Journal of Theoretical and Applied Information Technology
30th November 2013. Vol. 57 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MEDICAL IMAGE AUTHENTICATION WITH ENHANCED WATERMARKING TECHHNIQUE THROUGH VISUAL CRYPTOGRAPHY

[1]UMAAMAHESHVARI ANNAMALAI, [2]THANUSHKODI K

[1]Assistant Prof., Department of Electronics and Communication Engineering, SSEC, COIMBATORE
[2]Director, ACET, COIMBATORE, INDIA
E-mail: [1]ums612@gmail.com, [2]thantan48@gmail.com

ABSTRACT

Technological evolution has increased the insecurity of the biomedical images produced day to day. Avoidance of the database hacking and preserving the privacy of digital biometric data stored in the central database has become of paramount importance. In order to preserve the security of the database, an enhanced visual cryptographic technique is proposed in this paper. Cryptographic technique allows information to be encrypted in such a manner that decryption cannot be handled by the non-legitimate user. The proposed method allows a secret sharing scheme, where an image is broken up into two shares and then overlaid in such a way that an unauthenticated person cannot reveal this secret image. The partitioned image is compared with all the images in the target using Hausdorff Distance metric algorithm. When both the images match, the authentication is provided. This paper also focuses on outsourcing data to an untrusted client to predict the category of the image without getting any information about the image itself and the final result of the classification. The experimental results show that our proposed method is efficient over the existing methods.

Keywords: *Authentication, Hausdorff Distance Metric, Privacy Preserving And Visual Cryptography*

1. INTRODUCTION

Medical images are stored for three purposes: diagnosis, database and long term storage. Due to the widespread usage of Internet, digital forms of images and texts can be saved, transferred and accessed easily. The images obtained must be kept perfectly without any loss of information before the image is diagnosed by the doctor. The image should be compressed by lossless algorithm or should be stored without using compression. When the image is diagnosed by a doctor at distant site, it cannot be exposed to public. However a person with privilege can access to images which are contained in database and can modify them maliciously. But the problem of hacking of data by any parties still exists. It is important to prevent any modifications in the images. Digital watermarking is a technology being developed to provide protection from illegal copying. Invisible watermarks when added to the image can't be perceived as such, and have wider applications than visible watermarks. In general an effective watermarking scheme should satisfy properties such as invisibility, robustness, security and low computational complexity. Watermarking provides a proof of ownership of digital data by embedding copyright statements. An embedded watermark should not be visible under normal observation or interfere with the functionality of the image. It must not affect the image quality as well. As this, the watermarked image must be perceptually imperceptible.

Visual Cryptography (VC) is basically a secret sharing scheme extended for the images. This scheme eliminates the complex computational problem in decryption process and the secret image can be restored by stacking operations. This property makes visual cryptography useful in low computation requirement. The hidden image can be revealed only when enough share images are obtained. It has the ability to restore a secret without the use of computations. Visual Cryptography when used in copyright protection enables reduction of rightful ownership, without using the original image. Also, the host will not be altered during the embedding. The main idea in visual cryptography is to split an image into two random shares which separately reveal no information on the original image. The original image can be reconstructed by superimposing the two shares. Mathematically the VC system is

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

described by XOR operation. To encode a secret employing a (2,2) VC scheme, original image is divided into two shares such that each pixel in the original image is replaced with a non- overlapping block of two sub pixels. When the two shares are stacked together, the black pixel in the original image remain black and the white pixels become grey. Although some contrast lost occurs, the decoded image can be clearly identified. Since each pixel in the original image is replaced by two sub-pixels in each share, the width of the decoded image is twice that of the original image.

The advances in digital measurement and engineering technologies enable the capture of massive amounts of data in medical field. The effort for data collection and processing, as well as its potential utility for research or business, creates value for the owner. The owner wishes to store them and allow access to his own, colleagues and other (trusted) doctors or scientists. This can be supported by outsourced servers that offer low storage costs for large databases. However care needs to be taken to safeguard data that are valuable or sensitive against unauthorized access. To ensure this security, only the feature set of image is given to the untrusted client to process the work given. This work is done by the untrusted client without knowing about the details of the data.

In this project a query image is selected and a watermark is embedded on the image using BTC technique. The image is transformed to well known Discrete cosine transform (DCT) and a watermark is added to selected coefficients of the transformed image. This watermarked image is called the stego image. Then finally invert the DCT to get an image very similar to the original one with included watermark. The detection procedure starts by first transforming the input image with DCT and tries to extract the watermark information from some selected coefficients. Now, the extracted watermark is subjected to visual cryptographic server to check for authentication i.e. to check whether that person is a registered doctor of a medical institute. This verification is carried out by computing Hausdorff distance metric between the extracted watermark and target database in the Visual cryptographic server. If the watermark is verified the authenticated message and the feature set of the query image is given to the untrusted client.

The Rest of this paper is organized as follows: section 2 provides the literature reviews of related topics. In section 3, authors have elaborately described the proposed technique for secure access to the database. The efficiency of this method is analyzed, and its results are presented in section 4. Finally, section 5 concludes the proposed work.

2. RELATED WORKS

In recent researches Medical image watermarks are used to authenticate (trace the origin of the image) and/or investigate the integrity (detect whether changes have been made) on medical images. There are two types: Robust and Fragile watermarks[1]. A fragile watermarking scheme detects any manipulation made to a digital image to guarantee the content integrity while the robust scheme prevents the watermark removal unless the quality of the image is greatly reduced. For our method, the watermark has to be semi-fragile and ideally it should degrade at around the same rates as the host image[2].

There are different methods that has been using for medical image watermarking. The watermark can directly be embedded in the LSB as described by Mohamed Ali et al[3]. Since the modification of the pixel data takes place in the LSB it is not visually perceptible. Mostafa et al. [4] presented a method for protecting the patient's information in which the information is embedded as a watermark in discrete wavelet packet transform(DWPT) of the medical image using the hospital logo as reference image. In paper[5]the watermarking of medical image in DCT and DWT domains is proposed and evaluated the performance based on PSR and MSE. In [6] (k, n) secret sharing scheme is used, which shares medical images among a health team of n clinicians such that at least k of them must gather to reveal the medical image to diagnose.

As per [7] a model where medical image regions are watermarked with the payload is presented. So that the perceptual degradation due to the watermarking is limited and describes an approach to ensure that impact on the image quality is well below the threshold of visual perceptibility. According to [8]using of DCT based watermarking schemes provides higher resistance to image processing attacks such as noise, JPEG compression, translation etc. In this approach the watermark is embedded in the mid-frequency band of the DCT blocks carrying low frequency components and the high frequency sub band components remains unused. Watermark is inserted by adjusting the DCT coefficients of the image and by using the private key. Watermark can then be extracted using the same private key without

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

resorting to the original image. The authors of [9]proposed a scheme of visual cryptography in which a private face image is dithered into two host face images such that it can be revealed only when both host images are simultaneously available. The paper [10]considers the problem of embedding a binary watermark in a grey-level image using the concept of Visual cryptography. This scheme offers a better security so that, attackers will not be able to detect ownership information. This scheme embeds and extracts the secret image without altering the host image and allows multiple watermarks to be embedded. The authors of [11]proposed a method in which binary image is split into two shares via 2-out-of-2 visual secret sharing scheme. Then one of the shares is embedded into the host image, and the other is held by the owner. When providing the ownership the owner has to extract the embedded share and recover the watermark with his own share.

In[12]various watermarking techniques such as spatial, frequency and statistical domain are studied and finally concludes that frequency domain technique are good for applications where exact watermark needed to be extracted and channels do not contain any noise. Unlike the traditional watermarking schemes, the watermarks are not embedded directly into the digital image in[13]Instead, the proposed method constructs independent Master shares for the users. When privacy happens the users can show their shares to reveal the watermark.[14]propose a Dual Watermarking Scheme based on DWT-SVD with chaos encryption algorithm to improve the robustness and protection along with security. Two watermarks are embedded in the host image. The secondary is embedded into primary watermark and the resultant watermarked image is encrypted using chaos based logistic map. This provides an efficient and secure way for image encryption and transmission.

In [15]a blind watermarking technique is done that uses watermark nesting and encryption. The advantage of this system is more number of bits can be embedded as compared to without watermark nesting and also a metadata about a watermark can be embedded. Due to encryption security of watermarks is also increased. The authors of paper [16]consider a cloud computing setting in which similarly querying of metric data is outsourced to a service provider. The data is to be revealed only to the trusted users, not to the service provider or to anybody else. Outsourcing offers the data owner scalability and low initial investment. The paper [17]focuses on the development of a privacy preserving automatic diagnosis system whereby a remote server classifies a biomedical signal provided by the client without getting any information about the signal itself.

Kekre et al.[18] proposed a method to search and retrieve similar images from a large database. In this Euclidian distance between the feature vectors of query image and the database images are considered.[19]presents innovative content based image retrieval techniques based on feature vectors as fractional coefficients of transformed images using DCT and walsh transform. Here the feature vectors are extracted in fourteen different ways from the transformed image. The paper [20]presents a fully reversible, dual-layer watermarking scheme with tamper detection capability for medical images. This scheme utilizes a concept of public-key cryptography and reversible data hiding technique. This is tested using medical images in DICOM format. The tamper localization function together with the reversibility of the watermarks makes this scheme a well-suited one for doctors as the scheme does not interfere with medical diagnosis. In this section, we analyzed the advancements and shortcomings of related study works. Considering those limitations, we propose this method for high security, privacy and retrieval efficiency.

3. PROPOSED METHOD

This section explains about the proposed work done for secured retrieval of medical images from the database through watermarking techniques. The proposed work is divided into three phases namely (1) Stego image generation, (2) Visual cryptography (3) Privacy preserving using untrusted client as shown in figure (1). The overall flow of the proposed work is shown in the figure (3). The detailed explanations of various phases are discussed in the corresponding subsections.

Figure 1: Mainframe of the proposed Work

3.1 Stego Image Generation

In this,the invisiblewatermarking techniqueis used which includes the process of selection of query image, secret image, embedding and extraction of watermark.To retrieve the images from the database, user gives a query image as input. The images related to the query image are retrieved from the database if the user has

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

authentication for retrieval. The invisible watermark is embedded into the data in such a way that the changes made to the pixel values are perceptually not noticed. It is used as evidence of ownership and to detect misappropriated images. The output of the embedding phase is the stego image. Figure (2) shows the process of embedding and extraction of watermark.

3.2Embedding And Extraction Process

In this process, the secret image is converted to binary message through the block adaptive technique, which is formulated from block truncation coding. It is a one-bit adaptive moment-preserving quantifier that preserves certain statistical moments of small blocks of the input image in the quantized output.

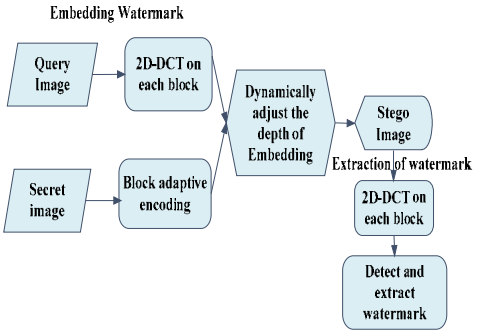

Figure 2: Embedding and Extraction of Watermark

For the conversion, the given secret image is segmented into n x n non overlapping blocks. Two quantizers namely mean and standard deviation values are determined using the equation (1) and (2) respectively for each pixel present in the blocks.

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

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

Here, x represents the total number of pixels in the given image and m_i denotes the value of the i^{th} pixel presented in an image block. The value obtained for $\bar{m}$ is set as the threshold value, which is compare with each pixel value m_i. Based on the comparison the binary message block is generated through the equation (3). 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.

$$BB = \int_0^1 \begin{cases} m_i \geq \bar{m} \\ m_i < \bar{m} \end{cases} \quad \text{-------(3)}$$

The query image is processed to determine the pixels. For this determination 2D-DCT (Discrete cosine Transform) is used. This technique is used to partition the image into parts of different importance and converts an image from the spatial domain to the frequency domain. The cover image is divided into 8x8 blocks and each block is processed using the DCT to determine the suitable pixels to insert the binary image values.Here, a threshold value for each block is determined using equation (4). Based on this threshold, pixel for embedding the binary values of secret image is determined.

$$p = \text{mod}(b(l,l),s) \quad (4)$$

The depth of the embedding information is adjusted by a quantizer S in equation (4). 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.

$$b(l,l) = \begin{cases} b(l,l) - p - \frac{Z}{4} & \text{if } p \leq \frac{Z}{4} \\ b(l,l) - p + 3*\frac{Z}{4} & \text{if } p > \frac{Z}{4} \text{ and } p \leq Z*\frac{Z}{4} \\ b(l,l) & \text{Otherwise} \end{cases} \quad (5)$$

Similarly, the equation (6) is used when the binary bit is zero.

$$b(l,l) = \begin{cases} b(l,l) - p + 5*\frac{Z}{4} & \text{if } p \geq 3*\frac{Z}{4} \\ b(l,l) - p + 3*\frac{Z}{4} & \text{if } p < 3*\frac{Z}{4} \text{ and } p \geq Z*\frac{Z}{4} \\ b(l,l) & \text{Otherwise} \end{cases} \quad (6)$$

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.

Journal of Theoretical and Applied Information Technology
30th November 2013. Vol. 57 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

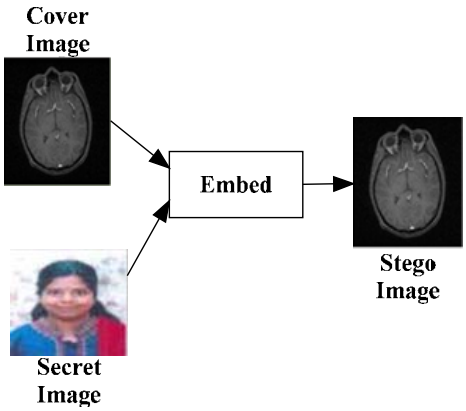

Figure 3: An illustrative example of stego image generation

The stego image is used to extract the watermarked image from the query image. The watermark extraction system segments the stego image into 8x8 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 equation (7).

$$V(m,r) = \begin{cases} 1 & if\ mod(b(l,l).s > \frac{s}{2} \\ 0 & Otherwise \end{cases} \quad \text{----- (7)}$$

To verify whether the generated stego image is similar to original image, some of the quality metrics such as MSE(Mean squared error), PSNR (peak signal to noise ratio), Normalized cross-correlation, Average difference structural content, Maximum difference are computed.

3.2.1 MSE and PSNR

The Mean square error (MSE) and the Peak signal to Noise Ratio (PSNR) are the two error metrics used to compare image compression quality. The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents the measure of the peak error. Lower the value of MSR, lower the error. To compute PSNR (9), the block first calculates the mean-squared error using the equation (8).

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[f(i,j)-f'(i,j)^2] \quad (8)$$

Here, M and N are the number of rows and columns in the input images, respectively.

$$PSNR - 10log_{10}(\frac{R^2}{MSE}) \quad (9)$$

Here, R is the maximum fluctuation in the input image data.

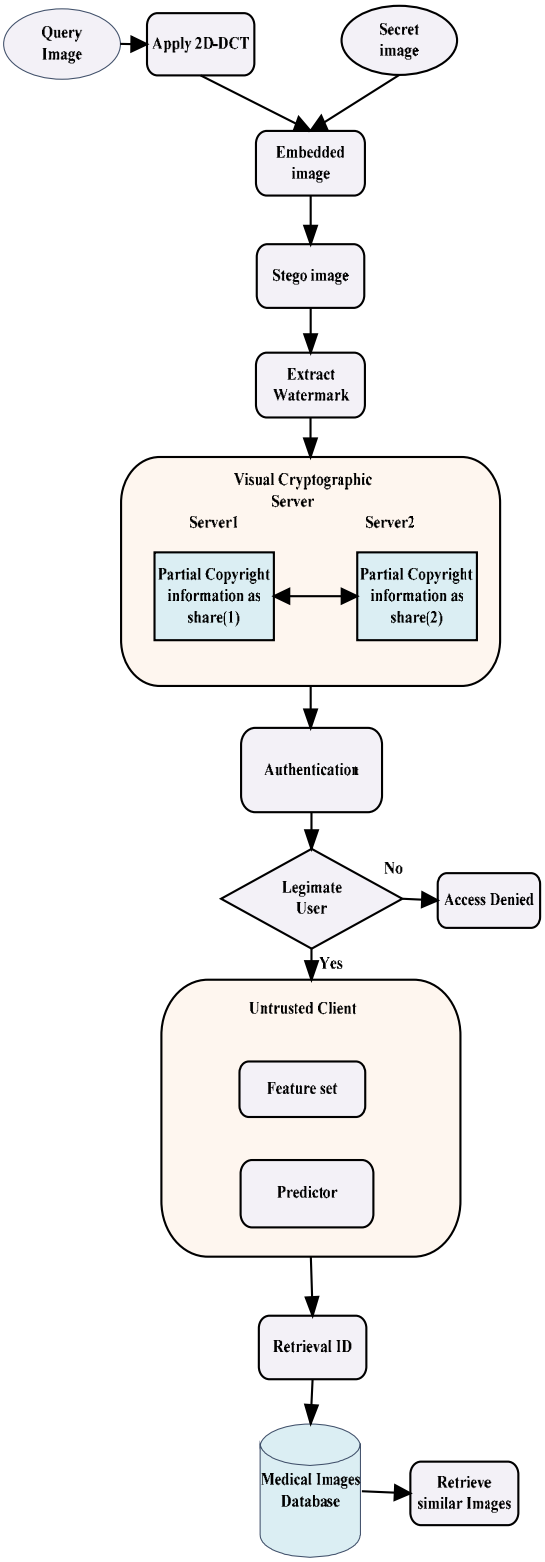

Figure 4: Overall flow of the Proposed Work

Journal of Theoretical and Applied Information Technology
30th November 2013. Vol. 57 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.2.2 Normalized Cross Correlation

Normalized correlation is one of the best known method that evaluate the degree of closeness between two functions. This measure can be used to determine the extent to which the original image and the stego image are close to each other, even after embedding data. This is calculated by using the equation (10).

NormalizedCross

$$\text{Correlation}=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}[f(i,j).f'(i,j)]}{\sum_{i=1}^{M}\sum_{j=1}^{N}[f(i,j)]^2} \quad (10)$$

3.2.3 Average difference

A lower value of Average Difference (AD) gives a "cleaner" image as more noise is reduced and it is computed using (11).

Average Difference

$$(\text{AD})=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[f(i,j)-f'(i,j)] \quad (11)$$

3.2.4 Maximum Difference

It is calculated using the equation (12) and it has a good correlation with MOS for all tested compression techniques so this is preferred as a very simple measure as a reference for measuring compressed picture quality in different compression systems. Large value of MD indicates that the picture is of poor quality.

Maximum Difference

$$(\text{MD})= \text{Max}(|f(i, j)-f'(i,j)|) \quad (12)$$

3.2.5 Structural Content

This measure effectively compares the total weight of an original image to that of a coded. It is therefore a global metric. The structural content is given by eq.(13) and if it is spread at 1, then the decompressed image is of better quality and large value of SC means that the image is of poor quality

Structural Content

$$(\text{SC})=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}[f(i,j)]^2}{\sum_{i=1}^{M}\sum_{j=1}^{N}[f'(i,j)]^2} \quad (13)$$

Both the original image and watermark image are converted into the binary image as shown in Figure 5.

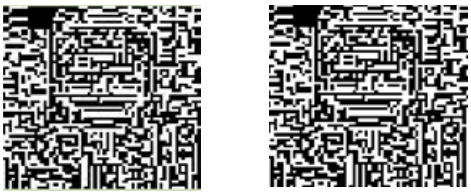

Figure 5: Binary image of original and extracted watermark image

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

1. Universal Image Quality Index (UIQI)

Consider the original and watermark image as $O=\{O_i|i=1,2,\ldots,X\}$, $T=\{T_i|i=1,2,\ldots,X\}$. With this, the UIQI can be determined from the equation 14).

$$R=\frac{4*\rho_{mn}*\bar{m}*\bar{n}}{(\rho_m^2+\rho_n^2)*((\bar{m})^2+(\bar{n})^2)} \quad (14)$$

Where, $\bar{m}, \bar{n}, \rho_m^2, \rho_n^2, and\ \rho_{mn}$ can be manipulated from the equation 9, 10, 11, 12, and 13.

$$\bar{m}=\frac{1}{x}\sum_{i=1}^{x}m_i \quad (15)$$

$$\bar{n}=\frac{1}{x}\sum_{i=1}^{x}n_i \quad (16)$$

$$\rho_m^2=\frac{1}{x-1}\sum_{i=1}^{x}(m_i-\bar{m})^2 \quad (17)$$

$$\rho_n^2=\frac{1}{x-1}\sum_{i=1}^{x}(n_i-\bar{n})^2 \quad (18)$$

$$\rho_{mn}=\frac{1}{x-1}\sum_{i=1}^{x}(m_i-\bar{m})(n_i-\bar{n}) \quad (19)$$

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 0 quality index is the combination of three different factors namely (1) luminance distortion, (2) loss of correlation, and (3) contrast distortion. Therefore, the definition of R can be redefined, and it is represented in the equation (20).

$$R=R_1*R_2*R_3 \quad (20)$$

$$R_1=\frac{\rho_{mn}}{\rho_m*\rho_n} \quad (21)$$

$$R_2=\frac{2*\bar{m}*\bar{n}}{((\bar{m})^2+(\bar{n})^2)} \quad (22)$$

$$R_3=\frac{2*\rho_m*\rho_n}{\rho_m^2+\rho_n^2} \quad (23)$$

$$R=\frac{\rho_{mn}}{\rho_m*\rho_n}*\frac{2*\bar{m}*\bar{n}}{((\bar{m})^2+(\bar{n})^2)}*\frac{2*\rho_m*\rho_n}{\rho_m^2+\rho_n^2} \quad (24)$$

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

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

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.

2. Structural Similarity Index Metric (SSIM)

SSIM value can be computed from the equation (25).

$$SSIM = \frac{(2\bar{m}\bar{n}+z1)(2\rho_{mn}+z2)}{(\rho_m^2+\rho_n^2+z2)((\bar{m})^2+(\bar{n})^2+z1)} \quad (25)$$

Here, $\bar{m}, \bar{n}, \rho_m^2, \rho_n^2, and\ \rho_{mn}$ 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.

3. 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 it can be verified whether the inserted and extracted watermark is same.

3.3 Visual Cryptographic model

In Visual Cryptographic server model the extracted watermarked image is divided into two shares such that each pixel in the original image is replaced with a non-overlapping block of two sub-pixels. Anyone who holds only one share will not be able to reveal any information about the secret image. To decode the image, each of these shares is Xeroxed into a transparency. Stacking both these transparencies will permit visual recovery of secret image.

Figure 6: The Image of the Extracted Watermark

Share 1 Share 2

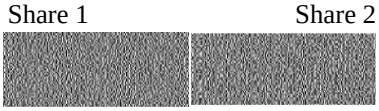

Figure 7: Two shares of the Extracted Watermark

Figure(6) shows the image of the extracted watermark and this watermarked image is divided into two shares (share 1, share 2) as shown in the figure (7). The visual Cryptographic model consists of server1, server2 and the target. Share 1 consists of the partial copyright information of the watermarked image that is stored in the server 1 and the share 2 consists of another part of the copyright information that is stored in the server 2.Exclusive-OR (XOR) operation is done between two shares to obtain the full image. The target consists of the full image .i.e. the stack of share 1 and share 2. The target consists of many images of registered watermark. When the given combined share (watermarked image) matches with anyone of the images in the target then the authentication is provided. This verification is done by computing Hausdorff distance metric between the extracted watermark and the registered watermark in the target database.

3.3.1Hausdorff Distance Metric

The Hausdorff distance measures the extent to which each point of a model set lies near some point of an image set and vice versa. Thus, this distance can be used to determine the degree of resemblances between two objects that are superimposed to one another. It is used as a similarity measure between a general face model and possible instances of the object within the image.

Given two finite point sets A= $\{a_1 \dots \dots a_p\}$ and B= $\{b_1 \dots \dots b_q\}$, the Hausdorff distance is defined as in eq.26 & 27.

$$H(A,b) = \max\left(h(A,B), h(B,A)\right) \text{ ---- (26)}$$

Where, $h(A,B) = \max_{a\in A} \min_{b\in B} \|a-b\|$- (27)

From the Hausdorff distance metric equation, the distance of the images, related to the extracted watermark image is obtained. If the distance is 0 then, that image is the expected image. i.e. if the distance is minimum then the images are more similar.

If both these images are equal then the authentication is provided to the user. Else the authentication to access the database is denied to the user.

3.3.2Privacy Preserving using untrusted client

Privacy Preserving is a concept in which similarly querying of metric data is outsourced to a service provider. The data is to be revealed only to trusted users and not to the service provider or to anyone else Outsourcing offers the data owner scalability and a low initial investment.

Journal of Theoretical and Applied Information Technology
30th November 2013. Vol. 57 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

According to our proposed method the privacy preserving server is used to make functions such as Image classification using(K-NN classifier) and Predicts the category of the image.

Figure (8) depicts our scenario for outsourcing data. It consists of three entities: a data owner, a trusted query user, and an untrusted server. On the one hand the data owner wishes to upload his data to the server so that users are able to execute queries on those data. On the other hand, the data owner trusts only the user and nobody else including the server.

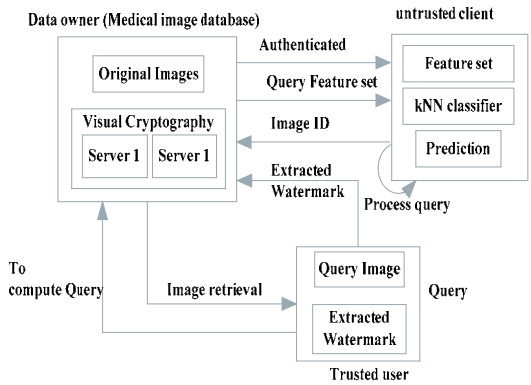

Figure 8: Scenario Overview

3.3.3K-NN classifier

The K-Nearest Neighbors algorithm is a nonparametric method in that no parameters are predictable. Alternatively, the proximity of neighboring input interpretation for the training data set, and interrelated output values are used to predict the output values of cases in the validation data set.

Moreover, k-NN process is used for classification purpose.An image is classified and assigned to a specified class through a majority vote of its k nearest neighbors. Here, the classifier 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. Authors used Euclidean distance for distance measure. By this way, the images of a database are classified under different classes accurately. K-NN classifier is better while comparing with other classifier.

3.3.4Prediction

Prediction is done on the images to find out whether it belongs to Grade 1, Grade 2 or Grade 3 of tumor. The images are classified based on the grade to which they belong to. So that, the retrieval can be done fast. If the Query image belongs to Grade 1 then, the category of the image is given to the data owner.

3.3.5 Retrieval

When a doctor (Trusted user) makes a query to the data owner, the query is processed and the feature set of the query image is given to the untrusted client. In the untrusted client side, the images are classified based on the kNN classifier and ID of the images very close to the query image is selected. As shown in the Figure (8),the grade of the query image is predicted and the category of the image is given to the data owner. Medical Image database on the owner side gives the entire image belonging to the given category to the user (Trusted client). Thus, the images are retrieved efficiently and securely from the database.

4. EXPERIMENTAL RESULTS

The proposed technique is experimented for its efficiency. For analysis purpose authors of this paper have taken a database containing 145 brain images. These images are collected from medpix dataset. The database consists of three different grades of tumor images.Grade I tumor - Astrocytoma, Grade IItumor- oligodendroglioma, Grade III tumor-Malignant oligodendroglioma. Authors assumed that only the doctors of the hospital have authentication to access the database image. For accessing the database, authorization details are provided through invisible digital watermarking images. The photos of doctors act as the watermarking images, which are embedded into the query image. For experimental purpose a brain image is taken as query image and embedded with the photo of the user to generate the stego image. This work uses 512 x 512 query images and the 64 x 64 watermark image.

The quality of the stego image is analyzed using various Quality metrics. The value obtained for each quality metrics is tabulated in table (1).The lower the value of MSE and high value of PSNR shows that the error is low. The value obtained for Normalized cross correlation shows that the original image and the stego image are close to each other. The value of structural content is 1 which shows that the image is of better Quality and

Journal of Theoretical and Applied Information Technology
30th November 2013. Vol. 57 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the Low value of Average Difference shows that the image is clean.

Table 1: Slice Quality Analysis

Quality metrics	Value
MSE	0.1506
PSNR	57.8942
Normalized cross correlation	1.0000
Average difference	-0.0176
Structural content	1.0000
Maximum Difference	5

Table (2) represents Watermark Quality Analysis by comparing results of various attributes. The value obtained for Quality and SSIM are equal to 1 which shows that the extracted watermark image and its corresponding original image is of greater similarity. In addition to that BER value is too small (0) than the predefined threshold that specifies that there is no 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.

Table 2: Watermark Quality Analysis

Attribute	Value
SSIM	1
Quality	1
Bit Error Rate	0

Table (3) shows the analysis of two classifiers, Bayesian and K-NN. The K-NN classifier is compared with Bayesian classifier and from the results obtained it is obvious that K-NN classifier gives 100% accurate classification of images.

Table 3: Classifier Analysis

Classifier	Sensitivity (%)	Specificity (%)	Accuracy (%)
Bayesian	65.9	75.44	62.06
K-NN	100	100	100

The images of the dataset are classified, in prior to access by an authenticated user. The classification is carried out using the k-NN classifier. The classifier classifies the images and groups the similar images under different categories. Depending on the GLCM features of the images in the dataset, they are classified into Grade -1, Grade -2 and Grade -3 as shown in figure (9). This classification process helps for efficient retrieval process.

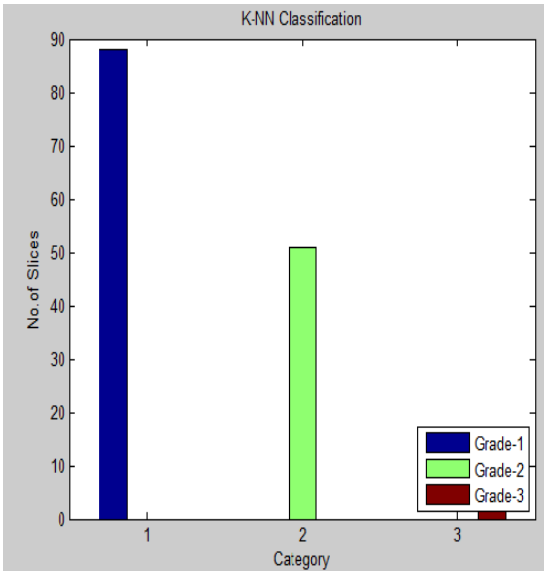

Figure 9: Chart showing various Grades of images

During retrieval, the query image's (after extraction of watermark image) GLCM features are estimated to determine the category of the image. If the query image belongs to particular grade, then ID of all the images belonging to that grade is retrieved. This retrieval ID is passed to the Medical image Database (Data owner) for retrieval of images by the trusted user. Figure (10) shows ID of all the images retrieved that belongs to Grade -1 category.

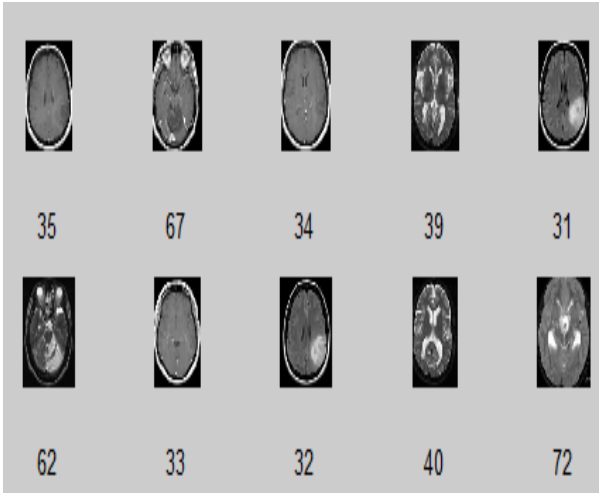

Figure 10: Retrieved Images from the Dataset

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table (4) shows the distance between the query image and the retrieved neighbor image ID's. With this data we can analyze that at what distance the retrieved images are placed from the query image.

Table 4: Distance between query image and neighbor image ID

Image ID	DistanceMeasure between Query and Retrieved Image
35	6.335525941638029e+000
67	7.749834365802461e+000
34	3.141894368332418e+001
39	5.600492795410948e+001
31	6.201822147901120e+001
62	6.768008529051279e+001
33	6.795805088871785e+001
32	7.125642249290304e+001
40	7.471456739317276e+001
72	7.756552675652740e+001

The efficiency of the proposed model is visualized in the graph shown in figure 11 & 12. The time taken by this visual cryptographic model to analyze each images in the dataset is presented in fig. 11. The time taken to retrieve the images is shown in fig 12.

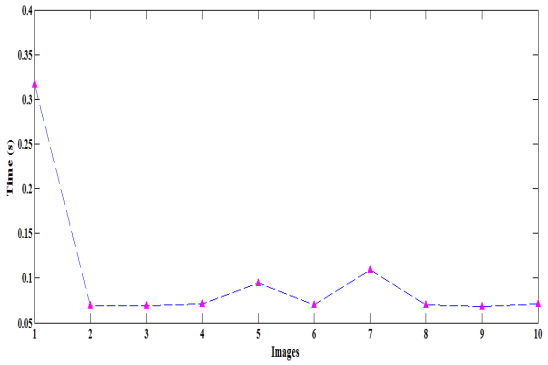

Figure 11: Time Analysis for Visual Cryptographic model

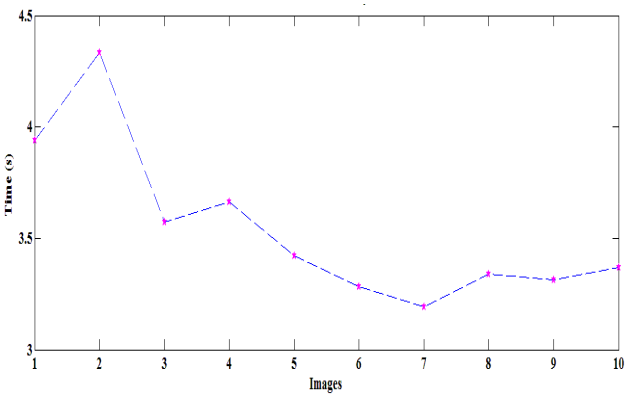

Figure 12: Retrieval Time Analysis

5. CONCLUSION

This paper is the enhancement of the former work done by the author on watermarking, and proposes a new method that can provide better security. The security of this scheme is ensured by the properties of visual cryptography and by the usage of untrusted client. Visual cryptography works in such a way that the data cannot be retrieved unless the retriever has the secret image.i.e. encryption is done in a manner by which the decryption cannot be done by an unauthenticated user. The advantage of the embedding scheme is that the Host image will not be altered during the process. Also outsourcing of the data to the untrusted client provides privacy preserving as they make the work done without getting any information about the data and about the final result. Existing solutions either offer query efficiency at no security and privacy, or they offer complete data privacy with sacrificing the query efficiency. The Experimental results prove that our proposed method offers retrieval efficiency, security and privacy. Some future options that can be explored are: Alternative region definitions, other than 8x8 blocks and other perceptual similarity, or error metrics can be used.

REFERENCES:

[1] B. Planitz and A. Maeder, "Medical image watermarking: A study on image degradation," in *Proc. Australian Pattern Recognition Society Workshop on Digital Image Computing, WDIC*, 2005.

[2] R. Kaur, "A Medical Image Watermarking Technique for Embedding EPR and Its Quality Assessment Using No-Reference Metrics," *International Journal of Information*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Technology and Computer Science (IJITCS), vol. 5, p. 73, 2013.

[3] M. A. Hajjaji, A. Mtibaa, and E.-B. Bourennane, "A Watermarking of Medical Image: Method Based'LSB'," *International Journal of Computer Science Issues*, 2011.

[4] S. A. Mostafa, N. El-sheimy, A. Tolba, F. Abdelkader, and H. M. Elhindy, "Wavelet packets-based blind watermarking for medical image management," *The open biomedical engineering journal*, vol. 4, p. 93, 2010.

[5] R. E. Philip and M. Sumithra, "Development Of A New Watermarking Algorithm For Telemedicine Applications," *Development*, vol. 3, pp. 962-968, 2013.

[6] M. Ulutas, G. Ulutas, and V. V. Nabiyev, "Medical image security and EPR hiding using Shamir's secret sharing scheme," *Journal of Systems and Software*, vol. 84, pp. 341-353, 2011.

[7] J. Natarajan and V. R. Rathod, "Medical Image Watermarking Using a Perceptual Similarity Metric," *MIT International Journal of Electrical and Instrumentation Engineering*, vol. 1.1,2011.

[8] B. Kaur, A. Kaur, and J. Singh, "Steganographic Approach for Hiding Image in DCT Domain," *International Journal of Advances in Engineering & Technology*, vol. 1, pp. 72-78, 2011.

[9] A. Ross and A. A. Othman, "Visual cryptography for face privacy," in *Proc. of SPIE Vol*, 2010, pp. 76670B-1.

[10] B. Surekha, G. Swamy, K. S. Rao, and A. R. Kumar, "A watermarking technique based on visual cryptography," *Journal of Information Assurance and Security*, vol. 4, pp. 470-473, 2009.

[11] C.-S. Hsu and S.-F. Tu, "Digital watermarking scheme with visual cryptography," *IMECS, Hong Kong (March 2008)*, 2008.

[12] K. S. Rawat and D. S. Tomar, "Digital Watermarking Schemes for Authorization against Copying or Piracy of Color Images," *Indian Journal of Computer Science and Engineering*, vol. 1, pp. 295-300, 2010.

[13] B. Surekha, G. Swamy, and K. S. Rao, "A multiple watermarking technique for images based on visual cryptography," *Computer Applications*, vol. 1, pp. 77-81, 2010.

[14] R. Dhanalakshmi and K. Thaiyalnayaki, "Dual watermarking scheme with encryption," *arXiv preprint arXiv:1002.2414*, 2010.

[15] P. Gupta, "Cryptography based digital image watermarking algorithm to increase security of watermark data," *International Journal of Scientific & Engineering Research*, vol. 3, pp. 1-4, 2012.

[16] M. L. Yiu, I. Assent, C. S. Jensen, and P. Kalnis, "Outsourced similarity search on metric data assets," *Knowledge and Data Engineering, IEEE Transactions on*, vol. 24, pp. 338-352, 2012.

[17] M. Barni, P. Failla, R. Lazzeretti, A.-R. Sadeghi, and T. Schneider, "Privacy-preserving ECG classification with branching programs and neural networks," *Information Forensics and Security, IEEE Transactions on*, vol. 6, pp. 452-468, 2011.

[18] H. Kekre and D. Mishra, "Digital Image Search & Retrieval using FFT Sectors of Color Images," *International Journal on Computer Science and Engineering*, vol. 2, pp. 368-372, 2010.

[19] H. Kekre, S. D. Thepade, and A. Maloo, "Image retrieval using fractional coefficients of transformed image using DCT and Walsh transform," *International Journal of Engineering Science and Technology*, vol. 2, pp. 362-371, 2010.

[20] C. K. Tan, J. C. Ng, X. Xu, C. L. Poh, Y. L. Guan, and K. Sheah, "Security protection of DICOM medical images using dual-layer reversible watermarking with tamper detection capability," *Journal of Digital Imaging*, vol. 24, pp. 528-540, 2011.