CHAPTER 8
SUMMARY AND DISCUSSIONS

8.1 Conclusions

This dissertation presents several novel approaches to address the problem of copyright violation by employing a biometric watermarking scheme and proposes frameworks that eliminates the traditional use of password or pin to govern the copyright of digital image data, offers interoperability, and deters piracy to protect artists and artwork sellers from incurring losses.

The proposed system has the underlying assumption that the user is willing to offer his/her biometric samples to the digital content distribution agency (which is considered as a reliable authority). Since it is not quite a known domain to the users, there might be reluctance on his/her part to offer biometric samples.

Although the algorithms proposed in the thesis have been specifically tailored for images, with suitable modifications, they can be easily extended to other multimedia content as documents, audio and video. As described in the literature earlier, biometric based authentication mechanisms provide an extra layer of protection as these traits are unique to each individual and copying or forging them is really a challenging task.

8.2 Contributions

The main objective of this research is to provide various mechanisms for using biometric identifiers like face, iris and offline handwritten signature of the legitimate user for the purpose of copyright protection. The main contribution of this dissertation lies in proposing algorithms which use biometric traits as watermarks and embed them to provide a completely attack resilient system thereby ensuring the rightful ownership of a digital image document. Embedding the watermarks in the transform domain ensure that the watermarks are imperceptible and at the same time robustness in maintained. This dissertation also proposed a biometric copyright protection solution wherein a double layer of security has been imparted to the digital content by incorporating multi-biometrics at different levels of wavelet decomposition of the images.
The proposed algorithms not only provide immunity against common signal processing attacks but also against geometric attacks such as scaling, rotation, cropping etc. The authentication of the results has been justified by using standard test benchmark StirMark for to validate the results obtained.

8.3 Future Scope

Further research is not limited to, but includes more work or decision making in the following areas:

- The proposed algorithms have been tested on a few biometric traits like face, iris and offline handwritten signatures, they can be extended or modified suitably to develop more generic algorithms which can be used based on the biometric trait available instead of being specific to a biometric trait.

- The algorithms can also be extended to include a coloured image which has not been done in the current survey. The algorithms can be used to incorporate more biometrics into each colour channel to provide multiple security levels, at the same time taking care of the image quality and it’s robustness.

- Although template matching and authentication has been incorporated in each algorithm, the algorithms can be enhanced and enriched by incorporating more advanced pattern recognition algorithms so that even if the watermarks are severely damaged, we are still able to identify the legitimate user.

- The trend of watermarking is shifting towards 3D watermarking, the mention of which can be found in [101-110]. The algorithms have the capacity to be extended to 3D models also.

- The time complexity and computational efficiency of the algorithms can be improved by executing them on a parallel computing platform such as GPU’s. As all the algorithms are operating on images and deal with executing the same operations over and over, the algorithms can speed up considerably on parallel platforms.

Future direction for these applications would also involve protecting various other forms of digital multimedia such as audio, video and animations in addition to providing support for other popular 3D graphic _le formats other than the .o_ format such as .max, .3ds, .blend, .lwo, .md2, .md3, .md4 and .x.