International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 5 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT195533

Medical Image Privacy Using Watermarking Techniques

B. Ananthapraba[1*], K. Thyagarajan[2]
[1*,2]Department of Computer Science, A.V.C. College, Mayiladuthurai, India
*Corresponding Author: ananthivis96@gmail.com

ABSTRACT

The amount of digital medical images has increased rapidly in the Internet. The necessity of fast and secure diagnosis is vital in the medical world. Nowadays, the transmission of images is a daily routine and it is necessary to find an efficient way to transmit them over the net. In this project we propose a new technique to cipher an image for safe and denoised transmission. The existing research deals with image cryptography, data hiding and steganography. There are several methods to encrypt binary or grey level images. Watermarking can be an answer to make secure image transmission. For applications dealing with images, the watermarking objective is to embed invisibly message inside the image. To embed the encrypted image in the patient information we have used watermarking technique. In this project, we concentrate to solve the privacy violation problem occurred when images are published on the medical applications without the permission. According to such images are always shared after uploading process. Therefore, the digital image watermarking based on DWT co-efficient. Watermark bits are embedded in uploaded images. Watermarked images are shared in user home page. So images can be difficult to misuse by other persons. In receiver side when the message is arrived then we apply the inverse methods in reverse order to get the original image and patient information and to remove watermark we extract the image before the decryption of message. We have applied and showed the results of our method to medical images.

Keywords : Medical image, Image Privacy, Watermarking, DWT co-efficient, Distortion

I. INTRODUCTION

Until recently the sole responsibility of keeping patients' records in confidence was with the Physicians. This meant that the Physician was not to disclose any medical information revealed by a patient or discovered by a physician in connection with the treatment of a patient to any unauthorized person. However, with the advent of recent computer technology, and it's permeation into the Medical field through E-health, Telemedicine, to name but a few, the challenges of confidentiality arising from the storage and transmission of medical data cannot be left to physicians alone. Indeed, transferring medical data such as radiological results from a medical database center to another one without applying security techniques means low level of privacy for patients. Medical information transmission has increased with the use of telemedicine. Security of medical information imposes three mandatory characteristics: confidentiality, reliability and availability. Confidentiality means that only the entitled users have access to the information and this can be achieved using encryption. Reliability has two aspects; i) Integrity: the information must not been modified by unauthorized people, and, ii) Authentication: a proof that the information belongs indeed to the correct patient and is issued from the correct source and one of the techniques to achieve this is watermarking. Availability is the ability of an information system to be used by the entitled users in the normal scheduled conditions of access and exercise. For storage and transmission, encryption is a very efficient tool, but once the sensitive data is decrypted, the information is not protected anymore. Once the images are in the open (plain-text) form, the major threat is the violation of the access rights and of the daily logs by the intruder. Telemedicine is important because it enables consultations by remote specialists, loss-free and immediate availability of individual patient information, and improved communication between partners in a health care system. Security is the most important issue during transmission of medical images.

As the medical images are sensitive so, it is necessary to protect them. Watermarking, digital fingerprint/signature, encryption, time of coding and encoding are the existing techniques for protecting images. But all this methods have some drawbacks. Medical image security is an important issue when digital images and their pertinent patient information are transmitted across public networks. Watermarking is made to introduce identifiers, which, by construction, are inseparable from the document they are embedded in. They may be seen as ultimate ramparts against usurpation and fabrication. Medical tradition is very strict with the quality of biomedical images, in that it is often not allowed to alter in any way the bit field representing the image (nondestructive). Watermarking technique is based on the data modification principle. Therefore, the watermarking method must be reversible, in that the original pixel values must be exactly recovered. This limits significantly the capacity and the number of possible methods. It also constrains to have dedicated routines to automatically suppress and introduce the mark in order to prevent the transmission of unprotected documents.

II. RELATED WORK

Hang Cheng et.al,…[1] considered a privacy-preserving image retrieval scheme which involves three parties: content owner, authorized user, and server. The content owner encrypts images in the JPEG format and then stores them into cloud servers. The authorized user, may be a content owner, has desire to retrieval images similar to the encrypted query image from encrypted database images. When receiving the encrypted query image, the server can calculate the distances between the encrypted query image and database images and then returns encrypted images similar to the query image in plaintext content, without knowing anything about the plaintext contents of the involved encrypted images. It is known that there exist the intra-block, inter-block, and inter-component dependencies among DCT coefficients of a color JPEG image. Moreover, in some sense, the three types of dependencies are similar between similar images. Based on the analysis, propose a novel scheme for encrypted JPEG images, where intra-block, inter-block, and inter-component dependencies among DCT coefficients are introduced. With this scheme, the encrypted JPEG images can be obtained through a combination of the stream cipher and permutation encryption and outsourced to a server. And also, with the given encrypted query image and the encrypted database images, it is easy for the server to calculate their similarities in encrypted domain by employing the techniques of a Markov process and multi-class support vector machine (SVM). As the purpose of scheme is to address the problem of image retrieval in encrypted domain while preserving the file size and format compliance for JPEG images, here, first take a partial image encryption technique into account to encrypt JPEG images. The problem is difficult to solve for the traditional cryptography. The most existing partial encryption techniques for JPEG images are mainly based on blocks shuffle, DCT coefficient permutation, and encrypting the signs of DCT coefficients. Recent work presents a novel partial encryption method based on a JPEG bit-stream, which aims to implement reversible data hiding in an encrypted gray JPEG image. The proposed encryption method cannot only meet the requirements of format compliance and file size preservation but also provide valuable information regarding the length of each variable length integer (VLI) code for DCT coefficients. More importantly, the encryption method can make the length of each VLI code remain unchanged before and after encryption. It means that one can still obtain the original length of any VLI code related to DCT coefficients from an encrypted JPEG image. Due to the dependencies of DCT coefficients in each component, their corresponding VLI code length may have similar relationships, which can be exploited to generate feature for image retrieval. The U and V components can be done similarly. But different encryption keys are adopted. After that, encrypt the quantization tables stored in the JPEG file header by using the stream cipher. In brief, the binary sequences with respect to the quantization tables from the file header are encrypted. In particular, different encryption keys are employed to different quantization tables for protecting the privacy of the quantized DCT coefficients. For better encryption, we further pseudo-randomly permute encoded binary sequences of DC coefficients in a same component when keeping their frequency position intact. And also, the encrypted bits within the same binary sequence stay their original unencrypted positions. With the proposed retrieval mechanism, the server without the encryption keys can perform image retrieval in encrypted domain. Considering an encrypted image, the server first parses its corresponding encrypted JPEG bit-stream to extract all Huffman codes for DCT coefficients of each component. The extraction operation, in this step, is readily accomplished because of file format compliance before and after encryption. Next, exploiting the Huffman tables obtained from the file header to decode Huffman codes, we can obtain the length of each VLI code next to the Huffman code. That is, any DC or nonzero AC coefficient can be represented as a nonnegative integer that is equal to the length of the corresponding VLI code.

Alfredo Rial, et.al,…[2] analyzed the main contribution of work is a formal security analysis of BSW protocols. We employ the ideal-world/real-world paradigm to define security of anonymous BSW protocols. With respect to classical asymmetric fingerprinting schemes, which define each security property separately, this definition leads to the construction of protocols that are secure under composition. The definition is general in the sense that it captures the security properties required for any copyright protection protocol that provides buyers with anonymity. Additionally, define security for blind and readable watermarking schemes, and analyze the properties that watermarking schemes should provide for the construction of secure BSW protocols. A zero-knowledge proof of knowledge is a two-party protocol between a prover and a verifier. The prover proves to the verifier knowledge of some secret input that fulfills some statement without disclosing this input to the verifier. The protocol should fulfill two properties. First, it should be a proof of knowledge, i.e., a prover without the knowledge of the secret input convinces the verifier with negligible probability. More technically, there exists a knowledge extractor that extracts the secret input from a successful prover with all but negligible probability. Second, it should be zero-knowledge, i.e., the verifier does not learn any information about the secret input. More technically, for all possible verifiers there exists a simulator that, without knowledge of the secret input, yields a transcript that cannot be distinguished from the interaction with a real prover. The buyer–seller watermarking protocol BSW is based mainly on two cryptographic primitives: group signatures and homomorphic encryption. Group signatures allow buyers to sign the purchase messages they send to the seller on behalf of the group of buyers. Thanks to that, the seller can verify the signature without knowing buyer's identity, and thus purchases are anonymous. When a pirated copy is found and traced back to a particular purchase, the corresponding signature can be opened to know the identity of the buyer that released the pirated copy. And note that, although in the description of our construction all the buyers belong to the same group, in practical implementations there can be several groups. We have proposed a security definition for copyright protection protocols in the ideal-world/real-world paradigm. Furthermore, we have analyzed the security of an anonymous BSW and proven that it fulfills our definition. Particularly, we have shown that the protocol is secure against any p.p.t. adversary when instantiated with a watermarking scheme, an encryption scheme, a group signature scheme, and zero-knowledge proofs of knowledge that provide security against any p.p.t. adversary. Unlike the other building blocks, no watermarking scheme has been proven to offer this security level, and thus the actual security of the protocol against malicious buyers is lowered to the security offered by the watermarking scheme. Combining encryption with digital watermarking, a buyer–seller watermarking (BSW) protocol is in fact an asymmetric fingerprinting protocol where the fingerprint is embedded by means of watermarking in the encrypted domain. The basic idea is that each buyer obtains a slightly different copy of the digital content offered by the seller. Such a difference, the watermark (or fingerprint), does not harm the perceptual quality of the digital content and cannot be easily removed by the buyer. Thanks to the latter property, when a malicious buyer redistributes a pirated copy, the seller can associate the pirated copy to its buyer by its embedded watermark. On the other hand, a malicious seller cannot frame an honest buyer because the buyer's watermark and the delivered watermarked content are unknown to the seller. As a consequence, the watermark tracing mechanism is discredited.

Jun Zhang, et.al,…[3] implemented the system and first, the participants and their roles in an image retrieval watermarking protocol are different from those in a buyer–seller watermarking protocol. In a buyer– seller watermarking protocol, the seller is the owner of a digital content, who conducts the watermark insertion, and the buyer can obtain a watermarked digital content. In contrast, in an image-retrieval watermarking protocol, the user is the owner of a query image, who should insert a watermark to protect its right, and the service provider of CBIR will search images according to the watermarked query image obtained from the user. The difference makes some existing security solutions inapplicable; e.g. the solution of the unbinding problem for a buyer–seller watermarking protocol is inapplicable in an image-retrieval watermarking protocol. Second, a new watermarking protocol should be easily embedded in real-world image retrieval systems. It should require a direct interaction between the user and the service provider. In the previous work, a three-party protocol was proposed to solve the user right problem in CBIR systems. However, that protocol is based on a trusted third party, WCA, and the user needs to contact WCA for requesting a watermark, which is against the user's habits in CBIR and will hinder the applications of CBIR. In this paper, a novel two-party watermarking protocol is proposed to overcome this shortcoming. The proposed protocol provides a higher security level by solving the problems that were not considered in the previous work. Third, different watermarking protocols have different requirements to balance the quality of watermarked digital content and the robustness of digital watermark. It is a hard problem behind buyer–seller watermarking protocols, since the customer requires high-quality digital content, which conflicts with the robustness of digital watermark. However, this problem is not serious in the CBIR systems, because the user cares about the retrieval performance instead of the quality of watermarked query image. In this paper, a novel research on content-based image retrieval of watermarked query images is reported to show that it is possible to improve the robustness of digital watermark by reducing the quality of watermarked query images without influencing retrieval performance. The user right problem. This problem has two aspects. On the one hand, the service provider of CBIR may distribute the user's private query image without authentication. On the other hand, the user may frame a service provider. The unbinding problem: In the context of CBIR, it means that the user may transplant the watermark embedded in a pirated copy into a copy of higher-priced query image. The anonymity of users: In CBIR, an ordinary user may not have any identifications and the anonymity of the user should be retained during the whole image retrieval session. Partial watermark removement: In the context of CBIR, this attack means that the service provider may remove its part of watermark, so as to defeat the user right protection. Secure verification problem. An arbitrator is able to remove an original watermark from an unauthorized copy and resell multiple copies of it with impunity. In this paper, we proposed a new two-party image-retrieval watermarking protocol, which can address six problems: the user right problem, the unbinding problem, the anonymity of users, partial watermark removal, secure verification problem and the dispute problem. The proposed protocol outperforms the existing three-parity protocol due to its feasibility and security. We also empirically researched CBIR with watermarked query images. The experimental results show that watermarking query images do not affect the retrieval performance; so the robustness of digital watermark can be improved by increasing its strength. Therefore, a low-quality query image has no significant effect to the image retrieval performance in our experiments. Further research is left for future work. Actually, the motivation could also be reduced for the service provider to distribute a low-quality watermarked query image without authorization.

Tiziano Bianchi,et.al,…[4] implemented the system to tackle the problem of watermark detection in the presence of an untrusted verifier (to whom watermark secrets cannot be disclosed), a possible solution offered by secure signal processing is represented by zero-knowledge watermark detection (ZKWD) that uses a cryptographic protocol to wrap a standard watermark detection process. In general, a ZKWD algorithm is an interactive proof system where a prover tries to convince a verifier that a digital content x is watermarked with a given watermark b without disclosing b. In contrast to the standard watermark detector, in ZKWD the Verifier is given only properly encoded (or encrypted) versions of security-critical watermark parameters. Depending on the particular protocol, the watermark code, the watermarked object, a watermark key or even the original unmarked object is available in an encrypted form to the verifier. The Prover runs the zero-knowledge watermark detector to demonstrate to the Verifier that the encoded watermark is present in the object in question, without removing the encoding. A protocol run will not leak any information except for the unencoded inputs and the watermark presence detection result. A flexible solution for zero-knowledge watermark detection is to compute the watermark detection statistic in the encrypted domain (e.g., by using additive homomorphic public-key encryption schemes or commitments) and then use zero-knowledge proofs to convince the Verifier that the detection statistic exceeds a fixed threshold. Apart from the foreseeable evolution of the hardware equipment or advancements in homomorphic encryption, an appealing solution from a signal processing point of view could be combining these schemes with partial encryption techniques, which are often employed in video encryption. In closely related fields, partial encryption has been employed in secure client-side watermarking and as a means for implementing commutative watermarking and encryption. The rationale behind such an approach is that signals are fuzzy entities, which do not require complete protection, so that we can trade off security for a better efficiency. Client-Side Asymmetric Fingerprinting: Although client-side embedding provides an elegant solution to the system scalability problem, the incorporation of the aforementioned technique in an asymmetric fingerprinting protocol does not appear an easy task. Here, the main problem is that the watermarking LUT should not be revealed to the Server. At the same time, neither the Client should have access to the watermarking LUT, since the knowledge of both decryption nor will watermarking LUTs immediately disclose the encryption LUT A common problem of fingerprinting is that several clients may collude and try to remove the fingerprint by comparing the respective watermarked copies. Collusion resistance can be achieved by using specific anticollusion codes in the design of the fingerprint. However, merging collusion resistant techniques and secure embedding is in general a difficult task. As to client-side embedding, a natural solution is to design the watermarking LUTs so that they produce a specific anti-collusion code for each client. Nevertheless, the above strategy still suffers from the fact that watermarking LUTs should be managed by a trusted third party. In secure server-side embedding, the fingerprint depends on private inputs from the Buyer, so that it is not easy to enforce the use of specific anti-collusion codes. A recently proposed solution consists in letting the Buyer pick up fingerprint elements from a list controlled by the Seller, in such a way that the Seller does not know the chosen elements. One of the main concerns is that zero-knowledge proofs do not provide protection against blind sensitivity attacks, but they can only slow the efficiency of this kind of attacks. Moreover, current solutions are still very complex for real life deployment and often made scarcely appealing by the fact that detectors can be implemented within secure environments. It is also worth noting that research on this particular subject has stalled in the last five years, probably due to the difficulty of bringing together the required expertise in both signal processing and cryptography.

Alessandro Piva, et.al,…[5] represented by the client-side watermark embedding: in this case, a server–client architecture is again adopted; however, in this case, the server is allowed to send a unique copy of the content to all the interested users through broadcasting systems, without the need to generate different watermarked copies (thus removing the bottlenecks present in the server-side watermark embedding approach); instead, each client will be in charge of embedding a personal watermark identifying the received copy. In this case, however, since the clients are untrusted, proper solutions need to be devised not to allow malevolent users to have access to the original content or to the watermark to be inserted. A new approach, defined as secure watermark embedding, has been proposed for facing such a problem: here, the server transmits the same encrypted version of the original work to all the clients, but a client-specific secret allows decryption of the content and at the same time implicit embedding of a personalized watermark, obtaining a uniquely watermarked version of the work. To move one step further in the field of secure client-side watermark embedding for multimedia content distribution, considered to improve the above-mentioned method through the adoption of a more robust watermarking scheme. By relying on the well-known results coming from the watermarking community on the superiority of the class of informed embedding (or host-interference rejecting) data hiding schemes with respect to the classical SS methods, aim was to modify the model proposed so that the secure client-side embedding scheme will be able to embed a watermark belonging to the quantization index modulation (QIM) class, that has rapidly become popular as one of the best performing watermarking strategies. In particular, we properly designed an LUT-based secure client-side embedding system allowing us to embed a spread transform dither modulation (ST-DM) watermark. As it will be demonstrated in the following sections, this modification is not straightforward, since the client-side embedding framework imposes some constraints that do not allow us to embed a pure ST-DM watermark. Still, the experimental results will confirm that the superiority of ST-DM versus SS watermarking exhibited in the classical embedding schemes is maintained also in the client-side embedding approach. First, we computed the perceptual degradation introduced by the two watermarking systems, to verify if a comparison between them with equivalent DWR is fair also from the point of view of perceptual quality. In Table III, two image quality metrics, namely the weighted peak signal-to-noise ratio (WPSNR) and the visual information fidelity (VIF), are considered in order to measure the perceived distance between original and watermarked image, using the two considered client-side watermarking systems (SS and ST-DM) for two fixed DWR (30 and 36 dB). The WPSNR is achieved as the PSNR weighted using the contrast sensitivity function (CSF) computed as to weight spatial frequency of error image. The VIF proposed is defined as the ratio between the distorted image information and the reference image information. For the two considered DWR values, the corresponding perceptual metrics demonstrate a good final visual quality of the protected contents for both SS and ST-DM: for a given image and a fixed DWR, the metrics assume almost indistinguishable values for both systems. This allows us to compare the different systems for fixed DWR values, thus ensuring the same perceptual quality of the watermarked images. In this paper, a new scheme following the secure client-side watermark embedding approach for data copyright protection in a large-scale content distribution environment has been proposed. Starting from the idea of LUT-based secure embedding, previously applied to the SS watermarking algorithms only, we modified the ST-DM, belonging to the informed watermark embedding algorithms, in order to design it specifically for the LUT-based secure embedding. A theoretical analysis of the detector performance under the most known attack models, namely the AWGN attack and the average collusion attack, has been carried out. The probabilities of missed detection and wrong accusation have been evaluated in the two cases. The agreement between theoretical and experimental results has been verified through several simulations, considering different values of WNR, different cover contents, different watermarking keys, and different customers, confirming the validity of analysis.

III. EXISTING METHODOLOGIES

The process of digital watermarking involves the modification of the original multimedia data to embed a watermark containing key information such as authentication or copyright codes. The embedding method must leave the original data perceptually unchanged. The major technical challenge is to design a highly robust digital watermarking technique, which discourages copyright infringement by making the process of watermarking removal tedious and costly.

3.1 RDH established method:

The present process is to safeguard incredibly private, exclusive or secret knowledge from unauthorized users. Here, privateness safety is a most important hindrance of many social networking websites. And work making use of Reversible information Hiding (RDH) strategies, goes to acquire its significance attributable to the exponential growth and secret conversation of skills person over the net. All social networking sites' architectures contain number of servers, databases, web site, information like textual content, photograph, video etc. In existing work, user try to upload an photo, the frontend program embed some privateness information into the photo using Reversible data Hiding (RDH) system utilizing and also retailer encrypted snapshot into database. To exhibit this image on buddy's wall, the frontend program exams the portraits embed privateness understanding fit with buddy's privateness understanding. If each privateness knowledge's are equal, then most effective the snapshot is visible to the neighbors. Or else, the person isn't a pal so the picture just isn't obvious. Right here, first system is embedding and 2nd one is to maintain the encrypted picture into database. Ordinarily of knowledge hiding, the photo will expertise some distortion due to knowledge hiding and cannot invert again to the fashioned photo object. That's, some parameter distortion has passed off to the duvet object even after the hidden information have been extracted out. Within the Reversible knowledge hiding, both photo and data are equally principal. The Reversible information hiding system, the customary duvet object losslessly recovered after the message is extracted.

3.2 Broadcast encryption scheme:

The development of privacy-maintaining knowledge is performed by means of the info owner each time individual information need be shared. The fundamental concept is that the info owner has proper control over access to his/her private information, above all those revealing identification knowledge and personal lifestyles (e.g., pictures, videos, copyrighted materials). More commonly, the information owner would act as a group manager who classifies contacts consistent with their roles (e.g., household, coworkers, and excessive university classmates, sporting activities club members) and supplies them the corresponding memberships. Every function defines a subgroup, the individuals of which can be restrained to targeted knowledge classes. A knowledge category is created by the info owner describing the set of information files that can be accessed as an entire by way of one or more subgroups. The granularity of information classes is adjustable depending on the fineness of favored access manipulate. For instance, when the categories are coarsely outlined as track, films, pics, my stories, etc, a subgroup of contributors who are approved to a class can entry the entire data in that class. This is normally undesirable since the info owner may want to liberate distinct information only to associated men and women (e.g., loved ones pics or videos simplest available to loved ones individuals). The data owners could have the freedom to create their possess classes headquartered on the quantity and sort of their subgroups, which is a design quandary and will not be elaborated extra. Broadcast encryption allows for a relevant transmitter to send encrypted knowledge to a suite of users such that best a privileged subset of users can decrypt the information. Broadcast encryption is designed for and largely applied within the cozy distribution of copyrighted media over the internet. The published encryption steps will also be defined in fig 3. Other functions of broadcast encryption incorporate encrypted file systems (e.g., windows EFS) for confined file sharing, mailing record applications for sending exclusive emails, etc. This requirement states that information privateness is preserved in the presence of collusion assaults the place two or more entities collude to receive extra information on the sufferer than what is to be had to each colluding person.

IV. PROPOSED METHODOLOGIES

Medical imagery is a field where integrity and confidentiality of content is a critical issue due to the special characteristics derived from strict ethics, legislative and diagnostic implications. Medical image watermarking means embedding the patient information within the medical image. Moreover, the exchange of medical images is done through un-secure open environment like Internet which results in the following issues of concern: 1. Authentication: A proof that information belongs to correct patient and is issued from the right source. 2. Integrity: Information has not been modified by un-authorized users. 3. Confidentiality: Only entitled users have access to the information. Digital watermarking can be used as an important tool for the security and copyright protection of digital multimedia content. Watermarking adds the additional requirement of robustness. An ideal watermarking system however would embed an amount of information that could not be removed or altered without making the cover object entirely unusable. So, watermarking is mainly prevent illegal copy or claims the ownership of digital media. Discrete Wavelet transform (DWT) is a mathematical tool for hierarchically decomposing an image. It gained widespread acceptance in signal processing, image compression & watermarking. It decomposes a signal into a set of basic functions, called wavelets. Wavelets are created by translations and dilations of a fixed function called mother wavelet. Wavelet transform provides both frequency and spatial description of an image. Unlike conventional Fourier transform, temporal information is retained in this transformation process. Its multi-resolution analysis analyzes the signal at different frequencies giving different resolutions. Discrete Wavelet Transformation is very suitable to identify the areas in the cover image where a secret image can be embedded effectively.

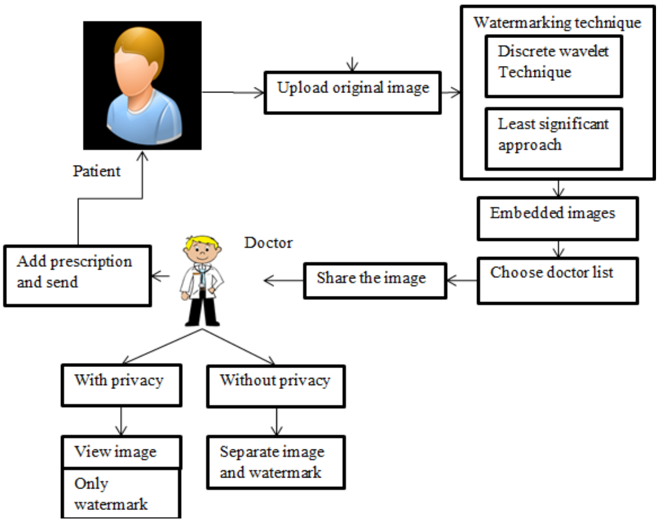

Fig 1 : Proposed framework

4.1 FRAMEWORK CREATION:

Data mining and storage solutions provide users and enterprises with various capabilities to store and process their data in either privately owned or third-party data centers that may be located far from the user–ranging in distance from across a city to across the world. Data mining relies on sharing of resources to achieve coherence. In this framework, we can have two types of users such as image owner and server provider. The person or organization that legally owns a cloud service is called image owner. The service owner can be the patients who are upload the images into cloud and the cloud provider that owns the storage within which the service resides. Service provider provides the storage space to the users. Storage space can be shared by multiple data owners. Image users can be considered as doctors to view the files

4.2 UPLOAD IMAGE:

The first stage of any sharing system is the image acquisition stage. After the image has been obtained, various methods of processing can be applied to the image to perform the many different vision tasks required today. However, if the image has not been acquired satisfactorily then the intended tasks may not be achievable, even with the aid of some form of image enhancement. The basic two-dimensional image is a monochrome (greyscale) image which has been digitized. Describe image as a two-dimensional light intensity function f(x,y) where x and y are spatial coordinates and the value of f at any point (x, y) is proportional to the brightness or grey value of the image at that point. In this module, we can upload various images such as natural images, face images and other images. Uploaded images can by any type and any size.

4.3 EMBED THE WATERMARK:

In this module, we can embed the watermark text into images. Digital media can be stored efficiently and can be manipulated very easily using computers, resulting in various security issues. The problem of protecting the copyright of digital media can be solved by digital watermark. Digital watermarking is a concept of hiding ownership data into the multimedia data, which can be extracted later on to prove the authenticated owner of the media. Watermarking ensures authenticating ownership, protecting hidden information, prevents unauthorized copying and distribution of images over the internet and ensures that a digital picture has not been altered. We can implement Discrete Wavelet Transform (DWT) domain image watermarking system for real time image. In the embedding process, the watermark may be encoded into the cover image using a specific location. This location values is used to protect the images. The output of the embedding process, the watermarked image, is then transmitted to the OSN home page.

4.4 PRIVACY SETTINGS:

Each user images are first categorized into privacy policy. Then privacy policies of each images can be categorized and analyzed for predict the policy. So we adopting two stages approach for policy recommendation than applying the common one-stage data mining approaches to mine both image features and policies together. The two-stage approach allows the system to employ the first stage to classify the policy as with privacy or without privacy. In the second stage, we can set without privacy means, prefer the user list details.

4.5 PROTECTION SYSTEM:

In this module, we can set the protection or blocking system to avoid third party aces without knowledge of image owners. This module is used to set the image with privacy. If user set with privacy settings means, all users are considered as third parties. Based on this setting, unauthorized user only views the image and can't be used. If he downloads means, only get water mark values. Finally provide hardware control system such as mouse controls and keyboard controls. Then disable the mouse operations and system print screen options. Mouse code and print screen controls values are extracted and to provide coding implementation to disable the coding as false settings. We can implement this concept in all browsers and to implement in all images which are shared by social users.

V. EXPERIMENTAL RESULTS

Properties for an efficient watermarking system are application dependent; one of the challenges in this area is that these properties compete with each other. None of the digital watermarking techniques have yet to meet all of these properties.

Robustness. Digital images commonly are subject to many types of distortions, such as filtering, resizing, and cropping. These distortions are still very common and represent an open issue with respect to the robustness of watermarking. However, the mark should be discovered if these distortions occurred.

Capacity. The capacity of the hidden data is another important issue where the watermarking algorithm should embed a predefined number of bits that can be hidden in the host signal. This number will depend on the application and there is no general rule for this. In general, the number of bits that can be inserted in the data is limited and in the LSB method; it is between (0.125 - 0.25) of the total size.

Invisibility. There are two types of invisibility due to the implementation method: perceptual invisibility, and statistical invisibility. In perceptual invisibility the watermark is hidden in such a way that it is hardly noticed. An unauthorized person should not be able to detect the watermark by means of statistical methods. For example, the availability of a large number of digital works watermarked with the same code should not allow the extraction of the embedded mark by applying statistically based attacks. A possible solution is to use a content-dependent watermark.

FRAMEWORK CREATION

We can create the framework server, patient and doctor. Each patient can be registering their details and also doctor register their details with specification. Finally server can be login and view the information

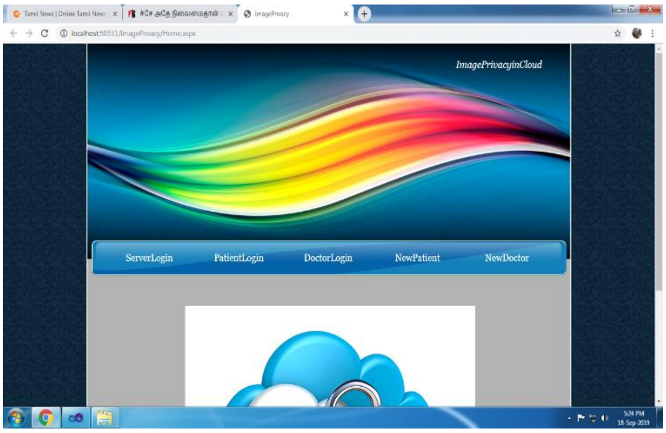

Fig 2 : Home Page

Fig 5. Server Login

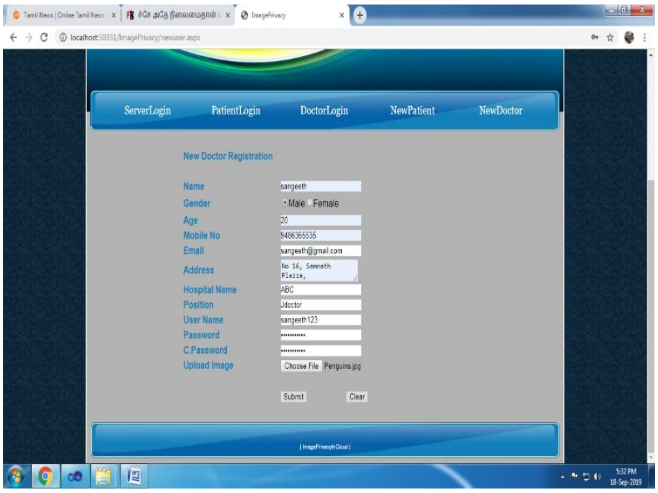

Fig 3. Doctor Registration

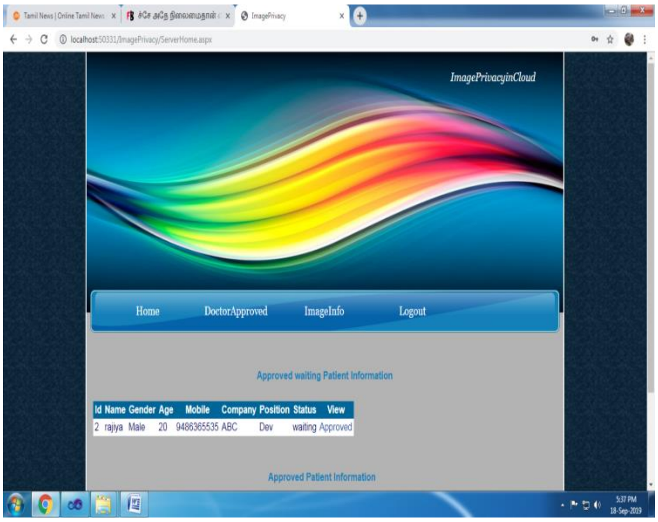

Fig 6. View Details

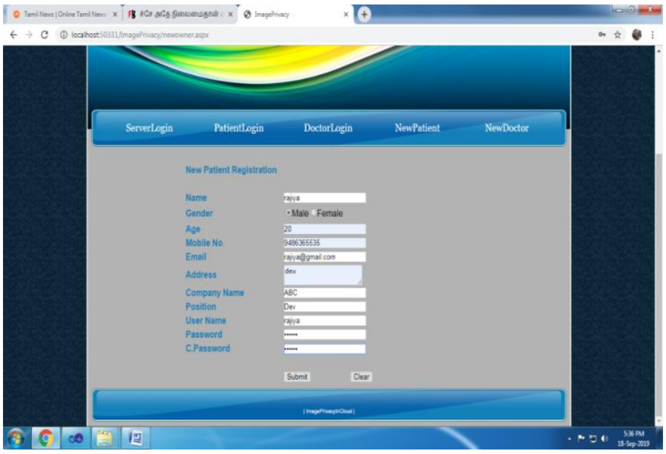

Fig 4. Patient Registration

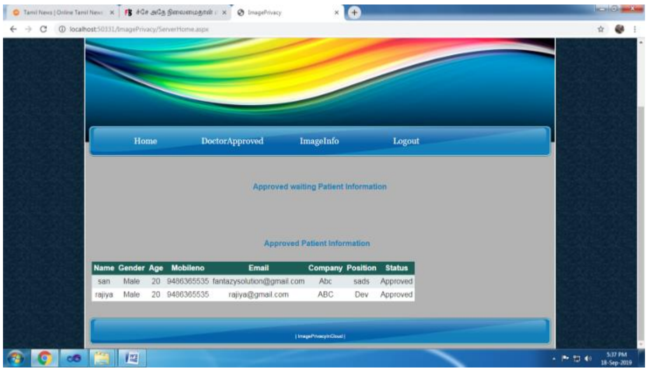

Fig 7. Approve The Patients

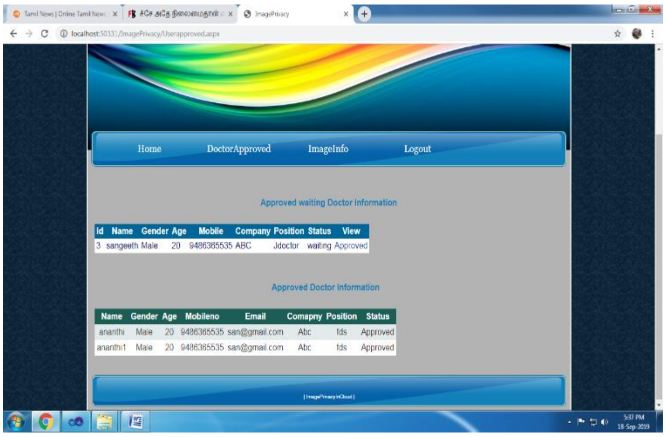

FIG 8. Approve the Doctors

UPLOAD IMAGE

The patient can upload the images into server and can be transfer to appropriate doctors.

FIG 9 View Doctor Details

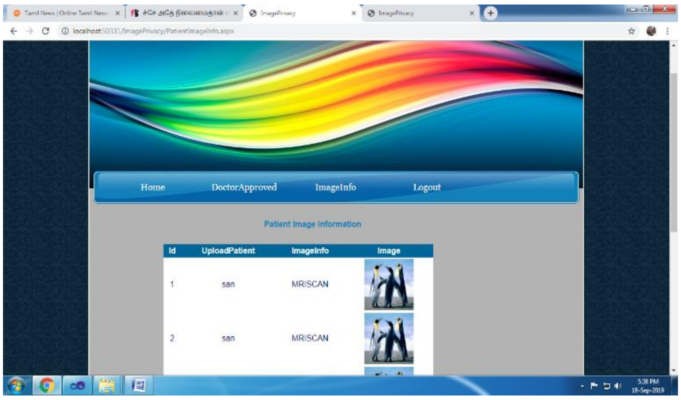

FIG 10. Upload Image

PRIVACY SETTINGS

Patient can be choosing the doctor from dropdown list and send the image with water mark text.

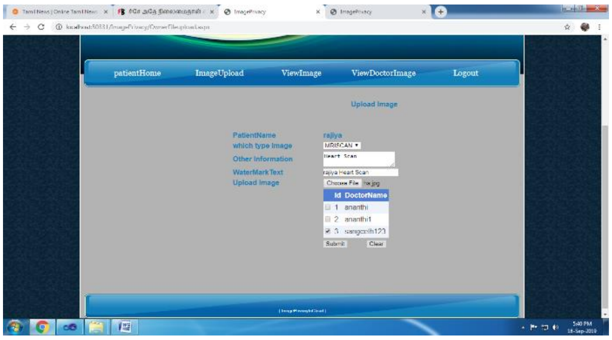

FIG 11 Image with Privacy

EMBEDDED WATERMARK

After that, watermark text can be added to the image in invisible format using Discrete wavelet transform algorithm. Based on this algorithm, low frequency pixels are select and add the watermark text.

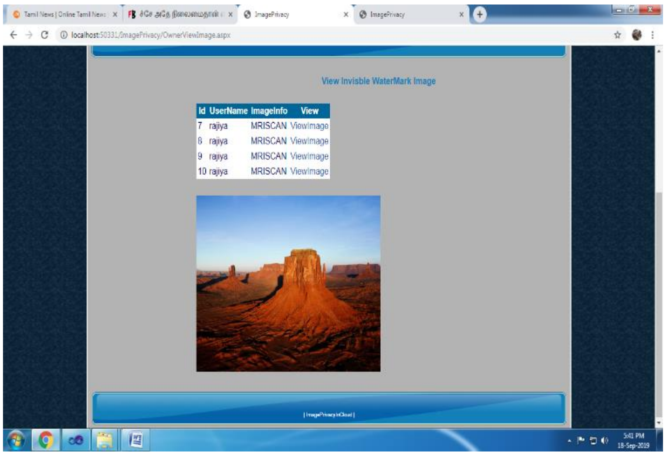

FIG 12 Watermarked Data

BLOCK THE CONTROLS

Finally we can also block screenshot options and right click in mouse operations. So unauthorized person unable access the images without permission

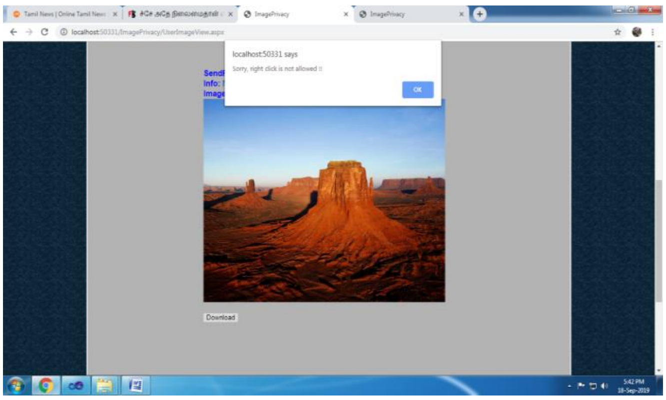

FIG 13 Block Controls

PROVIDE PERMISSION

Authorized person can be download the images with watermark text without any distortions

Fig 14 Image with Permission

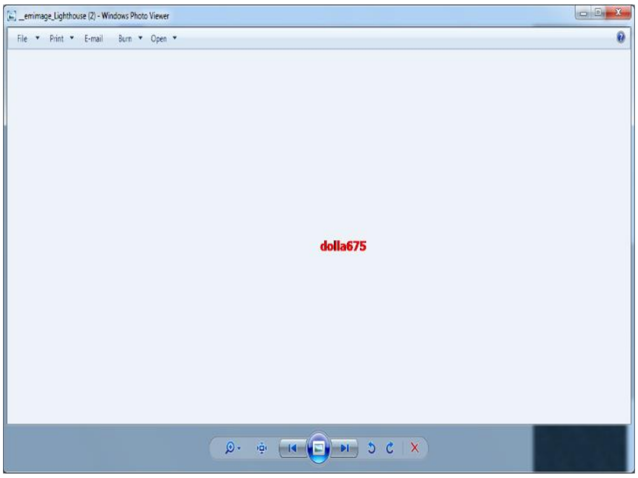

Fig 15 Image Without Permission

PERFORMANCE METRICS

Mean Square Error (MSE), MSE is computed by averaging the squared intensity of the original (input) image and the resultant (output) image pixels as in following equation

$$MSE = \frac{1}{NM}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1} e(m,n)^2$$

Where e(m, n) is the error difference between the original and the distorted images. ii) Peak Signal-to-Noise Ratio (PSNR), Signal–to-noise ratio (SNR) is a mathematical measure of image quality based on the pixel difference between two images. The SNR measure is an estimate of quality of reconstructed image compared with original image. PSNR is defined as in following equation

$$PSNR = 10\log\frac{s^2}{mse}$$

where s = 255 for an 8-bit image. The PSNR is basically the SNR when all pixel values are equal to the maximum possible value.

ALGORITHM	PSNR VALUE
LSB BASED BIT SELECTION	60.12
MSB BASED BIT SELECTION	61.15
DWT ALGORITHM	70.18

TABLE 1. PSNR COMPARISON

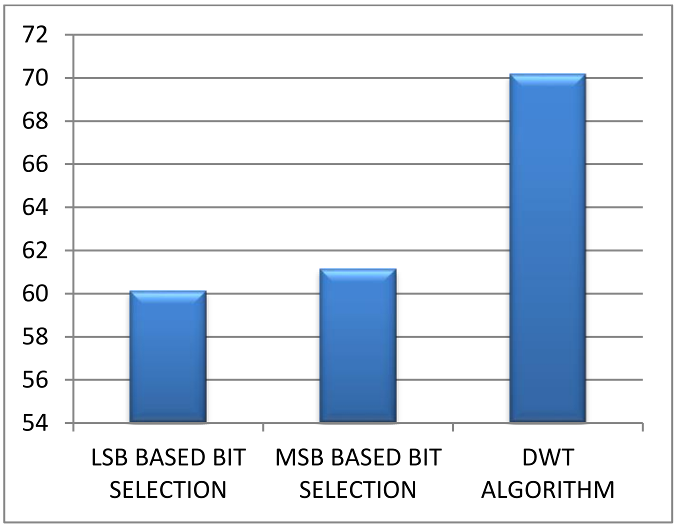

FIG 16. PSNR Comparison

From the above table and chart, proposed DWT algorithm can be provide high PSNR than the existing algorithms.

VI.CONCLUSION

The appearance of well-known secure storage systems has triggered within the compromise of conventional notions of privateness, certainly in visual media. With a view to facilitate useful and principled protection of picture privateness online, we have got supplied the design, implementation, and evaluation of photo shield gadget that successfully and successfully protects client's photo privateness across famous cloud storage. The digital watermarking approach based fully on DWT coefficients modification for social networking offerings has been presented on this paper. In the embedding manner, the coefficients in LL sub-band had been used to embed watermark. Within the extraction process, normal coefficient prediction based on imply clear out is used to boom the accuracy of the extracted watermark. We advocated that, as a complement to the actual security tools, watermarking can raise up the security level of information system by detecting system failure, manipulation errors, virus and malicious actions. It provides an ultimate guarantee of authentication that no other protection may ensure.

VII. REFERENCES

[1]. H. Cheng, X. Zhang, J. Yu, and F. Li, "Markov process based retrieval for encrypted jpeg images," in Proc. of 10th International Conference on Availability, Reliability and Security. IEEE, 2015, pp. 417-421.

[2]. A. Rial, M. Deng, T. Bianchi, A. Piva, and B. Preneel, "A provably secure anonymous buyer-seller watermarking protocol," Information Forensics and Security, IEEE Transactions on, vol. 5, no. 4, pp. 920-931, 2010.

[3]. J. Zhang, Y. Xiang, W. Zhou, L. Ye, and Y. Mu, "Secure image retrieval based on visual content and watermarking protocol," The Computer Journal, vol. 54, no. 10, pp. 1661-1674, 2011.

[4]. T. Bianchi and A. Piva, "Secure watermarking for multimedia content protection: A review of its benefits and open issues," IEEE Signal Processing Magazine, vol. 30, no. 2, pp. 87-96, 2013.

[5]. A. Piva, T. Bianchi, and A. De Rosa, "Secure client-side st-dm watermark embedding," Information Forensics and Security, IEEE Transactions on, vol. 5, no. 1, pp. 13-26, 2010.

[6]. D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Advances in Cryptology-Eurocrypt. Springer, 2004, pp. 506-522.

[7]. D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. of IEEE Symposium on Security and Privacy. IEEE, 2000, pp. 44-55.

[8]. E.-J. Goh et al., "Secure indexes." IACR Cryptology ePrint Archive, vol. 2003, p. 216, 2003.

[9]. R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proc. of 13th ACM conference on Computer and communications security. ACM, 2006, pp. 79-88.

[10]. J. Shen, H. Tan, J. Wang, J. Wang, and S. Lee, "A novel routing protocol providing good transmission reliability in underwater sensor networks," Journal of Internet Technology, vol. 16, no. 1, pp. 171-178, 2015.

Cite this article as :

B. Ananthapraba, K. Thyagarajan, "Medical Image Privacy Using Watermarking Techniques", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 5, pp. 235-248, September-October 2019.
Available at doi :
https://doi.org/10.32628/CSEIT195533
Journal URL : http://ijsrcseit.com/CSEIT195533