International Journal of Soft Computing 9 (1): 27-36, 2014
ISSN: 1816-9503

Efficient Authenticated and Secure Medical Image Retrieval Using Dynamic Binary Encoded Watermark

[1]A. Umaamaheshvari and [2]K. Thanushkodi
[1]Sree Sakthi Engineering College, Karamadai, 641 104 Coimbatore, India
[2]Akshaya College of Engineering and Technology, Kinathukadavu, India

Abstract: Technical advancement has increased the availability of medical images which made the retrieval process for a query hectic. Therefore, an efficient and secure retrieval technique is required along. To address this requirement, this study has proposed a new technique named Secure and Efficient Image Retrieval (SEIR) technique. Here, to avoid the copyright violation as well as unauthorized user access SEIR uses the watermarking technique to provide authentication to the medical images. Watermarking technique is carried out by embedding the watermark into the query image using the Dynamic Binary Encoding (DBE) technique. Thereby, the proposed technique allows only the authenticated people to access the images presented in a database. In order to make the retrieval process efficient, SEIR uses the kNN classifier which classifies the images in the database depending on the feature characteristic. This classification process consumes less time to retrieve the pertinent document. Therefore, the SEIR technique is secured as well as it is efficient. The experimental results show, how SEIR is efficient as well as secure.

Key words: Authentication, copyright protection, image retrieval, watermarking, SEIR

INTRODUCTION

Doctors and research scholars highly depend on the medical images that are in the digital format for diagnosis and research purpose, respectively. Due to its simplicity, it is preferred by many doctors and research scholars which increases the availability of the digital images in the medical field. This made the retrieval of specific information difficult. In addition, the medical images are highly confidential it should be accessed only by its legitimate users. In order to achieve the efficiency and confidentiality over the images, this research has proposed a technique named SEIR that incorporates both the classification and digital watermarking techniques. It is the most significantly used technique in the electronically-driven fields to work against privacy and malicious manipulation.

Watermarking plays an important role in securing multimedia data by providing copyrighting and content verification. The effectiveness of the watermarking usually depends on the following properties imperceptibility, readily extractable, unambiguous and robustness. Among the aforementioned four properties imperceptibility and robustness has major impact and most needed attributes for digital watermarking. It is always a challenging task to achieve a trade-off between these two properties. The digital watermarking can be classified into two as shown in Fig. 1. This study uses the invisible digital watermarking and its process is as shown in the Fig. 2.

The watermarking is performed by embedding the watermark into the query image which generates a stego image through DBE technique. Database processes the stego image and extracts the watermark separately and compares the watermark with the original image for

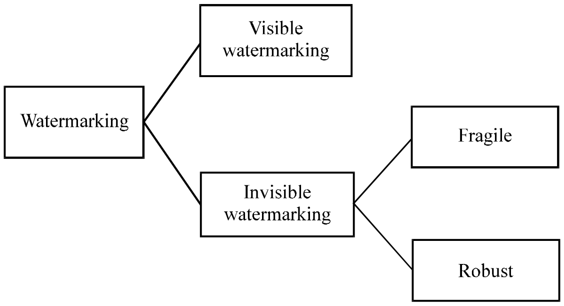

Fig. 1: Watermarking schemes

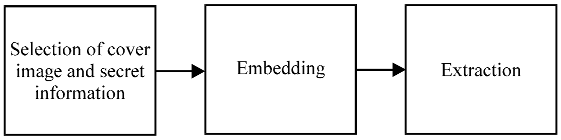

Fig. 2: Invisible watermark’s mainframe

Corresponding Author: A. Umaamaheshvari, Sree Sakthi Engineering College, Karamadai, 641 104 Coimbatore, India

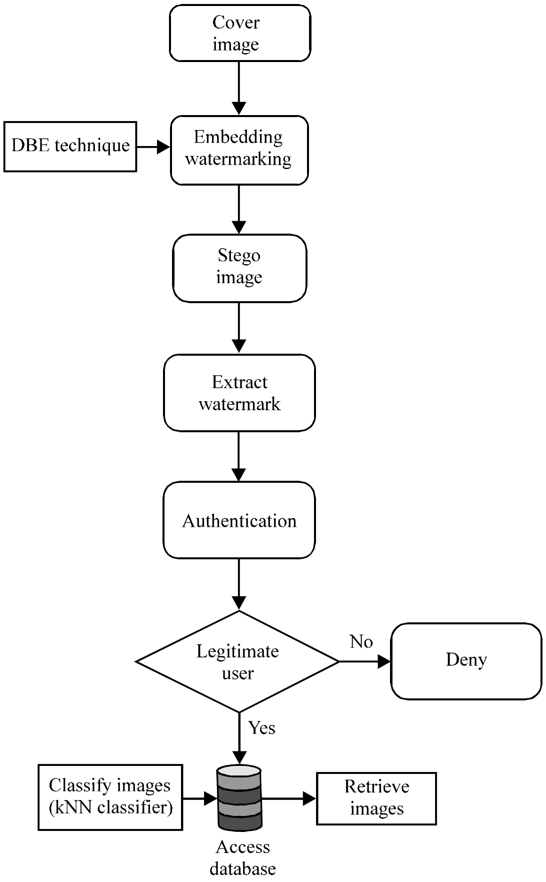

Fig. 3: Overall flow of SEIR

verifying the authenticity of the user. If they are equal then the database allows the user to access the images of the database. Thus, the authentication for the database is achieved through invisible digital image watermarking. Here, an assumption is made in this research that different types of watermarks are distributed to the users by the authority of the image repositories. Therefore, only the authorized users have their corresponding watermark. The difference in the watermark specifies the access control of the user.

The kNN classifier is used to classify the images as either normal or abnormal in the database depending on the state of tumor which improves the efficiency of the proposed system. The search for retrieval process is carried based on the state of queried image. This classification scheme will reduce the time required to process the required set of images. The overall flow of SEIR's authentication and retrieval process is represented in Fig. 3.

Literature review: This study presents a survey on various watermarking techniques for multimedia data. In the beginning, hidden labels were used to detect the ownership and distribution of information in an image or video. Koch and Zhao (1995) have studied the decisive factors and difficulties in implementing hidden labels. With this they have proposed a method named Randomly Sequenced Pulse Position Modulated Code (RSPPMC) for the JPEG based models. This is robust against the low pass filtering, lossy data compression and/or color space conversion. Depending on the hidden label watermark techniques were used for copyright protection of multimedia data. Some techniques have also used secret key to select the pixels of an image where the watermarks can be embedded. Such methods were affected by attacks like compression, blurring, etc. To overcome the drawback faced by the Secret Key Method, a novel approach was proposed by Kutter *et al.* (1997) which uses amplitude model and resistant to aforementioned attacks. Signature bits were multiplied with the modified pixel values presented in the blue channel. Depending on the luminance proportion the multiplication can be either subtractive or additive. The extraction of watermark from the original image can be taken without the original image. Similar Chang *et al.* (2005) and Nyeem *et al.* (2011) used key based technique to frame a model for watermarking. Here, they presented only the general description of key models.

Bors and Pitas (1996) implement the watermark, some blocks in the given images were selected using Gaussian classifier. Different pixels presented in the selected blocks were modified without violating the watermark conditions of Discrete Cosine Transform (DCT) coefficients. Here, they considered the following two constraints. Embedding the linear constrains among the DCT coefficients and circular detection region is defined in the DCT domain. This technique was resistant against the compression. Consequence of the above research, Piva *et al.* (1997) also used the DCT coefficients to insert the sequence of real numbers that were pseudo-randomly selected. The proposed technique has exploits the masking properties in order to obtain the invisibility. Extraction of watermark from an image was also carried without the help of original image. It is also robust against most of the geometric distortions. In addition to that Chaudhry (2009), Lu *et al.* (2006) and Saxena (2008) focused on DCT based digital watermarking. Lu *et al.* (2006) segregate the original image into four sub-images using sub-sampling technique. The secrete data should be in binary form that should be embedded into two sub-images' DCT coefficients. These coefficients were selected using the secret key generator. The extracted watermark can be compared among the DCT coefficients of the sub-images. For comparison, it does not require the original image. In the study, Chaudhary (2009) has studied about the technique Least Significant Bit (LSB) watermarking based on DCT. They have also focused on the Discrete Wavelet Transform for wavelet based watermarking and multiple spatial watermarking in color image. However, they implemented and tested a slightly modified version of multiple spatial watermarking in color image technique. This technique was suitable for invisible watermarking that was implemented in spatial domain.

Singular Value Decomposition (SVD) techniques were also used for watermarking which preserved the one-way and non-symmetric properties that were not attained through DFT and DCT transforms. This technique was used by Aslantas (2009), Chang *et al.* (2005) and Lai and Tsai (2010). Aslantas (2009) have used SVD to withstand highly against all possible attacks without any compromise on transparency. It also used the evolution algorithm (DE) to obtain the above mentioned. In order to embed the watermark data, the host image's singular values were changed through multiple scaling factors. To obtain ultimate robustness and efficient transparency, the changes were optimized by DE. For satisfying the requirements of robustness and imperceptibility. Lai and Tsai (2010) incorporated both the DWT and SVD technique and proposed a hybrid image-watermarking mechanism. Through this technique, the watermark was embedded to the singular value of original image's DWT sub-bands instead of embedding it to the wavelet coefficients. This technique has the capability to withstand against the classical attacks.

Similarly, Fractional Fourier Transform (FRFT) was also used by Dian-Hong *et al.* (2007) and Feng *et al.* (2005) in order to obtain the blind digital watermarking technique. Dian-Hong *et al.* (2007) have analyzed the Hermite matrix for direct Discrete Fourier Transform computation and Chirp signals hidden in the host image's low frequency band in wavelet domain. This technique outperforms the existing spatial algorithm. Feng *et al.* (2005) discussed the energy distribution of two-dimensional signal at different FRFT domain. Multiple chirps were used to directly embed the watermark in the spatial domain. This technique retains the quality of the image. The DWT technique was briefly discussed by Kamran *et al.* (2006) along with the comparison of two different watermarking schemes that were based on DWT. In blind image watermarking is obtained through cryptography based technique which embeds enormous number of watermark bits in a gray scale image without compromising the imperceptibility and security of the watermark (Gupta, 2012).

A new technique was framed to cast the watermark on digital images by Pitas (1996) which was done through randomly selecting image pixels and adding luminous values that were small into the image pixels. In addition to that statistical based detection mechanism was also proposed. Another statistical based watermark detection technique was proposed in the postulates by Zeng and Liu (1999) for validation and detection of the invisible watermark. This detection technique can be made robust against when it was combined with the visual models for encoding the watermark. Puate and Jordan (1996) have proposed a technique that depended on a fractal coding and decoding method. The fractal coding mechanism is used to determine the spatial redundancy that present inside an image through generating relationship among different parts. This is used as a means of embedding the watermark. This technique was robust against the low pass filtering and JPEG conversion attacks.

Chaos and Fresnel Transform Based Watermarking algorithm were proposed by Wang *et al.* (2012). The original image is converted (i.e., transformed) to Fresnel diffraction and watermark were embedded into the amplitude spectrum that achieved after scrambling using the chaotic sequence.

The major challenge faced by the watermarking technique was that it should not reduce the quality of the original image after embedding process. A pioneering method was proposed by Wolfgang and Delp (1999) with the aim of embedding watermark into an image without affecting the quality of it. This method consists of two watermarking mechanisms that were depended on the visual models. The visual models were used to identify the upper bounds of an image on watermark insertion which yields maximum strength on the transparency. They have also proposed watermarking schemes in two different frameworks: block based discrete cosine transform and multi-resolution wavelet transforms. This technique was robust against classical attack as well as achieves good transparency.

Various technique discussed so far were focused mainly on the robustness of watermarking. Conversely, fragile watermark was used to detect slight modifications that were present in an image. In two different fragile watermarks were compared (Wolfgang and Delp, 1999). The first method used hash function for both the original and modified images to attain digest of the image. If digest were different then it is concluded that the image was forged. The hashing technique was used to spatially localize the changes. Second method used Variable-Watermark 2-dimensional algorithm (VW2D) also referred as semi-fragile watermark. Here, compassion to changes was user-defined. It accepts the images that have either with little modification or with no change.

MATERIALS AND METHODS

This study gives detailed working of SEIR technique which is divided into three different phases namely: Stego image generation, Authentication and Retrieval. Figure 4 depicts the workflow of the SEIR technique.

Generation of Stego image: To access the database, user should provide a stego image. The stego image can be generated through various steps as shown in the Fig. 5.

Embedding process: The watermark is segmented into n×n non overlapping blocks. For embedding the watermark into query it is transformed into binary message. The conversion process is taken through block adaptive technique which is formulated from block truncation coding mechanism. A quantifier named mean value is determined using the Eq. 1 for each pixel present in the blocks:

$$\bar{m} = \frac{1}{x}\sum_{i=1}^{x} m_i \tag{1}$$

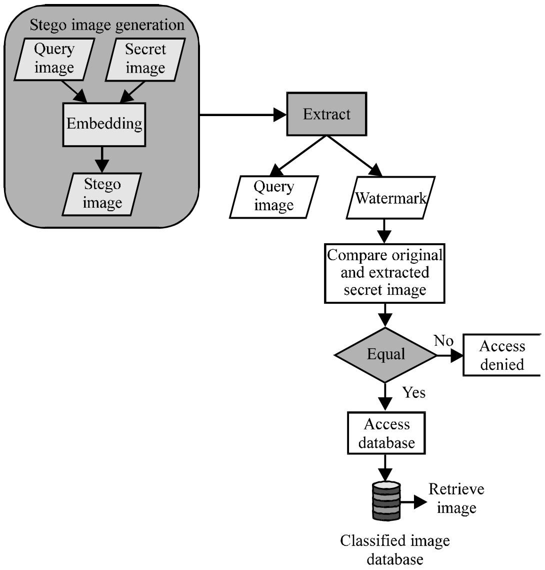

Fig. 4: Detailed workflow of SEIR technique

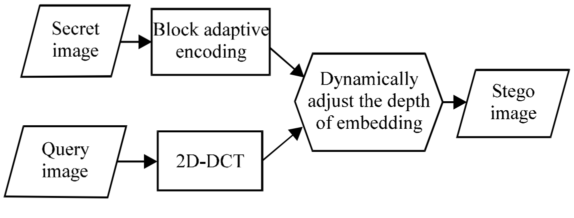

Fig. 5: Construction of Stego image

Where:

x = The total number of pixels in the given image
m_i = The value of the ith pixel presented in an image block

The value obtained for $\bar{m}$ is set as the threshold value which is compared with each pixel value m_i using the Eq. 2:

$$BB = \begin{cases} 0 & m_i \geq \bar{m} \\ 1 & m_i < \bar{m} \end{cases} \tag{2}$$

The comparison result from Eq. 2 is used to frame the binary message for the watermark. If the pixel value is greater than or equal to the threshold value then the corresponding block of the binary messages is replaced with 1. Otherwise, zero is inserted into the binary message block.

The cover image (query image) is also processed to determine the pixels where the values of binary message block can be embedded without affecting its quality. For determination of appropriate pixels in cover image, 2D-DCT (Discrete Cosine Transform) is used. This technique is used to partition the image into parts of different importance and coverts an image from the spatial domain to the frequency domain. Its main advantage is that it has very less or negligible error rate as well as high compression rate. Initially, the cover image is divided into 8×8 blocks. Each block is processed using the DCT to determine the suitable pixels to insert the binary message values. Here, a criterion named P is introduced whose value for each block is determined using Eq. 3. Based on this value, pixel for embedding the binary values of secret image is determined:

$$P = \mathrm{mod}(b(1,1),S) \tag{3}$$

In Eq. 3, the depth of embedding information is adjusted by a quantifier S. By this, the depth of embedding the values can be adjusted dynamically. However, the stability of the watermark will be too low if the value of S is small and if the value of S is higher then it reduces the quality of the image. Therefore, this process carries 32 as the value for S. The b(1, 1) expresses the value of a pixel presented in a particular block. For each block, the p-value is changed. Once the p-value is set upon a block then its pixels are processed to embed the binary values. If the binary value is 1, then it uses the Eq. 4 to modify the pixel value. The binary value 1 is not directly inserted into the image rather it changes the value of pixel so that the intensity is slightly modified without affecting the quality of the image:

$$b(1,1) = \begin{cases} b(1,1)\text{-}P\text{-}\frac{5}{4} & \text{if } P \leq \frac{5}{4} \\ b(1,1)\text{-}P\text{+}3\times\frac{5}{4} & \text{if } P > \frac{5}{4} \text{ and } P \leq 2\times\frac{5}{4} \\ b(1,1) & \text{Otherwise} \end{cases} \quad (4)$$

Similarly, the Eq. 5 is used when the binary bit is zero:

$$b(1,1) = \begin{cases} b(1,1)\text{-}P\text{+}5\times\frac{5}{4} & \text{if } P \geq 3\times\frac{5}{4} \\ b(1,1)\text{-}P\text{+}\frac{5}{4} & \text{if } P < 3\times\frac{5}{4} \text{ and } P \geq 2\times\frac{5}{4} \\ b(1,1) & \text{Otherwise} \end{cases} \quad (5)$$

Inverse function of the DCT transforms is applied to the block that has been embedded with the binary image. The above last two process is continued still all the binary information of watermark image have been added successfully into all the blocks of the cover image. Figure 6 illustrates the generation of stego image as an example.

Authentication: On receiving stego image as input, database checks the authentication of the user by extracting the watermark image from the cover image and compare the extracted watermark with the original image. If both the images are similar then the database considers the user as the authorized user. The Database's Watermark Extraction System, segments the stego image into 8×8 blocks and applies the DCT transform on each block. To carry out the extraction process it is necessary to remember the quantization value (S) which helps to detect the DC coefficients where the binary messages are embedded. The binary image value that is either 1 or 0 is found from the corresponding pixel using the Eq. 6. Both the original image and watermark image are converted into the binary image as shown in Fig. 7:

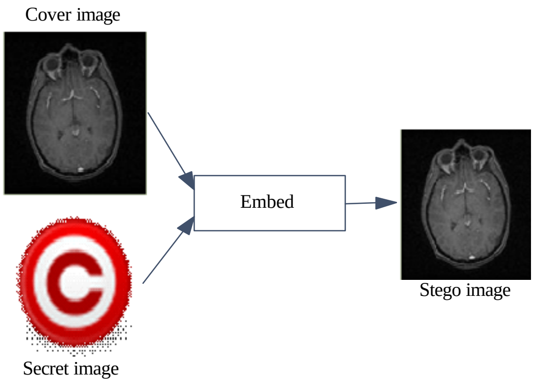

Fig. 6: An illustrative example of Stego image generation

$$Y(m, n) = \begin{cases} 1 & \text{if } \operatorname{mod}(b(1,1), S > \frac{S}{2}) \\ 0 & \text{otherwise} \end{cases} \quad (6)$$

Then, both images are compared and analyzed using the following parameters.

Universal Image Quality Index (UIQI): Consider the original and watermark image as $O = \{O_i|i = 1, 2, ..., X\}$, $T = \{T_i|i = 1, 2,...,X\}$. With this, the UIQI can be determined from the Eq. 7:

$$R = \frac{4\times\rho_{mn}\times\bar{m}\times\bar{n}}{(\rho_m^2+\rho_n^2)\times(\bar{m}^2+\bar{n}^2)} \quad (7)$$

where, $\bar{m}$, $\bar{n}$, ρ_m^2, ρ_n^2 and ρ_{mn} can be manipulated from the Eq. 8-12:

$$\bar{m} = \frac{1}{x}\sum_{i=1}^{x} m_i \quad (8)$$

$$\bar{n} = \frac{1}{x}\sum_{i=1}^{x} n_i \quad (9)$$

$$\rho_m^2 = \frac{1}{x\text{-}1}\sum_{i=1}^{x}(m_i\text{-}\bar{m})^2 \quad (10)$$

$$\rho_n^2 = \frac{1}{x\text{-}1}\sum_{i=1}^{x}(n_i\text{-}\bar{n})^2 \quad (11)$$

$$\rho_{mn} = \frac{1}{x\text{-}1}\sum_{i=1}^{x}(m_i - \bar{m})\,(n_i - \bar{n})^2 \quad (12)$$

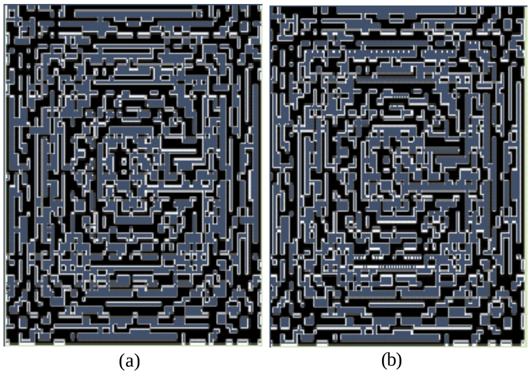

Fig. 7: Binary image of original and extracted watermark image; a) original image; b) extracted watermark image

The value of R is dynamic and it can take the value in the range [0, 1]. R = 1 is the best value and it can be obtained only when, $O_i = T_i$, i = 1, 2, ... , X. The distortion of this quality index is the combination of three different factors namely luminance distortion, loss of correlation and contrast distortion. Therefore, the definition of R can be redefined and it is represented in the Eq. 13:

$$R = R_1 \times R_2 \times R_3 \tag{13}$$

$$R_1 = \frac{\rho_{mn}}{\rho_m \times \rho_n} \tag{14}$$

$$R_2 = \frac{2 \times m \times n}{m^2 + n^2} \tag{15}$$

$$R_3 = \frac{2 \times \rho_m \times \rho_n}{\rho_m^2 + \rho_n^2} \tag{16}$$

$$R = \frac{\rho_{mn}}{\rho_m \times \rho_n} \times \frac{2 \times m \times n}{m^2 + n^2} \times \frac{2 \times \rho_m \times \rho_n}{\rho_m^2 + \rho_n^2} \tag{17}$$

The R_1 is used to measure the correlation coefficients between the m and n. The second component R_2 is used to determine the closeness of luminance value between the m and n. The contrast between the original and watermark image are tested using R_2. Therefore, the UIQI value between the original and the extracted watermark image should be near to one. If the value is too low then it is regarded that the user is not authorized person to access the database.

Structural Similarity Index Metric (SSIM): SSIM value can be computed from the Eq. 18:

$$\text{SSIM} = \frac{(2 \times m \times n + z1)(2 \times \rho_{mn} + z2)}{(\rho_m^2 + \rho_n^2 + z2)(m^2 + n^2 + z1)} \tag{18}$$

Here, $\overline{m}$, $\overline{n}$, ρ_m^2, ρ_n^2 and ρ_{mn} can be determined same as in UIQI and the z1 and z2 denotes the constants. If the UIQI and SSIM values are greater then the extracted watermark image and its corresponding original image have greater similarity.

BER: The difference among the compared images is manipulated using the bit-error rate. If this value is lower than the predefined threshold then the user is allowed to access the database otherwise, the corresponding user is not allowed to access the image.

Based on these three quality parameters the user is classified as either authenticated or not. This procedure acts as a detection system at the database to allow only the legitimate users to access the database. Once if the user is identified as authenticated then he/she can retrieve the images present in the database.

Retrieval of relevant images: Once the user is identified as a legitimate user by the database then they are allowed to access the images present in it. To make the access and retrieval process efficient, researchers classify the images presented in it using kNN classification technique. This classification technique makes use of GLCM features to identify similar images under a class. Therefore, for each image in the database, the GLCM features are extracted and classified under specified classes.

Classification

GLCM feature extraction: The intensity variations at a pixel of an image can be measured using the GLCM feature values. Such feature can be extracted from the image using the following two steps. The distance between the pairwise spatial co-occurrences of pixels that are separated by a particular angle are measured and tabulated using the matrix named co-occurrence matrix. Set of scalar quantities are manipulated which are used to characterize the various aspects of the underlying texture. The table prepared at step one is used to manipulate the various combinations of gray-level that co-occur in the given image. The co-occurrence matrix is usually of size N×N where the N denotes the number of different gray scale level of an image. The relative frequency of an image can be represented using an element C(x, y, d, α) where x is the gray level at the pixel C at a particular location and j is the gray level presented at a pixel that is located at a distance d from C at an angle α. Spatial domain quantitative description can be derived from GLCM.

kNN classifier: An image is classified and assigned to a specified class through a majority vote of its k nearest neighbors. Here, the classier takes the pattern that is very close to each other in the space for feature which belongs to the class having the similar pattern. The neighbors are the images that are correctly classified into the well known class. Researchers used euclidean distance for distance measure. By this way, the images of a database are classified under different classes accurately.

Retrieval: Database processes the input cover image and finds GLCM features of it. Having the patterns derived from the patterns predicts the class to which it can belong. On predicting the class, similar images are retrieved from the database and presented to the user. Thus, the images are retrieved efficiently and securely from the database.

RESULTS AND DISCUSION

The proposed SEIR technique is experimented for its efficiency in retrieval. For analysis purpose images have been taken from database containing 150 brain images. These images are collected from Internet Brain Segmentation Repository (IBSR) dataset. The database consists of two different set of images one set with brain tumor and another without brain tumor. Researchers assumed that only the doctors and research scholars of the hospital have authentication to access the database. For accessing the database, authorization details are provided through invisible digital watermarking scheme. The photos of doctors and scholars act as the watermark images which are embedded into the query image. Query images are the images that act as the keyword for retrieving the similar images from the database. For experimental purpose a brain image is taken as query image and embedded with the photo of the user to generate the stego image. The query image, watermark image that is taken for experimental purpose and its stego image are as shown in the Fig. 8. This research uses 512×512 query image and the 64×64 watermark image.

Once the query image is provided to database, the SEIR technique stimulates the extraction process to extract the watermark image from the stego image in the form of binary image. The extracted binary watermark image, i.e., the photo of the user is compared with the binary image of corresponding original image. Figure 9 shows the binary version of both the watermark (photo of doctor) image and original image.

These binary images are tested using UIQI, SSIM, and BER attributes. Table 1 presents the comparison results. For the BER the threshold value is taken as 10 for this experiment. The quantized attribute result shows that the UIQI and SSIM values are very small which implicitly says that the binary image of the watermark that is extracted from the stego image and its corresponding original images are similar. In addition to that BER value is too small than the predefined threshold that specifies the difference between the two compared image. Therefore, these values represent that the user is an authorized and he/she is allowed to access the database.

The images of the dataset are classified in prior to access by an authenticated user. The classification is carried using the kNN classifier. The classifier classifies the images and groups the similar images under different classes. Here, there are only two different class are present namely normal and abnormal. Depending on the GLCM features of the images in the dataset, they are classified into either normal or abnormal class. This classification process helps for efficient retrieval process. Since, the query image search only the subgroup of image not all the images. During retrieval the query image's (after extraction of watermark image) GLCM features are estimated to determine the class of the image. If the query image is normal then the images under the normal is either accessed or retrieved from database. Figure 10 represents the first 10 images that are relevant to the query image (shown in Fig. 8 which is normal). Figure 10 shows only the sample of images that are retrieved from the database (not all images that are normal). The kNN classifier uses Euclidean distance for finding the similar images. Table 2 represents the distance between the query image and the retrieved image (only for first 10 images).

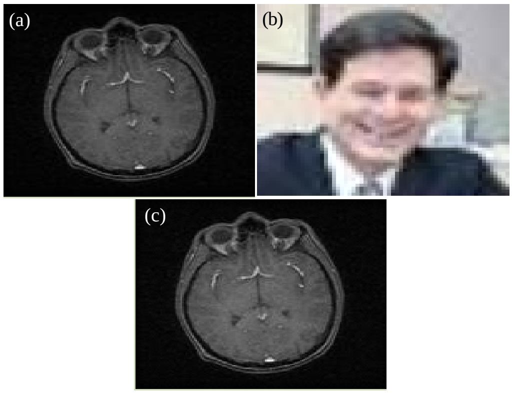

Fig. 8: a) Cover image; b) watermark image and c) stego image

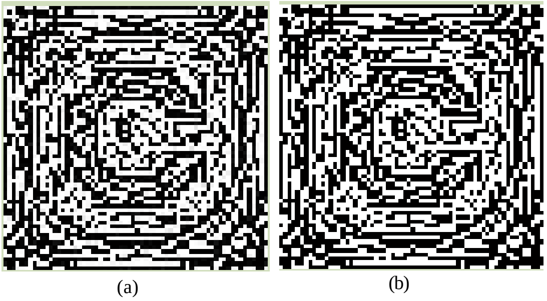

Fig. 9: Binary image; a) binary form of original image and b) binary form of extracted watermark image

Table 1: Quantization attributes and their corresponding values

Attributes	Values
UIQI	0.6314
SSIM	0.9870
BER	0.4570

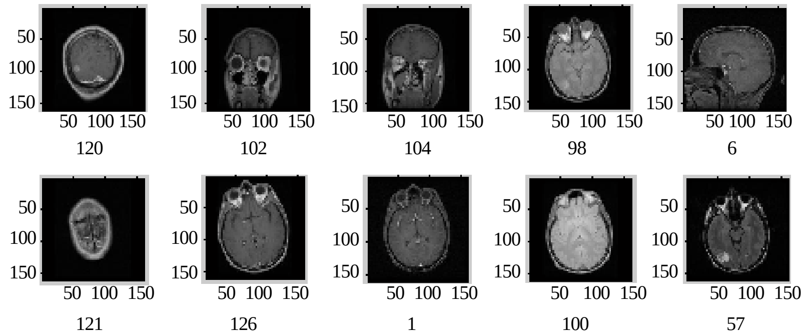

Fig. 10: Retrieved image from dataset

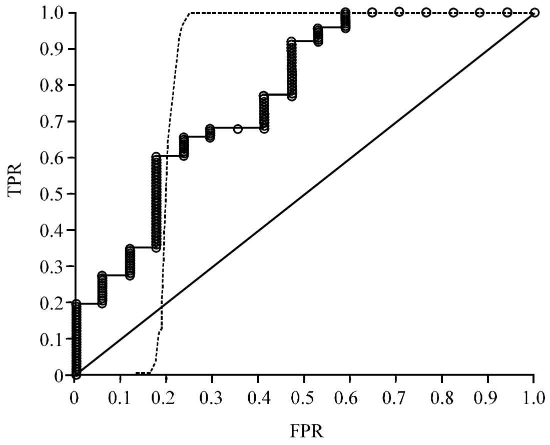

Fig. 11: ROC graph for normal class

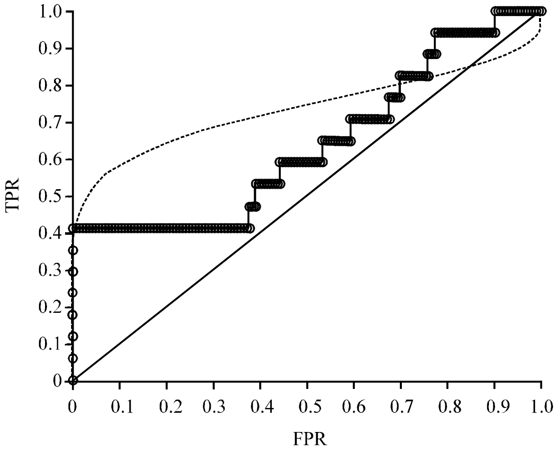

Fig. 12: ROC graph for abnormal class

Table 2: Distance measure

Image ID	Distance measure between query and retreived image
118	9.318677117507195e-001
119	9.318677117507195e-001
62	9.525650407533984e-001
129	1.650545144412410e+000
30	1.772163982825642e+000
17	2.559035972744737e+000
59	3.256842202238974e+000
12	3.638208543358343e+000
61	4.994641318842526e-000
130	5.712627347987588e+000

Table 3: Confusion matrix for classification techniques

Classifiers	True positive	False positive	False negative	True negative	Accuracy (%)
Bayesian	15	59	2	74	59.33
SVM	0	0	17	133	88.67
K-NN	7	0	10	133	93.33

The efficiency of GLCM feature based kNN classification is determined and that is represented in the confusion matrix. Table 3 denotes the confusion matrix for the kNN, SVM and Bayesian classifiers. It is clear that only 10 among 150 images are misclassified which represents that the kNN classifier used in this research has the classification accuracy as 93.33%. The accuracy of SVM and Bayesian is determined as 88.67 and 59.33%. From the results, it is clear that the kNN classifier functions better than the other classification technique for this application.

Another way besides the confusion matrix to compute the efficiency of the classifier is the ROC graph. The ROC graph usually has False Positive (FPR) on x-axis and True Positive (TPR) on y-axis. If the points in the graph denotes (0, 1) then it implicitly represents that images are classified perfectly. Zero in x-axis and one in y-axis express that the false positive rate is 0 and the true positive rate is 1. Likewise, if (1, 0), (0, 0) and (1, 1) represent the incorrect classification, all classifications are negative and all the classifications are positive respectively. Figure 11 and 12 denotes the ROC graph for normal and abnormal class classification.

It is clear from the Fig. 11 that the images for normal classes are predicted accurately. No images are misclassified.

Similar to the ROC graph, precision and recall graphs are used to estimate the efficiency of the retrieval process. Precision number of images that are retrieved is

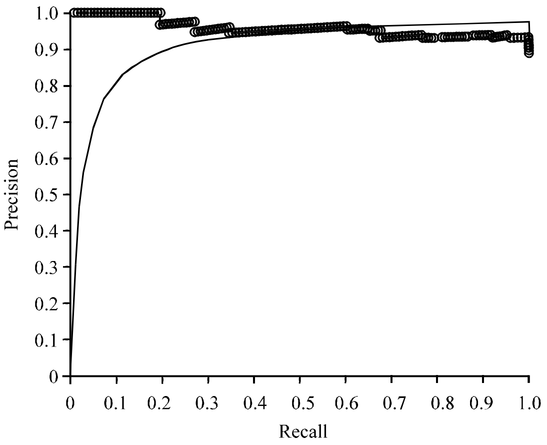

Fig. 13: Retrieval efficiency for normal class

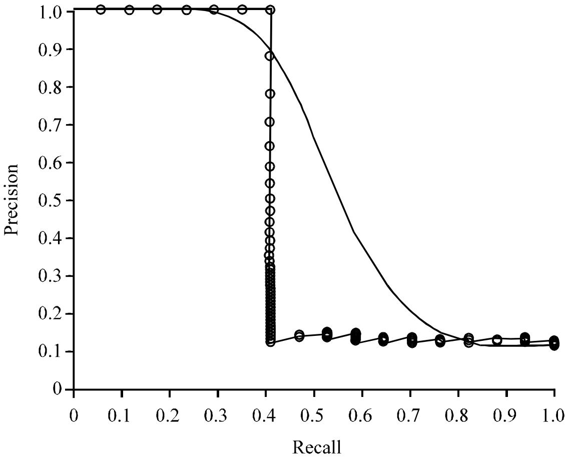

Fig. 14: Retrieval efficiency for abnormal class

relevant to the query image while the recall denotes the number of related image that are retrieved. Precision is a measure that expresses the fraction of returned (retrieved) images that are relevant which is purely based on the measure and understanding of relevance. Precision can be calculated using the Eq. 19:

$$\text{Precision} = \frac{P_{\text{img}} \cap R_{\text{img}}}{R_{\text{img}}} \qquad (19)$$

In the Eq. 19, P_{img}, R_{img} interpreted as relevant images and retrieved images respectively. The recall value can be estimated through the Eq. 20:

$$\text{Recall} = \frac{P_{\text{img}} \cap R_{\text{img}}}{P_{\text{img}}} \qquad (20)$$

Figure 13 and 14 represent the precision and recall graph for the normal class and abnormal class image retrieval's efficiency. Figure 13 and 14 express that the images are retrieved efficiently.

CONCLUSION

This study deals with the issues of providing authentication to the users of a database containing medical images. To provide authentication, researchers have proposed an SEIR technique based on invisible digital watermarking and kNN classifier. SEIR motivates the users to provide the stego image as their query which is generated through embedding the watermark image to the query image by using the DBE technique. On receiving the stego image, database extracts the watermark image and compares it with its corresponding original image. If both the images are equal then the user is allowed to access or retrieve the image. Otherwise, their access is denied. To make the retrieval process efficient the images in the database are classified under two different classes namely: normal and abnormal. The classification process is carried out using the kNN classifier. The query image is also processed to find the features based on which the class for the input image is identified. Once the image's class is determined then all the images under the specified class are retrieved. The experimental analysis shows that the proposed SEIR retrieves the images in the database efficiently. The retrieval efficiency is measured using precision and recall.

REFERENCES

Aslantas, V., 2009. An optimal robust digital image watermarking based on SVD using differential evolution algorithm. Optics Commun., 282: 769-777.

Bors, A.G. and I. Pitas, 1996. Image watermarking using DCT domain constraints. Proceedings of the International Conference on Image Processing, Volume 3, September 16-19, 1996, Lausanne, Switzerland, pp: 231-234.

Chang, C.C., P. Tsai and C.C. Lin, 2005. SVD-based digital image watermarking scheme. Pattern Recognition Lett., 26: 1577-1586.

Chaudhry, S.H., 2009. Digital image watermarking. NUST-SEECS. http://hdl.handle.net/123456789/363.

Dian-Hong, W., L. Dong-Ming, Y. Jun and C. Fen-Xiong, 2007. An improved chirp typed blind watermarking algorithm based on wavelet and fractional Fourier transform. Proceedings of the 4th International Conference on Image and Graphics, August 22-24, 2007, Sichuan, China, pp: 291-296.

Feng, Z., M. Xiaomin and Y. Shouyi, 2005. Multiple-chirp typed blind watermarking algorithm based on fractional Fourier transform. Proceedings of the International Symposium on Intelligent Signal Processing and Communication Systems, December 13-16, 2005, Hong Kong, China, pp: 141-144.

Gupta, P., 2012. Cryptography based digital image watermarking algorithm to increase security of watermark data. Int. J. Sci. Eng. Res., 3: 1-4.

Kamran, H., A. Mumtaz and S.A.M. Gilani, 2006. Digital image watermarking in the wavelet transform domain. Proc. World Acad. Sci., Eng. Technol., 13: 86-89.

Koch, E. and J. Zhao, 1995. Towards robust and hidden image copyright labeling. Proceedings of the IEEE Workshop on Nonlinear Signal and Image Processing, June 20-22, 1995, Neos Marmaras, Greece, pp: 452-455.

Kutter, M., F. Jordan and F. Bossen, 1997. Digital signature of color images using amplitude modulation. Proceedings of the SPIE Electronic Imaging, Storage and Retrieval for Image and Video Databases, Volume 3022, February 13-14, 1997, San Jose, CA, USA., pp: 518-526.

Lai, C.C. and C.C. Tsai, 2010. Digital image watermarking using discrete wavelet transform and singular value decomposition. IEEE Trans. Instrument. Measur., 59: 3060-3063.

Lu, W., H. Lu and F.L. Chung, 2006. Robust digital image watermarking based on sub-sampling. Applied Math. Comput., 181: 886-893.

Nyeem, H., W. Boles and C. Boyd, 2011. Developing a digital image watermarking model. Proceedings of the International Conference on Digital Image Computing Techniques and Applications, December 6-8, 2011, Noosa, QLD, Australia, pp: 468-473.

Pitas, I., 1996. A method for signature casting on digital images. Proceedings of the International Conference on Image Processing, Volume 3, September 16-19, 1996, Lausanne, Switzerland, pp: 215-218.

Piva, A., M. Barni, F. Bartolini and V. Cappellini, 1997. DCT-based watermark recovering without resorting to the uncorrupted original image. Proceedings of the International Conference on Image Processing, Volume 1, October 26-29, 1997, Santa Barbara, CA. USA., pp: 520-523.

Puate, J. and F. Jordan, 1996. Using fractal compression scheme to embed a digital signature into an image. Proceedings of SPIE Photonics East, Volume 96, November 18, 1996, Boston, MA., USA., pp: 108-118.

Saxena, V., 2008. Digital image watermarking. Ph.D. Thesis, Department of Computer Science and Engineering, Jaypee Institue of Information Technology University, India.

Wang, Z., S. Lv, J. Feng and Y. Sheng, 2012. A digital image watermarking algorithm based on chaos and fresnel transform. Proceedings of the 4th International Conference on Intelligent Human-Machine Systems and Cybernetics, Volume 2, August 26-27, 2012, Nanchang, China, pp: 144-148.

Wolfgang, R.B. and E.J. Delp, 1999. Fragile watermarking using the VW2D watermark. Proceedings of the SPIE Security and Watermarking of Multimedia Contents, Volume 3657, January 23, 1999, San Jose, CA., USA., pp: 204-213.

Zeng, W. and B. Liu, 1999. A statistical watermark detection technique without using original images for resolving rightful ownerships of digital images. IEEE Trans. Image Process., 8: 1534-1548.