A Review on Multi-Layer Security of Biomedical Image data for Tele-health applications

[1]Lomesh Sahu
[1]Research Scholar
[1]Department of Computer Science,
[1]Institute of Engineering, SAGE University, Indore, India.

Abstract : Health services are now relying heavily on telecommunications which has opened up a new avenue called tele health services. In this technological aspect, the health related data is stored and shared among remote nodes to facilitate diagnosis and analysis. Robotic surgeries, remote diagnosis and data warehousing are the fundamental avenues where tele health services are needed. This automatically brings about the necessity for security of tele health data specifically image related data. Images are the most widely used data formats shared due to the amount of information they contain. Hence, conventional security measures are now being replaced with multi-layer security techniques for enhanced security. This paper primarily focusses on image encryption based techniques, image steganography based techniques and multi-layer or multi-level hybrid technique. The salient features of previous work done in the domain is also cited. The performance evaluation parameters are also discussed.

***IndexTerms*–Bio-medical data, image processing, multi-level security, image encryption, image steganography, transform domain, noise effects, peak signal to noise ratio (PSNR).**

I. INTRODUCTION

Tele health services are becoming extremely popular these days with applications such as robotic surgeries, remote diagnosis and data warehousing. However, they face the security breach issue with confidentiality being a big challenge for medical organizations. A typical biomedical image is shown in the figure below.

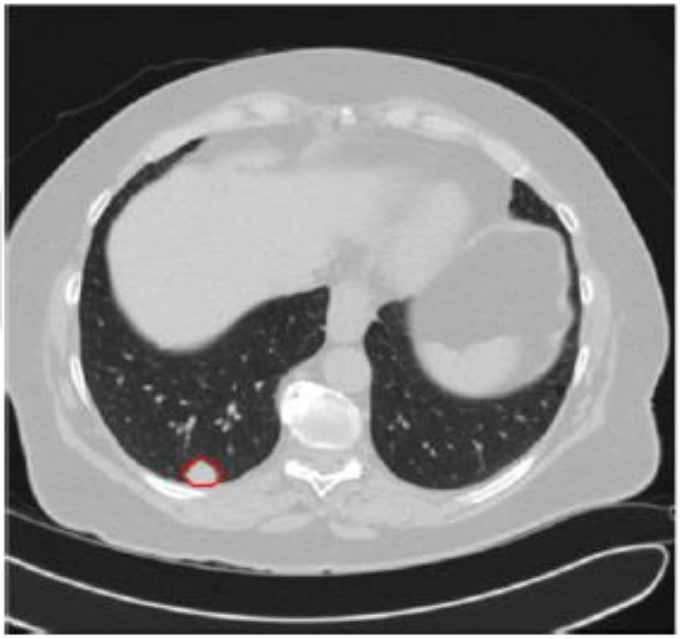

Figure.1 A Typical CT Image

Images are the most common forms of data to be shared and stored due to the enormous amount of visual information and perspective they offer. An image may be considered to be a two dimensional signal or function of two spatial dimensions mathematically given by:

$$I = f(x, y) \qquad (1.1)$$

Here,
I is the intensity or gray scale value
f stands for a function of
x, y are the coordinates
The pixels of the image render three critical pieces of information which are the:

- Coordinates
- Intensity or brightness
- Color or RGB vale

It is necessary to encrypt the image in such a way that it can be restored after decryption or any security mechanism. The generic encryption mechanism is depicted in the figure below.

1.1 Image Encryption

The encryption process relies on a transform of the plain text image into a cipher text image based on some encryption algorithm and a key. The process is shown in the figure below.

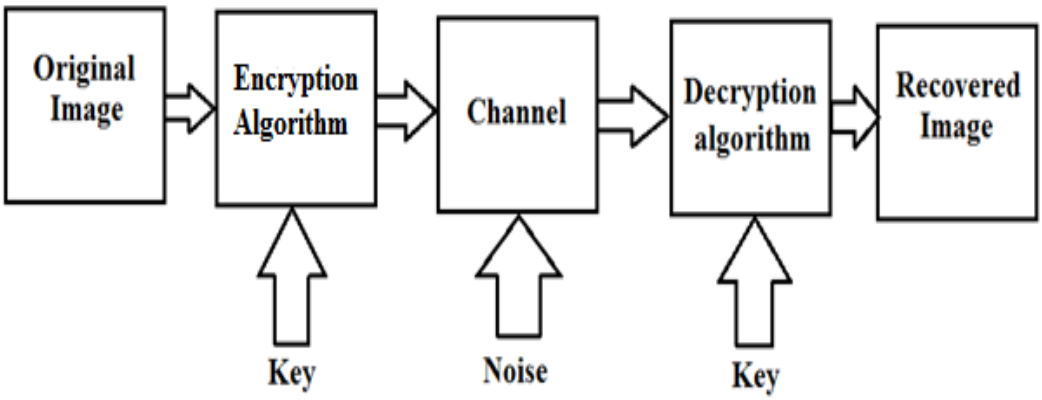

Figure.2 The image encryption process

In the basic encryption process, the image is encrypted by a manipulation process called the encryption algorithm and the output of the encryption block is given mathematically by:

$$I_{cipher} = f(I_{plain}, key) \quad (1.2)$$

Here,
I_{cipher} is the cipher text image
I_{plain} is the plain text image
f is the encryption algorithm
key is the one used for encryption and decryption

1.2 Image Steganography

The concept of steganography is a different concept wherein the image or data is hidden in another image or data format. The figure below explains the concept.

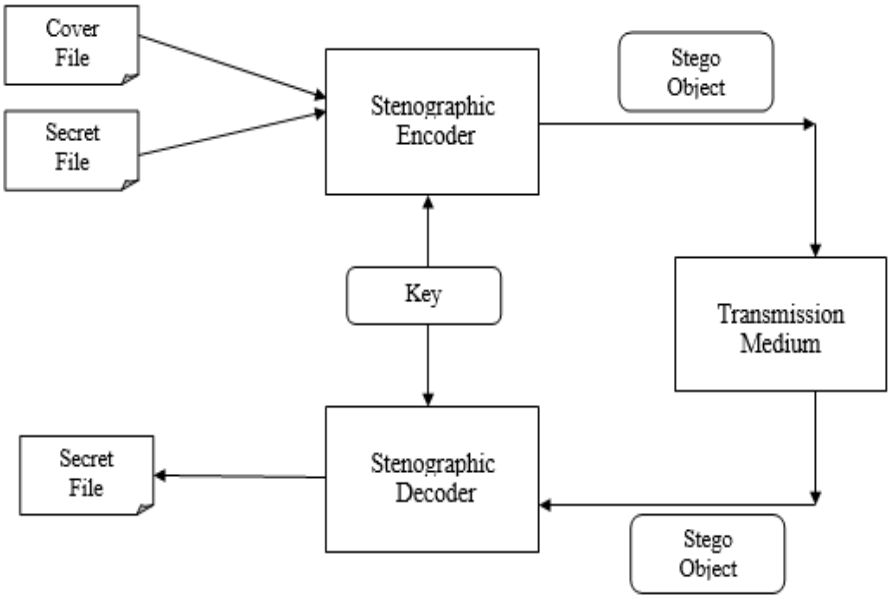

Figure.3 The Image Steganography process

The steganography process is different from the encryption process in the sense that in this process, the data is not encrypted but hidden in a cover data file and makes it imperceptible for adversaries. The reverse process of the steganography renders perceptibility to the stenographic data. While encrypted data is evident to adversarial attacks, stenographic data is less perceptible to attackers.

1.3 The Multi-Level Data Security Architecture

The multi-layer security architecture comprises of multiple data manipulation modules shown in the figure below:

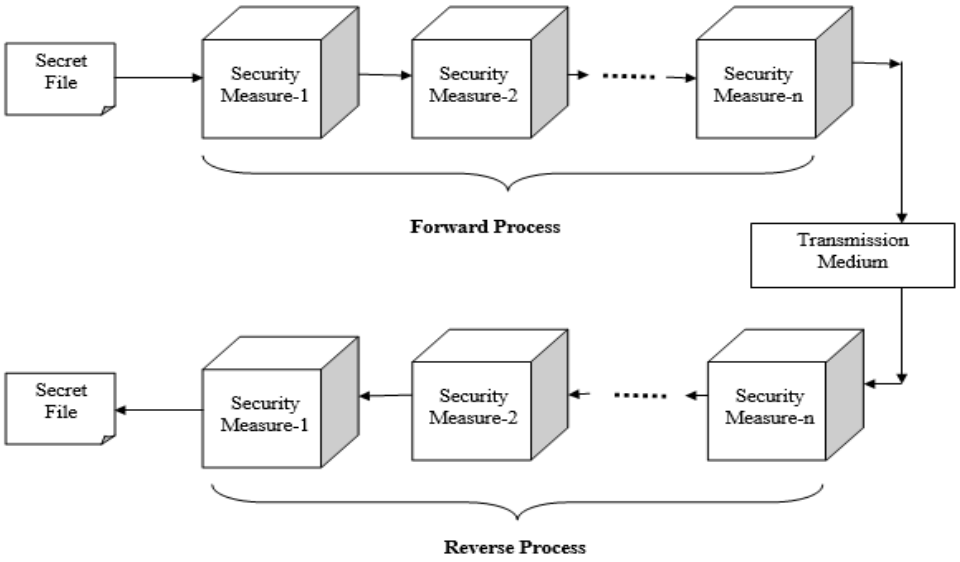

Figure. 4 The multi-layer security architecture

In this architecture, the image goes through a series of manipulations creating a multi-layer security measure. The reverse process of the transmitting end occurs at the receiving end.

II. Multi-Layer Security in the Transform Domain

Most times, to enhance the security metric of images, they are manipulated in the transform domain. The commonly used transforms are the discrete cosine transform(DCT) or the Discrete Wavelet Transform given by:
The DCT is defined as:

$$y(k) = w(k)\sum_{i=1}^{N} x(n)\cos\left(\frac{\pi(2n-1)(k-1)}{2N}\right) \quad (2.1)$$

Here
$w(k) = 1/\sqrt{N}$ for k=1 and
$w(k) = \sqrt{2/N}$ for 2< k<N

The wavelet transform can be given by

$$C(S,P) = \int_{-\infty}^{\infty} f(t)\,((S,P,t))dt \quad (2.2)$$

Here S stands for scaling
P stands for position
t stands for time shifts.
C is the Wavelet Transform

The transform domain manipulations makes it difficult for adversaries to obtain the reverse of the manipulations by brute force. Moreover, the transform domain separates the spectral components of the images making it to process the image easier compared to the spatial domain. Hence to implement multi-layer security, the transform domain is one of the most common choices for the sake of security.

III. Noise Effects in Images

Images are often degraded by noise and interference effects which commonly are:

Gaussian Noise: This is the type of noise occurring due to electronic gadgets storing the image data. It has the property that it has a constant noise power spectral density for all frequencies. Mathematically:

$$N_{Gaussian} = k\forall f \quad (3.1)$$

Here,
N stands for the noise
k is the constant noise psd
f stands for frequency

Salt and Pepper Nosie: This is the type of the noise which occurs in the form of white and black dots on the images created by the fluctuations of the gain of the analog to digital converters (ADCs) of the devices

Speckle Noise: This is the form of a multiplicative noise in which a multiplicative factor either enhances or degrades the intensity of the pixels.

Poisson Noise: This is the type of noise and blurring effect when the pixels captured by the capturing sensor is less than the number of pixels to create the image.

IV. PREVIOUS WORK

Sriti Thakur et al. in [1] proposed a technique using the discrete cosine transform and the discrete wavelet transform for a multi layer security mechanism for biomedical image security. They also used the singular value decomposition for the process of retaining the significant information of the image.

C Yu et al. in [2] proposed the Fresnel transform along with the chaos maps and hologram effect that is generated by coding. The Fresnel transform has the salient property of adhering to the properties of an irreversible transform and the occurrence of chaos makes it even more difficult for the attackers to decode the image.

LY Zhang et al. in [3] proposed the diffusion mechanism for image encryption in which the pixels of the image were mapped onto another set of values based on the pixel diffusion map. The technique however could render limited randomness due to the operation of diffusion matrices.

Y Li et al. in [4] proposed a hyper-chaos technique which is different from the conventional chaos mechanism by dint of the fact that in this technique, the chaos is applied at the bit level and not only at the pixel level which makes it extremely challenging for adversaries to break the code.

X Chai et al. in [5] proposed a compressive sensing approach in which the pixel values are sensed and an attack like environment is created while transmitting the image. This process tries to emulate an attack condition in which the data is jammed deliberately by the attacker.

A Belazi et al. in [6] proposed a technique using the fractional transform and chaos. The fractional transform has the property of making the transform coefficients imaginary or complex numbers thereby breaking more difficult. The chaos also makes the process more secure to threats.

L Xu et al. in [7] proposed a technique that used bit level permutation and chaotic maps. In this case, the chaos is implemented by the chaotic map while the bit level permutation occurs at the bit level thereby rendering multi-level security to the data.

N Zhou et al. in [8] proposed a combined approach of hyper chaos and compressive sensing, In this case, the hyper chaos implements the chaos in the bit level and deliberate jamming is implemented by the compressive sensing approach to secure the images.

S Trambadia et al. in [9] proposed a restoration technique for images. This approach makes the images more immune to the noise and disturbance effects and hence renders higher clarity and quality to the images after they are restored, This restoration process is necessary since images are degraded by noise effects while capturing, storage and transmission.

J.S. Armand et al. in [10] proposed block cipher encryption along with chaos. The block cipher encrypts pixels contrary to serial or stream ciphers since they pick up blocks for encryption. The chaos being an effective mechanism helps to render greater security compared to single level encryption.

V. EVALUATION PARMAETRES

The 1) Peak Signal to Noise Ratio which is mathematically defined as,

$$PSNR = Max(\frac{S}{N}) \quad (5.1)$$

Here,
S represents Signal Power
N represents noise power
2) Mean Square Error (MSE) which is mathematically defined as:

$$MSE = \frac{1}{N}\sum_{t=1}^{N} {e_t}^2 \quad (5.2)$$

Here,
N is the number of pixels
e is the error between the pixels of the actual and extracted images

VI. CONCLUSION

The previous discussions and related work clearly indicate that the chances of successful attack are more in case of single layer of encryption or data hiding. The system becomes more immune to attacks when the security mechanism is manifold. Hence the concept of multi-layer or multi-level security is prevalent for data security in tele health services. The use of chaos and transform domain manipulation is common among the techniques used. The performance metrics are the peak signal to noise ration and the mean square error. The peak signal to noise ratio (PSNR) should be as high as possible and the Mean Square Error (MSE) should be as low as possible. The salient features of the previous work provide a headway into further avenues of implementation of an improved scheme.

References

[1] Lin Teng, Xingyuan Wang, Juan Meng, " A Chaotic Color Image Encryption using Integrated Bit-Level Integration", Springer 2018
[2] C Yu, J Li, X Li, X Ren, BB Gupta, "Four-image encryption scheme based on quaternion Fresnel transform, chaos and computer generated hologram", Springer 2018
[3] LY Zhang, Y Liu, F Pareschi, Y Zhang, "On the security of a class of diffusion mechanisms for image encryption", IEEE 2018.
[4] Y Li, C Wang, H Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation", Elsevier 2017.
[5] X Chai, Z Gan, Y Chen, Y Zhang, "A visually secure image encryption scheme based on compressive sensing", Elsevier 2017.

[6] A Belazi, AAA El-Latif, AV Diaconu, R Rhouma, "Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms", Elsevier 2017.
[7] L Xu, Z Li, J Li, W Hua, "A novel bit-level image encryption algorithm based on chaotic maps", Elsevier 2016.
[8] N Zhou, S Pan, S Cheng, Z Zhou, "Image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing", Elsevier 2016.
[9] S Trambadia, P Dholakia, "Design and analysis of an image restoration using wiener filter with a quality based hybrid algorithms", IEEE 2015.
[10] J.S. Armand Eyebe Fouda , J. Yves Effa, Samrat L. Sabat , Maaruf Ali , "A fast chaotic block cipher for image encryption", ELSEVIER 2014.
[11] Zhenxing Qian, Xinpeng Zhang, Shuozhong Wang, "Reversible Data Hiding in Encrypted JPEG Bitstream", IEEE 2014
[12] A Bakhshandeh, Z Eslami "An authenticated image encryption scheme based on chaotic maps and memory cellular automata", Elsevier 2013.
[13] K Gu, G Zhai, X Yang, W Zhang, "A new reduced-reference image quality assessment using structural degradation model", IEEE 2013
[14] YW Tai, S Lin, "Motion-aware noise filtering for de-blurring of noisy and blurry images", IEEE 2012