Open Access **Baghdad Science Journal** **P-ISSN: 2078-8665**
2020, 17(1):178-189 **E-ISSN: 2411-7986**

DOI: http://dx.doi.org/10.21123/bsj.2020.17.1.0178

Mobile-based Telemedicine Application using SVD and F-XoR Watermarking for Medical Images

Hanaa Mohsin Ahmed

Received 21/11/2018, Accepted 11/6/2019, Published 1/3/2020

Abstract:

A medical- service platform is a mobile application through which patients are provided with doctor's diagnoses based on information gleaned from medical images. The content of these diagnostic results must not be illegitimately altered during transmission and must be returned to the correct patient. In this paper, we present a solution to these problems using blind, reversible, and fragile watermarking based on authentication of the host image. In our proposed algorithm, the binary version of the Bose_Chaudhuri_Hocquengham (BCH) code for patient medical report (PMR) and binary patient medical image (PMI) after fuzzy exclusive or (F-XoR) are used to produce the patient's unique mark using secret sharing schema (SSS). The patient's unique mark is used later as a watermark to be embedded into host PMI using blind watermarking-based singular value decomposition (SVD) algorithm. This is a new solution that we also proposed to applying SVD into a blind watermarking image. Our algorithm preserves PMI content authentication during the transmission and PMR ownership to the patient for subsequently transmitting associated diagnosis to the correct patient via a mobile telemedicine application. The performance of experimental results is high compare to previous results, uses recovered watermarks demonstrating promising results in the tamper detection metrics and self-recovery capability, with 30db PSNR, NC value is 0.99.

Key words: Authentication, Fragile watermarking, Ownership, Tamper detection, Telemedicine

Introduction:

Telemedicine using mobile devices offers ease of access to medical services as patients may obtain a diagnosis from medical staff sooner in the form of a Patient Medical Report (PMR) transmitted through a mobile network. Exchanging the patient medical image (PMI) and PMR between the patient and medical services introduces challenges, such as the integrity (PMR and preserving the content of PMI) and the time and cost of transmission. The watermarking technique is a solution to these problems. In this situation, PMR is embedded in PMI through a watermark resulting in much less bandwidth memory as normally required for transmission (1, 2, 3).

Watermarking techniques are classified, from the human perception point of view, as visibly or invisibly embedded information into either a cover data or via dual watermarking (4).

Department of computer science, University of Technology, Baghdad, Iraq.
*E-mail:110113@uotechnology.edu.iq
*ORCID ID: 0000-0002-8133-6512

Invisible watermarking prevents the PMR from being seen by unauthorised persons, and the techniques are categorised into fragile watermarking, semi-fragile watermarking, robust watermarking, and hybrid watermarking (2, 5, 6). Fragile watermarking prevents the PMI and PMR of patients from being changed by unauthorised people due to their sensitivity to modifications (6, 7). Fragile watermarking techniques are forthcoming utilising either a secret or public key to provide security (6). The watermark information (PMR and the binary version of PMI) is a binary format to be embedded into the pixel values of the PMI. This information is retrieved for medical image content authentication or patient integrity (8). The embedding methods are either spatial domain or frequency domain and use embedding operations such as AND, OR, XOR, and XNOR (7). The watermark information, in the spatial domain, is directly embedded into PMI pixels value, while in the transform domain it is embedded into the transform version of PMI. Opposed to frequency methods, spatial methods are sensitive to noise, fast Fourier Transform, and lossy compression attacks.

However, some of these methods are considered as fast, simple, of high capacity and immune to cropping attacks (2). Fragile watermarking techniques are either reversible or non-reversible, or blind or nonblind. The blind techniques do not need the original medical image (that's why it is suitable for mobile based telemedicine applications), and reversible techniques can produce the original (PMI and PMR) from the watermark cover (8, 9). The most important characteristics for these methods are the ability to recover without distortion of the actual PMI, and the tamper proofing added with authentication (8). The purpose of integrity and authentication of PMI and PMR in fragile watermark application is to find and localize a place of tampering (8,9). PMI authentication and recovery capabilities using fragile watermarking include watermark generation and embedding along with tamper localization and some of these methods have PMI self-recovery capabilities (6). Many researchers used secret sharing schema (SSS) (3) to increase tamper recovery capabilities, while others used Bose_Chaudhuri_Hocquengham (BCH) code (10) to increase error correction though it is time consuming. Advantages of medical images include saving both memory and bandwidth, detachment avoidance, security, and confidentiality. Requirements include imperceptibility, reversibility, integrity control, and authentication (8). In the methods that use reversible and authentication fragile watermarking schema, watermarked medical image evaluating matrices uses two benchmarking groups: imperceptibility of transmission PMI and robustness of watermark information (2,8).

My contributions in this paper for fragile based watermarking are: 1. Improving correction capabilities in transmission and block based medical images. 2. Increasing similarity between recovered watermark and host watermark. 3. Improving Fridrich and Goljan scheme. 4. Finding new scheme for SVD based blind watermarking.

In this research, a blind reversible fragile watermark is used for both PMI and PMR. The patient uses telemedicine to send his or her PMR and PMI to medical services using a mobile camera, which is used as input to self-embed fragile watermarking schemes like that adopted by Fridrich and Goljan (1) for applications of authentication and integrity verification. The proposed method includes improvements relating to using HCB and secret sharing, which deal with error correction in transmission and repair (PMI and PMR), as well as using fuzzy exclusive Or (F-XoR) and SVD embedding operations. With this process, PMR is extracted from authentic binary PMI. The proposed algorithm provides a new solution for applying SVD as the embedding operation for blind watermarking using SSS. Section 2 of this paper is concerned with preliminaries of secret sharing, reviewing Fridrich and Goljan's schema, and describing F-XoR and SVD. Section 3 then presents the proposed self-embedding schemes with an evaluating metric. Discussion is provided in Section 4, while Section 5 includes our conclusion and future work.

Literature Review

One of the most interesting algorithms used by the researchers is singular value decomposition (SVD), which is a numerical analysis algorithm developed for a variety of applications. From the viewpoint of image-processing applications, SVD includes two properties related to its singular value of an image: 1) stability when adding a small perturbation to an image and 2) intrinsic algebraic image properties (11, 12,13, 14). That's why SVD has been greatly used in watermarking for many applications (8,15,16). Based on SVD, many fragile watermarking schemes have been introduced in the last decades (2). Byun et al. proposed image authentication based on SVD using fragile watermarking scheme, in which the resulted binary authentication data after applying SVD is embedded into the least significant bits (LSBs) of original image (11). These methods can be further divided as tamper localized fragile watermarks and tamper localization and recovery (self-recovery). Zhang et al. proposed image authentication using a pixel based fragile watermarking scheme, in which SVD characteristics are used to generate the watermark. Arnold transform is applied to the watermark that is embedded in the LSBs of the original image for tamper detection capabilities (8). Dadkhah et al. presented an SVD based watermarking method for tamper detection and recovery, in which a mixed partitioning method for image blocks with size 2x2 and 4x4 is performed to enhance the detection precision of watermarking algorithm (12). Irshad et al. (6), introduced an SVD fragile watermarking algorithm to resolve two problems (safety and recovery) using 4x4 blocks and average value of 2x2 blocks for tamper location and self-recovery. Recent studies on medical image watermarking in telemedicine introduced reversible image watermarking, while others use Transform based image watermarking. Priya Selvam et al. (1) proposed a non-key blind and reversible hybrid transform watermarking scheme for telemedicine applications. For this scheme the watermark is embedded into host image using Integer Wavelet Transform and Discrete Gould Transform. Although this scheme provides high equality watermarking, it

has high computation complexity and low payload capacity. Falgun and Vinag (2) introduced a block based watermarking technique that uses both Discrete Wavelet Transform and SVD for telemedicine applications, in which two watermarks (hamming error correcting code of PMR and image) are embedded into the SVD-DWT of image region (3) of interest. The approach is robust under different signal processing attacks. (14) Sriti Thakur et al. introduced a scheme that uses hybrid transform (DWT, DCT, and SVD) image watermarking with chaotic encryption. Rajitha and shivendra (17) introduced DWT-SVD based self-authentication image scheme for telemedicine application. In this scheme the first phase is pre-processing, the second is self-authentication, and the final step is tamper detection.

Preliminaries

The following sub sections provide a brief explanation for the methods used by our proposed scheme.

Secret Sharing Technique (18)

The schema of Shamir's (*t*, *n*)-threshold describes a perfect (*t*, *n*)-threshold schema using Lagrange interpolation. This means that for any *t* different points, $(x_i, f(x_i))$, where $f(x)$] is a polynomial and has a degree below *t*. Hence, *f*(*x*) is determined by:

$$f(x) = \sum_{i=1}^{t} y_i \prod_{1<j\le t, i\neq j} \frac{x-x_j}{x_i-x_j}$$

(1)

The definition of Shamir's schema states that for a secret, $s \in \mathbb{Z}/p\,\mathbb{Z}$,using p as a prime number, the secret is set via equal a_0 and randomly choosing in $a_0, a_1 \dots, a_{t-1}$ in $\mathbb{Z}/p\,\mathbb{Z}$. The trusted party performs calculation, where:

$$f(x) = \sum_{k=0}^{t-1} a_k\, x^k,$$

(2)

for all $1 \le i \le n$. shares $(i, f(i))$ are allocated to *n* different parties. The secret is recovered from any *t* shares (*i*, *f*(*i*)), for $I \subset \{1, \dots, n\}$, and $s = a_0 = f(0)$, by:

$$s = f(0) = \sum_{i\in I}^{t} f(x_i) \prod_{j\in I, i\neq j}^{t} \frac{i}{j-i} mod p$$

(3)

Secret sharing schema (3, 6) as described in (18) is applied in the proposed scheme because secret sharing can recover tampered locations (errors in block-based medical images).

Fridrich and Goljan Schema

Fridrich and Goljan offered the original self-embedding-based fragile watermarking schemes for authentication applications with the single objective of embedding the compressed form of an image into the image itself. This is comprised of five components as shown in Fig.1. Block decomposition, watermarking generation, block mapping and watermark embedding, authentication and tamper location, and tampered region recovery (1,19).

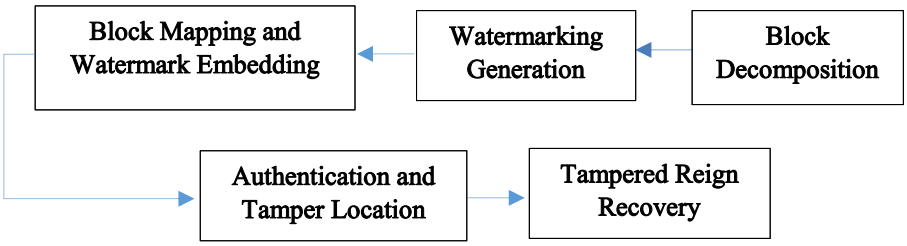


Figure 1. The Fridrich and Goljan Schema.

Fridrich and Goljan schema as described in (1) is applied to the proposed scheme with an improvement in the schema by encoding the compressed version of the original PMR with BCH (7, 4, 1) code before embedding the F-XoR into the binary PMI, which is capable of a correction error of one bit (18). Because this schema can have a compressed form of the original medical image embedded into the image itself, by applying the decompression operation to the deduced embedded image, the resulting original image is used for exact diagnosis by doctors.

F-XoR Operation (20, 21)

A fuzzy set *A* in *X*, where *X* is any set, is defined as:

$$\mu_A: X \to [0,1], \text{ where, } \mu_A = \begin{cases} 1 & x \in A \\ 0 & x \notin A \end{cases}, \quad (4)$$

For any fuzzy sets *A* and *B*, the fuzzy AND operation is defined as:

$$\mu_{A\cup B} = max\{\mu_A, \mu_B\}, \quad (5)$$

Fuzzy OR operation is defined as:

$$\mu_{A\cap B} = min\{\mu_A, \mu_B\}, \quad (6)$$

The fuzzy NOT operation is defined as:

$$\mu_{A^c} = 1 - \mu_A, \quad (7)$$

Then, the F-XoR operation is defined as:

$$\mu_{A\oplus B} = max\{min\{\mu_A, \mu_{B^c}\}, min\{\mu_{A^c}, \mu_B\}\}, \quad (8)$$

Where μ_{B^c} is fuzzy NOT operation that defined over set *B*.

F-XoR operation is used in proposed scheme to embed the secret message into the image as our contribution in this paper.

SVD

The method applies a decomposing function to the input PMI into one singular value matric which is a diagonal matric of size equals to MXN, and two orthonormal matrices known as left (U) with size of mXN, and right (V) with size of NXN such as (2):

$$PMI = USV^T \quad (9)$$

This method is used in the proposed scheme because of its singular values properties and capabilities that are related to embedding small perturbation into PMI that does not change singular value significantly, as it is immune to attack by transposition, flipping, translation, rotation. A new blind reversible SVD is presented in this paper with secret sharing and BCH.

The Proposed Method for Self-Embedding Schemes

The method shown in Fig.2. depends on the block based secret sharing authentication technique to PMR and PMI via the shares. The shares are used to carry several authentication indications, one for patient medical report Block (a_{PMRB})and two for patient medical image block(a_{MIB1}, a_{MIB2}), as well as to support and repair tampered data (using the other six shares for each 3x3 block size of PMI and 1x3 block size of PMR). This process uses the Fridrich and Goljan authentication schema with improvements by using the SVD, F-XoR operation for embedding and BCH (7,4,1). Our recommended method is implemented using MATLAB. The following blocks illustrate the framework of the proposed method. beginning with either a patient using the front mobile camera to take an image that is used later in a telemedicine application or an image from the selected dataset.

Block Decomposition: The binary version of the user's PMR, which is coded by HCB, into nonoverlapping blocks is divided, then converted into the greyscale component of the user's coloured PMI of size *N*x*N*, where *N* mod 3 is an equal positive integer such as *B*, into a binary image using the mean as a threshold value, and divided the resulting binary image into nonoverlapping blocks 3×3. The result after performing the next two steps over all PMI blocks is the StegoPMI (SPMI) of the greyscale component. The subscript *B* is used in this paper to indicate "Block."

Watermarking Generation: The PMR_B were F-XoR with the first line of binary PMI_B and the results of three bits are F-XoR to generate the authentication bit, a_{PMRB} , of PMR_B. The next two lines of binary PMI_B are F-XoR to generate two authentication bits of binary MI_B, one for each line as a_{MIB1} and a_{MIB2}. The resulting authentication bits are concatenated with their correspondence to represent 12 bits. For every three sets of four-bit words, to represent three decimal numbers, $D_i, i = 1, 2, 3$, these numbers are input to the Shamir function mod 7, which produces six shares, $S_j, j = 1, 2, 3, 4, 5, 6$ (each three decimal numbers input to BCH (7,4,1)). The nine resulting numbers $D_{\mathrm{i}}, S_{\mathrm{j}}, \mathrm{i} = 1, 2, 3$, and $\mathrm{j} = 1, 2, 3, 4, 5, 6$, represent the generated watermark block (GW_B). Fig.3. is an example of a GW_B for a PMI taken from the front camera of the mobile device.

Block Mapping and Watermark Embedding: We performed SVD on the previous results of GW_B, such that:

$$\mathrm{GW_B} = U_{\mathrm{GW_B}} S_{\mathrm{GW_B}} V^T_{\mathrm{GW_B}} \quad (10)$$

as well as on the previously used PMI_B, such that:

$$PMI_B = U_{\mathrm{PMI_B}} S_{\mathrm{PMI_B}} V^T_{\mathrm{PMI_B}} \quad (11)$$

We computed:

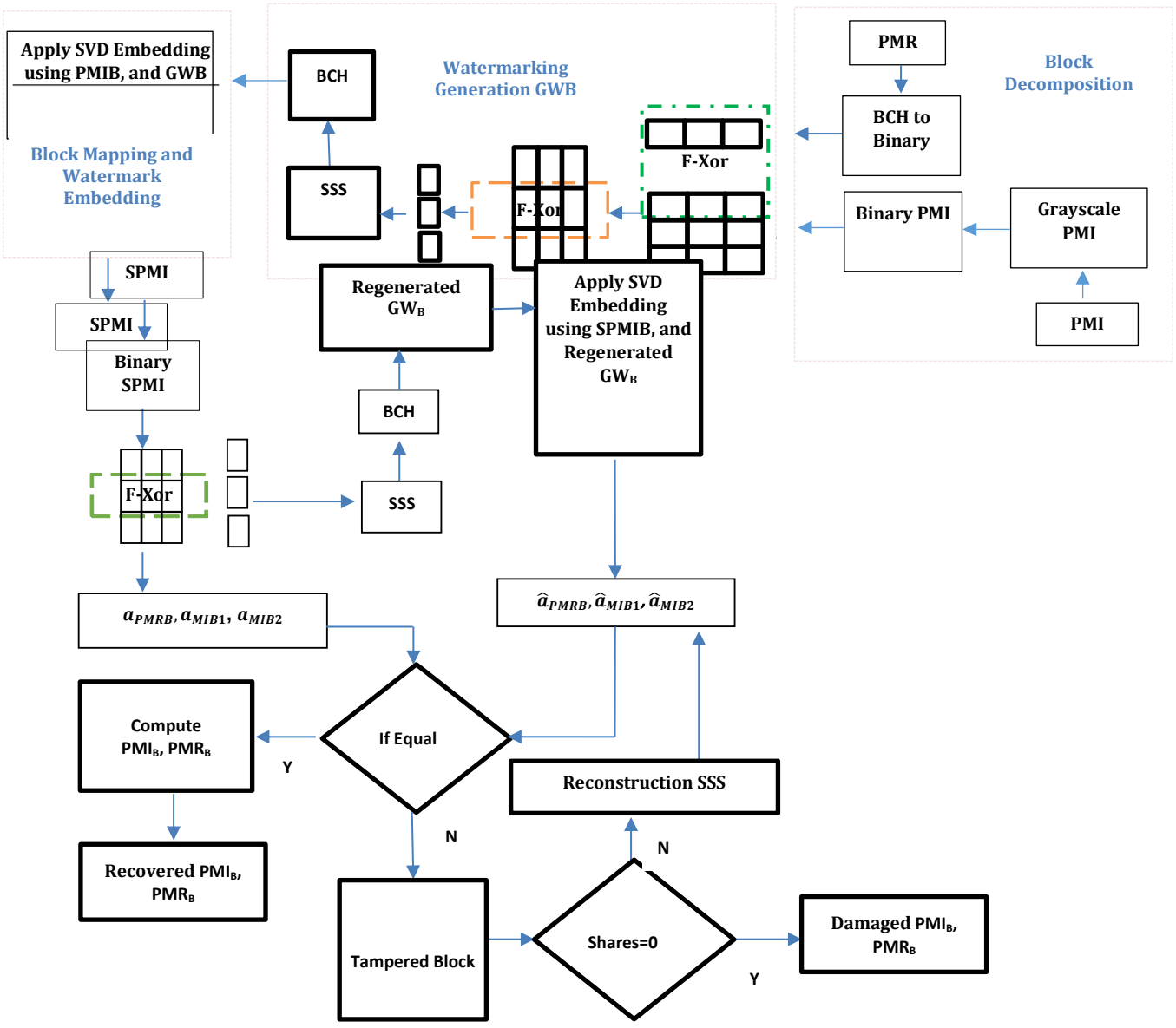
$$S_{\mathrm{PMI_B}}{}^{new} = S_{\mathrm{PMI_B}} + \left(k * S_{\mathrm{GW_B}}\right), \quad (12)$$

Where k is the strenghth scale, which equals 0.74and then computed

$$SPMI_B = U_{\mathrm{PMI_B}} S_{\mathrm{PMI_B}}{}^{new} V^T_{\mathrm{PMI_B}} \quad (13)$$

The result creates the blue component of the coloured $SPMI_B$ cover.

Baghdad Science Journal
P-ISSN: 2078-8665
E-ISSN: 2411-7986



B: Tamper detection and recovery

Figure 2(A,B). The proposed method.

The PMR_B is F-XoR with the first line of binary PMI_B	0 0 0 ↓ ↓ ↓
Results of three bits are F-XoR to generate the authentication bit, a_{PMRB} , of PMR_B	0 0 1 → a_{PMRB} =F-XoR (0, 0, 1) =1 1 1 0 0 0 0
The next two lines of binary PMI_B are F-XoR to generate two authentication bits of binary MI_B, one for each line, that is, a_{MIB1} and a_{MIB2}.	0 0 1 1 1 0 → a_{MIB1}=F-XoR (1, 1, 0)=0 0 0 0 → a_{MIB2}=F-XoR (0, 0, 0)=0
The resulting authentication bits are concatenated with their correspondence to represent 12 bits.	1 0 0 0 0 0 1 1 a_{PMRB} a_{MIB1} a_{MIB2}
For every three sets of four-bit words, to represent three decimal numbers, $D_i, i = 1, 2, 3$.	1 0 0 0 0 0 1 1 0 0 0 D_1=8 D_2=3 D_3=0
These numbers are input to the Shamir function mod 7	s d S_1 S_2 S_3 S_4 S_5 S_6 8 3 4 0 3 6 2 5 8 0 1 1 1 1 1 1 3 0 3 3 3 3 3 3
Six shares are produced, S_j, j = 1, 2, 3, 4, 5, 6	S_1 S_2 S_3 S_4 S_5 S_6 100 00 11 110 10 101 001 01 01 001 01 001 011 11 11 011 11 011
Each three decimal numbers input to BCH (7, 4, 1).	1000010 1100011 1110111 1100010 1110011 1101001 011 1000010 0011 0111 1100010 0011 1001 66 3 7 98 3 9
The nine resulting numbers (D_i, S_j, i = 1,2,3, and j = 1, 2, 3, 4, 5, 6) represent the generated watermark block GW_B.	8 3 0 66 3 7 98 3 9

Figure 3. Example of GW_B for a PMI from the front camera of the mobile device.

Authentication and Tamper Location: The blue component of the user's coloured SPMI is converted into a binary image using the mean as a threshold value and dividing the resulting binary image into nonoverlapping 3x3 blocks. The three lines of elements of binary SMI_B are F-XoR to generate three authentication bits of binary SMI_B, one for each line as a_{PMRB}, a_{MIB1}, and a_{MIB2}. The resulting authentication bits are re-concatenated with the correspondence to represent 12 bits. Every three sets of four-bit words represent three decimal numbers, $D_i, i = 1, 2, 3$. These numbers are input to the Shamir function mod 7, which produces six shares, $S_j, j = 1, 2, 3, 4, 5, 6$. Each of the three decimal numbers are input to BCH (7,4,1)). The nine resulting numbers ($D_i$and S_j) represent a re-generated watermark block GW_B. SVD is performed on the previous results of GW_B, such that:

$$GW_B = U_{\mathrm{GW_B}} S_{\mathrm{GW_B}} V^T_{\mathrm{GW_B}} \quad (14)$$

as well as on the previously used $SPMI_B$, such that:

$$SPMI_B = U_{S\mathrm{PMI_B}} S_{S\mathrm{PMI_B}} V^T_{S\mathrm{PMI_B}} \quad (15)$$

We also compute:

$$S_{\mathrm{SPMI_B}}{}^{new} = (S_{\mathrm{SPMI_B}} - S_{\mathrm{GW_B}})/k \text{ , where } k \text{ equals } 0.74, \quad (16)$$

then compute, $\hat{a}_{PMRB}, \hat{a}_{MIB1}$, and $\hat{a}_{MIB2}$ using the LSB of the first column. The difference between (a_{PMRB}, a_{MIB1}, and a_{MIB2}) and ($\hat{a}_{PMRB}, \hat{a}_{MIB1}$, and $\hat{a}_{MIB2}$) is localised as a tamper block. Otherwise, the block is authentic. Finally, we computed

$$PMI_B = U_{\mathrm{SPMI_B}} S_{\mathrm{SPMI_B}}{}^{new} V^T_{\mathrm{SPMI_B}} \quad (17)$$

which creates the blue component of the reconstructed coloured PMI_B image.

Tampered Reign Recovery: For each block that is indicated as a tampered location, we perform a reconstruction of the Shamir (3,6) threshold scheme, then recover the authentication signals $\hat{a}_{PMRB}, \hat{a}_{MIB1}$, and $\hat{a}_{MIB2}$. These are checked to see

if they match a_{PMRB}, a_{MIB1}, and a_{MIB2} . If not, then the same process is repeated for the other three hidden sheers. Until all the blocks are recovered, apply extraction using the F-XoR operation to separate the PMR from PMI; otherwise, the PMI and PMR are damaged.

Proposed Method Metric Evaluation and Discussion

To achieve its performance, the proposed algorithm is applied to a dataset selected from MedPixTM (22), as in Fig.4., and the others are from real volunteer patients consisting of ten pairs of PMIs and PMRs. Fig.5. shows ten pairs that represent dataset corresponding results (SPMI and recovered PMR) produced by the proposed method in noiseless environment. The evaluation metrics are used to evaluate image watermark, recovery metrics and image tampering. Image tampering can be in two types of attack (intentional, and unintentional), a number of which are used in this paper (white Gaussian noise, salt and paper noise, histogram equalization, median filtering, joint picture expert group (JPEG), scaling, and resizing). Finally, a comparison with some previous work using the famous Lena image is presented in this paper.

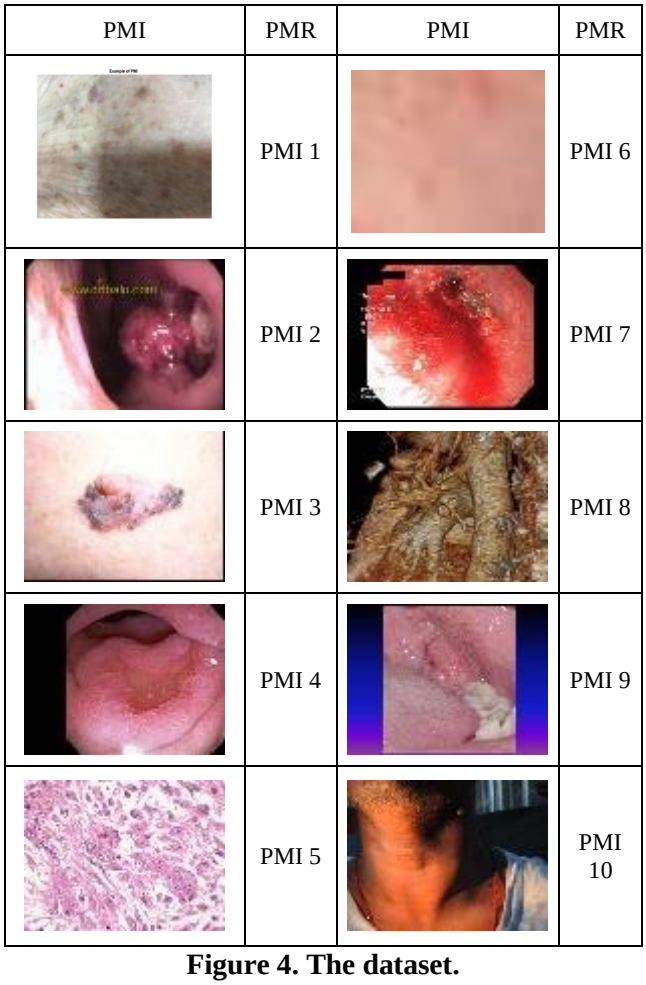


Figure 4. The dataset.

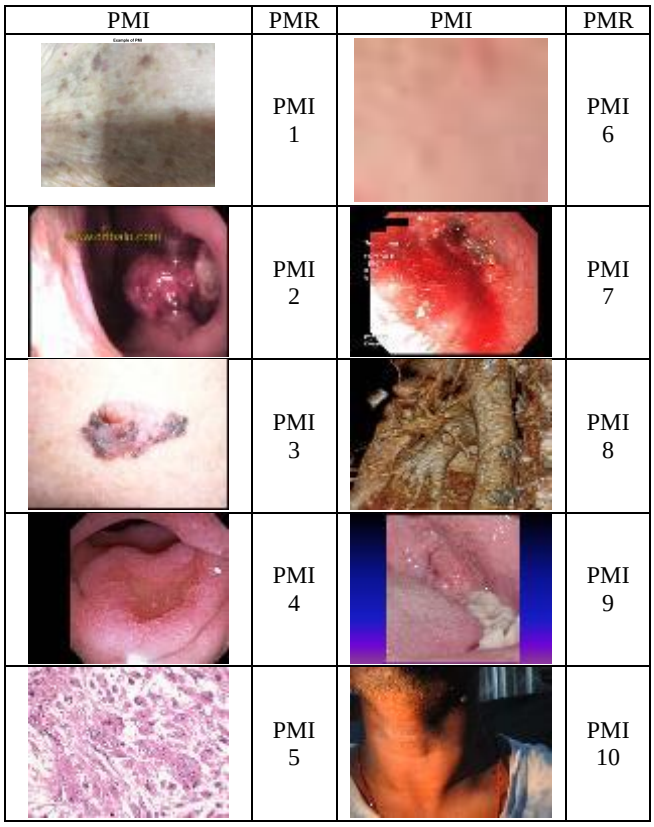


Figure 5. The dataset after applied proposed scheme.

Watermark and Recovery Metrics

Peak Signal-to-Noise Ratio (PSNR): The PSNR is an accepted measure of visual inspection and watermarking between any original image I of size $m \times n$ and its (watermarked/reconstructed) image I' of size $m \times n$ defined as (23):

$$PSNR = 10\, log_{10} \frac{255^2}{MSE}, MSE = \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} \left(I(i,j) - I'(i,j)\right)^2}{m \times n} \quad (18)$$

Normalised Correlation Coefficient (NC): The NC is an accepted measure of similarity between two images with value $W_{ij}, W'_{ij,}$ of image size $m \times n$ defined as (23):

$$NC = \frac{\sum_i \sum_j W_{ij} W'_{ij}}{m \times n} \quad (19)$$

If the watermark bit = 1, then the value of double is the values placed at position (i, j) of the image, which is otherwise set to –1.

Structural Similarity Index (SSI): The SSI is an accepted measure of similarity between two images, x and y (one being considered of perfect quality), defined as (23):

$$SSI(x,y) = [I(x,y)]^{\alpha} * [C(x,y)]^{\beta} [S(x,y)]^{\gamma}, \quad (20)$$

$$I(x,y) = \frac{2\mu_x * \mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1}, \quad (21)$$

$$C(x,y) = \frac{2\sigma_x * \mu\sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2}, \quad (22)$$

$$S(x,y) = \frac{2\sigma_{xy} + C_3}{\sigma_x + \sigma_x + C_3} \quad (23)$$

where $I(x,y), C(x,y),$ and $S(x,y)$ are luminance, contrast, and structure similarities, respectively, between the two images *x* and *y*, $\alpha, \beta, \gamma > 0$ are the mean of I and standard deviation, respectively, with weak denominator, C_3, where is (23):

$$C_3 = {C_2}/{2} \quad (24)$$

Tamper detection matric

For N blocks: The probability of false acceptance (PFA): The PFA is the probability of classifying a block as authentic when it is a tampered block and is defined as (17):

$$PFA = 1 - \frac{N_{td}}{N_t}, \quad (25)$$

The probability of false rejection (PFR): The PFR is the probability of classifying a block as tampered when it is a tampered block and is defined as (17):

$$PFR = 1 - \frac{N_{ad}}{(N-N_t)}, \quad (26)$$

The probability of false detection (PFD): The PFD is the probability of classifying a block as authentic when it is, in fact, a tampered block and is defined as (17):

$$PFD = \frac{N_t}{N} \times PFA + (1 - \frac{N_t}{N}) \times PFR, \quad (27)$$

where N is the number of blocks, N_t is the number of tampered blocks, N_{td} is the number of tampered blocks correctly detected and $N_{ad}$is the number of authentic blocks incorrectly detected.

Perceptual invisibility is the most significant metric for any fragile watermarking scheme to indicate its capabilities for image recovery. The results where the watermark recovered metric applied are listed in Table 1. The first column represents PSNR (dB) of the pairs of PMIs and its corresponding SPMI. The second column represents NC of the pairs of PMIs and its corresponding recovered PMI. The third column represents the SSI. The resulted values of PSN, NC, SSI indicate that the proposed scheme has a good capability for image recovery.

Fig.6. shows the PSNR change of different recovered PMI with tamper percentages (10,20,30,40,50) of PMIs. Fig.7. represents changes in FPR, FNR, and TDR for different tampered PMIs with respect to tampering percentage. The performance of proposed scheme is quite good under (30%) of tampering and satisfactory for (50%) of tampering.

The proposed algorithm was tested by several attacks experiments (e.g., white Gaussian noise, salt and paper noise, histogram equalization, median filtering, joint picture expert group (JPEG), scaling, and resizing) and the resulted values are shown in Table 2. It is clear that these attacks have some impact on SPMI. There will be little distortion after the SPMI is attacked, especially in the case of histogram equalization, rotation and Gauss noise of intensity (0.050) attacks. The value of PSNR will be bellow 30db, while where no attacks tack place, the value of PSNR will be approximately 50db. This points out that the proposed algorithm has good invisibility with very little distortion to SPMI.

Extracted watermark was compared with original watermark to deduce the NC value under the same set of attacks. From the results shown in Table 3, it can be noticed that NC values are very high, most of which are around 0.9. This means that there is some identicality between the original and extracted watermarks.

Salt and paper noise may occur in many stages of processing of image (e.g., cutting, decoding, or transmission). Table 3presents results of values of salt and paper noise attack. The NC value become very small when noise is 0.1, that is because salt and paper noise has an effect on embedded watermarks.

JPG images are usually used in image transmission because of reduced SPMI size. Fig.8. shows impact of compression rates of 30%, 50%, and 70% to the resulted value of NC. It can be seen that the value of NC decreases when the compression intensity increases, which affects the similarity between original watermark and extracted watermark.

Table 2 demonstrates the rapid change in the value of PSNR that corresponds to the histogram equalization and strong noise that attacks SPMI, even though in this case the extracted watermark information is close to original watermark, which indicates that the proposed algorithm has good robustness against common image processing attacks.

The proposed scheme is applied to the dataset and examined in two cases for tamper-detection metrics. The first case is a noiseless environment, where the tampered blocks are equal zero across the dataset, the average time needed for authentication is 0.965 seconds, and for embedding is 2.184 seconds. In the second case, the watermark image is tampered by a set of attacks, where the average time needed for authentication is 2.943 seconds and for embedding is 2.154 seconds.

In order to perform the comparison between proposed work with previous works ((14), and (17)), the proposed algorithm was applied to a public test image known as Lena image, and performs PSNR, and NC to deduce their value. Table 4, presents the values of resulted PSNR and NC, indicating that the proposed scheme has improvements as compared to previously describes schemes ((14), and (17)).

Table 1. Watermark recovered metric.

Evaluation Measures PMI	PSNR (dB)	NC	SSI
PMI 1	43.819	0.9954	0.996
PMI 2	43.797	0.9976	0.995
PMI 3	44.235	0.9964	0.992
PMI 4	44.116	0.9945	0.982
PMI 5	44.376	0.9919	0.931
PMI 6	44.178	0.9977	0.943
PMI 7	44.012	0.9946	0.982
PMI 8	43.772	0.9967	0.964
PMI 9	43.802	0.9917	0.902
PMI 10	44.236	0.9956	0.937

Table 2. PSNR under tamper attacks

Attack type		Image1 PSNR	Image2 PSNR	Image3 PSNR	Image4 PSNR	Image5 PSNR	Image6 PSNR	Image7 PSNR	Image8 PSNR	Image9 PSNR	Image10 PSNR
Gauss Noise	0.001	44.879	44.800	44.768	44.899	44.679	44.099	44.834	44.379	44.299	43.995
	0.005	42.997	43.097	42.559	42.695	42.999	42.091	42.009	42.349	41.994	42.917
	0.010	36.295	36.090	36.765	36.436	36.100	35.995	36.193	36.390	36.290	36.205
	0.050	25.116	25.116	25.116	25.116	25.116	25.116	25.116	25.116	25.116	25.116
Salt and paper	0.001	34.976	34.854	34.740	34.299	33.998	34.865	34.296	34.109	34.698	34.539
	0.005	31.678	31.009	30.650	31.676	31.038	31.629	31.778	31.699	31.630	30.998
	0.02	30.010	30.019	30.608	30.250	30.887	30.077	30.410	29.910	30.110	30.599
	0.1	23.865	23.788	22.999	23.757	23.792	23.045	23.786	23.911	23.700	23.642
Median filtering	3x3	32.852	33.791	33.564	32.992	33.3492	32.899	33.892	33.732	33.542	33.800
Rotation	45^0	24.233	24.005	24.853	24.940	24.291	24.780	24.110	24.198	24.112	23.933
Scaling	1/2	30.916	30.813	30.817	30.546	30.924	30.973	30.087	30.999	29.996	30.116
JPG compression	80%	35.297	35.263	35.261	35.864	34.998	35.643	35.643	35.277	35.232	35.284
Histogram equalization		24.635	24.673	24.622	24.693	24.613	24.815	24.015	24.009	23.695	24.930

Table 3. NC under tamper attacks

Attack type		Image1 NC	Image2 NC	Image3 NC	Image4 NC	Image5 NC	Image6 NC	Image7 NC	Image8 NC	Image9 NC	Image10 NC
Gauss Noise	0.001	1	1	0.9998	0.9993	1	1	1	1	0.9899	1
	0.005	0.9821	0.9811	0.9804	0.9657	0.9765	0.97821	0.9231	0.9729	0.9721	0.9077
	0.010	0.8761	0.8851	0.8761	0.8453	0.8543	0.8999	0.8822	0.87743	0.8061	0.8469
	0.050	0.8884	0.8954	0.8754	0.8934	0.8644	0.8943	0.8987	0.8804	0.8754	0.8765
Salt and paper	0.001	0.8074	0.8077	0.8173	0.8062	0.8099	0.8056	0.8176	0.8154	0.8059	0.8055
	0.005	0.9880	0.9668	0.9808	0.9084	0.9269	0.9188	0.9858	0.9898	0.9388	0.9188
	0.02	0.9654	0.9654	0.9654	0.9654	0.9654	0.9654	0.9654	0.9654	0.9654	0.9654
	0.1	0.9045	0.9060	0.9065	0.9015	0.9345	0.9095	0.9141	0.9035	0.9065	0.9042
Median filtering	3x3	0.7887	0.7859	0.7834	0.7821	0.7277	0.7067	0.7803	0.7819	0.7743	0.7234
Rotation	45^0	0.8676	0.8546	0.8663	0.8497	0.8487	0.8398	0.8469	0.8549	0.8740	0.8481
Scaling	1/2	0.9456	0.9432	0.9431	0.9402	0.9410	0.9486	0.9356	0.9064	0.9450	0.9326
JPG compression	80%	0.9515	0.9486	0.9105	0.9335	0.9025	0.9397	0.9609	0.9535	0.9155	0.9450
Histogram equalization		0.9866	0.9854	0.96354	0.9954	0.9564	0.9876	0.9054	0.9114	0.9488	0.9397

Table 4. PSNR and NC under tamper attacks for Lena image, [14], and [17]

Attack type		Proposed method		[14]		[17]	
		PSNR	NC	PSNR	NC	PSNR	NC
Gauss Noise	0.001	44.567	1	74.6099	1	54.567	1
	0.005	42.9654	0.9999	60.6305	0.9811	52.9654	0.9716
	0.010	36.564	0.9867	52.6099	0.8851	46.564	0.8431
	0.050	25.078	0.8954	44.6305	0.8654	35.278	0.8921
Salt and paper	0.001	34.898	0.9977	36.898	0.8077	44.856	0.8137
	0.005	31.865	0.9668	331.865	0.9608	41.965	0.9601
	0.02	30.004	0.9654	32.004	0.9654	40.614	0.9751
	0.1	23.754	0.9060	33.754	0.9168	32.700	0.9160
JPG compression	80%	35.263	0.9659	45.263	0.9469	435.233	0.9612

Baghdad Science Journal
P-ISSN: 2078-8665
E-ISSN: 2411-7986

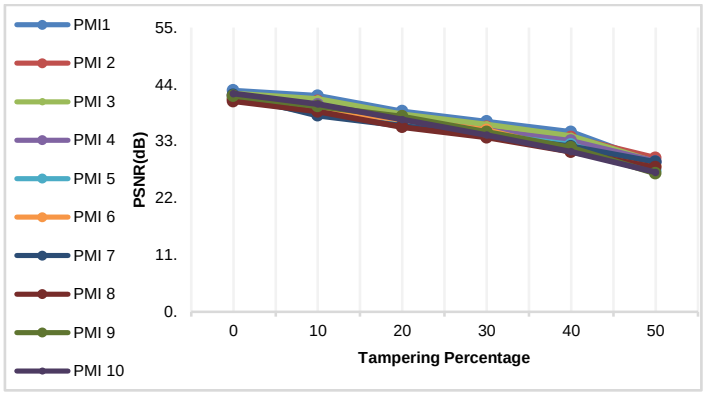
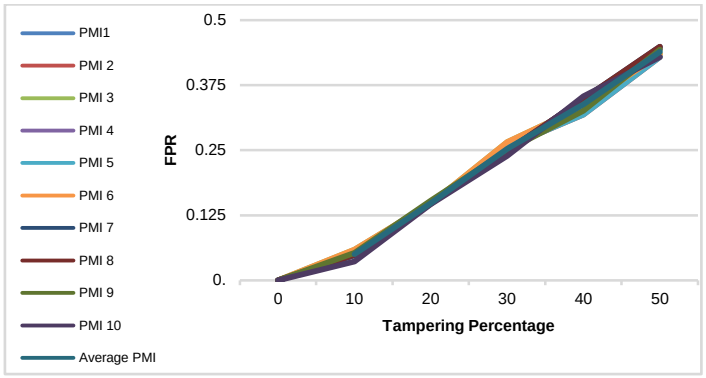
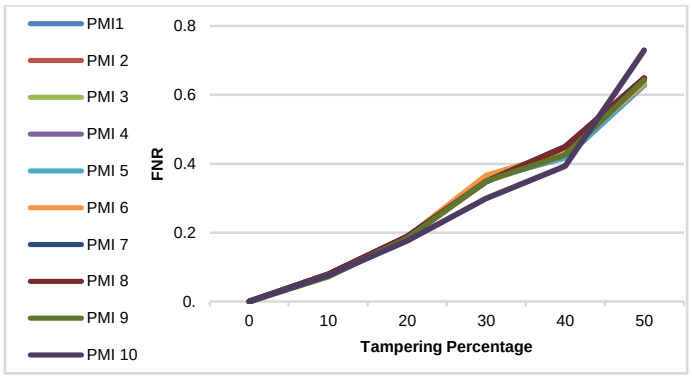


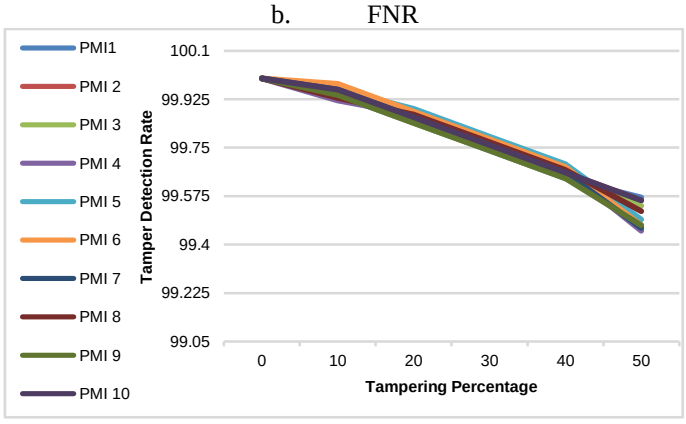
Figure 6. PSNR of different recovered PMIs with respect to the tampering percentage.



a. FPR



b. FNR



c. TDR

Figure 7. Change of a: FPR, b: FNR, c: TDR of tampered PMI with respect to tampering percentage.

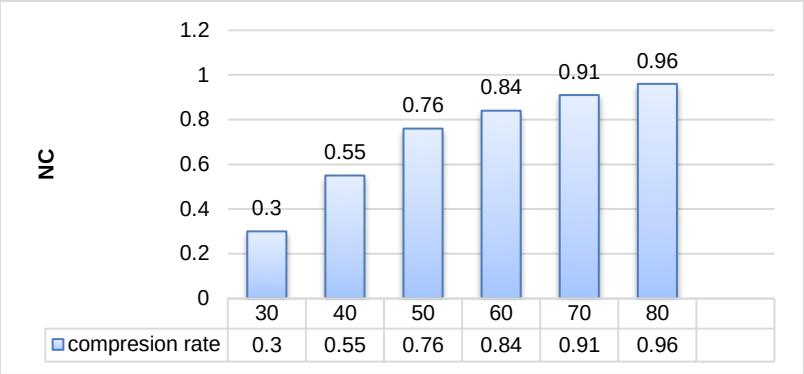


Figure 8. Impact of compression rates

Conclusions and Future Work

A watermarking algorithm is applied to mobile telemedicine with tamper detection and recovery capabilities. The proposed authentication algorithm uses the Fridrich and Goljan schema with additional capabilities to correct errors in one bit using BCH $(7, 4, 1)$ and correcting errors in a 3×3 block using SSS.

Our algorithm recovers the original PMI and proves the ownership of patients (e.g., it will send the diagnostic to the correct patient). The approach uses a combination of embedding methods; F-XoR embedding and SVD. It has been found that, as known, F-XoR restricts the modification of the cover image bits that are used for embedding watermark to half, and also BCH and SSS increases the capability of tamper correction hence it results in increasing the similarity between the host watermark and the reconstructed one. From previous embedding work using SVD, it can be observed that other methods use the original cover, while our method is blind based on SSS. The results demonstrate the immunity of the proposed method to the transmission noise.

Because H264 video coding is typically used to transmit from mobile devices and computers for real-time applications, our outlook is to study the application of the algorithm using H264 video coding and applicability to decrease size of block, which may affect the tampering dedication in future work.

Conflicts of Interest: None.

References:

1. Selvam P, Balachandran S, Iyer SP, Jayabal R. Hybrid transform based reversible watermarking technique for medical images in telemedicine applications. Optik. 2017 Sep 1;145:655-71.
2. Thakkar FN, Srivastava VK. A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications. MTAP. 2017 Feb 1;76(3):3669-97.
3. Ulutas M, Ulutas G, Nabiyev VV. Medical image security and EPR hiding using Shamir's secret sharing scheme. J Syst Software. 2011 Mar 1;84(3):341-53.
4. Inamdar VS, Rege PP. Dual watermarking technique with multiple biometric watermarks. Sadhana. 2014 Feb 1;39(1):3-26.
5. S Katzenbeisser, FA Petitcolas. Information hiding. Artech house; 2016.
6. Ansari IA, Pant M, Ahn CW. SVD based fragile watermarking scheme for tamper localization and self-recovery. IJMLC. 2016 Dec 1;7(6):1225-39.
7. Singh AK, Kumar B, Singh G, Mohan A, editors. Medical image watermarking: techniques and applications. Springer; 2017 Aug 11.
8. Zhang H, Wang C, Zhou X. Fragile watermarking for image authentication using the characteristic of SVD. Algorithms. 2017 Mar;10(1):27.
9. Parah SA, Bashir A, Manzoor M, Gulzar A, Firdous M, Loan NA, Sheikh JA. Secure and reversible data hiding scheme for healthcare system using magic rectangle and a new interpolation technique. InHealthcare Data Analytics and Management 2019 Jan 1 (pp. 267-309). Academic Press.
10. Liu Y, Hu M, Ma X, Zhao H. A new robust data hiding method for H. 264/AVC without intra-frame distortion drift. Neurocomputing. 2015 Mar 3;151:1076-85.
11. Byun SC, Lee SK, Tewfik AH, Ahn BH. A SVD-based fragile watermarking scheme for image authentication. InInternational Workshop on Digital Watermarking 2002 Nov 21 (170-178). Springer, Berlin, Heidelberg.
12. Dadkhah S, Manaf AA, Hori Y, Hassanien AE, Sadeghi S. An effective SVD-based image tampering detection and self-recovery using active watermarking. Signal Processing: Image Communication. 2014 Nov 1;29(10):1197-210.
13. Jia SL. A novel blind color images watermarking based on SVD. Optik-Int. J. Light Electron Opt. 2014 Jun 1;125(12):2868-74.
14. Thakur S, Singh AK, Ghrera SP, Elhoseny M. Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications. MTAP. 2019 Feb 1;78(3):3457-70.
15. Gao G, Wan X, Yao S, Cui Z, Zhou C, Sun X. Reversible data hiding with contrast enhancement and tamper localization for medical images. Info Sci. 2017 Apr 1;385:250-65.

16. Di Martino F, Sessa S. Fragile watermarking tamper detection with images compressed by fuzzy transform. Info Sci. 2012 Jul 15;195:62-90.
17. Bakthula R, Shivani S, Agarwal S. Self authenticating medical X-ray images for telemedicine applications. MTAP. 2018 Apr 1;77(7):8375-92.
18. Tian L, Zheng N, Xue J, Li C. Authentication and copyright protection watermarking scheme for H. 264 based on visual saliency and secret sharing. Multimed Tools Appl. 2015 May 1;74(9):2991-3011.
19. Fridrich J. Protection of digital images using self-embedding. InSymposium on Content Security and Data Hiding in Digital Media, New Jersey Institute of Technology, May 1999 1999.
20. Bedregal BC, Reiser RH, Dimuro GP. Xor-implications and E-implications: classes of fuzzy implications based on fuzzy Xor. ENTCS. 2009 Aug 4;247:5-18.
21. De Silva CW. Intelligent control: fuzzy logic applications. CRC press; 2018 May 2.
22. MedPixTM Medical Image Database, available at, last seen 21/3/2019 http://rad.usuhs.mil/medpix/medpix.htm
23. Zhang Z, Wu L, Xiao S, Gao S. Adaptive reversible image watermarking algorithm based on IWT and level set. EURASIP JASP. 2017 Dec;2017(1):15.

تطبيق التطبيب عن بعد على الهاتف المحمول باستخدام تحليل القيمة المفردة والحصري أو الغامض للصور الطبية

هناء محسن احمد

قسم علوم الحاسوب، الجامعة التكنولوجية، بغداد، العراق.

الخلاصة:

منصة الخدمات الطبية عبارة عن تطبيق متنقل يتم من خلاله تزويد المرضى بتشخيصات الأطباء بناءً على المعلومات المستقاة من الصور الطبية .يجب ألا يتم تبديل محتوى هذه النتائج التشخيصية بشكل غير قانوني أثناء النقل ويجب إعادته إلى المريض الصحيح. في هذه المقالة، نقدم حلاً لهذه المشكلات باستخدام علامة مائية عمياء وقابلة للانعكاس وهشة استنادًا إلى مصادقة صورة المضيف. في الخوارزمية المقترحة، يتم استخدام الإصدار الثنائي من ترميز بوس_شوهوري _هوكوينجهام (BCH)للتقرير الطبي للمريض (PMR) والصورة الطبية الثنائية للمريض (PMI) بعد استخدام الغامض الحصري أو (F-XoR) لإنتاج العلامة الفريدة للمريض باستخدام مخطط المشاركة السرية .(SSS) يتم استخدامه لاحقًا كعلامة مائية ليتم تضمينها في مضيف (PMI) باستخدام خوارزمية تحليل القيمة المفرد (SVD) العمياء القائمة على العلامة المائية. وهو حل جديد اقترحناه أيضًا بتطبيق SVD على صورة العلامة المائية العمياء. تحافظ الخوارزمية الخاصة بنا على مصادقة محتوى (PMI) أثناء النقل وملكية (PMR) للمريض لنقل التشخيص المصاحب فيما بعد إلى المريض الصحيح عبر تطبيق التطبيب عن بعد المحمول. يستخدم تقييم الخوارزمية لدينا علامات مائية مسترجعة توضح النتائج الواعدة لمقاييس الأداء العالية مقارنتا مع نتائج الاعمال السابقة في مقاييس الكشف عن التزوير وإمكانية الاسترداد الذاتي، مع قيمة 30NB PSNR، قيمة NC هي 0.99.

الكلمات المفتاحية: مصادقة، العلامات المائية الهشة، الملكية، كشف التزوير، التطبيب عن بعد.