CHAPTER 9

CONCLUSION AND FUTURE SCOPE

The focus of this research work is to analyze the science of data protection and also suggests a new software protection method using steganography, encryption and unique hardware identifiers which is much easier and also provides better protection in an effective manner. A variety of the existing software and data protection methods were studied and analyzed as part of this research work.

The first step in the research work was to identify the issues in software industry due to current levels of software piracy, copyright infringement etc. In Chapter 1 numerous real-life problems like piracy, packet sniffing, various types of hackings etc. are analyzed and also identified various threats. The main research issues and challenges relevant to the problem are thoroughly analyzed. Currently used protection techniques like serial numbers and other techniques are examined and experimented to find out its strength and weakness’ in protecting of data. This initial analysis helped to propose a new technique which will have all the positives of the existing techniques and also will manage the weakness of the existing techniques for effectively handling the protection of software as well as data. This new proposed system can be made extensible to make the protection even more effective also.

A detailed literature survey was performed to know about the trend and innovation applied in the development of protection methods over years. From literature survey it is observed that, various studies of different protection methods have been tried out in the past. The most popular cryptographic algorithms are TDES, AES, Blowfish and RSAT and these algorithms provide good security. However, cryptography methods have a lot of limitations in protection of data. All types of data
cannot be protected by cryptography as it can handle text only. Hence cryptography is often combined with other protection techniques like steganography to offer enhanced protection. Steganography can be a solution for protecting all types of data like text, audio, video, image etc. This is the reason why this thesis proposes steganography as the protection method to be used. Different types of steganography techniques are studied and compared to find their advantages and disadvantages. Spatial Domain Transform Steganography techniques are comparatively easier to use and maintain. From literature survey we can observe that different steganography algorithms have been proposed over time with each, offering different protection capabilities. Also, wireless implementations of this technique are not commonly used. In the literature survey, protection method using hardware method is also discussed and noted that this is usually more complicated and has several implementation difficulties.

The performance analysis of Cryptography was done to find out the difference in using the different cryptography algorithms. The algorithms mentioned in literature survey were tested and analyzed. Explanation of the whole process is provided as part of Chapter 3. From the experimentation results it was noted that the most effective cryptography algorithm AES was chosen for the proposed protection framework.

Different popular steganography techniques were studied from the literature survey are analyzed detail in Chapter 4. Some of the commonly used spatial domain steganography methods are experimented to find out its strength and weakness by analyzing the performance in detail. Steganography methods discussed like the LSB, MSB, RGB and PVD are quite easy to use and maintain. They have some good points too. However, the major issue with these method is that because of noise the image quality easily degrades and hence they are easily detectable. They can be easily reverse engineered and can be hacked easily. To avoid this a new steganography
algorithm was developed as part of the thesis work which changes the pixel values lesser and hence the image quality remains good also cannot be hacked easily.

For further improving the protection framework an extra security layer can be added by using the existing hardware features, it is discussed in Chapter 5. The thesis considers various hardware protection methods and compares them. Further on how these hardware protection methods can be useful for protecting of data and how it can rectify the limitations of existing methods is studied in the literature survey. Hence, the solution to use an existing hardware feature was found. Which can reduce the cost and at the same time it’s easy to use and maintain. Also, it increases the protection.

By studying all the various methods as well as the new methods that have been proposed, this thesis suggests a new a protection method for digital data which is more efficient. This proposed protection method combines the techniques of Steganography, cryptography and hardware authentication method, gives maximum protection which is cost effective, easy to implement and suitable for all types of systems including wireless (mobiles)/ desktops, laptops or tablets. This new method can prevent piracy, unauthorized access of files or data and protect confidential data efficiently. Since two encoding algorithms are used, it helps to keep the data safe and it is not easy to do crypt analysis or reverse engineering and also the image pixels are having lesser changes, the data it is not easy to retrieve it using Steganalysis methods.

In order to prove the performance of the proposed model, an extensive performance evaluation of the model was performed. In Chapter 7, performance analysis and test results are clearly analyzed. For making sure that the performance of the protection framework is perfect, image quality analysis, data quality analysis and security threats are also considered and verified using standard quality measurements.
From the results, it is inferred that the proposed model outperforms from the other models included for comparison.

The contribution of the thesis can be summarized as follows:

- The SteganoDB structure specified can accept any data definition structure over than the concept of database.
  
  The SteganoDB structure can do all the operations (insertion, deletion, updation etc..) easily than a file based operation.
  
  The SteganoDB structure can contain non-related data hence can be reused.
  
  SteganoDB can be used not only for protection it can be used for other applications also.

- The Pixel Pattern based Steganography algorithm is effectively storing data into an image with minimal noise.
  
  The Pixel Pattern based Steganography algorithm uses two encryption techniques AES and Substitution cipher method, hence it gives maximum protection.

- This algorithm alone can be used for file protection or message protection.

- The Digital Data Protection combines the advantages of cryptography, steganography and hardware protection techniques.
  
  The overall structure of Digital Data Protection is a hybrid architecture and hence it is not easily hackable.
  
  The Digital Data Protection framework is an extensible model.
Future Scope for Enhancements

The following extensions may be carried out for future research with the proposed model. The main objective of the protection framework is to achieve maximum protection and keep the data efficiently.

1. Enhance the pixel pattern algorithm by using modern processors multithreading capabilities which will make it faster.

2. The protection method can also protect audio/video files from piracy.

3. Add multiple configuration options into piracy prevention method. Add more effective encryption methods.

4. Enhance algorithm to capture biometric information or iris capturing and add it as part of steganography method, this increases the security level.

5. Enhance the algorithm using with network authentication, for services like online gaming, secure chatting etc.

6. Explore secure e-governance areas like management of personal data like Aadhar card, PAN card data etc.

7. Enhance the SteganoDB package and extent its data storing capabilities.