ITC 4/50

Information Technology and Control
Vol. 50 / No. 4 / 2021
pp. 645-655
DOI 10.5755/j01.itc.50.4.28957

Cost-Effective Watermarking Scheme for Authentication of Digital Fundus Images in Healthcare Data Management

Received 2021/04/22 | Accepted after revision 2021/05/18

http://dx.doi.org/10.5755/j01.itc.50.4.28957

HOW TO CITE: Klington, A. G., Ramesh, K., Kadry, S. (2021). Cost-Effective Watermarking Scheme for Authentication of Digital Fundus Images in Healthcare Data Management. *Information Technology and Control*, 50(4), 645-655. https://doi.org/10.5755/j01.itc.50.4.28957

Cost-Effective Watermarking Scheme for Authentication of Digital Fundus Images in Healthcare Data Management

A. George Klington

Department of Computer Science and Engineering; St. Mother Theresa Engineering College, Thoothukudi, Tamil Nadu, India; e-mail: georgeklington@gmail.com

K. Ramesh

Department of Computer Applications; Anna University Tirunelveli, Tamilnadu, India; e-mail: rameshk7n@yahoo.co.in

Seifedine Kadry

Faculty of Applied Computing and Technology, Noroff University College, Kristiansand, Norway; e-mail: s.kadry@gmail.com

Corresponding author: georgeklington@gmail.com

This paper presents a cost-effective watermarking scheme for the authentication of healthcare data management. The digital fundus images are one particular class of medical images and it is widely used for screening mass population, identifying early symptoms of various diseases in healthcare. The mass volume of such data and its management requires an effective authentication scheme, while it is exchanged on an open network. The proposed scheme uses a watermarking technique to authenticate the digital fundus images. The watermark is generated concerning the portions of the original image using Singular value decomposition (SVD) and the remaining portions are used for embedding. The embedding process uses interleaving concepts across the red and blue planes of the original images to make the number of embedding as constant. The constant number of embedding is fixed for the original size of the given image to make the scheme as computationally cost-effective. The experiment showed the maximum capacity of the proposed scheme is 329960 bits for an image of size 565x584x3. It modifies 43% of the total number of embedded pixels against jittering attacks at an average. Comparative analysis showed that the proposed scheme uses only 1/3 of the original image size for embedding by retaining good imperceptibility of 54 dB. The net performance of the proposed scheme is found to be constant and it makes a scheme as cost-effective.

KEYWORDS: Digital Fundus Images, Healthcare Data Management, Singular Value Decomposition, Watermarking Scheme.

1. Introduction

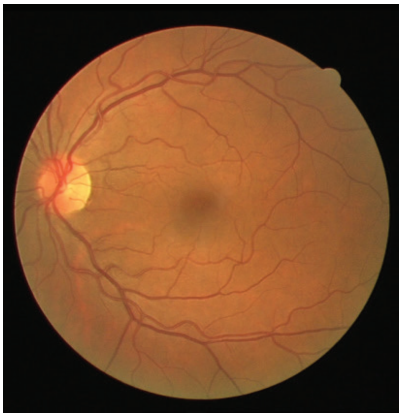
The Telemedicine is the latest health care practice that connects communication technologies and information systems to healthcare infrastructure. This integration facilitates remote consultation, remote diagnosis, online prescription of medicines, and remote guided surgery. It keeps and shares all the healthcare information in digital formats such as documents, audio, images, and videos through open networks. It opens the room for everyone to access the data easily and modify. This situation demands security schemes for two important tasks. They are authentication and ownership verification and content security [4,22]. The authentication and ownership verification ensures that received content is coming from the intended sender and it is received as sent by the sender. It verifies the owner of the content and integrity. The content security ensures that content is protected from the view of unauthorized users. Only authorized users can view the content. The watermarking schemes known for authentication and ownership verification and cryptography are known for content security [22-23].

The watermarking is effective in authentication and ownership verification of the digital contents that are being exchanged over insecure open networks. The watermarking involves two processes. Embedding is a first process done at the sender's side where information about the original content will be hidden inside the original content. This hidden information becomes secret data that is used to assess authentication and verification. The secret data may either be generated using original data or independent of original data based on the application. The output of the embedding process is embedded data that secret data inside the original data in an unseen manner. This embedded data will then be sent to the receiver. The extraction is the second process done on the receiver's side. The embedded data sent by the sender is received by the receiver and from this, the embedded secret data is being extracted with the knowledge of either original data or secret data. The extracted secret data will then be used for the assertion of authentication and verification

The medical images are one class of information widely used in healthcare where X-Rays, CT Scan Images, MRI Images, Fundus Images, and other modality of images are in use. These images are captured and exchanged for diagnosis purposes. Hence, the protection of such images in healthcare is challenging and essential. The fundus images are captured using a specialized fundus camera and used in the department of ophthalmology. The fundus is an interior surface of a human eye containing blood vessels, retina, and optical disks. These images are mainly employed in diagnosis for two reasons. To identify the early symptoms of diseases other than eye diseases and to identify eye issues. The sample fundus image is shown in Figure 1.

Figure 1

Sample Fundus Image (originally taken from Drive Grand Challenge data set)



The fundus images are exchanged for diagnosis purposes and any modifications done on the images for authentication and ownership verification need to be recovered after the process. Failing this, the diagnosis process becomes critical. Hence, a set of special requirements need to be devised for medical image watermarking. This paper proposes a cost-effective watermarking scheme fundus image by satisfying the special requirements of reversibility, imperceptibility, and fragility.

1.1. Requirements

As mentioned above, the fundus images impose special requirements for watermarking applications. The below given three requirements are considered in the work.

Reversibility: The reversibility refers to the restoration of original data at the embedding process after the extraction of secret data from it. The embedded secret data is for assertion and it is being embedded during the embedding process by modifying the original data. These modifications need to be recoverable. Therefore, the original data can be used for diagnosis after authentication and verification [28].

Imperceptibility: The imperceptibility refers to the capacity to which the embedded secret data is not producing any external artifacts on the original data. It means that secret data is hidden inside the original data in an unnoticeable manner.

Fragility: The fragility refers to the sensitiveness of the watermarking scheme against any kind of attack. If embedded data is attacked, it should change the hidden secret data to validate the authentication at the receiver side.

2. Related Works

Reversible Schemes: Error expansion is a key technique used in the reversible watermarking schemes where error between the original data and predicted data is expanded to insert the secret data. The literature showed that The Difference Expansion (DE), Interpolation Error Expansion (IEE), and Prediction-Error Expansion (PEE) are key techniques based on error expansion concepts [2, 3, 5-8, 10-14, 20, 21,]. The difference expansion technique takes the difference between two pixels of an image reference pixel and another neighbor pixel. The difference is expanded to insert secret data. Interpolation- Error Expansion technique uses the interpolation of two pixels and better estimation reduces the error in the interpolation and Prediction-Error Expansion technique uses different methods to predict the target value to reduce error and better prediction values reduce degradations [2, 3, 5-8, 10-14, 21]. The histogram shifting is another key technique in reversible watermarking. It takes a histogram of an image where the distribution of various pixels value in an image is obtained. The lowest distributed pixels are taken, emptied, and earmarked for reversibility. Then, the highest distributed pixel is taken and all the pixels between these highest and lowest distributed pixels are added by one to insert the secret data. Many works have been reported using histogram shifting concepts [9, 15, 16, 18, 27, 29, 34-38]. It is observed from the literature that prediction error expansion techniques are widely used in the reversible watermarking scheme [20].

Imperceptible Schemes: The imperceptibility needs to be incorporated during the embedding process. The embedding process should modify the original data in such a way that it should not create any external artifacts on original data. The embedding broadly has been done in two domains of an image spatial and transformed. The spatial domain methods use and modify the pixel values directly for embedding. The least significant bit (LSB) and spread spectrum and correlation are popular in the spatial domain. The transformed domain uses and changes the frequency values of the pixels for embedding. The popular methods are discrete cosine transforms (DCT), discrete wavelet transforms (DWT), discrete Fourier transform (DFT), singular value decomposition (SVD), and Karhunen-Loeve transform (KLT) [19, 30-32]. It is observed from the literature that imperceptibility is linked to the capacity (the size of secret data). The capacity of imperceptibility needs to be balanced [1].

Fragile Schemes: The fragile schemes are classified into two categories pixel-based and block-based. The pixel-based schemes embed the secret data into a pixel of an image whereas, in block-based, it embeds in a block of an image. During the attack, the pixel or block of an image is modified to validate the authentication process. The fragility can be extended to the recovery of original data from its corrupted version. It is observed from the literature that the fragility is linked to the capacity (size of secret data). The capacity and fragility need to be balanced [26]. It is also found that reversibility is linked to fragility and capacity. The reversibility limits the capacity for recovery and it affects the fragility. If all the pixels of an image are embedded with secret data, fragility will be improved. In case of any modification in embedded images will lead to changes in embedded secret data. However, it is an ideal case and the capacity, fragility, and reversibility to be balanced in real-time [28].

The review of the literature shows the reversibility, imperceptibility, and fragility are being addressed independently. Few works have combined these three requirements. In [23], the chaotic based watermarking scheme has been used for fundus images combining all above mentioned three requirements. In [33], the SVD based watermarking scheme is presented for fundus images combining all three requirements. In the context of cost-effectiveness, the scheme in [23] uses chaotic maps and it is time-consuming and requires much computation. The scheme in [33], computes SVD for all the pixels of an image and it requires much computation and timing requirements. Hence, this paper presents a cost-effective watermarking scheme for fundus image authentication and it satisfies the requirement of reversibility, imperceptibility, and fragility. The review of the literature revealed the tradeoff relationship between reversibility, imperceptibility, and fragility. The reversibility demands a fewer number of embedding and it will fail the fragility. The imperceptibility is good for fewer number of embedding and it is affected, when the number of embedding increases. Hence, the scheme needs to be optimized for better performance. The proposed scheme finds optimal capacity (number of watermark bits) to satisfy the reversibility, imperceptibility, and fragility.

3. The Proposed Scheme

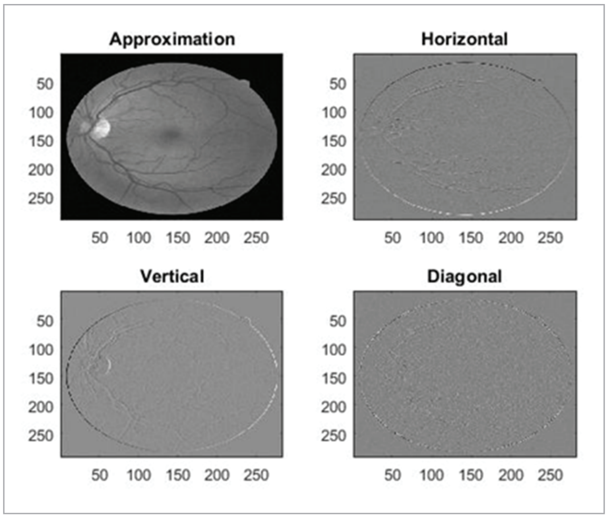
The proposed watermarking scheme uses discrete wavelet transformation and singular vector decomposition.

Discrete Wavelet Transformation: Discrete Wavelet Transform (DWT) is a multi-level transformation. It divides an image into four sub-bands LL, HL, LH, and HH in the first level where LL give approximation coefficients of an image. The LH, HL, and HH give detailed coefficients. The LH refers to Horizontal Information, HL refers to Vertical Information and HH refers to Diagonal Information. If the further level of decomposition is preferred, any one or more of the subbands in the first level is further divided into four bands. The sequence is continued until a preferred level is reached. The single-level wavelet decomposition of Figure 1 is shown as an example in Figure 2.

The wavelet transformation is a promising technique for image watermarking. It reduces computation time and memory requirements [33]. The Haar wavelet is a family of wavelet which is simple and easy to implement. It is reversible and requires fewer memory requirements for the computation. Since the proposed scheme is targeted for reversibility, the Haar Wavelet is used in the proposed scheme.

Figure 2

Single Level Wavelet Decomposition



Singular Value Decomposition: The singular value decomposition is an algebraic transform and it is recently employed in image processing for various applications such as rank approximations, orthogonal subspaces, image denoising, image compression, image authentication, and image forensics. A digital image I whose size is M x N is represented by SVD as follows.

$$[I]_M^N = [U]_M^M [S]_M^N [V^T]_N^N , \tag{1}$$

where $M \geq N$, $U = [u_1, u_2, u_3, ..u_m]$, $V = [v_1, v_2, v_3, ..v_n]$,

$$S = \begin{bmatrix} \sigma_1 & & & \\ & \sigma_2 & & \\ & & o & \\ & & & \sigma_n \end{bmatrix}.$$

The U and V are orthogonal matrixes whose size is MxM and NxN respectively. It represents the geometry of an original image I. The S is an MxN matrix whose diagonal elements represent singular values of an original image I. The U and V are singular vectors and S is a singular matrix. The singular matrix possesses luminance of an image concerning the pair of U and V. The singular values of an image consist of two properties. It will not affect the quality of an image if the singular values of an image change. It is up to some extent and small modifications of singular value will retain the quality of the original image. The stability of the singular values is naturally high [17]. Hence, the singular values will not be affected by the image processing attacks. The proposed scheme uses cover dependent watermark where the watermark is generated using the original image using SVD.

The Proposed Watermarking Scheme: The proposed watermarking scheme is explained using two algorithms embedding and extraction. The embedding algorithm works as follows.

3.1. The Embedding Algorithm

Step 1: Read the MxNxK Input Fundus Image (I) in the TIFF format. Where M is the number of rows, N is the number of columns and K is the number of planes. Read the Secret Data. The secret data is textual information about the input Fundus images. This is shown in Figure 3. This will be confidentially shared with the sender and receiver. It acts as a key in the process.

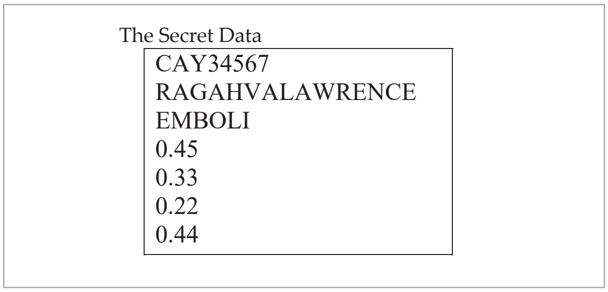
Step 2: Watermark Generation: Here, the watermark is generated using the original image and secret data using SVD as below.

2.1: Read the secret data file, convert the contents into a binary string. Refer to this as String 1.

2.2: Read the Green Plane of I.

2.3: Apply Wavelet Decomposition to this Green Plane at Single Level.

Figure 3
The Secret Data



The Secret Data

CAY34567
RAGAHVALAWRENCE
EMBOLI
0.45
0.33
0.22
0.44

2.4: Take the Approximate Component and divide it into 3x3 non-overlapping blocks.

2.5: Apply SVD for every block and takes the component S only.

2.6: Compare the list of S values and convert them into the binary string as below. Refer to this as String 2. If the current S value is in increasing order with respect to previous S value, then assign 1, else assign -0.

2.7: Equalize string 1 and string 2. Apply XOR between them to prepare the final string.

2.8: Replicate the final string into the length of MxN.

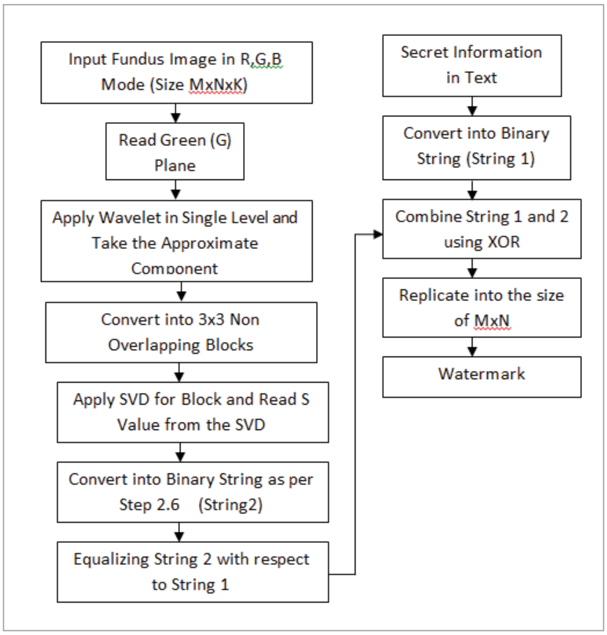
2.9: Rearrange the final binary string of length MxN in 2-D. This is the watermark is to be embedded inside the original image I. The watermark is generated with the blend of the original image and secret data. If the original or secret data is changed the watermark will change. This is facilitated by wavelet and SVD.

Step 3: The red and blue plane of I is taken for embedding. The odd-numbered rows of the red plane and even-numbered rows of the blue plane are taken. The watermark bits are embedded in the respective locations of the original image using the Least Significant Bit Embedding (LSB) method. The final image will be an embedded image and it is transferred to the receiver.

Step 4: When LSB is used in embedding, it changes pixels values of original images 50% after embedding. However, this will contract with the reversibility of the scheme. To retain reversibility, the locations of changes of original image pixel values after the embedding is shared as a location map along with the embedded image. The location maps are simple binary images in the size of the original image and it contains only two values 0 or 1. The one refers to the changes in the pixels LSB after embedding and zero refers to no changes after the embedding. The proposed watermarking generation steps are illustrated in Figure 4.

Figure 4

Proposed Watermark Generation


Input Fundus Image in R,G,B Mode (Size MxNxK)
Read Green (G) Plane
Apply Wavelet in Single Level and Take the Approximate Component
Convert into 3x3 Non Overlapping Blocks
Apply SVD for Block and Read S Value from the SVD
Convert into Binary String as per Step 2.6 (String2)
Equalizing String 2 with respect to String 1
Secret Information in Text
Convert into Binary String (String 1)
Combine String 1 and 2 using XOR
Replicate into the size of MxN
Watermark

3.2. The Extraction Algorithm

The extraction process is carried out at the receiving end. From the sender, the receiver receives an embedded image and location map. First, read the embedded image and extracts the Green Plane from it. Apply Step 2 of the embedding process and generate the watermark. This is a reference watermark to be used for validation of the authentication. Next, read the pixels of Red and Blue planes of the embedded image in the order of odd and even as discussed in the embedding process. Covert the pixels into binary and read the LSB and store its separate place. This is an extracted watermark [25]. The extracted watermark and reference watermark should be equal for successful authentication [24]. Failing which, the authentication process is failed. To bring back the actual original image after the extraction, the LSB of the pixels of red and blue planes are inverted, if the corresponding location map is 1.

Thus, the reversibility is achieved in the scheme. To make the scheme as fragile the Green plane is untouched in the process and it is used to generate watermark at embedding and extraction process. In case of any attacks, this process will generate two different watermarks to validate the authentication. At the same time, the Red and Blue Planes are also prone to attack. Here, the embedded watermark will vary from embedding to extraction to validate the authentication.

4. Results and Discussion

The experiment is conducted to analyze the proposed scheme performances quantitatively. An exclusive test bed of 1000 images of the sized 565x584x3 was collected from STARE and DRIVE databases [23]. The experiments were executed in MATLAB R2016b using an image processing toolbox. The peak to signal ratio (PSNR) is used as a metric in measuring Reversibility and Imperceptibility. When PSNR is taken between two images namely A and B, it refers to the number of pixels that are changed in B concerning A. Here A is considered as Clear Image, and B is considered as Noisy Image. Thus, the PSNR is used to measure the changes of B concerning its clean version (A). The PSNR is calculated as follows and it is represented in decibel (dB).

$$PSNR\ (A,B) = 10\log_{10}(\frac{MAX^{2}}{MSE}), \qquad (2)$$

where MAX refers to the maximum possible intensity value in the image. In our case, MAX=255 and the pixels are represented in unsigned 8-bit integer. MSE refers to the mean square error between A and B and it is calculated as follows:

$$MSE(A,B) = \frac{1}{mn}\sum_{i-0}^{m}\sum_{j=0}^{n}[A(i,j)-B(i,j)]^{2}. \qquad (3)$$

The higher PSNR values refer to the quality of the image is high. If MSE becomes 0 and PSNR becomes INF. It refers to the case where A and B are the same and this is used as a metric for measuring reversibility.

4.1. Reversibility Experiment

For the reversibility, the original image and extracted image are taken as A and B respectively. From the experiment, it is found that MSE(A, B) is 0. Thus, the proposed scheme is reversible. The LSB embedding is irreversible by nature. To make this as reversible, a location map is created in the same size as the original image in 2-D. It contains the binary data where 0 refers to no changes in the location after embedding and 1 refers to the changes in the location after embedding. This location map will also be shared with an embedded image. During extraction, the LSB of locations is inverted, if it is 1. Thereby, the proposed scheme brings back the original image without any loss. The LSB characteristics are shown in Table 2.

4.2. Imperceptibility Experiment

For the imperceptibility, the original image and embedded image are taken as A and B respectively. The PSNR(A, B) is taken for each plane and analyzed. The sample results are shown in Table 1. From the experiment, it is found that the Green plane is not modified since it is untouched for embedding. The Red and Blue planes are modified almost equally since the odd and even process of embedding. It is also observed from Table 1 that net modification done on the Red and Blue plane is nearly 45dB and it is constant overall images. The Odd and Even row concepts of the proposed scheme equally takes the number of pixels from the Red and Blue plane for embedding. The maximum difference of changes in the red and blue plane is 0.07 and it is negligible as shown in Figure 5.

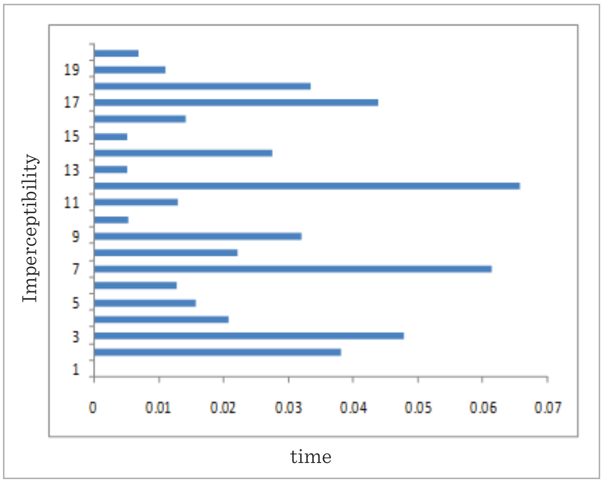
Table 1

Imperceptibility Results of the Proposed Scheme

Test Image	Red Plane	Green Plane	Blue Plane
Image 1	54.154	100	54.154
Image 2	54.1829	100	54.1449
Image 3	54.1689	100	54.2167
Image 4	54.1404	100	54.161
Image 5	54.1613	100	54.1457
Image 6	54.1447	100	54.1321
Image 7	54.1985	100	54.1371
Image 8	54.1488	100	54.1268
Image 9	54.1573	100	54.1254
Image 10	54.143	100	54.1378
Image 11	54.1487	100	54.1616
Image 12	54.176	100	54.1103
Image 13	54.1319	100	54.1269
Image 14	54.1285	100	54.1559
Image 15	54.1474	100	54.1424
Image 16	54.1564	100	54.1423
Image 17	54.1837	100	54.1399
Image 18	54.1869	100	54.1536
Image 19	54.1352	100	54.1242
Image 20	54.1509	100	54.1576

Figure 5

Imperceptibility - Difference of Changes between Red and Blue Plane



The net average PSNR for imperceptibility is 54dB and it is good enough to retain the original look of the image under normal vision condition. It is shown in Figure 6 where no external artifacts are found in the embedded image. However, this will vary, if the number of locations used for embedding is increasing and the watermark size is increased. The proposed scheme generates the watermark in the size of MxN (565x584 in our experiment) and it is constant. Hence, the imperceptibility of the proposed scheme is also constant. In addition to this, the proposed scheme uses LSB embedding and it brought 50% of changes in original image pixels as per its characteristics given in Table 2.

Table 2

Coalition game for the proposed model

Original LSB Value	Watermark Bit to be embedded	Original LSB After Embedding	LSB Changed from Original After Embedding
0	0	0	NO
0	1	0	YES
1	0	0	YES
1	1	1	NO

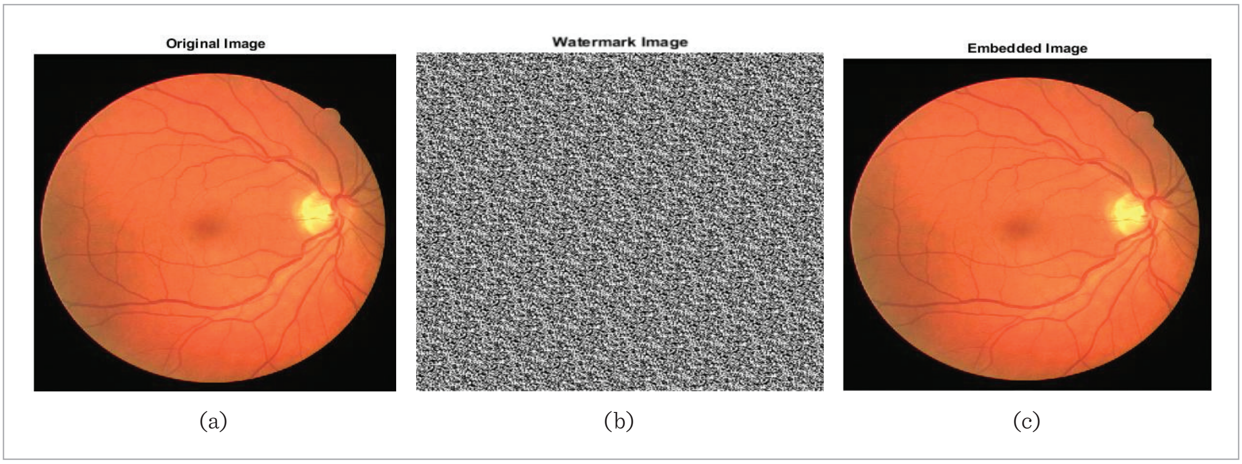
Table 3

Energy and security matrix representation using payoff in coalition game

Schemes / Parameters	Work in [2]	Work in [4]	Proposed Scheme
Reversibility	Reversible	Reversible	Reversible
Embedding Capacity (Size of the watermark)	30000 bits	989880 bits	329960 bits
Imperceptibility	60dB	26dB	54 dB
Fragility	20 %	48%	43%
Level of the Computational Complexity	High. Uses Chaotic Models and it is time-consuming.	High. Uses DWT in all the three planes to generate share images.	Low. It uses DWT only at Green Plane for Generating Watermark.
Cost-Effective	Achieves 20% of fragility at the size of 30000 bits.	Achieves 48% of fragility at the size of 989880 bits. This is achieved by using the entire image pixels for embedding.	Achieves 43% of fragility at the size of 329960 bits. It just uses 1/3 of the original image pixels for embedding.

Figure 6

a) Original Image (taken from Review of Optometry Data Set); b) Watermark Generated; c) Embedded Image



4.3. Fragility Experiment

For the fragility experiment, the jittering attack has been simulated on the embedded image in different scales ranging from 5% to 95% and a measured number of bits changed in the extraction process.

It is observed from the Table 3 that proposed scheme nearly changes 43% of original watermark bits against jittering attack. From Figure 7, it clearly is shown that the proposed scheme initially changes a higher number of pixels for the modifications from 5% to 20%,and later it stabilizes the changes around 150000 bits. Thereby, the proposed scheme changes 43% of original watermark bits against jittering attack at an average

4.4. Comparative Analysis

For the comparative analysis, the works in [23] and [33] are taken, since it is related to the proposed scheme and its requirements as listed in section 2. The detailed analysis is carried out using the same testbed as discussed above in this section. The details are summarized in the Table 3.

From the comparative analysis, it is found that the proposed scheme uses only 1/3 of the original image pixels for embedding and yields 43% of fragility against jittering attacks. Moreover, it uses only DWT at the green plane for embedding. The imperceptibility of the proposed scheme was found to be effective

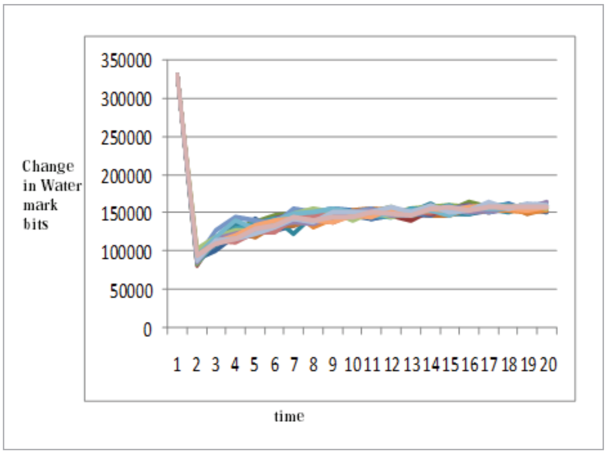
Table 4

Fragility of the Proposed Scheme against Jittering Attack

Test Image	Total Number of Watermark Bits	Average No. of Bits of Watermark Changed for 5% to 95%	Net Changes
Image 1	329960	139928.2	42
Image 2	329960	141420.5	43
Image 3	329960	145586.1	44
Image 4	329960	143107.2	43
Image 5	329960	142960.8	43
Image 6	329960	141659.5	43
Image 7	329960	143358.5	43
Image 8	329960	143895.9	44
Image 9	329960	143931.5	44
Image 10	329960	143665	44
Image 11	329960	143807.9	44
Image 12	329960	141628.1	43
Image 13	329960	147254.6	45
Image 14	329960	141740.2	43
Image 15	329960	144666.3	44
Image 16	329960	141369.7	43
Image 17	329960	145122.3	44
Image 18	329960	143241.4	43
Image 19	329960	142591.2	43
Image 20	329960	141818.8	43

Figure 7

Fragility of the proposed scheme - Number of watermark bits changes from 5% to 95% of Modifications



concerning the embedding capacity. The cost-effectiveness of the proposed scheme is measured in terms of the number of embedding required to keep the reversibility, imperceptibility, and fragility tradeoff. By nature, reversibility, imperceptibility and fragility are in trade-off and it can be optimized. The optimization may increase the overload. As in Table 4, the work in [23] is limited to the maximum watermark size of 30000 bits. When the number of bits is increased, the imperceptibility is decreased. The fragility rate achieved in the scheme is 20% and it is limited by the capacity of 30000 bits. The work in [33] improves the fragility to 48% and it uses all the pixels of the original image to achieve this. The proposed scheme optimizes the fragility to 43% by using one-third of the pixels of the original image for embedding. This 1/3 is constant for any size of the original images. The performance of the proposed scheme and existing schemes [23] and [33] are linearly dependent on the size of the original image. Thereby, the proposed scheme becomes computationally cost-effective compared with the schemes in [23] and [33].

5. Conclusion

This paper presents a cost-effective watermarking scheme for digital fundus images for authentication. The scheme generates the watermark using the original image and secret information. The green plane of the original image is used for generating watermark and it is untouched in embedding. The red and blue planes of the original image are used for embedding where odd rows taken from the red plane and even rows are taken from a blue plane. Thereby the proposed scheme used a constant number of pixels in the red and blue plane for embedding to make the process cost-effective. The green plane is used only for watermark generation at the embedding and extraction process. The experiment showed the maximum capacity of the proposed scheme is 329960 bits for an image of size 565x584x3. It modifies 43% of the total number of embedded pixels against jittering attacks at an average. Comparative analysis showed that the proposed scheme uses only 1/3 of the original image size for embedding by retaining good imperceptibility of 54 dB. Thereby, the proposed scheme outperforms the existing schemes in terms of cost-effectiveness.

References

1. Agarwal, N., Singh, A. K., Singh, P. K. Survey of Robust and Imperceptible Watermarking. Multimedia Tools, 2019, Appl 78, 8603-8633. https://doi.org/10.1007/s11042-018-7128-5

2. Alattar, A. M., Reversible Watermark Using Difference Expansion of Quads. In 2004 IEEE International Conference on Acoustics, Speech, and Signal Processing, 2004, 3, 377.

3. Alattar, A. M. Reversible Watermark Using the Difference Expansion of a Generalized Integer Transform. IEEE Transactions on Image Processing, 2004, 13(8), 1147-1156. https://doi.org/10.1109/TIP.2004.828418

4. Al-Haj, A., Abandah, G., and Hussein, N., Crypto-Based Algorithms for Secured Medical Image Transmission. IET Information Security, 2015, 9(6), 365-373. https://doi.org/10.1049/iet-ifs.2014.0245

5. Boato, G., Azzoni, M., Carli, M., Battisti, F., Egiazarian, K. O. Difference Expansion and Prediction for High Bit-Rate Reversible Data Hiding, Journal of Electronic Imaging, 2012, 21(3), 033013. https://doi.org/10.1117/1.JEI.21.3.033013

6. Caciula, I., Coltuc, D. Capacity Control of Reversible Watermarking by Two-Thresholds Embedding: Further Results. In International Symposium on Signals, Circuits and Systems ISSCS2013, 2013, 1-4. https://doi.org/10.1109/ISSCS.2013.6651230

7. Caciula, I., Coltuc, D. Capacity Control of Reversible Watermarking by Two-Thresholds Embedding. In 2012 IEEE International Workshop on Information Forensics and Security (WIFS), 2012, 223-227. https://doi.org/10.1109/WIFS.2012.6412653

8. Chrysochos, E., Varsaki, E. E., Fotopoulos, V., Skodras, A. N. High Capacity Reversible Data Hiding Using Overlapping Difference Expansion. In 2009 10th Workshop on Image Analysis for Multimedia Interactive Services, 2009, 121-124. https://doi.org/10.1109/WIAMIS.2009.5031447

9. Coatrieux, G., Pan, W. Cuppens-Boulahia, N., Cuppens, F., Roux, C. Reversible Watermarking Based on Invariant Image Classification and Dynamic Histogram Shifting. IEEE Transactions on Information Forensics and Security, 2012, 8(1), 111-120. https://doi.org/10.1109/TIFS.2012.2224108

10. Coltuc, D., Tudoroiu, A. Multibit Versus Multilevel Embedding in High Capacity Difference Expansion Reversible Watermarking. In 2012 Proceedings of the 20th European Signal Processing Conference (EUSIPCO) 1791-1795.

11. Coltuc, D. Improved Embedding for Prediction-Based Reversible Watermarking. IEEE Transactions on Information Forensics and Security, 2011, 6(3), 873-882. https://doi.org/10.1109/TIFS.2011.2145372

12. Dragoi, C., Coltuc, D. Improved Rhombus Interpolation for Reversible Watermarking by Difference Expansion. In 2012 Proceedings of the 20th European Signal Processing Conference (EUSIPCO), 2012, 1688-1692.

13. Dragoi, I. C., Coltuc, D. Adaptive Pairing Reversible Watermarking. IEEE Transactions on Image Processing, 2016, 25(5), 2420-2422. https://doi.org/10.1109/TIP.2016.2549458

14. Dragoi, I. C., Coltuc, D. Local-Prediction-Based Difference Expansion Reversible Watermarking. IEEE Transactions on Image Processing, 2014, 23(4), 1779-1790. https://doi.org/10.1109/TIP.2014.2307482

15. Fujiyoshi, M. A Histogram Shifting-Based Blind Reversible Data Hiding Method with a Histogram Peak Estimator. In 2012 International Symposium on Communications and Information Technologies (ISCIT), 2012, 313-318. https://doi.org/10.1109/ISCIT.2012.6380913

16. Huang, L. C., Tseng, L. Y., Hwang, M. S. A Reversible Data Hiding Method by Histogram Shifting in High Quality Medical Images. Journal of Systems and Software, 2013, 86(3), 716-727. https://doi.org/10.1016/j.jss.2012.11.024

17. Kaliappan, M., Mariappan, E., Prakash, M. V., Paramasivan, B. Load Balanced Clustering Technique in MANET Using Genetic Algorithms. Defence Science Journal, 2016, 66(3). https://doi.org/10.14429/dsj.66.9205

18. Khan, A., Malik, S. A. A High Capacity Reversible Watermarking Approach for Authenticating Images: Exploiting Down-Sampling, Histogram Processing, and Block Selection. Information Sciences, 2014, 256, 162-183. https://doi.org/10.1016/j.ins.2013.07.035

19. Kulkarni, A. S, Lokhande, S. S. Imperceptible and Robust Digital Image Watermarking Techniques in Frequency Domain. International Journal of Computer Technology and Electronics Engineering, 2017, 3, 33-36.

20. Menendez-Ortiz, A., Feregrino-Uribe, C., Hasimoto-Beltran, R., Garcia-Hernandez, J. J. A Survey on Reversible Watermarking for Multimedia Content: A Robust-

ness Overview. IEEE Access, 2019, 7, 132662-132681. https://doi.org/10.1109/ACCESS.2019.2940972

21. Naheed, T., Usman, I., Dar, A. Lossless Data Hiding Using Optimized Interpolation Error Expansion. In 2011 Frontiers of Information Technology, 2011, 281-286. https://doi.org/10.1109/FIT.2011.59
22. Poonkuntran, S., Rajesh, R. S., Eswaran, P. Analysis of Difference Expanding Method for Medical Image Watermarking. In International Symposium on Computing, Communication, and Control, 2011, 1, 31-34.
23. Poonkuntran, S., Rajesh, R. S. Chaotic Model-Based Semi Fragile Watermarking Using Integer Transforms for Digital Fundus Image Authentication. Multimedia Tools and Applications, 2014, 68, 79-93. https://doi.org/10.1007/s11042-012-1227-5
24. Pradeepa, S., Manjula, K. R., Vimal, S., Khan, M. S., Chilamkurti, N., Luhach, A. K. DRFS: Detecting Risk Factor of Stroke Disease from Social Media Using Machine Learning Techniques, Neural Processing Letters, 2020, 1-19. https://doi.org/10.1007/s11063-020-10279-8
25. Pradeepa, S., Manjula, K. R., Vimal, S., Khan, M. S., Chilamkurti, N., Luhach, A. K. DRFS, Detecting Risk Factor of Stroke Disease from Social Media Using Machine Learning Techniques. Neural Processing Letters, 2020, 1-19. https://doi.org/10.1007/s11063-020-10279-8
26. Rakhmawati, L., Wirawan, W., Suwadi, S. A Recent Survey of Self-Embedding Fragile Watermarking Scheme for Image Authentication with Recovery Capability. Journal of Image Video Processing, 2019, 61. https://doi.org/10.1186/s13640-019-0462-3
27. Sachnev, V., Kim, H. J., Suresh, S., Shi, Y. Q. Reversible Watermarking Algorithm with Distortion Compensation, EURASIP Journal on Advances in Signal Processing, 2010, 1-12. https://doi.org/10.1155/2010/316820
28. Shanmugam, P., Jayaprakasam, M. Integer Transform-Based Watermarking Scheme for Authentication of Digital Fundus Images in Medical Science: An Application to Medical Image Authentication. In Handbook of Research on Multimedia Cyber Security, 2020, 114-145. https://doi.org/10.4018/978-1-7998-2701-6.ch006
29. Shin, S. Y., Yoo, H. M., Ko, Y. H., Kang, H. S., Suh, J. W. Reversible Watermarking Without Underflow and Overflow Problems. In 2012 IEEE 55th International Midwest Symposium on Circuits and Systems (MWSCAS), 2012, 980-983. https://doi.org/10.1109/MWSCAS.2012.6292186
30. Singh, A. K., Dave, M., Mohan, A. Hybrid Technique for Robust and Imperceptible Multiple Watermarking Using Medical Images, Journal of Multimedia Tools and Applications , 2018, 75(14), 8381-8401. https://doi.org/10.1007/s11042-015-2754-7
31. Singh, A. K., Dave, M., Mohan, A. Hybrid Technique for Robust and Imperceptible Image Watermarking in DWT-DCT-SVD Domain. National Academy Science Letters, 2014, 37(4), 351-358. https://doi.org/10.1007/s40009-014-0241-8
32. Singh, A. K. Improved Hybrid Algorithm for Robust and Imperceptible Multiple Watermarking Using Digital Images, Multimedia Tools and Applications, 2017, 76(6), 8881-8900. https://doi.org/10.1007/s11042-016-3514-z
33. Singh, A., Dutta, M. K. A Robust Zero-Watermarking Scheme for Tele-Ophthalmological Applications, Journal of King Saud University-Computer and Information Sciences, 2020, 32(8), 895-908. https://doi.org/10.1016/j.jksuci.2017.12.008
34. Tsai, Y. Y., Tsai, D. S., Liu, C. L. Reversible Data Hiding Scheme Based on Neighboring Pixel Differences. Digital Signal Processing, 2013, 23(3), 919-927. https://doi.org/10.1016/j.dsp.2012.12.014
35. Wang, X. T., Chang, C. C., Nguyen, T. S., Li, M. C. Reversible Data Hiding for High Quality Images Exploiting Interpolation and Direction Order Mechanism, Digital Signal Processing, 2013, 23(2), 569-577. https://doi.org/10.1016/j.dsp.2012.06.015
36. Wang, Z. H., Lee, C. F., Chang, C. Y. Histogram-Shifting-Imitated Reversible Data Hiding, Journal of systems and software, 2013, 86(2), 315-323. https://doi.org/10.1016/j.jss.2012.08.029
37. Wu, H. T., Huang, J., Zhang, Y., You, J., Reversible Image Watermarking by Rhombus Prediction and Histogram Modification. In 2012 International Conference on Audio, Language and Image Processing, 2012, 165-169. https://doi.org/10.1109/ICALIP.2012.6376605
38. Yan, Y., Cao, W., Li, S. High Capacity Reversible Image Authentication Based on Difference Image Watermarking. In 2009 IEEE International Workshop on Imaging Systems and Techniques, 2009, 179-182.