DESIGN AND ANALYSIS OF VISUAL SECRET SHARING SCHEMES

By

Sachin Kumar

Department of Mathematics

Submitted in fulfillment of the requirements of the degree of Doctor of Philosophy

to the

Indian Institute of Technology Delhi
July 2012

Certificate

This is to certify that the thesis entitled **Design and Analysis of Visual Secret Sharing Schemes** submitted by **Mr. Sachin Kumar** to the Indian Institute of Technology Delhi, for the award of the Degree of Doctor of Philosophy, is a record of the original bonafide research work carried out by him under my supervision. The thesis has reached the standards fulfilling the requirements of the regulations relating to the degree. The results contained in this thesis have not been submitted in part or full to any other university or institute for the award of any degree or diploma.

New Delhi
July 2012

Prof. R. K. Sharma
Department of Mathematics
Indian Institute of Technology Delhi
New Delhi - 110016

Acknowledgements

This thesis would not have been possible without the guidance and the help of several individuals who in one way or another contributed and extended their valuable assistance in the preparation and completion of this study.

First and foremost, I would like to record my deepest gratitude to my thesis supervisor, Prof. R. K. Sharma, for his continuous support, unflinching encouragement, valuable suggestions, and his positive thinking during my candidature. He always allowed me to pursue my own research interests and motivated me in developing independent thinking and research skills. This thesis would not have been accomplished without his invaluable support.

I would like to extend my sincere thank to my SRC (Student Research Committee) members: Prof. S. K. Gupta, Dr. S. Dharmaraja and Dr. Anuradha Sharma for their valuable time and guidance. I also extend my appreciation to Prof. B. S. Panda, Head of Department as well as all faculty members and staff of Department of Mathematics, IIT Delhi, for their co-operation and support. I am thankful to IIT Delhi authorities for providing me the necessary facilities and support to pursue my research work.

Words fail me to express my love and appreciation to my family for their unflagging support and encouragement throughout this journey. My parents, Balesh Devi and Ram Kumar deserve special mention for their inseparable support, prayers and sacrifices. No words can be ever enough to thank my wife Alka for her constant encouragement, understanding and endless patience. It would not have been possible to complete this work without her support, which has taken the load off my shoulder

and helped me to carry out my research work smoothly. The supportive attitude of my loveable son Atharva extended during this study is really heart rending as sometimes I could not able to finish his tiny demands. I also appreciate my sister Rishu, my brother-in-law Vineet and their children Ishika and Vidisha for their love and continued encouragement. I would also thank my in-laws family for their support and confidence in my ability to succeed.

Special thanks to my friends Sunil, Alok, Sweta, Bhavya, S. N. Shadangi, Laxmi, Amit, Aniruddha and others that I forgot to mention for their valuable friendship and endless support. I would also like to thank Dr. Mukesh Kumar, Dr. Parmod Kumar and Dr. Sunil Kumar for their constant encouragement and valuable suggestions.

Most importantly, I thank the almighty God for countless blessing, strength, and the resources to complete my academic pilgrimage.

New Delhi *Sachin Kumar*

Abstract

A secret sharing scheme permits a secret to be shared among participants in such a way that only qualified subsets of participants can reconstruct the secret, but any unqualified subset of participants has absolutely no information about the secret. Among the various secret sharing schemes, Visual Secret Sharing (VSS) schemes are developed to encrypt a secret visual information. Aside from the obvious applications to information sharing, VSS schemes can be applied to access control, copyright protection, digital watermarking and visual authentication. Hence, this subject has emerged as an important area of research and has been enthusiastically pursued by many researchers. The present thesis is devoted to *Design and Analysis of VSS Schemes* for better quality and performance.

We design and analyze two different classes of VSS schemes, namely based on random grids and Boolean operations. The first three schemes are based on random grids and last one is based on Boolean operations. In the random grids-based VSS, we first analyze the existing random grids-based non-threshold VSS schemes for improving the visual quality of the reconstructed image. The Boolean XOR operation is proposed as the decryption operation in the random grids-based non-threshold VSS schemes. The proposed operation does the lossless secret reconstruction for any number of participants and removes the problem of perfect alignment of the shares. Second, we design a non-threshold scheme for recursive hiding of the secret images by random grids, which hides the additional secret information in the shares

of larger secrets in a recursive manner. The proposed scheme increases the secret information conveyed per bit of the shares to nearly 100% without any pixel expansion and code book requirement. Next, we design a VSS scheme for general access structures by random grids. Compared to the existing VSS schemes for general access structures, the proposed scheme generates the shares of size same as that of the original image and does not require any code book prior to the encryption process. The superiority of the proposed scheme is shown by comparing it with the related works.

In Boolean operations-based VSS, we design a (k, n)-threshold VSS scheme based on Boolean operations. We propose two different algorithms to encrypt a secret image for (k, n)-threshold access structures. The advantages of the proposed scheme are that it has no pixel expansion and achieves the better visual quality of the reconstructed image compared to the random grids-based (k, n)-threshold VSS scheme.

The formal proofs, security analysis and experimental results are given to demonstrate the correctness and feasibility of all the proposed schemes.

Contents