Digital Image Authentication Algorithm Based on Fragile Invisible Watermark and MD-5 Function in the DWT Domain

Asst. Lect. Nehad Hameed Hussein
Department of Software Engineering
Baghdad College of Economic Sciences
Email: it_engineer85@yahoo.com

ABSTRACT

Using watermarking techniques and digital signatures can better solve the problems of digital images transmitted on the Internet like forgery, tampering, altering, etc. In this paper we proposed invisible fragile watermark and MD-5 based algorithm for digital image authenticating and tampers detecting in the Discrete Wavelet Transform DWT domain. The digital image is decomposed using 2-level DWT and the middle and high frequency sub-bands are used for watermark and digital signature embedding. The authentication data are embedded in number of the coefficients of these sub-bands according to the adaptive threshold based on the watermark length and the coefficients of each DWT level. These sub-bands are used because they are less sensitive to the Human Visual System (HVS) and preserve high image fidelity. MD-5 and RSA algorithms are used for generating the digital signature from the watermark data that is also embedded in the medical image. We apply the algorithm on number of medical images. The Electronic Patient Record (EPR) is used as watermark data. Experiments demonstrate the effectiveness of our algorithm in terms of robustness, invisibility, and fragility. Watermark and digital signature can be extracted without the need to the original image.

Keywords– Fragile watermark; Image authentication; DWT; adaptive threshold; HVS; MD-5; RSA.

خوارزمية أثبات اصالة الصور الرقمية بالاعتماد على العلامة المائية الهشة المخفية و دالة ملخص الرسالة الخامسة ضمن نطاق تحويل المويجات المنفصلة

م.م. نهاد حميد حسين
قسم هندسة البرامجيات
كلية بغداد للعلوم الاقتصادية

الخلاصة

في هذا البحث تم عمل خوارزمية للتحقق من اصالة الصور الرقمية من خلال الاعتماد على تقنيات العلامة المائية والتوقيع الرقمي. اولا يتم تحويل الصورة الى المجال الترددي باستخدام تقنية تحويل المويجات المنفصلة DWT وثم ادخال العلامة المائية في الصورة بعد تحويلها الى النظام الثنائي. قمنا باستخدام الترددات العالية والمتوسطة في الصورة لغرض اخفاء العلامة المائية لضمان عدم تأثر الصورة و عدم رؤية العلامة المائية المضافة بالعين البشرية. يتم اخفاء البيانات في عدد من الترددات العالية في الصورة التي يتم اختيارها من خلال معادلة متغيرة مع كل مستوى من التحويل المويجي. اضافة الى وجود العلامة المائية يتم اخفاء خلاصة العلامة المائية والتي يتم احتسابها باستخدام خوارزميات (MD5, RSA). تم تطبيق الطريقة على عدد من الصور الطبية مع

استخدام بيانات سجل المريض الالكتروني كعلامة مائية. التجارب العملية اثبتت قوة الخوارزمية وامكانية كشفها لاي هجوم او تعديل على الصورة.

الكلمات الرئيسية: العلامة المائية الهشة, اصالة الصور الرقمية, تحويل المويجات المنفصلة, نظام الرؤية البشري, خلاصة الرسالة.

1. INTRODUCTION:

The evolution of information systems, supported by advances in information and communication technologies, enables digital information likes digital images to be shared between organizations and personals more easily. At the same time, more attention should be paid to protect and authenticate these information. Image watermarking and digital signatures technologies are an effective solutions to meet such requirements. Medical images are good example of images that required to be authenticated before sharing it between the consultants or healthcare centers.

Digital watermarking is a technology that embeds watermark data (copyright information) such as identification numbers, personal information, or serial numbers, into digital data **Cox, et al. 2000**. In digital images watermarking should take care the image fidelity degradation so that the embedded watermark should be small as possible and not be visible. A high fidelity means that the watermarked image is very similar to its original image or more precisely, they are indistinguishable.

Image authentication is a technique for inserting information (digital signature) into an image for authentication and integrity. In the receiver side, the inserted information will be extracted and compared with the original information to decide image authenticity and integrity. MD-5 and SHA-1 are the well-known algorithms used for digital signature creation.

In this paper, a new method for digital image authentication based on the watermark and digital signature is proposed. The proposed algorithm aims to achieve image authentication through fragile invisible watermark and MD-5/RSA algorithms. Medical images are selected as test images and the watermark will be taken from Electronic Patient Record (EPR) including: Patient record number, Patient name, Age, Gender, Medical state, Dr. Name, Hospital name, and Region of residence.

In addition to the watermark, the digital signature will be computed and embedded in the image. MD5 and RSA (Rivest-Shamir-Adleman) algorithms are used to generate the digital signature from the watermark. MD5 used for computing 128-bit digest and RSA used for encrypting the computed digest.

After that, the image is decomposed by 2-level DWT and the watermark and digital signature are embedded in the selected coefficients in the middle and high frequency sub-bands according to the adaptive threshold that based on the watermark length and the middle and high frequencies coefficients of each DWT level. These sub-bands are used for authentication data embedding in order to ensure the watermark invisibility and high image fidelity.

The remaining of the paper is organized as follows: Literature survey is discussed in section 2, methods used in this paper are studied in section 3, and the algorithm details including authentication data generation, embedding, and extraction are discussed in section 4. The experimental results and performance analysis are evaluated in section 5. Finally, conclusions are detailed in section 6.

2. LITERATURE SURVEY

In the literatures mainly two types of watermarking techniques are discussed: (1) spatial domain based and (2) frequency domain based approaches. In spatial domain approaches, the watermark data are embedded in the least significant bit (LSB) of the cover image pixels. However, the LSB insertion method is easy to be attacked.

In frequency domain approaches, a mathematical transform is applied to the image to embed watermark into the transform coefficients, then apply inverse transform to get the embedded image. The most frequent used methods are Discrete Wavelet Transform (DWT)**,** Discrete Cosine Transform (DCT), and Discrete Fourier Transform (DFT). As the frequency domain methods always have good robustness to common image processing such as compression, noise, filtering, rotation, cutting, etc., they now come into more widespread used **Wang et al. 2009,** and **C. Li and H Song, 2008**.

Sinha and Singh 2003 proposed a technique to encrypt an image for secure transmission using digital signature of the image. They embedded the authentication data in the spatial domain. **Chang, C., Tseng, H. 2004**, proposed spatial domain method by exploiting the correlation between adjoining pixels for determining the bit number to be embedded at certain specific pixel. If the pixel is located in edge areas, we can embed more data than the smooth areas. **Cong Jin et.al 2006** described watermarking scheme using wavelet transform and HVS. In this method watermark is embedded using adaptive embedding based on HVS. It considers sensitivity of human eye towards noise, luminous and textures. Watermark is inserted using adaptive gain factor which is calculated from noise sensitivity, luminosity, edge distance and texture area.

Po. Chen and Y. Tseng 2007, proposed a new frequency domain method for image watermarking. In this system, first transform the cover image into sub bands. The secret image is embedded into LL sub band of cover image. **Yang, Hengfu and Sun, Xingming 2007** proposed an image-adaptive semi-fragile watermarking technique for image authentication and tamper detection. The algorithm embeds the watermark in coefficients of the vertical and the horizontal detail sub-bands of image sub-block. It is utilizing HVS so it is highly adaptive to the original image characteristics.

Chuanmu L. and Haiming S., 2008 proposed invisible watermarking scheme for image authentication in DWT. The binary watermark is generated by a chaotic map using adaptive threshold. Using a secret key, select some perceptually significant coefficients from detail sub-bands of 3-level DWT of the host image for watermark embedding.

In 2012, Baisa L. et.al explored method of watermark in medical images using Region of Interest ROI method. In this method watermark is embedded in ROI only. They use Arnold transform for watermark scrambling and wavelet transform for host image decomposition. **K. Raval and S. Zafar 2013** proposed adaptive watermark embedding procedure using DWT and DCT, first watermarked image is decomposed through DWT transform and choosing the high frequency bands for watermark embedding according to adaptive factor function. DCT transform is applied for watermark message for reformatting and reshaping before embedding it. **N. Grover and A. Mohapatra 2013** proposed technique for authenticating the shared images on the social networks through embedding the secret data related to person’s login detail and current timestamp in the original image using adaptive steganography. The watermark bits are embedded in the DWT low frequency bands.

M. Dhoka, J. Kadam 2014 proposed a method of invisible watermark to medical image using Bi-orthogonal wavelet filter and transformed domain watermark embedding. In their method, they transformed both original image and watermark using DWT and Bi-orthogonal wavelet filter coefficients. Comparison is made on basis of PSNR and normalized correlation (NC).

Our contribution is based on new methods in the watermarking embedding techniques, where the image is watermarked in the frequency domain providing watermark robust, invisibility, and more security against many attacks types. However while the recent papers are influenced on the image authentication through watermarking embedding only, we will focus on embedding the digital signature of watermark also in the image in the invisible manner without affecting the image fidelity. This gives two ways for ensuring the image authentication through watermark and digital signature.

3. METHODS

3.1 Discrete Wavelet Transform

DWT is information processing method was presented in the late 1980's. It's used for multi-resolution analysis, it is particularly useful for the analysis of non-stationary signals, including image processing **Chang Gao, 2009**.

The basic idea is to decompose the image into sub-bands at different frequency and different space. In DWT, the image is first decomposed in four sub-bands, low frequency band (LL1), horizontal detail band (HL1), vertical detail band (LH1), and diagonal detail band (HH1). The LL1 band is further can be decomposed into four sub-bands obtaining LL2, HL2, LH2 and HH2. LLi sub-band can be further decomposed to generate other four sub-bands and so on **Al-Haj and T. Manasrah, 2007**.

The LL band can be treated as an approximation of the image. Any modification done to this band is visually most perceptible. The other three bands are high frequency bands that characterize the marginal information of the corresponding direction and have little energy. These bands contain the detail information of an image like the edge information and texture. **Fig. 1** depicts a two level decomposition of MRI medical image using DWT.

Since human eyes are much more sensitive to the low-frequency part (LL sub-band), in the suggested algorithm, we will use regions that known to be less sensitive to human visual system (HVS) that are high frequency sub-bands for watermark and signature embedding. This makes the watermark is invisible and maintains better image fidelity and quality.

3.2 Human Visual System

Visual psychology researchers have found that masking characteristics of the human visual system when embedding authentication information improves digital watermarking robustness and imperceptibility **Dumitru et al. 2008**.

The advantage of using the DWT is that it is known to more accurately model the aspects of the HVS as compared to the FFT or DCT **Cong Jin, et al. 2006**. Some of the significant features the DWT provides are excellent spatial localization, frequency spread, and multi-resolution characteristics, which are similar to the theoretical models of the HVS **Dumitru et al. 2008**.

We will benefit from the HVS characteristic that is known to be less sensitive to the middle and high resolution sub-bands (LH, HL, and HH) for generating invisible watermark through embedding the watermark and digital signature in the middle and high frequencies sub-bands only. This causes to increase in the robustness with a little or no impact on image quality and fidelity **Dumitru et al. 2008**.

3.3 Performance Evaluation Metrics

3.3.1 Peak signal-to-noise ratio (PSNR)

PSNR is the ratio between the maximum possible value (pixel) of image and the power of distorting noise that affects the quality of its representation. The proposal is that the higher the PSNR, the better degraded image has been reconstructed to match the original image and the better the reconstructive algorithm **Rajendra et al, 2012**. PSNR is defined via the mean squared error (MSE). Given M x N image I and its reconstructed one K, MSE is:

$$MSE \ = \frac{1}{mn}\sum_{i=0}^{m-1} \ \sum_{j=0}^{n-1}[I\ (i,j) - K\ (i,j)]\ ^2 \qquad (1)$$

$$PSNR = 10. log_{10} \ \left(\frac{MAX^2}{MSE}\right) \qquad (2)$$

Here, *MAX* is the maximum possible pixel value of the image.

3.3.2 Structural Similarity (SSIM)

SSIM index measures the similarity between two images in a manner that is more consistent with human perception than MSE and PSNR. It attempts to measure the change in luminance, contrast, and structure in an image. SSIM result closer to 1 means the reconstructed image very similar to the original image **Wang et al, 2004**. The SSIM metric is calculated between the original image x and reconstructed image y images with common size N x M is:

$$\mathrm{SSIM}(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \qquad (3)$$

Where, μ_x is the average of x, μ_y is the average of y, $\sigma^2{}_x$ is the variance of x, $\sigma^2{}_y$ is the variance of y, and finally σ_{xy} is the covariance of x and y;

3.3.3 Normalized Hamming Distance (NHD)

NHD is used for measuring the similarity between the embedded and extracted watermarks **Z. M. Lu and S. H. Sun, 2009**. The correct watermark extraction percentage (CWEP) and correct signature extraction percentage (CSEP) are defined as normalized hamming distance between embedded and extracted watermarks and digital signature signatures, respectively.

$$CWEP = 1 - \frac{1}{L}\sum_{i=1}^{L}(W_i \oplus \ W1_i) \qquad (4)$$

$$CSEP = 1 - \frac{1}{N}\sum_{i=1}^{N}(S_i \oplus \ S1_i) \qquad (5)$$

Where W, W1 denote the embedded and extracted watermarks with L bits length. S, S1 are the embedded and extracted digital signature with N bits length. $\oplus$ is X-OR logic operator. The higher the CWEP and CSEP value, the more similarity there is between W and W1, and S and S1 respectively. When CWEP and CSEP values equal to 1, means W1= W and S1=S.

4. PROPOSED DIGITAL IMAGE AUTHENTICATION ALGORITHM

The proposed algorithm is fragile invisible watermark and digital signature based for digital image authentication and tampers detecting. The watermark invisibility mains the embedded watermark cannot be perceived in HVS **Mahavir D. and Jitendra K., 2014**. Fragile watermark is readily altered or destroyed when the host image is modified through a linear or nonlinear transformation **Chang Gao, 2009**. That is, it may interest for parties to verify that an image has not been edited, damaged, or altered since it was marked.

The data that will be embedded in the digital image includes watermark and digital signature. Watermark data is patient-related data or EPR that includes: Patient record number, Patient Name, Age, Gender, Medical state, Dr. Name, Hospital name, Country, and Region of residence.

Digital signature is computed for the watermark data using MD-5 and RSA algorithms. MD-5 algorithm is used to generate 128-bit digest from the watermark. RSA algorithm is used for encrypting the digest that results the digital signature.

The suggested technique based on adaptive threshold to embedding the watermark and digital signature into the digital image in such a way that it is undetectable by the HVS. The adaptive thresholding method is employed to determine appropriate coefficients to hiding watermark and digital signature in the high frequencies regions in the image.

The threshold is variable according to the middle and high frequencies sub-bands coefficients of each DWT level making the hiding coefficients are different for each image.

First, the digital image is decomposed into seven regions using 2-level DWT and the middle and high frequency regions are selected for watermark and digital signature hiding. These frequencies give the details of the image and any changes in them are not easy notes by HVS, so that we will use them in order to ensure watermark invisibility and image fidelity. In this technique, low frequencies are excluded when inserting authentication data in order to preserve ROI and digital image fidelity.

Second, according to the computed adaptive threshold, the watermark data and digital signature are embedded in the appropriate coefficients. By using the adaptive threshold, the watermark and signature aren’t hidden in all middle and high frequencies coefficients but in number of them only.

However, the suggested algorithm is composed of three sections: authentication data generation, authentication data embedding, and its extraction or verification. **Table 1** shows the main symbols used in the paper and **Fig. 2** shows the block diagram of the algorithm (embedding and extracting).

4.1 Authentication Data Generation Process:

One of the most important features of the suggested algorithm is the type of the watermark data. The suggested watermark data is text type, like patient information. The watermark data used in the algorithm testing is collected from the EPR that is storing in the hospital database.

However, EPR data that used as watermark include: Patient record number, Patient Name, Age, Gender, Medical state, Dr. Name, Hospital name, and Country or Region of residence.

These data will be collected in one string and converted from ASCII to binary to forming the binary watermark $W= \{W_0\ W_1\ W_2 \dots\ W_{L-1}\}$ where W_i $(1 \geq i \leq L)$ is the *ith* bit in the binary watermark.

The digital signature *S* is used for demonstrating the authenticity of image. Here we used MD-5 and RSA algorithms for generating the digital signature from the watermark data. The depending of the digital signature on the watermark itself making any attempt to change or remove the watermark is detectable. This means the algorithm provides dual methods for image authenticating.

The watermark and its digital signature forming the authentication data used in the embedding process. However, the authentication data generation steps are listed in the algorithm below *algorithm_1* and its flowchart is shown in **Fig. 3**.

```
ALGORITHM_1: Authentication Data Generation
Input: Text Watermark and Encryption Private Key Kp.
Output: Authentication Data String (Watermark W, Digital Signature S)
BEGIN:
Step1: Collect the data that forming the watermark data in one string.
Step2: Binarize the collected watermark data and store in $W_L$ variable string.
Step3: Compute the digital signature $S$ using the following steps.
        i. Generating a 128-bits digest $D$ from the binary watermark $W_L$ using MD-5 algorithm.
       ii. Encrypting the digest using RSA algorithm for providing the digital signature $S$. The
           digest will be encrypted using sender private key $K_p$.
Step4: Concatenate $S$ and $W_L$ and store in one string of binary numbers called authentication
string $Auth\_S$.
                    $Auth\_S = \{S_0\ S_1\ S_2 \ldots S_{127}\} \parallel \{W_0\ W_1\ W_2 \ldots W_{L-1}\}$
END:
```

4.2 Authentication Data Embedding Process

The aim of this algorithm is to hiding the watermark data and digital signature (*Auth_S*) into the digital image. This algorithm should be implemented in the image sender side. However, this algorithm consists of five steps.

1. Applying 2-level DWT to the digital image.
2. Computing the adaptive threshold for each level.
3. Determining the hiding coefficients which are used for hiding the watermark and signature bits.
4. Embedding the authentication data (*Auth_S*) in the determined hiding coefficients.
5. Performing the inverse wavelet transform IDWT to construct the watermarked medical image.

4.2.1 Apply Discrete Wavelet Transformation

DWT is applied twice to decomposing the image to seven sub-bands in the frequency domain. The first level of DWT produces four sub-bands, termed LL1, LH1, HL1 and HH1. The LL1 band is iteratively decomposed to obtain four levels are LL2, LH2, HL2, and HH2. The six DWT sub-bands (LHi, HLi, and HHi) are used in the embedding process.

4.2.2 Compute of Adaptive Threshold

After transforming the image into frequency domain through DWT, the adaptive thresholds are computed for each level. Here, we describes the method for computing threshold value (T), which is adaptive to different level characteristics. The threshold value is calculated according to the decomposition level and watermark length L. In the 2-level decomposition, the average of coefficients C for 1-level high frequency sub-bands (LH1, HL1, HH1) is computed and the threshold T_1 is calculated by Eq. (6), also the average of coefficients C for the 2-level high frequency sub-bands (LH2, HL2, HH2) is computed and the threshold T_2 is calculated by the same equation.

$$T_i = 2^{|(log_{10}\, AVR(C_i))|}\ mod\ (L + i) \qquad (6)$$

AVR (C_i) function finds the average of coefficient C in i-level. The authentication bits are embedded only in the selected coefficients in the high and middle frequency bands according to the adaptive threshold. **Fig. 4** shows how the adaptive threshold can be computed. The computed threshold is adaptive because it depends on the DWT level and the largest coefficient in the level.

The algorithm which computes threshold values in wavelet domain it very simple to implement and computationally is more efficient. It has following steps (algorithm_2):

```
ALGORITHM_2: Adaptive Thresholding Algorithm
Input: DWT middle and high frequency sub-bands (LHi, HLi, HHi) and Watermark length L
Output: Adaptive threshold of each DWT level ($T_1$, $T_2$).
Step1: For every DWT level, do the following.
BEGIN:
Step2: Load the coefficients C of LHi, HLi, and HHi sub-bands of i-level DWT.
Step3: Find the average of coefficients in i-level sub-bands (LHi, HLi, and HHi).
Step4: Compute the threshold value ($T_i$) using Eq. (6).
Step5:  Save the threshold values results in $T_i$.
END:
```

4.2.3 Watermark and Digital Signature Hiding

This step is used to decide what the sub-bands and coefficients are to be used for the authentication data hiding. Some of the coefficients in the high levels (HH_1 and HH_2) and the middle levels (HL_1, LH_1, HL_2 and LH_2) will be used for authentication bits embedding. Embedding data in the middle and high sub-bands (LH, HL and HH) ensures a higher image fidelity and authentication data invisibility.

On the contrary, we exclude LL_2 sub-band to preserve image ROI. In spite of embedding data in the low frequency sub-band improve the watermark robustness but it is highly perceptible by human eye making the embedded authentication data is visible.

However, the coefficients are selected using adaptive threshold according to the following steps:

1. For each level, all coefficients of the LH_i, HL_i and HH_i sub-bands are firstly concatenated into a single sequence. Three coefficients with the same coordinate of the three sub-bands, which correspond to the same spatial location, are continuously adjacent in the new sequence. However the coefficients are rearranged in the following way:

$\{C_{LHi}(0,0), C_{HLi}(0,0), C_{HHi}(0,0), C_{LHi}(0,1), C_{HLi}(0,1), C_{HHi}(0,1),...., C_{LHi}(N-1,M-1), C_{HL2}(N-1,M-1), C_{HH2}(N-1,M-1)\}$.

Where *N* and *M* are the horizontal and vertical size of the sub-band respectively.

2. Then, the *Auth_S* bits are embedded in the LSB of the hiding coefficients which are satisfying the condition as follows:

$$|\ Coefficient\ Magnitude\ | > Threshold\ of\ Level\ (T) \qquad (7)$$

All the coefficients in i-level sub-bands (LHi, HLi, and HHi) are tested for satisfying the previous condition. However, the pseudocode of embedding process is listed below.

```
j=0;  // the start of the Auth_S string.
FOR  i= 1 TO i≤2   // i=1,2 (the number of DWT levels)
Begin:
Sort (C)
```

```
WHILE ($\{C_{i\text{-level}}\} \neq \{\emptyset\}$)
Begin:
IF ($|C_k| > T_{i\text{-level}}$)     //k is the kth coefficient in the i-Level.
Auth_$S_j \rightarrow$ LSB ($|C_k|$)
End IF
j= j+1;
k= k+1;
End WHILE
End FOR
```

4.2.4 Inverse of Wavelet Decomposition

Finally, the authenticated image is reconstructed by performing the inverse wavelet transformation IDWT.

However, the embedding algorithm of the suggested technique is listed below (algorithm_3) while its flowchart is shown in **Fig. 5**.

ALGORITHM_3: Authentication Data Embedding

Input: Digital Image $I_{M \times N}$, and Authentication String (*Auth_S*)
Output: Authenticated Image $AI_{M \times N}$.
BEGIN:
Step1: Perform 2-level DWT for the input image.
Step2: For each level do the following
BEGIN:

1. Compute adaptive threshold value T_i according to the Algorithm_2:
2. Determine hiding coefficients according to the following steps:
   i. Sorting the coefficients of the sub-bands LHi, HLi, and HHi where the three coefficients with the same coordinate of the three sub-bands, which correspond to the same spatial location, are continuously adjacent in the new sequence.

   $\{C_{LHi}(0,0),\ C_{HLi}(0,0),\ C_{HHi}(0,0),\ \ C_{LHi}(0,1),\ C_{HLi}(0,1),\ C_{HHi}(0,1)\ ,\ldots,\ C_{LHi}(n-1,m-1),\ C_{HLi}(n-1,m-1),\ C_{HHi}(n-1,m-1)\}.$

   ii. For coefficients in LHi, HLi, and HHi sub-bands, the hiding coefficients are determine by using computed adaptive thresholding.
3. Repeat the following steps until every bit in *Auth_S* string is embedded.
   i. Read the high and middle frequency coefficients of current DWT level sequentially and select the coefficients which are satisfying the condition in Eq. (7):

   | Coefficient Magnitude | > i-level Threshold.

   ii. Embed the *jth* bit from *Auth_S* string in the LSB of the *jth* hiding Coefficient.

End:
Step3: Reconstruct the authenticated image $AI_{M \times N}$ by using IDWT.
Step4: Save and display the authenticated image.
End:

4.3 Extraction and Verification Algorithm

The first step of the extraction algorithm consists also of decomposition of the authenticated image with the same wavelet levels used in the embedding process. The authentication string bits are extracted from DWT coefficients which are selected according to the same method used in embedding process after computing the adaptive threshold for each level. Another necessary procedure is to acquire the digital signature and watermark from the extracted data.

In addition to its dependency on the watermark extraction, the verification process is also depended on the extracted digest, the extracted digest is compared with the computed digest of the extracted watermark data before making the decision about the image authenticity.

The below algorithm is used to extract an authentication data and acquire the watermark and digital signature from the authenticated medical image. **Fig. 6** shows the extraction process flowchart.

ALGORITHM_4: Extraction & Verification Algorithm

```
Input: Authenticated Image $AI_{M x N}$ and Decryption Key $K_u$
Output: Watermark W, Digital Signature S, and Decision about image authenticity.
BEGIN:
Step1: Load the authenticated image.
Step2: Perform 2-level DWT for the input image.
Step3: For each level, do the following:
    i.   Compute the adaptive threshold $T_i$ according to the Algorithm_2:
    ii.  Sort the coefficients of i-level sub-bands (LHi, HLi, and HHi) in sequential manner as in
         the embedding process.
    iii. Find the coefficients which are its magnitude greater than the value of i-level threshold $T_i$.
                    | Coefficient Magnitude | > i-level Threshold.
    iv.  Extract the embedded bit from each coefficient which is satisfying the previous condition.
    v.   Create new string called Auth_S1 string that will receive the extracted bits.
    vi.  Insert the extracted bit in the Auth_S1 string. The extracted bits are inserted sequentially in
         the Auth_S1 string.
Step5: Do the following after extract all authentication bits from that coefficients which are
satisfying the stated condition.
    i.   Take the first 128-bits from Auth_S1 string and store in new string called S1 that is the
         extracted digital signature.
    ii.  Store the remaining bits from Auth_S1 string in new string called W1 that includes the
         extracted watermark W1.
    iii. Decrypt the extracted digital signature S1 using RSA algorithm with $K_u$ as decryption public
         key.
    iv.  Store the decrypted S1 in new string called D1 that is the extracted digest D1.
    v.   Compute the Digest value for the extracted watermark W1 using MD-5 algorithm
    vi.  Store the result digest in new string called D.
Step6: Decision if the image is authentic or unauthentic.
```

```
    i.  If $D=D1$ then the image is authentic and display the extracted watermark on the screen.
    ii. Else: Display error message "the medical image is unauthentic"; this means the medical
        image is either replaced or modified.
End.
```

The experimental results and performance analysis of the technique will be presented in the next section, we will apply the algorithm on some medical images with different sizes of authentication data and test the technique robustness through applying some attacks on the authenticated images.

5. EXPERIMENTAL RESULTS

In order to test the proposed algorithm, we will apply the algorithm on medical images for different medical cases with various characteristics. The medical images are selected because of the importance of the authentication process in the medical applications over Internet like tele-radiology, tele-surgery, and telemedicine. The images are captured using MRI technique with size of 512×512 and 8-bits gray level. Also, these medical images are present different textural characteristics, various percentage of homogeneous regions, edges, and details.

The algorithm is applied on all ten images but the results of four images only exhibited. **Fig. 7** shows the original medical images which are used in this experiment.

For the purpose of proving the effectiveness of the proposed algorithm, the authentication data (watermark and digital signature) is hidden in the ten medical images with three different sizes are: 400, 600, and 800 Bytes. The digital signature size is constant in each case that is 128-bits. **Fig. 8, 9,** and **10** show the original medical images and their watermarked versions with 400, 600, and 800 Bytes authentication data capacity, respectively.

As can be seen in **Fig. 8**, the original images are in upper row and the authenticated images are appeared in the lower row. The amount of degradation caused by the embedding of watermark and signature is very difficult to distinguish by the HVS and thus the fidelity of the medical image was not affected.

The main reason for this is due to exclude areas of important details and textures during the embedding of watermark data into the medical image (LL2) sub-band. Also, the amount of authentication data play main role in as this situation.

By contrast, the results images shown in **Fig. 9** display a tiny amount of degradation that it is possible to distinguish by the expert person. While the watermarked images shown in **Fig. 10** have significant amount (also acceptable) of degradation that can be denoted by the general humans. The reason for this is the large amount of watermark data that affect the reconstruction image process (inverse of wavelet) after the data is embedded.

As a result, the degradation in the reconstructed medical image increases when the amount of embedded data is increased. This also confirms the conflicting relationship between two factors are quality and capacity. Thus, there must be a tradeoff between these two factors to achieve the ideal solution to resolve the conflict.

This problem was relatively solved through defining the maximum authentication data that can be embedded in the algorithm by 800 bytes or 100 ASCII characters. This number seems enough in the text watermark length for using personal information or secret message as watermark data. The maximum number of embedded data can be updated in the algorithm code.

However, in any case the image degradation remains acceptable because the main image details (LL2 sub-band) is not affected by the algorithm in any case.

5.1 Image Fidelity Evaluation

In additional to above, the proposed algorithm is evaluated in terms of fidelity of digital image in numerical form for more accuracy. For that, two image quality metrics are used that are PSNR and SSIM. PSNR and SSIM metrics are computed using Eq. 2 and 3, respectively.

A larger PSNR and SSIM indicate that the authenticated image more closely resembles the original image, meaning that the algorithm makes the embedded data more imperceptible.

Table 2 shows the calculated results for ten authenticated medical images which are used in this experiment with three authentication data (400, 600, and 800 byte).

As shown in **Table 2**, as long as the size of embedding data is small the PSNR and SSIM metrics are high, hence the fidelity of the reconstructed images is high. These metrics are decreased as long as the watermark size is increased causing to affect the image fidelity. But even with 800 byte authentication data, the image quality is acceptable where the metrics remains relatively high.

Generally speaking, image with PSNR greater than 35 dB and SSIM closer to 1 is acceptable as HVS cannot distinguish the difference **Cox, et al, 2000, and T. Ahsan,** and **T. Mohammad, 2012**. Therefore, the suggested algorithm produces authenticated image with very much acceptable fidelity because the PSNR in all the tests with different authentication data sizes remains more than 35 dB and SSIM is very closer to 1.

In numerical form, for the suggested technique application on the ten selected images with 400 byte of authentication data the average of PSNR is 43.817 and the average of SSIM is 0.9142. With 600 byte the average of PSNR is 40.969 and the average of SSIM is 0.8759. While with 800 byte, the average of PSNR is 38.281 and the average of SSIM is 0.8227.

Fig. 11 and **12** shows the comparison of the PSNR and SSIM metrics respectively of the ten images after embedding the authentication data with 400 byte, 600 byte, and finally 800 byte capacity.

5.2 Tests of Tampering Detection

There are many ways to tamper the digital images that may be intended or unintended like noise adding, image cropping, resizing, compressing, blurring, filtering, cutting, contrast adjustment, objects insertion, etc. Therefore, for testing algorithm robustness and watermark fragility we will apply some of the tampers and attacks that cause to modifying or changing the digital images and then check the authenticity of the images by the watermark and digital signature means.

Fig. 13 shows the eight examples of attacked medical images which are previously authenticated by using the suggested technique with 400 bytes. Here, all medical images are unauthentic, because the attacks cause to changing the values of images pixels hence the DWT coefficients.

The similarity between the embedded and extracted watermark and digital signature is measured by the CWEP and CSEP using Eq. 4 and 5, respectively. CWEP and CSEP values equal one in the previous tests because the authenticated images are not geometrically processed or attacked. This means the embedded and extracted watermarks and signatures are identical demonstrating the watermark fragility. On the other side, when the authenticated image is attacked, the CWEP and CSEP metrics results are not equal one (just nearing to one) as shown in **Table 3**.

Table 3 shows the computed PSNR, CWEP and CSEP after applying many attacks on the authenticated images with 400 bytes. The images are unauthentic because the original and extracted watermark and signature aren't identical where CWEP and CSEP aren't equal one.

6. CONLUSIONS

An efficient digital images authentication scheme based on adaptive fragile watermark and MD-5 has been presented. The algorithm used middle and high DWT frequencies for watermark and digital signature embedding. This makes the watermark is invisible and fragile where the HVS can't distinguish the changing in images when embedding the watermark in the high frequencies.

Moreover, the algorithm can't only achieve image authentication purpose, but also achieves copyright protection and tamper detection purpose. For authentication purpose, the digital signature is computed for the watermark using MD-5 and RSA algorithms and embedded in the digital image.

Experimental results demonstrate that the proposed scheme can be used for copyright protection and tamper detection by the invisible fragile watermark. The main characteristics of our scheme are as follows. (1) The fragile watermark for image copyright protection is robust to many mild and maliciously attacks. (2) By employing adaptation of watermarking method, enhancing watermark security, distributing, and fragility. (4) The authenticity of medical image is improved through providing double methods for copyright protection and authentication through watermark and digital signature.

REFERENCES:

- Cox J., Miller M.L., Linnartz J.M., and Kalker T., 2000, *A Review of Watermarking Principles and Practices, in Digital Signal Processing for Multimedia Systems*, K.K. Parhi, T. Nishitani, eds., New York, Marcel Dekker, Inc. P 332.
- Chuanmu L. and Haiming S., 2008, *A Novel Watermarking Scheme for Image Authentication in DWT Domain*", IEEE Transactions on Image Processing, Vol. 5, No. 3, pp 122-129.
- Ali Al-Haj and Tuqa Manasrah. 2007, *Non-Invertible Copyright Protection of Digital Images Using DWT and SVD*, Springer, 2nd International Conference on Digital Information Management, ICDIM '07. Vol. 27, No. 13, 114–118.
- Wang Z., Alan C. B., Hamid R. H., and Ereo P. S, 2004, *Image Quality Assessment: From Error Visibility to Structural Similarity,* IEEE, Transactions on Image Processing, VOL. 13, NO. 4, PP. 600-612
- Rajendra B. P., Vinayaka k., Mysura B. R, 2012, *Biorthogonal Wavelet Transform Digital Image Watermarking,* Springer, Proceedings in 2nd Conference of Advanced Computer Security Techniques, Vol. 2 NO.3 PP. 1223- 1229.
- Mahavir D. and Jitendra K., 2014, *Digital Watermarking for Medical Images using Biorthogonal Wavelet Filters and Transformed Watermark Embedding,* International Journal of Advanced Computer Research, ISSN: 2249-7277 ISSN Vol. 4 NO. 2, PP. 2277-2284.
- Chang Gao, 2009, *Image Authentication Method Based On DWT In Color JPEG Images*, IEEE, International Conference on Environmental Science and Information Application, Vol. 1, No. 1, pp 70-80.

- O.Dumitru, M. Mitrea, and F. Prêteux, 2008, *Theoretical limits in DWT image and video watermarking*, Mathematics of Data/Image Pattern Recognition, Compression, and Encryption with Applications, SPIE, USA, Vol. 8, No. 5, pp 823-829.

- Cong J., Feng T. and Yru F., 2006, *Image Watermarking Based HVS Characteristic of Wavelet Transform*, IEEE, International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Vol. 11, No. 13, pp 660-668.

- Lu Z. M. and Sun S. H., 2009, *Digital Image Watermarking Technique Based on Vector Quantization*, Springer, 2nd International Conference on Information Security, Vol. 1, No. 2, pp 230-237.

- Tanveer A., and Tahseen M., 2012, *Digital Watermarking Based Image Authentication and Restoration by Quantization of Integer Wavelet Transform Coefficients*, IEEE/OSA/IAPR International Conference on Informatics, Electronics & Vision, Vol. 15, No. 27, pp 222-228.

- N. Grover and A. Mohapatra 2013, *Digital Image Authentication Model Based on Edge Adaptive Steganography*, Second International Conference on Advanced Computing, Networking and Security, PP 233 – 239.
- K. Raval and S. Zafar, 2013, *Digital Watermarking with Copyright Authentication for Image Communication*, International Conference on Intelligent Systems and Signal Processing (ISSP), Page(s):102-109.

- Yang, Hengfu and Sun, Xingming, 2007, *Semi-Fragile Watermarking for Image Authentication and Tamper Detection Using HVS Model*. Page(s):1112-1117.

- Chang, C.C, Tseng, H.W., 2004, *A Steganographic method for digital images using side match*, Pattern Recognition, vol. 25, pp.1431-1437.

- Po-Yueh Chen and Yue-chi Tseng, 2007, *A Study of DWT based steganography using Coefficient analysis*, pp.242-248.

- Sinha and K. Singh, 2003, *A technique for image encryption using digital signature," optics communications*, vol. 218, no.4, pp.229-234.

- Baisa L. Gunjal, Suresh N. 2012, *ROI Based Embedded Watermarking of Medical Images for Secured Communication in Telemedicine*, World Academy of Science, Engineering and Technology Vol: 6.

Table 1. Paper symbols and abbreviations

Symbol	Description
$\mathrm{I}_{\mathrm{M\ x\ N}}$	Digital image with M X N dimensions
$\mathrm{AI}_{\mathrm{M\ x\ N}}$	Authenticated image with M X N dimensions
W_{L}	Watermark data with L-bits length
W1	Extracted Watermark Data

D	Digest
D1	New Digest
S	Embedded Digital Signature
S1	Extracted Digital Signature
Auth_S	Embedded Authentication Data (concatenation of S and W)
Auth_S1	Extracted Authentication Data
C_{DWT}	Selected Hiding DWT Coefficients
ThF	Threshold Computation Function
T_i	Computed Threshold for i-level DWT
EmA	Embedding Algorithm
ExA	Extraction Algorithm
EA	Encryption Algorithm (RSA)
DA	Decryption Algorithm
RSA	Rivest-Shamir-Adleman Cryptosystem
MD-5	Message-digest algorithm
K_p	Sender Private Key
K_u	Receiver Public Key

Table 2. PSNR and SSIM metrics of three watermark capacity.

Authenticated images	**Auth. data Size=400 Bytes**		**Auth. data Size=600 Bytes**		**Auth. data Size=800 Bytes**	
	PSNR	**SSIM**	**PSNR**	**SSIM**	**PSNR**	**SSIM**
Image01	44.85	0.928	42.65	0.892	40.12	0.819
Image02	43.45	0.898	41.63	0.834	38.59	0.782
Image03	46.13	0.934	43.05	0.902	40.86	0.860
Image04	43.06	0.918	40.98	0.887	38.30	0.847
Image05	42.33	0.909	40.12	0.882	37.56	0.824
Image06	43.92	0.902	39.97	0.875	36.88	0.837
Image07	43.25	0.927	41.15	0.841	39.11	0.787
Image08	45.23	0.921	41.97	0.886	38.66	0.815
Image09	43.52	0.912	40.35	0.884	37.44	0.821
Image10	42.43	0.893	37.82	0.876	35.29	0.835

Table 3. PSNR, CWEP, and CSEP of attacked watermarked image**.**

Attack Type	**PSNR**	**CWEP**	**CSEP**
Gaussian Noise (5%)	18.5573	0.782	0.817
Salt & Pepper Noise (5%)	15.8391	0.804	0.771
Object Insertion	22.7751	0.865	0.870
Contrast Adjustment	23.8749	0.906	0.842
Image Sharpening	19.7101	0.868	0.905

JPEG Compression (70%)	21.0298	0.842	0.858
Region Cutting	17.9011	0.818	0.763
Image Blurring	22.0881	0.917	0.711

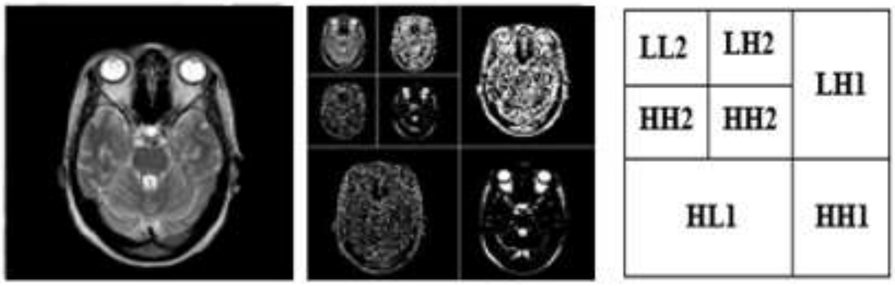


Figure 1. 2-level DWT decomposition.

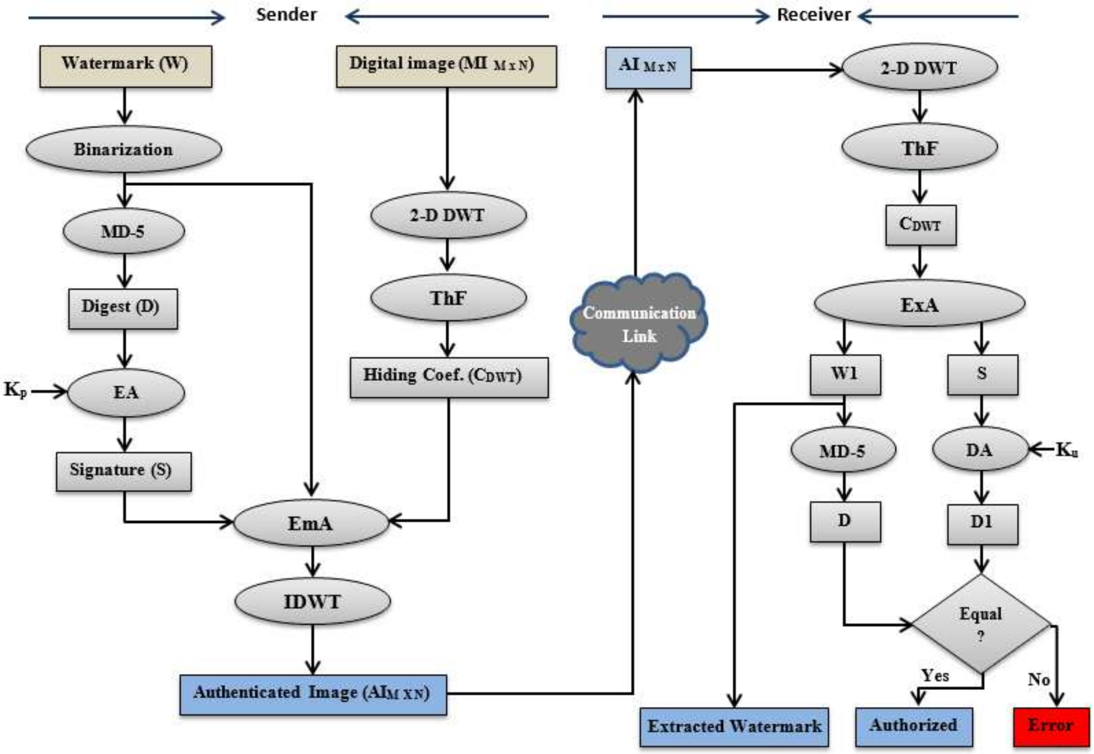


Figure 2. Proposed authentication model.

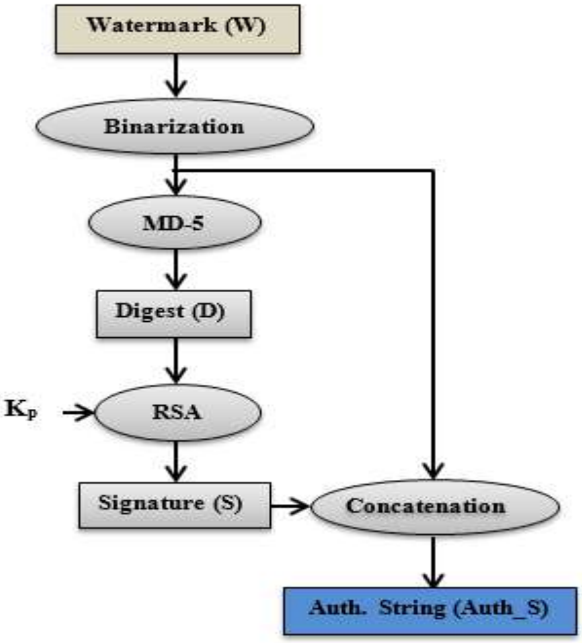


Figure 3. Authentication data generation algorithm.

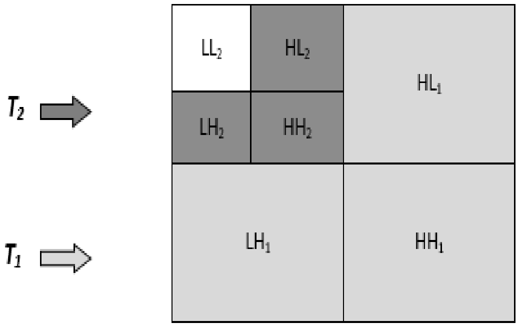


Figure 4. Adaptive thresholding.

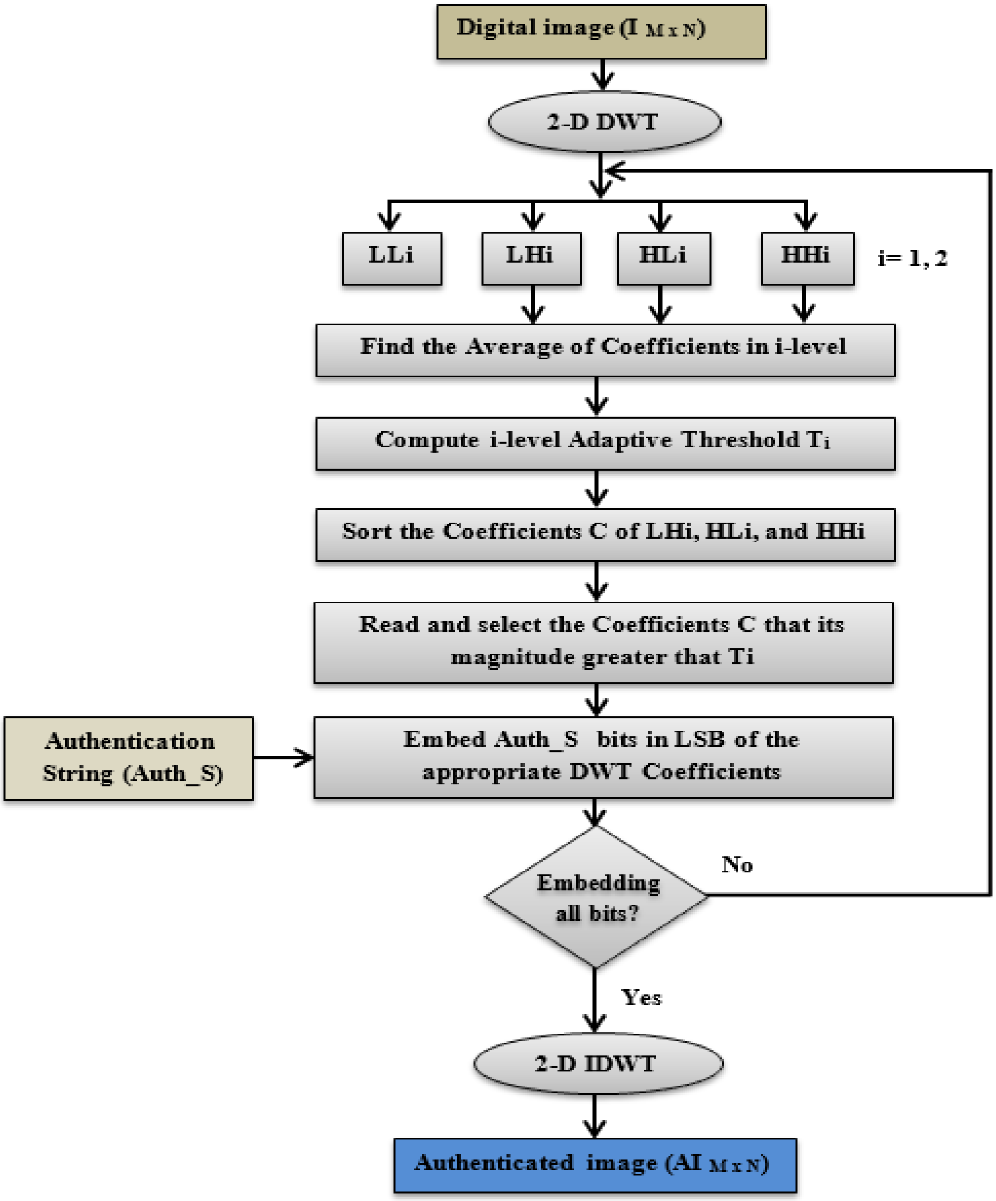

Digital image (I M x N)
2-D DWT
LLi
LHi
HLi
HHi
i= 1, 2
Find the Average of Coefficients in i-level
Compute i-level Adaptive Threshold Ti
Sort the Coefficients C of LHi, HLi, and HHi
Read and select the Coefficients C that its magnitude greater that Ti
Authentication String (Auth_S)
Embed Auth_S bits in LSB of the appropriate DWT Coefficients
Embedding all bits?
No
Yes
2-D IDWT
Authenticated image (AI M x N)

Figure 5. Watermark and digital signature embedding algorithm

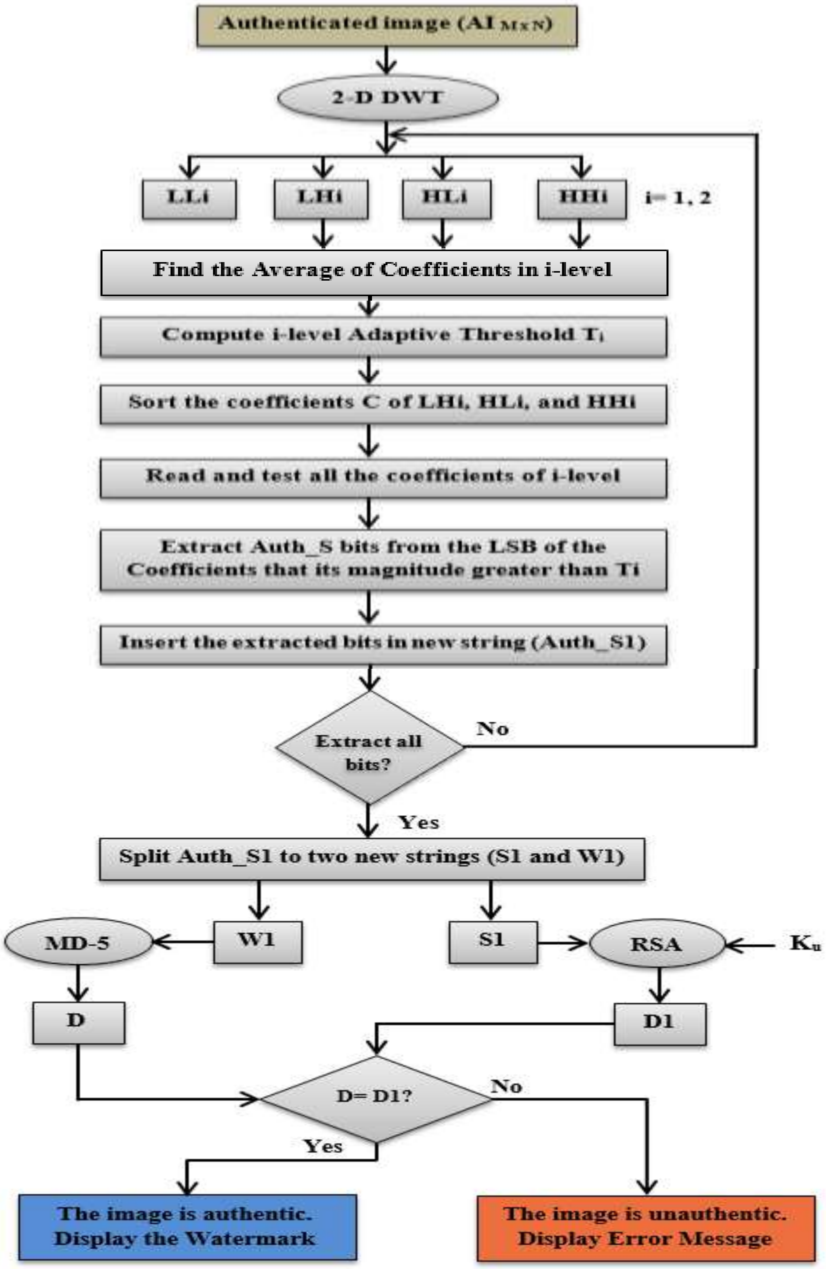

Authenticated image (AI M x N)
2-D DWT
LLi
LHi
HLi
HHi
i= 1, 2
Find the Average of Coefficients in i-level
Compute i-level Adaptive Threshold Ti
Sort the coefficients C of LHi, HLi, and HHi
Read and test all the coefficients of i-level
Extract Auth_S bits from the LSB of the Coefficients that its magnitude greater than Ti
Insert the extracted bits in new string (Auth_S1)
Extract all bits?
No
Yes
Split Auth_S1 to two new strings (S1 and W1)
MD-5
W1
S1
RSA
Ku
D
D1
D= D1?
No
Yes
The image is authentic. Display the Watermark
The image is unauthentic. Display Error Message

Figure 6. Extraction and verification algorithm.

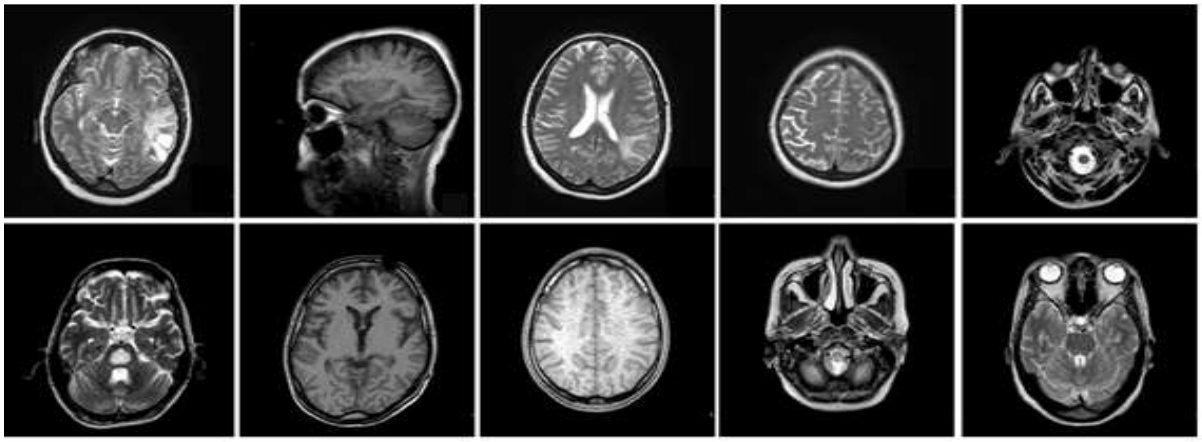


Figure 7: Test images used in the experience.

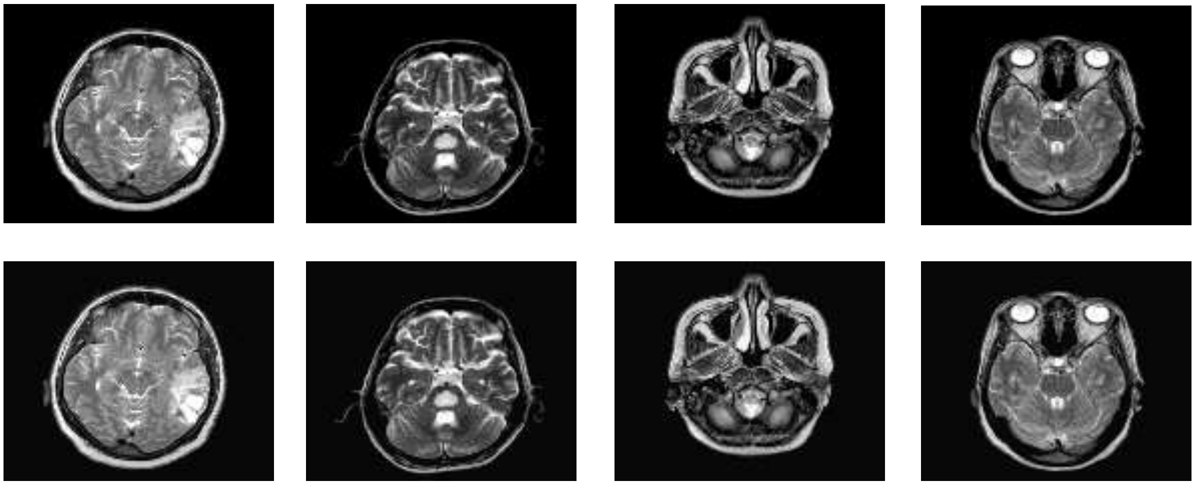


Figure 8 Test images with its authenticated versions (*Auth_S*= 400 Bytes).

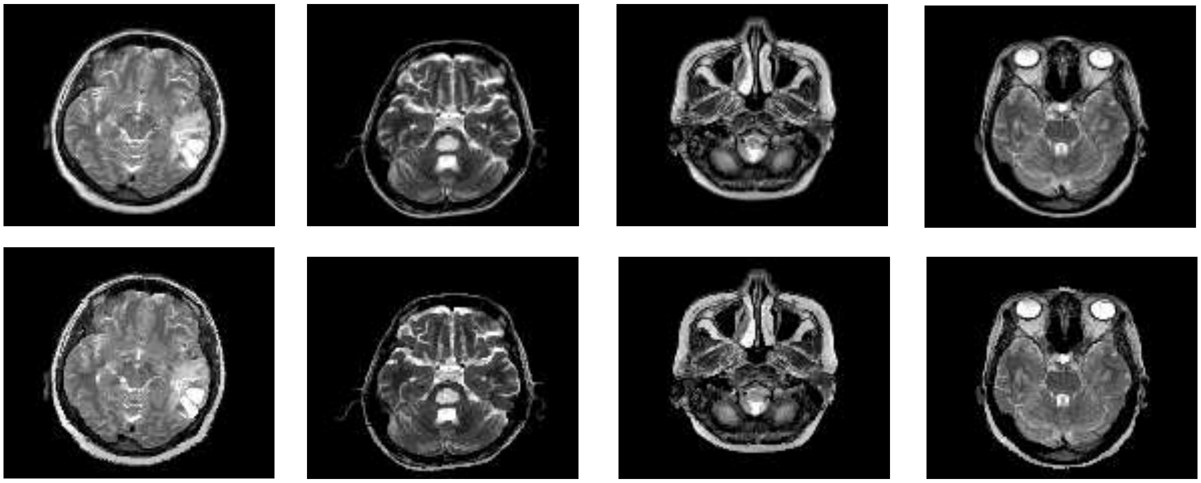


Figure 9 Test images with its authenticated versions (*Auth_S*= 600 Bytes).

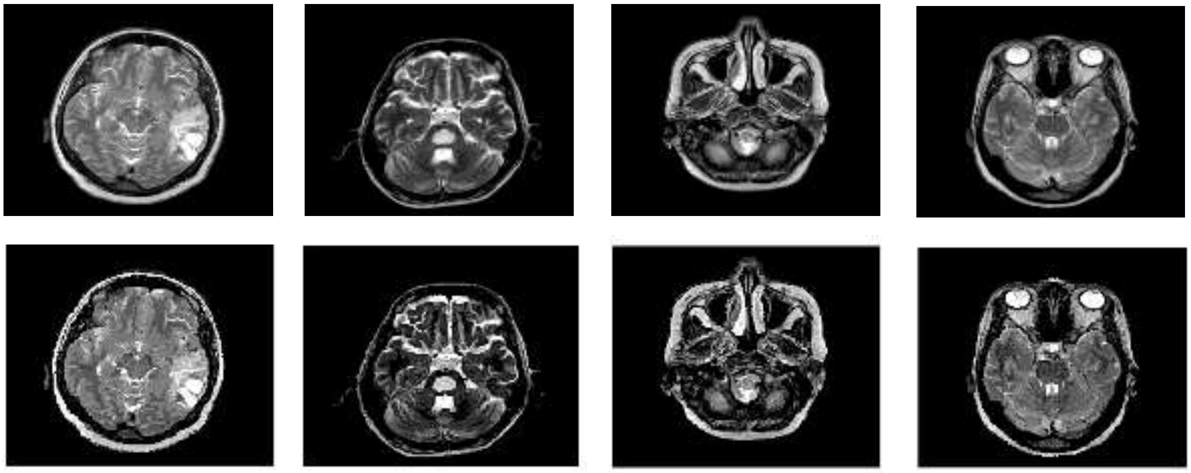
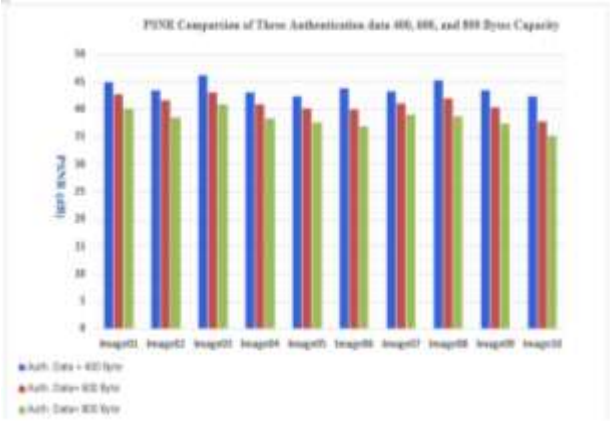


Figure 10 Test images with its authenticated versions (*Auth_S*= 800 Bytes).



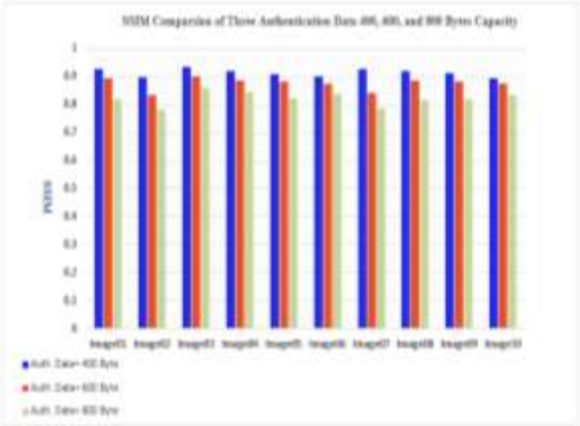
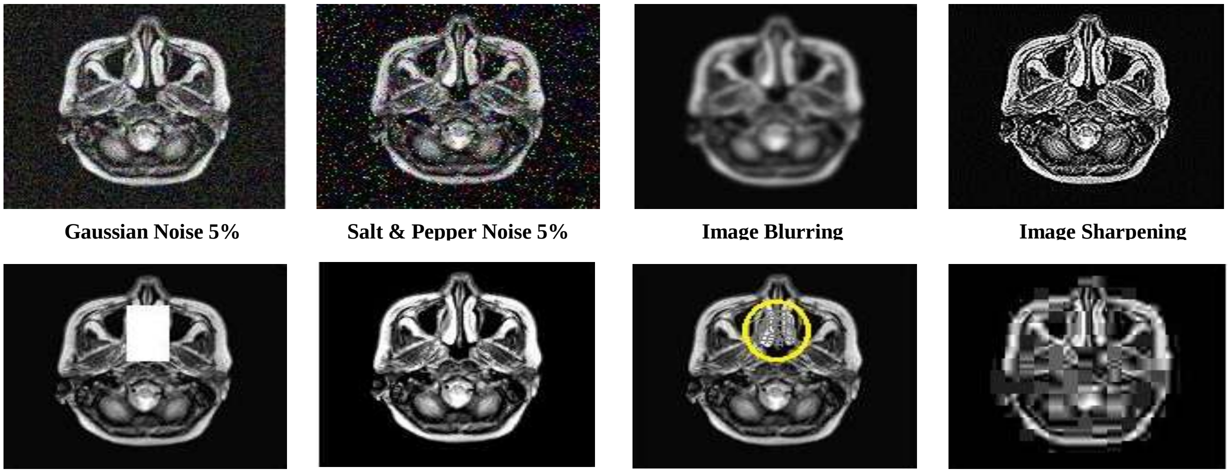


Figure 11. PSNR comparison of three Auth. data (400, 600, and 800 Byte)

Figure 12. SSIM comparison of three Auth. data (400, 600, and 800 Byte)



Gaussian Noise 5% **Salt & Pepper Noise 5%** **Image Blurring** **Image Sharpening**

Image Cutting **Contrast Adjustment** **Object Insertion** **JPEG Compression 70%**

Figure 13. Authenticated images after Sample Attacks.