# Different Crypto - Watermarking Techniques

**Disha Karkera[1] Rutuja Dolas[2] Nishigandha Wagh[3] Akshada Kale[4] Prof. Reshma Vartak[5]**
[1,2,3,4,5]Department of Computer Engineering
[1,2,3,4,5]Terna Engineering College, Nerul, Navi Mumbai

*Abstract*— Digital image watermarking is a technology that has made to protect digital images from illicit manipulations. Digital watermarking is a concept intimately related to steganography, in that they both hide a message inside a digital signal. Watermarking tries to hide a message related to the actual content of the digital signal, but in steganography the digital signal has no relation to the message, and it is used as a cover to hide its existence. Watermarking is used for providing a kind of security for various types of data. It may be image, audio, video, etc. Watermarking is different to steganography; it has the extra requirement of robustness against possible attacks. Using digital watermarking, copyright information can be implanted into the multimedia data. This is implemented by using algorithms. Information such as image, number or text with special implication can be embedded. The purpose of this can be for copyright protection, covert communication, authenticity distinguish of data file, etc.

***Key words:*** Medical Images; Telemedicine; Encryption; Watermarking

## I. INTRODUCTION

Telemedicine has increased the number of ways in which healthcare can be delivered across places and countries instead of requiring the provider and the recipient to be present in the same place. Telemedicine is the exchange of medical images between remotely located healthcare entities. A major obstacle telemedicine faces is providing authenticity, confidentiality and integrity for transmitting medical images. We propose a hybrid algorithm which combines encryption and digital watermarking techniques in order to provide the required authenticity and integrity services.

## II. WATERMARKING

### A. *The main Feature of Watermarking [1]*

*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

*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.

### B. *Watermarking Techniques*

*1) Least Significant Bit Coding (LSB):*
The LSB of the carrier signal is substituted with the watermark. The bits are embedded in a sequence which acts as the key. The sequence should be known in order to retrieve it back. The watermark encoder first selects a subset of pixel values on which the watermark has to be embedded. It then embeds the information on the LSBs of the pixels from this subset. LSB coding is a very simple technique but the robustness of the watermark will be too low. With LSB coding almost always the watermark cannot be retrieved without a noise component

*2) Advantages:*
1) Most straight forward and the simplest method.
2) Easy to implement and low complexity.

*3) Disadvantages:*
1) Transformed pixels are lost.
2) Simple attack like random cropping or shuffling will destroy the coded watermark.
3) The depth is limited. In order to minimize the possible audible distortion, only the least

### C. *Discrete Cosine Transform (DCT):*

DCT represents the entire image as coefficients of various frequencies of cosines. The DCT of the image is calculated by taking 8x8 blocks of the image, which are then transformed one by one. The 2D DCT of an image offers the result matrix such that top left corner represents lowest frequency coefficient while the bottom right corner is the highest frequency coefficient. FM represents the mid band frequencies of 8x8 block, FL represents lowest frequency components and FH represents higher frequency components. Any of the bands can be used as embedding region. However if watermark is embedded to the FL band then it will create more visual effect. If FH is taken as embedding band then it cannot withstand the image processing operations like compression. That's why FM is chosen as the embedding region as to provide additional resistance to lossy compression techniques, without doing significant modification of the cover image.

*1) Advantages:*
1) The visibility of image will not get affected and the watermark will not be removed by any kind of attack.

*2) Disadvantages:*
1) Certain higher frequency components tend to be suppressed during the quantization step.
2) DCT technique doesn't work with scaling attacks.

### D. *Discrete Wavelet Transform (DWT):*

The wavelet transform provides the time-frequency representation of a given signal. The transforms are based on small waves, called wavelet, of varying frequency and limited duration. The wavelet transform decomposes the image into three spatial directions, horizontal, vertical and diagonal.

 

Hence wavelets reflect the anisotropic properties of HVS more precisely. Magnitude of DWT coefficients is larger in the lowest bands (LL) at each level of decomposition and is smaller for other bands (HH, LH, and HL). A two dimensional transform can be accomplished by performing two separate one dimensional transforms. First, the image is filtered along the x-dimension using low pass and high pass analysis filters and decimated by two. Low pass filtered coefficients are stored on the left part of the matrix and high pass filtered on the right. Because of decimation the total size of the transformed image is same as the original image. Then, it is followed by filtering the sub-image along the y-dimension and decimated by two. Finally, we have split the image into four bands denoted by LL, HL, LH and HH and one level decomposition and figure shows one level and second level decomposition.

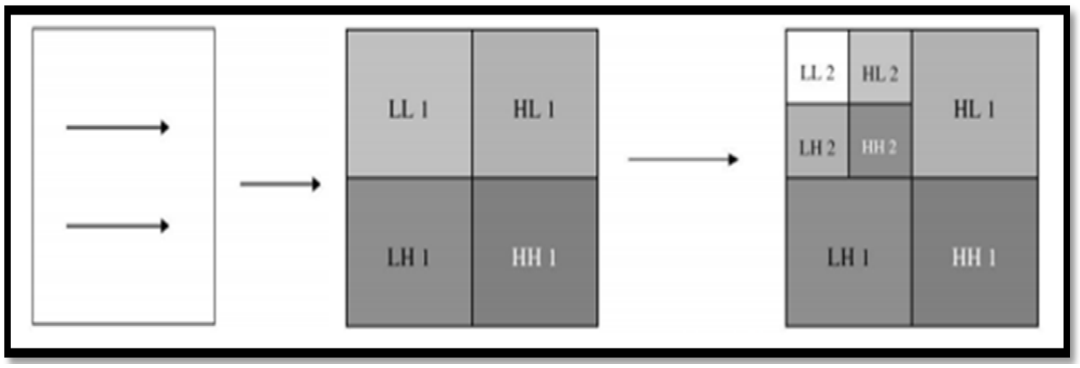


Fig. 1: Wavelet decomposition based on DWT

*1) Advantages:*

1) Allows good localization both in time and spatial frequency domain.
2) Higher compression ratio which is relevant to human perception.
3) More robust to cropping.

*2) Disadvantages:*

1) Cost of computing may be higher.
2) Longer compression time.
3) Noise/blur near edges of images or video frames

*E. Parameter*

In watermarking, the watermarked image is tested in both visual quality and quantitatively using peak signal to noise ratio (PSNR)

*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-[2]

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

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-[2]

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

## III. 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 [1] Medical images plays a vital role in Multimedia and Telecommunication technologies need different means of remote access and sharing of patient data. Transmission of medical image of patient to doctor have several issues. The security issues are named such as authentication, confidentiality and availability.

The most impotent security services required are [9]-

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) Patient information confidentiality service: There should be evidence that the information belongs to the correct patient.

Watermarking is a method, it modifies the grey level values of image pixels, in order to insert a message and the cryptographic algorithms are considered as a priori protection technique in watermarking .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.[6]

*A. Classification of Cryptography Algorithm*

The basic classification of cryptographic algorithms is shown in figure 1.Many authors have compared these algorithm on the basis of time complexity and space complexity. This paper compares these algorithms on the basis of parameters like key length and management; Security. Many authors have compared these algorithm on the basis of time complexity and space complexity. Algorithms on the basis of parameters like key length and management, Security and limitations pertain to each algorithm limitations pertain to each algorithm.

*1) Data Encryption Standards (DES):*

It was developed in the early 1975 at IBM labs by Horst Fiestel. DES uses 56 bits key for encryption and decryption. It completes the 16 rounds of encryption on each 64 bits block of data. DES is a symmetric encryption system that uses 64-bit blocks, 8 bits (of which are used for parity checks (to verify the key's integrity). Each of the key's parity bits (1

 

every 8 bits) is used to check one of the key's octets by odd parity, that is, each of the parity bits is adjusted to have an odd number of '1's in the octet to which it belongs. The key therefore has a real useful length of 56 3bits, which means that only 56 bits are actually used in the algorithm. So it would take a maximum of 256 or 72,057,594,037,927,936, attempts to find the correct key.

*2) Blowfish Algorithm:*

It is basically a symmetric block cipher having variable length key from 32 bits to 448 bits. It RIPEMD

operates on block size 64 bits. It is a 16-round Feistel cipher .It uses simple operations that are efficient on microprocessors. e.g., exclusive-or, addition, table lookup, modular- multiplication. It does not use variable-length shifts or bit-wise permutations, or conditional jumps. It employs pre-computable sub keys. On large-memory systems, for faster operation these sub keys can be pre-computed. If the sub keys are not computed it will result in slower operation, but it should still be possible to encrypt data without any pre-computations. It consists of a variable number of iterations. For a small key size applications, the trade-off between the complexity of a differential attack and a brute-force attack make a large number of iterations superfluous.

*3) AES (Advanced Encryption standard):*

The Advanced Encryption Standard is a symmetric block cipher used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world for sensitive data encryption. AES is actually, three block ciphers, AES-128, AES-192 and AES-256. In AES each cipher in three block ciphers encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128 bits, 192 bits and 256 bits, respectively. In Advanced encryption standard has 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit key.

*4) Hashing:*

A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length.

- Popular Hash Functions
- Message Digest (MD)
- Secure Hash Function (SHA)
- RIPEMD
- Whirlpool
- Applications of Hash Functions

*5) Password Storage:*

An intruder can only see the hashes of passwords, even if he accessed the password. He can neither logon using hash nor can he derive the password from hash value since hash function possesses the property of pre-image resistance.

*6) Data Integrity Check:*

Data integrity check is a most common application of the hash functions. It is used to generate the checksums on data files. This application provides assurance to the user about correctness of the data. The process is depicted in the following illustration –

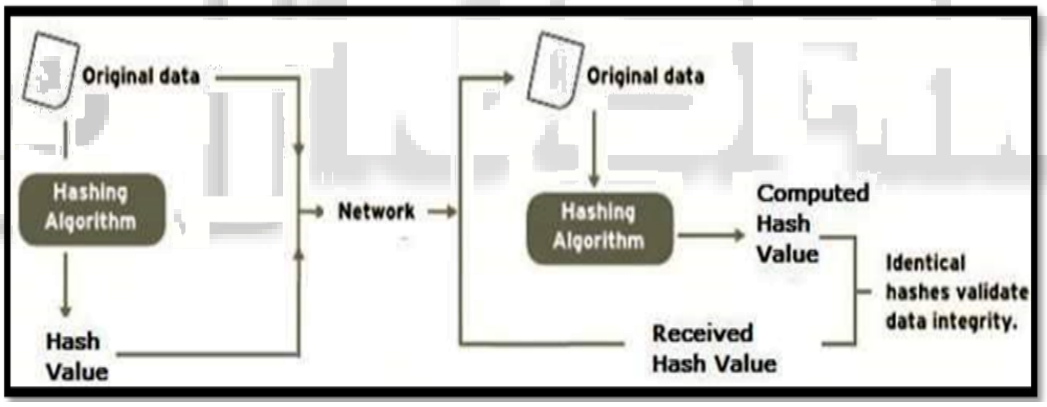


Fig. 2: Hash function for data integrity

The integrity check helps the user to detect any changes made to original file. It however, does not provide any assurance about originality. The attacker, instead of modifying file data, can change the entire file and compute all together new hash and send to the receiver. This integrity check application is useful only if the user is sure about the originality of file.

## IV. Related Work

In this section several techniques that combine both encryption and watermarking algorithms are highlighted. A summary of reported algorithms is shown in Table l.

Algorithm [4] applied a reversible data hiding algorithm on encrypted medical images. The medical image was first encrypted using the electronic code book (ECB) mode of AES standard, and then data hiding in the encrypted domain was done using bit-substitution based method.

Algorithm [5] projected reversible watermarking techniques and applied it on numerous medical image modalities. The projected algorithm is region-based, and therefore the RSA public key technique was used to offer secured transmission. It permits us to enter the relevant data with the image that has confidentiality, integrity and authentication by embedding RSA encrypted digital signature with the image. Here we are comparing the lossless watermarking techniques for numerous medical image modalities like magnetic resonance imaging (Magnetic resonance imaging), us (Ultrasonic), PET (Positron emission tomography), endoscopic and angiographic pictures. For the discussions we are ready to take ROI supporting lossless watermarking systems. This lossless watermarking is accountable for convalescent the altered medical image content of the system.

Algorithm [6] a joint watermarking/encryption algorithmic program was proposed. The algorithmic program combines quantization index modulation (QIM) and therefore the AES block cipher algorithm in the cipher block chaining

 

(CBC) mode. Join watermarking and encryption using cryptography algorithm like Advanced Encryption Standard (AES) and RC4. It combines 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 centre 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 use to stream of bits/bytes of plaintext and in block cipher Advanced Encryption Standard (AES) is used to operate on the block of data.

Algorithm [7] a randomized cryptographic fusion watermarking system was planned. The system operates by encrypting the patient info and embedding the encrypted information within the medical image by bitwise operation. During this technique, first, the document of the patient is encrypted and so the cipher is arbitrarily embedded within the medical image using bit wise operation for authentication. Owing to embedding, a number of the main points of the medical image is also corrupted, which may be recovered by using reversible property. The planned algorithmic program provides high payload capability, less procedure quality, security, validation, reversible quality and privacy of the patient.

Algorithm [8] consists of two procedures: watermark ebedding procedure and watermarking extraction procedure. Prior applying embedding procedure, the cover image is segmented into two regions, ROI and RONI, and then divided into 16x 16 blocks. The RONI region is used for embedding multiple watermarks in the frequency domain by applying the DWT transform three times on each block.

| | Algorithm | PSNR(db) | Distortion |
|---|---|---|---|
| [4] | AES + Correlation based | 52.2 | Low |
| [5] | RSA + DSA + Hashing + LSB | 73 | Very low |
| [6] | AES + Correlation based | 60 | High |
| [7] | AES + DWT | 60 | Low |
| [8] | Hashing + Correlation based + DWT | 98.10 | No |

Table 1:

## V. Conclusion

Combining encryption and watermarking techniques will offer secure transmission of medical images over vulnerable public networks. The various watermarking techniques and identified research trends are mentioned. The reversible watermarking method used for data hiding and highest embedding capacity was achieved. Watermarking cannot guarantee authentication, in several research work there was cryptography algorithm issued to achieved authentication and security. A comprehensive combination of watermarking with cryptography compatible with high security should be planned.

## References

[1] Sameeka Saini" A survey on watermarking webcontents for protecting copyright" IEEE,2014
[2] Md.Moniruzzaman,Md.AbulKayumHawladerandMd.FoisalHossain "Wavelet Based Watermarking Approach of Hiding Patient Information in Medical Imagefor Medical Image Authentication"IEEE,2014 pp.374-378.
[3] HuiLiang,Siau-ChuinLiewandJasniMohd.Zain"A Review of Reversible Medical ImageWatermarking SchemewithTamperLocalizationandRecoveryCapability "IEEE,2014 pp.188-192
[4] W. Puech, An Efficient Hybrid Method for Safe Transfer of Medical Images. 2nd international ConJerence: E-Medical Systems, TUNlSIA, Pages: 29-31, 2008.
[5] A. Umamageswari, U. Ferni, and G. Suresh, ASurvey on Security in Medical ImageCommunication. International Journal oJ Computer Applications, Vol. 30, No.3, 2011.
[6] D. Bouslimi, and G. Coatrieux, A joint Watermarking/Encryption Algorithm for Verifying Medical Image Intejrity and Authenticity in Both Encrypted and Spatial Domains. 33' Annual international ConJerence oJ the iEEE EMBS Boston, Massachusetts USA, 2011.
[7] P. Viswanathan and P. Krishna, Randomized Cryptographic Fusion Watermarking Medical Image with Reversible Property. International Journal of Computer information Systems, Vol. 2, 2011.
[8] Ali AI-Haj, Noor Hussein and Gheith Abandah, Combining Cryptography and Digital Watermarking for Secured Transmission of Medical Images. 978-1-5090-1470-5 4/16/$31.00 ©2016 IEEE.

 