Novel and Robust Methodologies for Image Security

A Thesis submitted by
Satendra Pal Singh

in partial fulfillment of the requirements for the award of the degree of
Doctor of Philosophy



Indian Institute of Technology Jodhpur
Department of Mathematics
June 2019

8
Conclusions and Future Work

The main aim of this thesis is to provide novel and robust algorithmic solutions for image security. The research contribution are concluded in Section 8.1 and the future directions are suggested in Section 8.2.

8.1 CONCLUSION

In this work, many novel solutions have been proposed, analyzed and evaluated for image security. These solutions are mainly based on three techniques: (1) Image hashing, (2) Encryption, and (3) Digital watermarking. Using these techniques, the proposed frameworks are designed specially for content authentication, data confidentiality protection and copyright protection to provide end-to-end security for image data.

The thesis emerges with the basic problem statement, motivation and a detailed literature survey in Chapter 1. The related state-of-the-art references are categorized and discussed thoroughly according to their major components. This chapter essentially reveals the prospective research directions in the area of image security. Then, a comprehensive review of mathematical preliminaries is given in Chapter 2. These introductory concepts are used in the various parts of the thesis and are essentially the integral part of the course of the thesis. This thesis addresses some of the critical issues of image security, which predominantly are content authentication, data confidentiality protection over communication, ownership identification and copyright protection. The content authentication problem is addressed by the perceptual hashing whereas data confidentiality protection is confirmed by the image encryption technique. For the ownership identification and copyright protection, digital watermarking terminology is considered as an efficient solution.

The discrimination capability and robustness are two important characteristic for any image hashing technique. While focusing on discrimination capability in this thesis, the invariance of the extracted features have been achieved and utilized in the generation of the perceptual hash functions. In Chapter 3, a chaos based robust and secure scheme was proposed for DCT based perceptual hash function. In this scheme, the test image is normalized using the geometric moments then normalized coefficients are further transformed into DCT domain. As, the singular values represent the important features, therefore, singular value decomposition is employed to generate the hash value. In this process, a secrete key based on non-linear chaotic map is also used to increase the unpredictability in the hash value. The claims of the proposed scheme is verified by detailed experimental analysis in terms of robustness and sensitivity analysis. However, the scheme has some limitation regarding the discrimination capability. To overcome this problem, an another approach has been presented in Chapter 4, using the global and local features to increase the discrimination capability. In this approach, KAZE algorithm was employed to extract the perceptual features whereas log polar mapping is used to estimate statistical features. Both the features equally contribute in the hash value. The proposed hashing scheme is modelled using optimal thresholding in wavelet domain to identify the variation in local contrast of the image content. The experimental results demonstrate that technique outperforms in terms of robustness and highly sensitive against content changing operations. The high robustness of the scheme is

experimentally verified using a series of experiments and analysis.

In next phase, the research on image encryption were carried out. In Chapter 5, a novel approach on medical image encryption was proposed. The proposed approach overcome the weakness in the security by employing a biometric to entail an efficient key management. The proposed approach modelled with parameterized all phase biothogonal transform (PR-APBST) to offer good image encryption. In this approach, the input image is firstly randomized using non-linear chaotic map and then encrypted with the help of fingerprint template of the user. The reverse process was applied with same parameters to decrypt the original image. The performance of the proposed scheme was evaluated using key sensitive analysis, edge distortion ratio, numerical analysis and, edge similarity analysis. The obtained results validate the effectiveness of the proposed scheme among existing encryption techniques.

In the concluding phase of the thesis, two watermarking techniques have been proposed with the objective of achieving robustness while maintaining good imperceptibility. It is evident that robustness and imperceptibility are two complementary characteristics of a watermarking system. Therefore, an optimal trade-off has to be defined to have a balance between robustness and imperceptibility. In order to achieve final goal, a robust blind watermarking scheme was proposed in Chapter 6 to address the problem related to copyright protection and owner identification. The proposed scheme generates a reference based watermarked image using lifting wavelet transform. The reference set was generated using a *d*-sequence based on random number generator. Using the reference set, the embedding of binary watermark was carried out to produce the watermarked image. On the other hand, a reference based blind extractor enables the extraction of the watermark from the watermarked image. The proposed approach is experimentally verified using a series of standard watermarking attacks and obtained results indicate that proposed model outperformed the existing exiting techniques in various aspect. The proposed model was designed only for binary watermark. For gray-scale watermark, a new watermarking approach was developed based on integer DCT and dynamic stochastic resonance (DSR) in Chapter 7. In proposed model, the host image is transformed into frequency domain using integer DCT and the embedding of watermark information was carried out using singular value decomposition. The novelity lies in the watermark extraction method, wherein a DSR phenomena was employed for successful extraction of watermark information. In extraction process, DSR reduce the effect of attacks or tempering iteratively and provide robust extraction of the watermark. This is due to the fact that when the watermarked image was tuned by the internal noise (due to possible attack), then hidden information of the watermarked was enhanced, and results in the robust watermark extraction. Also, the bistable system parameters used in DSR algorithm are iteratively optimized for lower computational complexity. The proposed DSR based model shows better performance among existing techniques in terms of robustness and computational complexity.

At the end, it is reported that the observations and findings of this thesis are reported and published in the peer-reviewed journals and reputed conferences, which can be seen in "List of Publications".

8.2 FUTURE WORK

The research work discussed in this thesis can be explored to pursue further research in relevant areas. The proposed solutions can be extended for multimedia security using video encryption, watermarking and hashing. The future direction of the proposed work can be summarized as follows.

- The proposed hashing techniques based on perceptual and statistical features can be extended to the audio and video authentication. Future work involves development of audio and video hashing using robust and invariant feature extraction utilizing frequency domain transformation. In addition, the framework can be designed for the classification and indexing of the video data. Furthermore, the special hash function can be designed to provide the efficient security for medical and document images.

- The image encryption method based on biometric feature have been developed for the medical images. However, the possibility of other biometric templates may be explored to develop the secure encryption system. The proposed techniques can be further extended to protect the confidentiality of the video data. In addition, the avenues are still open to develop efficient key dependent transformation such as PR-APBST, that can provide more robust encryption for the multimedia data.

- As mentioned before, the perceptual hash function provides the digital signature for multimedia data, therefore the incorporation of the hashing function in the digital watermarking system will be more advantageous in various scenario. The estimated hash value can be embedded into the host image to produce the watermarked media. The design, implementation and testing of the such framework can help to provided complete security to multimedia data.