Applications of Mathematics in Some Modern Cryptographic Schemes [Times New Roman=18]

Avishek Adhikari,
[Arial=12] Department of Pure Mathematics,
University of Calcutta
35 Ballygunge Circular Road,
Kolkata 700019, India
e-mail : amath@caluniv.ac.in / avishek.adh@gmail.com
website: ttp://www.imbic.org/avishek.html

Abstract **[Times New Roman=13]**

[Times New Roman=12, Page margin Left=right=1.5", Top=bottom=1"]
In the modern busy digital world, the word "cryptography" is well known to many of us. Every day, knowingly or unknowingly, in many places we do use different techniques of cryptography. Starting from the log-in into PC, sending e-mails, withdrawal of money from ATM using PIN code, operating the locker at the bank with the help of a designated person from the bank, sending message using mobile phone, buying things through internet using credit card, transferring money digitally from one account to another over internet, everywhere we are applying cryptography.

Keywords: linear algebra, pixel expansion, relative contrast, system of linear equations.
MSC 2010 Codes: 15A03, 94A60.

1 Introduction

In this paper we put forward an efficient construction, based on linear algebraic technique, of a t-(k,n)*-Visual Cryptographic Scheme (VCS) for monochrome images in which t participants are essential in a (k,n)-VCS. The scheme is efficient in the sense that it only requires solving a system of linear equations to construct the required initial basis matrices. To make the scheme more efficient, we apply the technique of deletion of common columns from the initial basis matrices to obtain the reduced basis matrices. However finding exact number of common columns in the initial basis matrices is a challenging problem. In this paper we deal with this problem. We first provide a construction and analysis of t-(k,n)*-VCS. We completely characterize the case of t-(n-1,n)*-VCS by finding a closed form of the exact number of common columns in the initial basis matrices and thereby deleting the common columns to get the exact value of the reduced pixel expansion and relative contrast of the efficient and simple scheme. Our proposed closed form for reduced pixel expansion of (n-1,n)-VCS matches with the

numerical values of the optimal pixel expansions for every possible values of n that exist in the literature. We further deal with the (n-2,n)-VCS and resolve an open issue by providing an efficient algorithm for grouping the system of linear equations and thereby show that our proposed algorithm works better than the existing scheme based on the linear algebraic technique. Finally we provide a bound for reduced pixel expansion

2 Conclusion and Open issues

In this paper we have put forward a construction and analysis, based on linear algebraic technique, of a t-(k,n)*-VCS for monochrome images in which t participants are essential in a (k,n)-VCS. We grouped the minimal qualified sets, taken two at a time, to form systems of linear equations solving which we constructed the initial basis matrices. We then, applied the technique of deleting the common columns occurring in the initial basis matrices to reduce the pixel expansion. We completely characterize the case of t-(n-1,n)*-VCS by deriving a closed form of the reduced pixel expansion and hence a closed form for the relative contrast too. We further investigated the case of an (n-2,n)-VCS and provided an algorithm to collect at least three minimal qualified sets at a time for grouping in such a way that the resulting
basis matrices, in their reduced forms, have almost optimal pixel expansions.
An interesting open issue would be to compute exact values of the reduced pixel expansions of any t-(n-2,n)*-VCS and more generally of any t-(k,n)*-VCS and derive a closed form for it.

3 Acknowledgement

We would like to thank the anonymous reviewers for their important and helpful comments. The author is partially supported by National Board for Higher Mathematics, Department of Atomic Energy, Government of India (No 2/48(10)/2013/NBHM(R.P.)/R\&D II/695). The third author is also thankful to the Centre of Excellence in Cryptology of Indian Statistical Institute.

References [Times New Roman=14]

[1] Times New Roman=12

[2] Avishek Adhikari, M. Bose, D. Kumar and Bimal Roy, *Applications of Partially Balanced and Balanced IncompleteBlock Designs in developing Visual Cryptographic Schemes,* IEICE TRANS. FUNDAMENTALS, Japan, Vol. E-90A, No. 5, pp. 949-951, May 2007.

[3] Avishek Adhikari, T. K. Dutta, and B Roy, *A New Black and White Visual Crypto-graphic Scheme for General Access Structures*, Recent Advances in Cryptology : In-docrypt 2004, Lecture Notes in Computer Science, Springer, 2004, 399-413.

[4] Avishek Adhikari, *DNA Secret Sharing*, IEEE World Congress on Evolutionary Com-putation 2006, CEC 2006, July 16-21, 1407-1411, 2006.