CHAPTER 6

CONCLUSION
CHAPTER 6

Conclusion

The results for different image are compared and it is seen that if the image is original without any single bit or single pixel distortion the system checks the authenticity of the image and gives the result as the image is validate .the system takes the image of any type ,kind and size respectively. The use of non regular low density parity check codes and the encryption methodology makes sure the authenticity of the image. And if the image is found to be unauthenticated it will give the result accordingly. So the system is useful in many applications such as defence, medical, scientific etc. purposes.

The findings are given below:

In this work we have shown that non regular low-density parity-check (LDPC) codes can be used to image authentication. The system can work with any type of image and the result shows that even a single bit distortion in the image can be detected. We can observe from the results that LDPC in the probability domain can be used to implement distributed source coding. A high performance is given by these codes. Distributed source coding is an ideal tool for the image authentication problem in which the data sent for authentication are highly correlated to the information available at the receiver. This method gives the better performance in all aspects in comparison to the previous work.

Moreover this chapter presents and investigates a novel image authentication scheme that distinguishes legitimate encoding variations of an image from tampered versions based on distributed source coding and statistical methods. A two-state lossy channel model represents the statistical dependency between the original and the target images. Tampering degradations are captured by using a statistical image model, and legitimate compression noise is assumed to be additive white Gaussian noise.

The rates of falsely deemed tampered blocks can reach zero, while keeping the undetected tampered pixel rates at about 2%, since most of the blocks falsely deemed untampered have only a few pixels tampered. In most cases, 1D and 2D spatial models achieve a lower undetected tampered pixel rate at a given falsely deemed tampered block rate.
Slepian-Wolf coding that exploits the correlation between the original and the target image projections achieves significant rate savings. The Slepian-Wolf decoder is extended using expectation maximization algorithms to address target images that have undergone contrast, brightness, and affine warping adjustment. The localization decoder infers the tampered locations and decodes the Slepian-Wolf bit stream by applying the sum product algorithm over a factor graph which represents the relationship among the Slepian-Wolf bit stream, projections of the original image and the target image, and the block states. Spatial models are applied to exploit the spatial correlation of the tampering. Distributed source coding is an ideal tool for the image authentication problem in which the data sent for authentication are highly correlated to the information available at the receiver.