Chapter 7

Results and Discussions

7.1 Results

A. Morlet Wavelet Fingerprint $Z_\phi$ Moment Invariant based Authentication System:

The proposed fingerprint verification is evaluated by standard database DB1, DB2, DB3, and DB4. The Morlet enhancement of fingerprint image provided good ridge continuity with less reduction of genuine minutiae. The $Z_\phi$ moment features evaluated by statistical analysis of algebraic and Zernike moments are invariant against affine transformations that provided less features authentication system. The experimental result is evaluated by means of EER, FAR, and FRR. The EER act as a performance indicator that indicates the point where FRR and FAR are maintained in average between Genuine acceptance rate (GAR=1−FRR) against FAR. The missing and alarm probability is also maintained normalized. The ROC provides minimum FAR and FRR, which shows that the proposed Morlet $Z_\phi$ invariant verification system resulted in more than 97% of accuracy when compared to various other previous methodologies.

B. Joint FED Spatial Fusion Watermarking System

The medical image spatial fusion watermarking system is evaluated by standard metrics like PSNR, RMSE, and SNR, which determined the quality of the fusion image. The RMSE range of value is from 0.006 to 0.007, which is very low and
means that there is no difference between the medical and fusion image. The PFE for CT, CR, XRAY, and SCAN provides less error rate than MR and US images, which result that there is very less deviation between the original medical image and fusion image compared to MR and US fusion image. The MSE of fused image with the fission image is 0 nad it tells that there is no variation between the fused image and fission image, meaning that it resembles or seems identical with the original fused image.

The SNR and PSNR resulted in large value meaning that the sensitivity of medical image is maintained. The MAE evaluation has got very low error that determines the closer prediction between the medical image and the fusion image. The coefficient variance provided no distinctive variance between the original image and the fusion image. The mutual information (MI) is larger when compared to other techniques and moves more than 7.166, which tells that the image quality is higher than the previous approaches. The Universal quality index (QI), sometimes nearer and most of the images reached 1 means due to the fusion quality of medical image that is not affected and Structure similarity (SSIM) also highly determines the maximum structure similarity between the fusion and the original medical image. From the performance evaluation there is no major effect of fusion in medical image and fission image and it resembles the original image. Hence, the algorithm has maintained the quality of the image with efficient fusion. The algorithm is also very simple that provided less computation cost and time complexity compared to previous approaches.

The embedding capacity of the proposed scheme is evaluated by hiding different size of secret image or text in the host image. From this evaluation it has been found that a maximum of 75% of 1 bpp of cover image can be embedded in the host image. Our human vision is sensitive to slight changes in the smooth regions which can be overcome by changing pixels in edge regions. The watermarking is based on region, hence it is observed that pixel alteration is inevitably in edge region and is not spread out in the host image. It has shown less rate of modification differences that assures the imperceptibility of the watermarked image.
There is no addition of visual artifacts in the LSB planes of the watermarked image with an embedding rate of 30\% and 50\%. The LSBM, LSBMR, and some PVD based methods are random embedding schemes, in that the smooth regions would be inevitably disturbed and especially for the LSBM due to its higher modification rate it looks more random compared with others.

The watermarked image is tested by chi square test that provides the outputs of two different curves along a grid where every vertical blue bar represents 1 to show the hidden data but the outputs are in red which shows that the probability that pairs of values follow a random distribution of LSB (a false positive) supposed to be not frequent. Then 0, the PoV are not random but are frequent in a normal image and hence there is no message hidden in the LSB. Then shows green, the average value of all LSB in one block of pixels is 128 by default. It is also tested by Invisible Secrets 2002 steganographic software to detect hidden messages which shows the message that file does not seem to contain hidden data. It shows that the proposed system can't be attacked statistically. The complexity of the algorithm is evaluated in terms of execution time that is a maximum of 16 seconds for embedding and for extraction it takes 10 seconds. These all shows that, the proposed system provides less time complexity and computation complexity in the watermark system.

C. Verification and Validation of Teleradiology Systems
In teleradiology, the primary objective of a watermarking scheme for medical images should be authentication (e.g., origin or content). EPR annotation and integrity control (tamper detection and recovery) can be a further goal to form a multiple watermarking scheme. The multiple watermarking schemes have the potential intelligence to address the rising problem in teleradiology. Their applicability in teleradiology naturally requires more explicit consideration on the performance evaluations and security analysis which includes overall computational complexity, speed, and cost benefit analysis. Multiple watermarking schemes and their complete assessment by defining the parameters properly such that they can offer a better complementary solution for achieving improved security in teleradiology which has been addressed.

To address these issues combined Morlet Wavelet Fingerprint $Z_\phi$ Moment
invariant variation based Authentication System, four step cipher and dual spatial fusion watermarking is proposed. In our joint FED system, the personnel authentication by using fingerprint is comparatively difficult for to attack by the hacker. Due to the fact, hackers do not intrinsically modify them, without the authentication of the fingerprint. It can also provide the additional service of indexing the medical data to retrieve from the database.

The experimental result provided accurate indexing and confidentiality and integrity to the medical image. The four step cipher algorithms with four bit symmetric key gives good security performance which are preserved against common cryptographic attacks like the ones based on cipher text only, known plain text, chosen plain text, and on chosen cipher text attacks. If $K_e$ or $I_e$ are known from the attacker, he has no other additional means than a regular cryptographic attack to get $K_e$ or to have an idea about the decryption function. This is due to the fact that the encryption and decryption are of different function and $I_e$ is embedded in the image based on spatial fusion with four bit $K_e$ watermarked encrypted. $I_p$ appears encrypted in $M_w$ and its presence does not reduce the entropy of the watermarked encrypted image. The attacker has no clues about $K_e$. If now, he knows the keys also we can retrieve the cryptographic attack based on known plain text and known cipher text. Though the attacker has a complete of data with with the original image $I$, it is difficult to identify the encryption key $K_e$ with decryption algorithm without the knowledge of $I_e$ fingerprint invariant. The Unauthorized Detection n Extraction of Messages of the key $K_e$ can’t be extracted in encrypted domain without the fingerprint authentication. The location of the $I_p$ is predicted by spatial fusion, an attacker cannot distinguish the bits from the others. Even though the structure of $I_e$ is known, fingerprint authenticity code cannot be derived without fingerprint. If at the same time the encryption $K_e$ becomes available it remains not possible to find exactly the locations of the bits of $I_e$. However, if the application framework is considered the knowledge of $K_e$ or equivalently of $I_e$ allows a clear text attack in the spatial domains as it gives some partial knowledge about $I_p$ to one attacker.

Unauthorized Embedding Attack of the inserted message available in the
encrypted domain depends on $K_e$ and $F$. One can try to modify arbitrarily the watermarked encrypted bit stream in order to introduce a falsified message $I_e$ but this will be detected at the decryption stage whereas it will not be possible to reconstruct the image. At the same time, the watermarked encrypted image will be claimed as unreliable due to the fact that $I_e$ depends on key $K_e$. If now $I_w$ and $I_e$ are available, an attacker may insert a new message in the encrypted domain but it will be difficult for him to make the message compliant with $I_v$. The knowledge of $K_e$ or $I_v$ gives him no advantage. On the contrary, it will be possible to detect that a pirate has modified $I_p$ based on $I_e$ without any knowledge.

Unauthorized Removal Attack of the data in an image is rejected if it is not reliable, that is, if it is not possible to verify its integrity and origins. As a consequence, valid watermarks should be present in all images and in their encrypted versions. If someone changes embedded messages, he should also provide a new set of encryption and fingerprint invariants. It all contributes and concludes that the proposed system satisfied the verification and validation issues for teleradiology systems in the optimum level.

7.2 Contributions

The specific contributions are made as follows

- The Modified Morlet wavelet based enhancement of the fingerprint image to provide good ridge continuity and smoothening is used to improve the fingerprint verification system.
- The $Z_\varphi$ Moment Invariant based Fingerprint Verification System is used to reduce the verification error rate with less features being used to index and verify confidentiality for patient data.
- The region based watermarking System based on spatial fusion satisfying the condition of fusion rules is attempted to embed the patient data without affecting the quality of medical image and is used to verify the availability for teleradiology.
- Joint Cryptographic Fusion Watermarking System is of combining the encryption and watermarking in a single system with less computation cost and is attempted
to verify the reliability for teleradiology.

- Joint FED scheme is of combining fingerprint verification and encryption with spatial fusion watermarking in a single system and is attempted to provide accurate verification and validation for teleradiology systems.

### 7.3 Conclusions

The joint FED system, which guarantees double a priori and a posteriori protection of medical images to solve all the security issues for teleradiology. The system gives access to ROI or medical text data in encrypted domain and in the spatial domain with fingerprint authentication, respectively. The combined MORLET enhancement with fusion of Zernike and invariant moment features are extracted and matched by evaluating the distance by mean, deviation, and variance. The binaries approach accurately determines the reference point and has been used to extract the moments having the invariant ability to affine transformations in various input conditions. The extraction of $Z\varphi$ moment’s invariant to affine transformation with Morlet enhancement improves the verification accuracy up to 97% as compared to other approaches. The ROC curve of authentication system shows high GAR and low FAR which verifies the accurate recognition system. The equal error rate, missing probability and alarm probability are maintained normalized by the proposed approach providing accurate recognition system.

This fingerprint invariant authentication proves the individuality and immutability of the person who verifies the image with confidentiality. Encryption of medical ROI and text verifies the image with reliability and dual spatial fusion watermarking system verifies the availability in region of embedding with reliability. Whereas the previous scheme of joint encryption watermarking solves only the reliability issues but FED system provides confidentiality, reliability, and availability of the medical image for teleradiology. The four step cipher makes our system compliant with the DICOM standard. Experimental results are evaluated for fusion and for watermarking system shown that the image distortion is very low.

The execution time for message decryption is not impacted and it has been
suggested that the way of combined invariant authentication, encryption, and dual watermarking does not interfere with each other during the verification and validation in the system. It depends on the knowledge of the encryption and fingerprint invariants. The data is embedded in the specified region by spatial fusion which provides robustness to medical image that can withstand to attacks. The function of our encryption algorithm, embedding algorithm, and spatial fusion algorithm are very simple which determines less complexity when compared to other approaches. The fingerprint invariant authentication system is slightly complex but only needs less features to authenticate and requires less substitution results in minimum distortion in medical image. The ROI and fingerprint embedded in the medical image using dual embedding scheme with spatial fusion in different locations performs accurate verification and validation for teleradiology.

7.4 Future Work

- Improve the accuracy of invariant fingerprint authentication system along with other existing fast methods such as Kintner’s or the $q$-recursive method.
- Morlet Wavelet Fingerprint $Z_\phi$ Moment invariant variation based Authentication System can be applied for cancer detection and in some other detection systems
- FED system must be applied in some other media like video and music for secure transfer of data.