Journal of Communications, Network & System Sciences*, vol. 5, no. 8, pp. 490-495, 2010. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [7] N. Mohananthini, Yamuna Govindarajan, and R. Vivek, "Comparison of Successive and Segmented Watermarking Techniques for Color Images," *Proceedings of National Conference on Emerging Trends in Information & Communication Technology, International Journal of Computer Applications*, pp. 13-16, 2013. [[Google Scholar](#)] [[Publisher Link](#)]
- [8] Rohit M. Thanki, and Komal R. Borisagar, "Compressive Sensing Based Multiple Watermarking Technique for Biometric Template Protection," *International Journal of Image Graphics and Signal Processing*, vol. 7, no. 1, pp. 53-60, 2015. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [9] K. Karthik, and M.A. Dorai Rangaswamy, "A Novel Three-Tier Protection for Digital Images Using Blind Watermarking Scheme," *International Journal of Advance Trends in Computer Science and Engineering*, vol. 4, no. 1, pp. 15-19, 2015. [[Google Scholar](#)] [[Publisher Link](#)]

Moreover, this work is also suitable for wireless domain applications due to the enriched version of data security protocol and data hiding algorithms. However, there are certain issues that can still be addressed to enhance this work further. Among these issues, noise balancing on data-encoded pixel bytes will further reduce the distortions caused due to data hiding. Also, some frequency domain transformation techniques can be applied here to handle the geometrical and compression related attacks. Apart from that, the work can still be extended to tackle the sensitive tampering-related issues on the host medical image and here, the distortion impact of both natural noise and tampering can be compared on the extracted watermark image for making a decision.

Acknowledgments

The author(s) express 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 with carrying out this research work.

Author's Contribution Statement

Saikat Bose: Framing of Concept, feasibility study, data curation, writing of original draft, analysis and interpretation of results.

Tripti Arjariya: Conceptualization, Guiding the manuscript preparation.

Anirban Goswami: Concept study, draft manuscript preparation, etc.

- [10] N. Mohananthini, and G. Yamuna, "Image Fusion Process for Multiple Watermarking Schemes against Attacks," *Journal of Network Communications and Emerging Technologies*, vol. 1, no. 2, pp. 1-8, 2015. [[Google Scholar](#)] [[Publisher Link](#)]
- [11] N. Mohananthini, and G. Yamuna, "Comparison of Multiple Watermarking Techniques Using Genetic Algorithms," *Journal of Electrical Systems & Information Technology*, vol. 3, no. 1, pp. 68-80, 2016. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [12] Nabin Ghoshal, and J.K. Mandal, "Discrete Fourier Transform Based Multimedia Color Image Authentication for Wireless Communication," *2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE)*, Chennai, India, pp. 1-5, 2011. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [13] Soumit Chowdhury, Ritesh Mukherjee, and Nabin Ghoshal, "Dynamic Authentication Protocol Using Multiple Signatures," *Wireless Personal Communications*, vol. 93, no. 3, pp. 3607-3638, 2017. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [14] N. Mohananthini, and G. Yamuna, "Multiple Successive Watermarking Scheme Based on Wavelet Transform," *International Journal of Emerging Trends & Technology in Computer Science*, vol. 2, no. 2, pp. 416-420, 2017. [[Google Scholar](#)]
- [15] Gaurav Bhatnagar, and Q.M. Jonathan Wu, "A New Robust and Efficient Multiple Watermarking Scheme," *Multimedia Tools and Applications*, vol. 74, no. 19, pp. 8421-8444, 2015. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [16] Vandana S. Inamdar, and Priti P. Rege, "Dual Watermarking Technique with Multiple Biometric Watermarks," *Sadhana, Indian Academy of Science*, vol. 39, no. 1, pp. 3-26, 2014. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [17] Natarajan Mohananthini, and Govindarajan Yamuna, "A Study of DWT-SVD Based Multiple Watermarking Scheme for Medical Images," *International Journal of Network Security*, vol. 17, no. 5, pp. 558-568, 2014. [[Google Scholar](#)] [[Publisher Link](#)]
- [18] T.E. Ives, "The New 'E-Clinician' Guide to Compliance," *Audiology Today*, vol. 26, no. 1, pp. 52-53, 2014. [[Google Scholar](#)]
- [19] Emmanuel Kusi Achampong, "Electronic Health Record (EHR) and Cloud Security: The Current Issues," *International Journal of Cloud Computing and Services Science*, vol. 2, no. 6, pp. 417-420, 2013. [[Google Scholar](#)] [[Publisher Link](#)]
- [20] S. Radharani, and M.L. Valarmathi, "Multiple Watermarking Scheme for Image Authentication and Copyright Protection using Wavelet Based Texture Properties and Visual Cryptography," *International Journal of Computer Application*, vol. 23, no. 3, pp. 29-36, 2011. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [21] A.K. Singh et al., "Joint Encryption and Compression-Based Watermarking Technique for Security of Digital Documents," *ACM Transactions on Internet Technology*, vol. 2, no. 1, pp. 1-20, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [22] Rohit M. Thanki, and Komal R. Borisagar, "Combined DCT-CS Theory Based Digital Watermarking Technique for Color Images," *Proceedings of National Conference on Emerging Trends in Information & Communication Technology, International Journal of Computer Applications*, pp. 17-23, 2013. [[Google Scholar](#)] [[Publisher Link](#)]
- [23] Mohananthini Natarajan, and Yamuna Govindarajan, "Performance Comparison of Single and Multiple Watermarking Techniques," *International Journal of Computer Network and Information Security*, vol. 7, pp. 28-34, 2014. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [24] Mahdi Babaei et al., "Robust Multi Watermarking Scheme for Multiple Digital Input Images in DWT Domain," *International Journal of Computer and Information Technology*, vol. 3, no. 4, pp. 834-840, 2014. [[Google Scholar](#)] [[Publisher Link](#)]
- [25] Ali Al-Haj, and Mahmoud Farfoura, "Providing Security for E-Government Document Images Using Digital Watermarking in the Frequency Domain," *Proceedings of 5th International Conference on Information Management (ICIM), IEEE*, Cambridge, UK, pp. 77-81, 2019. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [26] C. Jeba Nega Cheltha et al., "A Review on Data hiding Using Steganography and Cryptography," *9th International Conference on Reliability, Infocom Technologies and Optimization*, Noida, India, pp. 1-4, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [27] Noruhida Alias, and Ferda Ernawan, "Multiple Watermarking Technique using Optimal Threshold," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 18, no. 1, pp. 368-376, 2020. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [28] Chandan Kumar et al., "SPIHT-Based Multiple Image Watermarking in NSCT Domain," *Concurrency and Computation Practice and Experience*, vol. 32, no. 1, pp. 1-9, 2018. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [29] Roopam Sadh, Nishchol Mishra, and Sanjeev Sharma, "Dual Plane Multiple Spatial Watermarking with Self-Encryption," *Sadhana, Indian Academy of Sciences*, vol. 41, no. 1, pp. 1-14, 2016. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [30] Soumit Chowdhury, Sontu Mistry, and Nabin Ghoshal, "Multi-Phase Digital Authentication of e-Certificate with Secure Concealment of Multiple Secret Copyright Signatures," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 10, pp. 3365-3380, 2019. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [31] Huwaida T. Elshoush et al., "A Novel Approach to Information Hiding Technique using ASCII Mapping Based Image Steganography," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 12, no. 2, pp. 65-82, 2021. [[Google Scholar](#)] [[Publisher Link](#)]
- [32] Katandawa Alex Kingsley, and Ari Moesriami Barmawi, "Improving Data Hiding Capacity in Code Based Steganography Using Multiple Embedding," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 11, no. 1, pp. 14-43, 2020. [[Google Scholar](#)] [[Publisher Link](#)]
- [33] Qi Li et al., "An Encrypted Coverless Information Hiding Method Based on Generative Model," *Information Sciences*, vol. 553, pp. 19-30, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]

- [34] Ashraf Abdel Raouf, "A New Data Hiding Approach for Image Steganography Based on Visual Color Sensitivity," *Multimedia Tools and Applications*, pp. 23393–23417, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [35] Roseline Oluwaseun Ogundokun, and Oluwakemi Christiana Abikoye, "A Safe and Secured Medical Textual Information Using an Improved LSB Image Steganography," *International Journal of Digital Multimedia Broadcasting*, vol. 2021, pp. 1-8, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [36] Mostafa M. Abdel-Aziz, Khalid M. Hosny, and Nabil A. Lashin, "Improved Data Hiding Method for Securing Color Images," *Multimedia Tools and Applications*, vol. 80, pp. 12641–12670, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [37] P.V. Sabeen Govind, and M.V. Judy, "A Secure Framework for Remote Diagnosis in Health Care: A High Capacity Reversible Data Hiding Technique for Medical Images," *Computer and Electrical Engineering*, vol. 89, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [38] Hussah N. AlEisa, "Data Confidentiality in Healthcare Monitoring Systems Based on Image Steganography to Improve the Exchange of Patient Information Using the Internet of Things," *Journal of Healthcare Engineering*, vol. 2022, pp. 1-11, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [39] Image Comparison in Matlab [Matrix Laboratory] Using Histograms, Coding Lab - TechOnTechnology, 2016. [Online]. Available: <http://codinlab.blogspot.in/2013/10/image-comparison-in-matlab-matrix.html>
- [40] Image Processing Toolbox, MathWorks, 2016. [Online]. Available: <http://in.mathworks.com/help/images/index.htm>