A Survey on Various Watermarking and Cryptography Techniques for Data Hiding in Medical Images

Mamta Mangtani[1] Narendrasinh Limbad[2]
[1]PG Scholar [2]Assistant Professor
[1,2]Department of Computer Engineering
[1,2]L. J. Institute of Engineering and Technology, Ahmedabad, Gujarat, India

Abstract— Water marking scheme is use for secure the data to protect digital content from unauthorized modification. The digital image watermarking technology is an important aspect about multimedia authentication and copyright protection, in order to enhance its reliability and security. Image watermarking scheme can effectively be used in medical image processing to authenticate or investigate the integrity on medical images. Join cryptography and watermarking is efficient method for security. Peak Signal to Noise Ratios and Normalized Correlation are computed to accesses the quality of the watermarked images and extracted the information of images.

Key words: Image Watermarking, Encryption Algorithm, Medical Image Security, PSNR, MSE

I. INTRODUCTION

The growth of the digital multimedia technology and the successful development of the internet raise the issue to protect copyright ownership. A better solution is digital watermarking. Embedding the specific information in digital content such as a picture, animation or sound without any perceptual changes in digital watermarking technology[1]

Digital data is widely used in various aspects of human life because it offers cost-efficiency and flexibility on data manipulation, storage and transmission. Medical imaging systems (such as Computed Tomography, Magnetic Resonance Imaging, X-ray imaging, Ultrasonography) require reliable security in storage and transmission of digital images. In medical image, the patient information has been embedded into the image as watermark image. As the doctor diagnose from medical images, special care is required to hide the information in medical images [2][3]

With the advancement of technology in communication network exchange the medical images between hospitals has become a usual practice now a day; medical images are revealing to an open network, where sensitive patient information is vulnerable to hackers attack. Possible security breaches such as tampering of images include false data which may lead to wrong diagnosis and treatment [4].

II. BACKGROUND

A. *The main Feature of Watermarking[12]*

1) Robustness: The ability to survive of watermark after variety of processing operations or attacks.
2) Security: The ability of watermark not to be removed or altered by hacker without having full knowledge of embedding algorithm
3) Imperceptibility: Watermark cannot be seen by human eye or not be heard by human ear, it should be only detected through special processing or dedicated circuits.
4) Verifiability: Watermark should be able to provide reliable evidences for the ownership of copyright protected information.
5) Computational cost: watermark should be produced by less complex algorithm and the computational cost should be low.
6) Capacity and data payload: Capacity of Watermark system is defined as the maximum amount of information that can be embedded in the cover file. The no of watermarked bits in a message is called as data payload and the maximum occurrences of data payload within a document are known as the watermark capacity.

B. *Classification of Watermarking*

The main two types of watermarking techniques: Visible and invisible watermarking [12].

- Visible watermarking: In Visible watermarking the generated watermark is visible to one and all, for an example the logo of some company can be viewed as visible watermarking.
- Invisible watermark: Invisible watermarking includes embedding a watermark to the main content that is unknown to the other users. An Invisible watermark is more secure and robust than visible watermark.

Four types of watermarking methods are developed to protect digital images: Robust Watermarking, Fragile Watermarking, Semi-Fragile Watermarking and Reversible Watermarking [4]

1) Robust Watermarking:

In Robust watermarking watermark is not affected by any manipulation. Robust watermark are able to withstand any external attacks[4]

Robust watermark could serve copyright protection and ownership identification is the purpose of secret message transmission.

2) Fragile watermarking:

In Fragile watermarking embedded watermark is destroyed upon any modification [4]

Fragile watermark on the other hand serve the purpose of tempore detection that also known as tamper proof watermark.

3) Semi-Fragile Watermarking:

In Semi-Fragile watermarking method watermark broken under all changes. Watermarks can survive certain degree of legitimate manipulation such as compression and cropping. Semi-fragile watermarking is usually not suitable for applications concerning legal and national security issues [4]

4) Reversible Watermarking:

Watermark can be removed and the image is restored to its original form in reversible watermarking [4]

According to working domain watermarking techniques have been classified into two categories: spatial domain and frequency domain.

a) Spatial Domain Watermarking

The watermarking technique based on the spatial domain, watermark data to be embedded directly in the pixel value. These approaches use minor changes in the pixel value intensity. The computational complexity is low in spatial domain based watermarking scheme [3]

The watermark code is embedding into the LSBs (Least Significant Bits) of the image. A change in LSB corresponds the change in I unit of image gray value. This method is simple to implement and does not produce serious alteration to the image however, it is not very strong against attacks [4]

b) Transform domain watermarking

The watermark technique based on frequency domain the watermark data to be embedded into the coefficients of the transformed image. The transformed image can be obtained from discrete cosine transform, discrete Fourier transform, and discrete wavelet transforms.

Discrete wavelet transform (DWT) is more effective than DCT and DFT.DWT provides both space and frequency localization with different resolution levels, it is more invisibility and robustness against different attacks [3]

DWT splits the image into four sub-bands of low and high frequencies. Therefore, a digital image is decomposed into low frequency sub-band (LL) and three high frequency sub-bands (HL, LH and HH)[3]

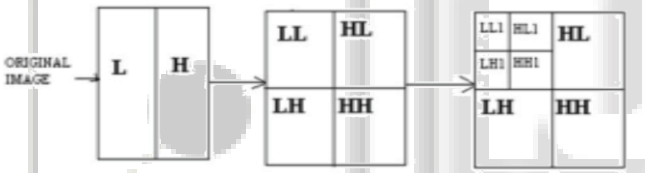

Fig. 1: wavelet decomposition based on discreet WT[8]

C. Parameter

In watermarking, the watermarked image is tested in both visual quality and quantitatively using peak signal to noise ratio (PSNR) and normalized correlation (NC) and mean square error (MSE)[7]

1) MSE:

The difference between the original image and the watermarked image evaluates Mean square error (MSE). The watermarked image is almost similar to the original image if the MSE value is low. MSE between the original image and watermarked image can be obtained by-[3]

$$\text{MSE} = \frac{1}{MN} \sum_{X=0}^{M-1} (I(x,y) - (I'(x,y))$$

Where I and I' are original and watermark image resolution M ×N

2) PSNR:

Analyses the visual quality of watermarked image in comparison with the original image PSNR can be used. The measurement of the peak error between original image and watermarked image as given as the PSNR can be obtained from the MSE and is given by-[3]

$$\text{PSNR} = 10 \log_{10} \frac{max2}{MSE}$$

3) NC:

To measure the Similarity between original watermark and extracted watermark Normalized correlation (NC) is used. The high value of NC is desired for image watermarking. For the original watermark image *W* of size *m*× *n* and the extracted watermark image *W'*, *NC* can be obtained by [3]

$$\text{NC} = \frac{\sum_0^{m-1} \sum_0^{n-1} (W(x,y) \times W'(x,y))}{\sum_0^{m-1} \sum_0^{n-1} W(x,y)2}$$

III. RELATED WORK

In digital watermarking, data hiding is process of hiding the information. Data conceal in watermarking is done through any channels like audio, video, image etc and send to receiver. Receiver will extract data from the media where it embeds data[6].Various existing methods that are used for data embedding an image and data extraction are discussed in following table I.

Many types of digital multimedia watermarking should be implemented with extra careful as modifying a certain region of the image.

ROI (Region of Interest) and RONI (Region of Non-Interest) watermarking:

The region that contains the most significant information related and accordingly must be stored without any distortion is called region of interest (ROI). Region of Non-Interest (RONI), which is the rest of the image that does not include ROI, is used as a host part to embed dual watermarks [11]

In medical image ROI is the significant part of the medical images that is used by doctors to diagnose the patient, and RONI is the area outside the ROI. Watermarking for tamper detection and recovery is done in the ROI area based [4] In medical images RONI generally contain the black background which encircles the ROI.

Method	PSNR (db)	Distortion	Description
Reversible data embedding using difference expansion	44	High [data large]	In this method conceal of data in difference of bits. Here two value of bit embed only one bit to its LSB.
Expansion embedding techniques for reversible watermarking	50	Low [data small]	Prediction error is used to embed data. Here prediction error and histogram shifting is combined.
Reversible data hiding	48.2	Low [data large]	In this method an image is encoded using an encryption key and add data to the encrypted image by consuming a data hiding key.
Separable reversible data hiding in encrypted image	39.0	No [data small]	There are Sender encrypt an uncompressed image by means of an encryption key. After that data is concealed by hider to the encrypted image, by means of a data hiding key.
Reversible watermarking algorithm using sorting and	49.58	Very low	In this method rhombus pattern prediction scheme involves. One pixel value is predicted by means of using four neighboring pixel.

prediction			These all pixel are together use to embed a bit.

Table 1: Comparison between Data hiding Techniques [6]

A. Cryptography

Cryptography is a technique of making the secret information or the information unreadable by apply some permutations or substitutions on it, commonly known as encryption and decryption [12] Medical images plays a vital role in Multimedia and Telecommunication technologies need different means of remote access and sharing of patient data [6]

Transmission of medical image of patient to doctor have several issues. The security issues are named such as authentication, confidentiality and availability [5]

The most impotent security services required are [5]:

1) Patient authentication services: Only authorized persons have right to use the information.
2) Medical image integrity service: The information has not been changed by unauthorized users.
3) 3)Patient information confidentiality service: There should be evidence that the information belongs to the correct patient.

Watermarking is a method, it modifies the gray level values of image pixels, in order to insert a message and the cryptographic algorithms are considered as a priori protection technique in watermarking [7]

Using joint the technique of watermarking and cryptography the information is protected and reliability is verified by its integrity and authenticity. In order to improve the security of medical images the watermarking techniques are used with encryption method [7]

In paper [3] discrete wavelet transform (DWT) domain and chaotic system based medical image watermarking scheme has been used for hiding patient information in medical image to authenticate.

Chaotic maps are used for digital image watermarking to increase the security. There are Logistic map is one of the simplest chaotic maps, which provides an efficient and secure way for image encryption. In this paper cryptography algorithm is not used.

DWT and chaotic system based medical image watermarking scheme has been proposed. In the proposed watermarking scheme, patient information has been embedded into the corresponding medical image as binary watermark image. DWT has been applied to the cover medical images to decompose the images into four sub-bands of low and high frequencies. The logistic map has been used to get the chaotic watermark from watermark image. Then, the chaotic watermark has been embedded into the low frequency sub bands (LL) of medical image without degrading the image quality.

Following papers are used to watermarking with cryptography.

Mehbooba P Shareef in[10] proposed watermarking using RC4 encryption. For watermarking prediction error expansion method is use. Watermarking cannot ensure authenticity and integrity of the information passed through the images. So for authentication RC4 algorithm is used.

RC4 is symmetric key encryption algorithm. The key for encryption and decryption is same and is shared by both the Sender and receiver.RC4 is stream cipher algorithm. In stream cipher algorithm watermark pattern can be of any size for encryption. The key can be exchanged by diffie-helman key exchange algorithm instead of embedding it in the image so that image distortion can be reduced and same key can be used for all the exchanges between a sender and receiver.

Suganya G in[7] join watermarking and encryption using AES,RC4.join watermarking and encryption using cryptography algorithm like Advanced Encryption Standard (AES) and RC4. It joint the stream cipher algorithm or block cipher algorithm with the watermarking technique Quantization index modulation. The Quantization index modulation technique is used to quantify the components of image according to a set of quantizes based on codebooks in order to embed a message. By substituting one image component with its nearest element in the codebook allows the insertion of images. If the message has to be inserted are first encoded then it is moved to the center of its nearest cell that encode Implementation with the cipher algorithm is achieved using Advanced Encryption Standard (AES) in Cipher Block Chaining (CBC) mode and RC4. Depending on the selected cipher algorithm, some constraints have to be added when building sub code books. In this case Two types of cryptographic algorithms are to be discussed: Stream cipher algorithm and another is block cipher algorithm. In stream cipher algorithm RC4 is preferred to used to stream of bits/bytes of plaintext and in block cipher Advanced Encryption Standard (AES) is used to operate on the block of data.

In medical image a new joint watermarking/encryption system is proposed which guarantees a priori and a posteriori protection. During Encryption Process the system gives access to insert two messages in the spatial domain and encrypted domain respectively during. Those two messages are used to verify the reliability of images in decryption part.

P.V.V Kishore, N.venktram in[8] introduced the concept of watermarking using RSA encryption. It joint DWT watermarking with RSA algorithm. RSA algorithm is used for encrypting the patient image using public key. RSA algorithm also used for securing the data over network. It contain two keys one for encryption and the other for decryption. Encryption is public and decryption key is private. Any one encrypt the data using public key and the person holding private key can only decrypt.

Manoj Kumar, Himanshu Agarwal[9] proposed Reversible watermarking scheme and combine DES algorithm. Reversible Watermarking scheme based on difference expansion that could be used in the secure transfer and for authentication DES algorithm is use. DES (Data Encryption Standard) is most widely used encryption scheme. Data Encryption Standard (DES), data are encrypted in 64-bit blocks using a 56-bit key. The algorithm transforms 64-bit input in a series of steps into a 64-bit output. The same steps, with the same key, are used to reversing the encryption process. DES algorithm is less secure than AES.

R.Eswaraiah, E.Sreenivasa Reddy[5] proposed paper A Fragile ROI-Based Medical Image Watermarking Technique with Tamper Detection and Recover. In this paper Region of Interest (ROI) and Least Significant Bit (LSB)

based fragile watermarking technique for tamper detection and recovery of medical images is proposed. First medical image is divided into ROI and RONI. Then In ROI authentication information is inserted and in RONI recovery information. To increase embedding capacity in ROI Every medical image has a region of interest (ROI) which is more important for diagnosis purpose. So, the ROI portion of the medical image has to be recovered lossless from watermarked medical image at receiver side. In this paper, for validate authenticity of ROI propose a spatial domain and fragile ROI based watermarking method which identify tampered regions in ROI and recover those tampered regions

IV. RESEARCH PAPER COMPARISON

Topic Name	Algorithm	Description
Wavelet Based Watermarking Approach of Hiding Patient Information in Medical Image for Medical Image Authentication[3]	DWT +chaotic maps	Logistic map is one of the simplest chaotic maps, which provides an efficient and secure way for image encryption
Medical image watermarking using RSA encryption in wavelet domain[8]	RSA+DWT	RSA is blocked cipher algorithm. RSA is public key encryption algorithm
Encryption-Enhanced Reversible Watermarking for Medical Images via Prediction and RC4 Encryption[10]	RC4	RC4 is stream cipher algorithm.RC4 is symmetric key encryption algorithm
Medical Image Integrity Control Using Joint Encryption and Watermarking Techniques[7]	AES and RC4+QIM	AES is block cipher algorithm. AES is symmetric key encryption algorithm
Reversible watermarking Scheme for Medical Images[9]	DES	DES is block cipher algorithm. DES is symmetric key encryption algorithm
A Fragile ROI-Based Medical Image Watermarking Technique with Tamper Detection and Recovery[5]	ROI+LSB	ROI portion of the medical image has to be recovered lossless from watermarked medical image at receiver side.

Table 2: Research Paper Comparison

V. CONCLUSION

I surveyed recent watermarking methods and identified research trends. I showed that the reversible watermarking method used for data hiding and highest embedding capacity was achieved. Watermarking cannot ensure authentication, in many research work there was cryptography algorithm is used to achieved authentication and security. A comprehensive combination of watermarking with cryptography compatible with high security has to be proposed.

REFERENCES

[1] Toshiki Ito,Ryo Sugimura,Hyunho Kang, Keiichi Iwamura,Kitahiro Kaneda,Isao Echizen,Niijuku, Katsushika-ku, Hitotsubashi, Chiyoda-ku"A New Approach to ReversibleWatermarking"IEEE,2014 pp.455-458.
[2] Nelmiawati,Mazleena Salleh, MalekNajib Omar" Pixel-Based Dispersal Scheme for Medical Image Survivability and Confidentiality" IEEE,2014 pp.298-303.
[3] Md.Moniruzzaman, Md.Abul Kayum Hawlader andMd.FoisalHossain"WaveletBasedWatermarkingApproach of Hiding Patient Information in Medical Image for Medical Image Authentication"IEEE,2014 pp.374-378.
[4] Hui Liang Khor ,Siau-Chuin Liew and Jasni Mohd.Zain"A Review of Reversible Medical Image Watermarking Scheme with Tamper Localization and Recovery Capability"IEEE,2014 pp.188-192
[5] R.Eswaraiah, E.Sreenivasa Reddy"A Fragile ROI-Based Medical Image Watermarking Technique with Tamper Detection and Recovery" IEEE,2014 pp.896-899
[6] Jitha Raj.T,E.T Sivadasan "A Survey Paper on Various Reversible Data Hiding Techniques in Encrypted Images" 2 IEEE,2015 pp. 1139-1143
[7] Suganya G, Amudha K" Medical Image Integrity Control Using Joint Encryption and Watermarking Techniques" IEEE,2014 Pages: 1 – 5
[8] P.V.V kishore,N.venktaram"Medical image watermaking using RSA encryption in wavelet domain" IEEE,2014 pp.258-262
[9] Manoj kumar, Himanshu Agarwal"Reversible watermarking Scheme for Medical Images"IEEE.2014 pp.844-847
[10] Mehbooba P Shareef, Divya T v,Nimisha Abraham,Tina Babu and Reshma KV"Encryption-Enhanced Reversible Watermarking for Medical Images via Prediction and RC4 Encryption" IEEE pp.1509-1513, April 3-5, 2014
[11] Afaf Tareef, Ahmad Al-Ani, Hung Nguyen, Yuk Ying Chung"A Novel Tamper Detection-Recovery and Watermarking System for Medical Image Authentication and EPR hiding" IEEE,2014 pp.5554-5557
[12] Sameeka Saini" A survey on watermarking web contents for protecting copyright" IEEE,2014

