DUAL WATERMARKING SYSTEM BASED MEDICAL DATA PROTECTION FOR TELEMEDICINE APPLICATION

Miss. V.J.MUTHULAKSHMI[1] Mr. N. SIVANESAN[2]
[1]Student, [2]Asst Professor, [1,2]Department of CSE, [1, 2]Sri Krishna Engineering College,
[1]lakshmimuthu51@gmail.com

Abstract- The project proposes the enhancement of protection system for secret data communication through encrypted data concealment in bio-metrics. The main theme of the proposed system is to maintain the multiple documents for a single patient such as digital scan image, personal details, and diagnosis results in a single file.The proposed technique has three different input data of a single person like fingerprint, diagnosis result, and scan image. Here the fingerprint is used for person identification purposes by using Minutiae information Extraction from fingerprint. Then the patient scan image is separated into two different components (detailed and approximation component). The diagnosis result was encrypted using logistic mapping method. The encrypted result was hidden in the detailed component of the image using ALSB. The data hiding technique uses the ALSB replacement algorithm for concealing the diagnosis results into the detailed coefficients. In the data extraction module, the diagnosis data will be extracted by using relevant key for choosing the relevant data to extract the data. By using the decryption keys, extracted text data will be decrypted from encryption to get the original information. The minutiae information from fingerprint is also embedded in the structural component of image using Singular Value Decomposition method. In the Extraction part the medical image and diagnosis results are extracted after the fingerprint recognition process. If the fingerprint features are mismatched the user can’t access the patient details. Finally the performance of this proposal in encryption and data hiding will be analyzed based on image and data recovery. The parameters like PSNR (Peak Signal to Noise Ratio), RMSE (Root Mean Square Error), PRD (Percentage Residual Difference), Correlation and SSIM (Structural Similarity Index Measure) are measured.

Keywords - Dual Watermarking, Telemedicine, Data Hiding

I. INTRODUCTION

Image processing is discussed, which provides the secret data communication through encrypted data concealment in encrypted images. The image is then separated into three different input data of a single person like fingerprint, diagnosis result, and scan image textural detail will have the high frequency of texture and noise so it save the personal detail and diagnosis report of patients. Structural detail will have the low frequency of visible region so it saves the fingerprint of the doctor. singular points detection is to use as reference points for fingerprint matching and classification. Generally, accurate and efficient singular points detection considerably affects the overall fingerprint identification system. Fingerprints contain ridges and valleys separately, and these ridges flow almost parallel to each other. However, in the singular point area, this pattern is changed. Data hiding is a process to hide data into cover media.

Data hiding process links two set of data, a set of secret data and another set of cover media data. reversible data hiding, this can recover the original image without any change in the shape of the image after the hidden data have been extracted. The reversible data embedding is also known as lossless data embedding. The feature of reversible data embedding achieves real reversibility. To separate the process of data extraction and image decryption, allocate some space for data embedding. From the application point of view reversible data hiding is used as an information carrier. To increase the payload capacity, first we select an embedding area in an image. Second embed both the payload and original value in this area. In this paper we present the high capacity and high visual quality, reversible data hiding for digital images. Our method can be applied to digital audio and video. This technique is used in military imagery, medical imagery and law forensics.

II. SCOPE

Dual watermarking method uses to reduce the bandwidth and improve the safety of secret carrier information. To make that information inaccessible to any intruder having a random method. Multiple documents can be sending in a single file. It protects privacy information during data communication over unsecure channel based on data encryption and data hiding technique. To improve the data hiding technique uses the logistic map encryption and adaptive LSB replacement algorithm for concealing the secret message bits into the encrypted image.

III. EXISTING SYSTEM

The existing system uses pixel difference expansion method for data embedding. The data hiding capacity is low in this technique. Bit modification technique is used. Patient data merging can be taken place when sending multiple documents. It introduced some error on data extraction.so its degrade the image quality more distortion due to hiding process when using spatial fusion algorithm no accurate extraction can be done in RSA algorithm. More computational time is needed for stream cipher algorithm.

IV. PROPOSED SYSTEM

Secret data concealment within patient scan images using logistic mapping based encryption, Lifting wavelet Transform, ALSBreplacement technique and singular value decomposition. In this framework first reserves enough space on original image and then convert the image into its encrypted versions with the encryption key. Data hiding will be analyzed based on image and data recovery. Then the patient scan image is separated into two different components are detailed and approximation component the diagnosis result was encrypted using logistic mapping method. Multiple documents can be sending in a single file and reduces the bandwidth.

V. METHODOLOGY

A. Minutiae Extraction

The accurate representation image of the fingerprint is critical to automatic fingerprint identification systems, because most of the commercial large-scale systems are dependent only on the feature-based matching from the all the fingerprint features, minutia point features is only the unique to discriminate amongst fingerprints robustly the complex fingerprint recognition problem will be reduced by minutiae feature to a point pattern matching issue. To achieve high accuracy minutiae with varied quality fingerprint images, the algorithm needs to separate foreground and background from noisy stages the fingerprint enhancement is to improve the clarity of ridges and valleys of the input images in the singular point area. which includes all ridge-valley regions and not the background based.

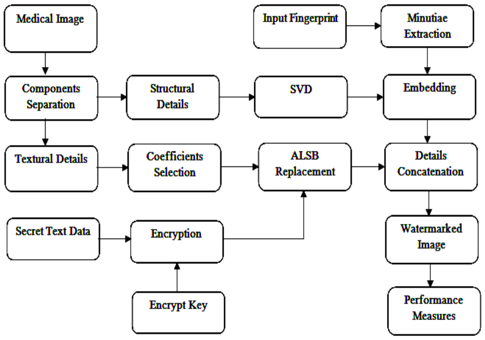

Fig 1 Block diagram of data protection

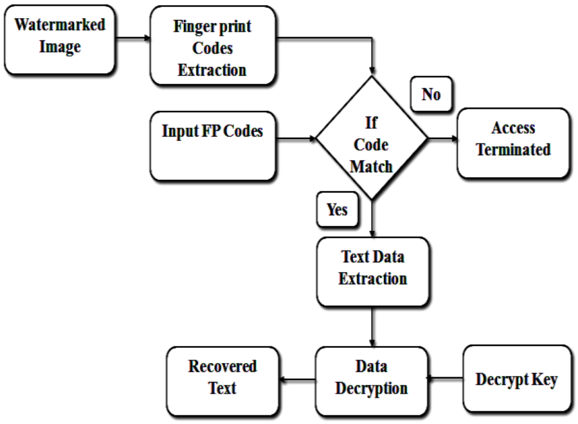

Fig 2 Block Diagram of Authentication and Text Data Extraction

The image enhancement algorithm must keep the original flow pattern without altering the singularity, the join broken ridges and clean artifacts between pseudo-parallel ridges, and not introduce false information. After that finally minutiae detection algorithm needs to be efficient. It can be classify as methods broadly into two categories:

1) Those that work on the images based on the binarized fingerprint

2)Images that work directly on gray-scale fingerprint images.

B. Lifting wavelet transformation

This technique is used to separate the component present in the spatial image. LWT decomposes the image into different subband images, namely, LL, LH, HL, and HH for embedding the messages in the pixel coefficients of subbands. Lifting scheme is a method which is used to convert DWT coefficients to Integer coefficients without losing information. LL subbands contains the significant part of the spatial domain image. High-frequency subband contains the edge information of input image which is given for reserved space foe hiding the text data.

The particular secret text data is embedded into the wavelet coefficients of high frequency subbands because it is non sensitive to human visual system.

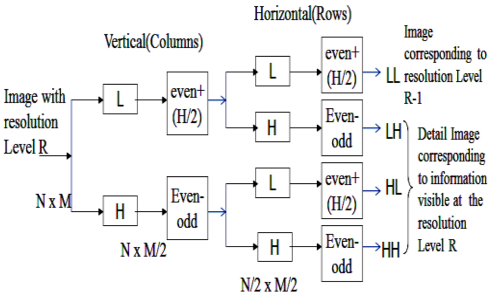
Horizontal(Rows)
Vertical(Columns)
Image with resolution Level R
N x M
L
H
even+ (H/2)
Even- odd
N x M/2
L
H
L
H
even+ (H/2)
Even- odd
even+ (H/2)
Even- odd
N/2 x M/2
LL
LH
HL
HH
Image corresponding to resolution Level R-1
Detail Image corresponding to information visible at the resolution Level R

Fig 3 Block Diagram of Lifting Wavelet Transformation

Step1: Column wise processing to get H and L H = (Co-Ce) and L = (Ce+ [H/2*]) Where Co and Ce is the odd column and even column wise pixel values

Step 2: Row wise processing to get LL,LH,HL and HH,Separate odd and even rows of H and L,Namely, Hodd – odd row of H,

Lodd- odd row of L,

Heven- even row of H,

Leven- even row of L,

LH = Lodd-Leven ,

LL = Leven + [LH / 2]

HH = Hodd – Heven ,

HL = Heven + [HH / 2]

Inverse Integer wavelet transform is formed by Reverse liftingscheme. Procedure is similar to the forward lifting scheme.

C. Logistic Mapping Based Encryption

This method is the advanced encryption standard to encrypt the image for secure transmission.It encrypts the diagnosis text values with encryption key value generated from logistic sequence with threshold function by bitxor operation .Here logistic map is used for generation of different map sequence.

It is very useful to transmit the secret image through unsecure channel securely which prevents data hacking. SVD has many good mathematical characteristics.
1)The size of the matrices from SVD transformation is not fixed and can be a square or a rectangle.

2)The SVs (Singular Values) of an image have very good standard it means when a small perturbation is added with the image, its SVs do not vary rapidly.

3)SVs represent algebraic image properties which are intrinsic and not visual. The finger print data will be concealing into singular values of structural details and this feature will preserve the hidden image from affine distortions.

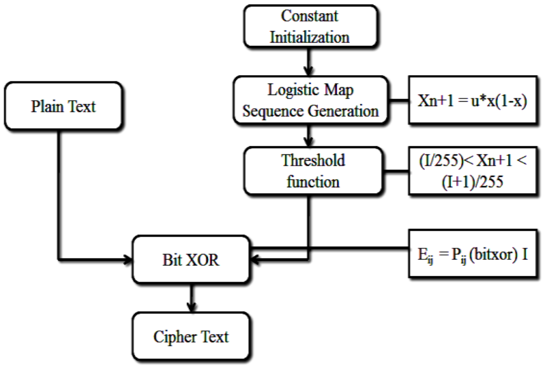

Fig 4 Logistic Mapping Process Flow

D. Singular Value Decomposition

SVD has many good mathematical characteristics. 1) The size of the matrices from SVD transformation is not fixed and can be a square or a rectangle.

2) The SVs (Singular Values) of an image have very good standard it means when a small perturbation is added with the image, its SVs do not vary rapidly;

3) SVs represent algebraic image properties which are intrinsic and not visual. The finger print data will be concealing into singular values of structural details and this feature will preserve the hidden image from affine distortions.

E. Embedding

The secret image will be decomposed into singular and two orthogonal matrix.These values are concealing into singular values of low frequency subbands by modifying it through key value.The key should be selected as least value to reduce the embedding error. The singular value of subband will be modified by,

Ms = Cs + (Ws * K)
Where, Cs – Singular value of cover image subbands,Ws – Singular value of secret data,Ms – Modified Singular matrix, K – Least Key Value.

F. Adaptive LSB Embedding

A 8-bit gray scale image matrix consisting m × n pixels and a secret message consisting of k bits. In that first bit of message is embedded into the LSB of the first pixel and the second bit of message is embedded into the second pixel and so on. The final result Stego-image which holds the secret message is also a 8-bit gray scale image and difference between the cover image and the Stego-image is not visually perceptible.

The quality of the image, however degrades with the increase in number of LSBs. The error between input and output image will be introduce by the hiding process and it is determined by mean square error and Peak signal to noise ratio determines the image quality.The basic concept of LSB substitution is to embed the confidential data at the rightmost bits (bits with the smallest weighting) so that the embedding procedure does not affect the original pixel value greatly. The mathematical representation for LSB method is: *x* represents the *i* th pixel value of the stego-image, *i x* represents that of the original cover-image, and *i m* represents the decimal value of the *i* th block in confidential data. The number of LSBs to be substituted is denoted as k. This method is easy and straightforward. However, when the capacity is greatly increased, the image quality decreases a lot and hence a suspected stego-image results. Furthermore, the confidential data might be easily stolen by simply extracting the k-rightmost bits directly.

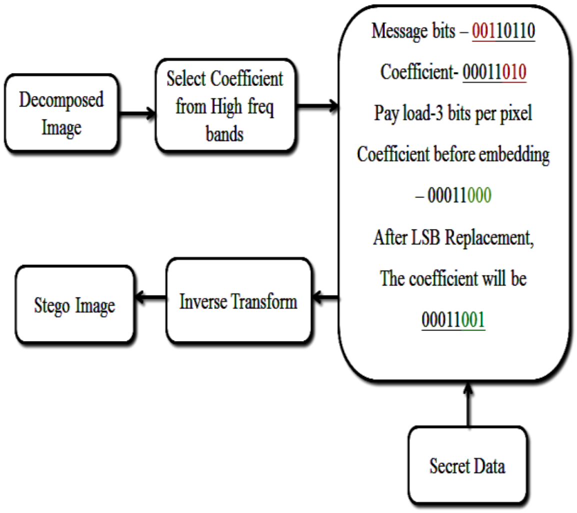
Decomposed Image
Select Coefficient from High freq bands
Message bits – 00110110
Coefficient- 00011010
Pay load-3 bits per pixel
Coefficient before embedding – 00011000
After LSB Replacement, The coefficient will be 00011001
Stego Image
Inverse Transform
Secret Data

Fig 5 ALSB Algorithm Flow

G. Quality measures for image

The Quality of the reconstructed image is measured interms of mean square error (MSE) and peak signal to noise ratio (PSNR) ratio. The MSE is often called reconstruction error variance ∇_q^2. The MSE between the original image f and the reconstructed image g at decoder is defined as:

$$\text{MSE}=\nabla_q^2 \frac{1}{N}\sum_{j,k}(f[j,k]-g[j,k])^2$$

Where the sum over j, k denotes the sum over all pixels in the image and N is the number of pixels in each image. From that the peak signal-to-noise ratio is defined as the ratio between signal variance and reconstruction error variance. The PSNR between two images having 8 bits per pixel in terms of decibels (dBs) is given by:

$$\text{PSNR} = 10 \log_{10}\left(\frac{255^2}{MSE}\right)$$

Generally when PSNR is 40 dB or greater, then the original and the reconstructed images are virtually indistinguishable. It is used to find the similarity between two different images with their intensities. It will be described by,

Cor_coef=[sum(sum(u1.*u2))]/ / [sqrt(sum(sum(u1.*u1))*sum(sum(u2.*u2)))];

Where, u1 = F1 – mean of F1, u2 = F2 – mean of F2F1 – Cover Image and F2 – Encrypted Image

VI. CONCLUSION

The minutiae information from fingerprint is embedded in the structural component of image using singular value decomposition method. In the extraction part the medical image and diagnosis results are extracted after the fingerprint recognition process. If the fingerprint features are mismatched the user can't access the patient details. Finally the performance of this proposal in encryption and data hiding will be analyzed based on image and data recovery. The parameters like peak signal to noise ratio, root mean square error, percentage residual difference, correlation and structural similarity index measure are measured. In separate data extraction and greatly improvement on the quality of marked decrypted image. The computer experiments show it will give excellent PSNR after embedding. The main aim of the project is to reduce the bandwidth while sending the multiple documents in a single file.we extended the research to match the fingerprint of the doctor in the proposed scheme. Eventually, arrived to the conclusion that dual watermarking scheme is more suitable to be implemented in telemedicine application.

REFERENCES

[1]P.Ruotsalainen,"Privacy and security in teleradiology,"Eur. J.Radiol., vol. 73, pp. 31–35, 2010.

[2]N.Hussain,W.Boles,and C.Boyd,"A review of medical image watermarking requirements for teleradiology," J.Digital Imag,vol. 26, no. 2, pp. 326–343, Apr. 2013.

[3]S.Wang W.Yangsheng,"Fingerprint enhancement in the singular point area," IEEE Trans. Signal Process., vol. 11, no. 1, pp. 16–19, Jan. 2004.

[4]A.K.Jain,S.Prabhakar,L.Hong and S.Pankanti, "Filterbank-based fingerprint matching," IEEE Trans. Image Process., vol.9, no. 5, pp. 846–859, May 2000.

[5]M. Tico, P. Kuosmanen, and J. Saarinen, "Wavelet domain features for fingerprint recognition," IEEE Electron. Lett., vol. 37, no. 1, pp. 21–22,Jan. 2001.

[6]C.H. Teh and R. T. Chin, "On image analysis by the methods of moments,"IEEE Trans. Pattern Anal. Mach. Intell, vol. 10, no. 4, pp. 496–513, Jul.1988.

[7]P. Viswanathan and P. V. Krishna, "Morlet Wavelet Fingerprint Invariant Automated Authentication system," Int. J. Recent Trends Eng,vol.4,no. 1, pp. 1–5, 2010.

[8]A. Khotanzad and Y. H. Hong, "Invariant image recognition by Zernike moments," IEEE Trans. Pattern Anal. Mach. In tell, vol. 12, no. 5, pp. 489–497, May 1990.

[9]D.Jablon, "Strong password only authenticated key exchange, computer communication review," ACM SIGCOMM Comput. Commun. Rev,vol. 26, no. 5, pp. 5–26, 1997.

[10]H. S. Malvar and D. A. F Florencio, "Improved spread spectrum: A new modulation technique for robust watermarking," IEEE Trans. Signal Process,vol. 51, no. 4, pp. 898–905, Apr. 2003.

[11]G. Pajares and J. M. de la Cruz, "A wavelet-based image fusion tutorial," Int. J. Pattern Recognit., vol. 37, no. 9, pp. 1855–1872, Sep. 2004.

[12]D. Bouslimi, G. Coatrieux, and C. Roux, "A joint encryption watermarking system for verifying the reliability of medical images," IEEE Trans. Inf.Technol. Biomed., vol. 16, no. 5, pp. 891–899, Sep. 2012.

[13]R. Anderson and C. Manifavas, "Chameleon: A new kind of stream cipher,"Fast Softw. Encrypt., vol. 1267, pp. 107–113, 1997.

[14]A. Adelsbach, U. Huber, and A. S. Sadeghi, "Fingercasting-joint fingerprinting and decryption of broadcast messages," in Proc. IEEE Inf. Security Privacy, 2006, pp. 136–147.

[15]L. Shiguo et al., "Joint fingerprint embedding and decryption for video distribution," in Proc. IEEE Int. Conf. Multimedia Expo, 2007, pp. 1523–1526.

[16]P. Viswanathan and P. VenkataKrishna,"Fusion of cryptographic watermarking medical image system with reversible property," Comput. Netw.Intell. Comput. Commun. Comput. Inf. Sci., vol. 157, 2011,no. 1, pp. 533–540.

[17]G. H. Qu, D. L. Zhang, and P. F. Yan, "Information measure for performance of image fusion," IEEE Electron. Lett., vol. 38, no. 7, pp. 313–315, Mar. 2002.

[18]N. Cvejic, C. N. Canagarajah, and D. R. Bull, "Image fusion metric based on mutual information and Tsallis entropy," IEEE Electron. Lett, vol. 42,no. 11, pp. 626–627, May 2006.

[19]G. Qu, D. Zhang, and P. Yan, "Information measurement for performance of image fusion," Electron. Lett., pp. 313–315, 2002.

[20]Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error measurement to structural similarity,"IEEE Trans.Image Process,vol. 13, no. 4, pp. 600–612, Apr. 2004.