ON SECURITY OF TWO DIMENSIONAL DATA (IMAGE DATA & VIDEO DATA)

DEEP CHANDRA MISHRA

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY DELHI

JANUARY 2018

ON SECURITY OF TWO DIMENSIONAL DATA (IMAGE DATA & VIDEO DATA)

by

DEEP CHANDRA MISHRA

Department of Mathematics

Submitted

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

to the

Indian Institute of Technology Delhi

January 2018

Dedicated to Lord

Ganpati

Certificate

*This is to certify that the thesis entitled of "**On Security of Two Dimensional Data (Image Data & Video Data)**" being submitted by **Mr. Deep Chandra Mishra** to the Indian Institute of Technology Delhi for the award of the degree of **Doctor of Philosophy** is a record of bona fide research work carried out by him under my guidance and 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 elsewhere, either in part or full, for the award of any degree or diploma.

Dr. R. K. Sharma
Professor
Department of Mathematics
Indian Institute of Technology Delhi

Acknowledgements

Firstly, my sincere thanks to Lord Ganpati and Maa Saraswati for giving me the strength and unlimited mercies to complete this work.

I would like to express my sincere gratitude to my supervisor Dr. R. K. Sharma, Professor and former Head, Department of Mathematics, Indian Institute of Technology Delhi, for his overwhelming support and guidance during my candidature. He has always encouraged and given continuous support during the work of my thesis Inspite of his busy schedule. He allowed me wide freedom in my choice of research area and guided me to study the same. I am fortunate that Prof. Sharma introduced me to such an interesting and challenging topic for the thesis. I could not have imagined having a better advisor and mentor for my Ph.D study. I am thankful to God for providing me Prof. R. K. Sharma Sir as my supervisor.

I am grateful to Prof. S. Dharmaraja, Head, Department of Mathematics, IIT-Delhi, for providing me necessary facilities for the completion of this work. I would like to express my deep sense of gratitude to the SRC members, Dr. Aparna Mehra, Department of Mathematics, IIT-Delhi, Dr. Ritumoni Sarma, Department of Mathematics, IIT-Delhi and Prof. M. P. Gupta, Head, DMS, IIT-Delhi, for their encouragement and invaluable suggestions. I am also thankful for my research collaborator Prof. M. Hanmadlu, Department of Electrical Engineering, IIT-Delhi who helped me as a part of this research work. I express my gratitude to all the faculty members *of the Department of Mathematics, IIT-Delhi. I am also thankful to Prof. Kumkum Rautela, Principal, Govt. P. G. College Lansdowne, Uttarakhand, for supporting me to manage my job along with in thesis completion.*

I express my extreme indebtedness to my parents, brothers, and friends for the patience and encouragement shown by them during this period, to whom I dedicate this thesis.

Lastly, I would like to extend my gratitude to CSIR, New Delhi, Govt. of India, Under Grant No. F. No. 09/086(1068)/2010-EMR-I for providing financial support.

Deep Chandra Mishra

Abstract

In this world of internet which is full of eavesdropping, modification of private information, safety of information is a major concern. Secure and appropriate transmission of two dimensional digital data (Image Data and Video Data) over open networks is an important and valuable agenda for research work in the area of security. In this thesis, we have presented various approaches for the security system of color image data and video data for appropriate and secured transmission in the open network without any loss of information over the geometrical domain, co-ordinate domain and frequency domain. The existing techniques discuss the security of image data or video data on the basis of keys only (which provides only one layer of security for image data or video data) in the geometrical domain, co-ordinate domain or frequency domain, but in this thesis we have presented multi-layers of security for RGB image data and video data in all domains (geometrical, co-ordinate and frequency domains). In this thesis, keys and arrangement of parameters are imperative for the correct decryption process. If an attacker knows about all possible correct keys but is not aware of the correct arrangement of the used parameters of geometrical domain, co-ordinate domain and frequency domain then he/she cannot recover the original information (original RGB image data or video data) from the encrypted data or ciphered data. The robustness of the presented approaches, not only depends on the possible correct keys, but also depends on the correct arrangement of parameters.

Some chapters of the thesis provide security of image data and video data by the symmetric-key-cryptosystem, while some chapters provide security of data through public-key-cryptosystem. Thus, the work in this thesis focuses on the security of RGB image data and video data using:

(i) Symmetric-key-security system, and

(ii) Public-key-security system.

Experimental results and security analysis on the standard examples of the presented security system are given for the justification of the robustness of the proposed cryptosystems for RGB images and videos. These methods or algorithms will be of potential use in digital RGB image processing and for secured and appropriate transmission of two dimensional data like image data and video data from one end (Sender) to the other end (Receiver).

सार

इंटरनेट की इस दुनिया में जो छिपी हुई है, निजी जानकारी के रूपांतरण कथन, जानकारी की सुरक्षा एक प्रमुख चिंता का विषय है। खुले नेटवर्क पर दो आयामी डिजिटल डेटा (छवि डेटा और वीडियो डेटा) के सुरक्षित और उपयुक्त संचरण सुरक्षा के क्षेत्र में अनुसंधान कार्य के लिए एक महत्वपूर्ण और मूल्यवान एजेंडा है। इस थीसिस में, हमने विभिन्न तरीकों को प्रस्तुत किया है रंग छवि डेटा और वीडियो डेटा की सुरक्षा व्यवस्था को खुली नेटवर्क में उचित और सुरक्षित प्रसारण के लिए बिना किसी भी सूचना के नुकसान के ज्यामितीय डोमेन, समन्वय डोमेन और आवृत्ति डोमेन पर। मौजूदा तकनीक केवल चाबियाँ के आधार पर छवि डेटा या वीडियो डेटा की सुरक्षा पर चर्चा करते हैं (जो छवि डेटा या वीडियो डेटा के लिए सुरक्षा का केवल एक स्तर प्रदान करता है) ज्यामितीय डोमेन, समन्वय डोमेन या आवृत्ति डोमेन में, लेकिन इस थीसिस में हमने आरजीबी छवि डेटा और वीडियो डेटा के लिए सुरक्षा की बहु-परतें प्रस्तुत की हैं सभी डोमेन में (ज्यामितीय, समन्वय और आवृत्ति डोमेन में)। इस थीसिस में, सही डिक्रिप्शन प्रक्रिया के लिए चाबियाँ और पैरामीटर आवश्यक हैं। यदि कोई हमलावर सभी संभव सही कुंजी के बारे में जानता है लेकिन ज्यामितीय डोमेन के उपयोग किए गए पैरामीटर, समन्वय डोमेन और आवृत्ति डोमेन की सही व्यवस्था से अवगत नहीं है तो वह एन्क्रिप्टेड डेटा या साइफर्ड डेटा से मूल जानकारी (मूल आरजीबी छवि डेटा या वीडियो डेटा) को पुनर्प्राप्त नहीं कर सकता। प्रस्तुत दृष्टिकोणों की मजबूती, न केवल संभव सही कुंजी पर निर्भर करता है, बल्कि पैरामीटर की सही व्यवस्था पर भी निर्भर करता है। थीसिस के कुछ अध्याय छवि डेटा और वीडियो डेटा की सुरक्षा सममित-कुंजी-क्रिप्टो सिस्टम से प्रदान करते हैं, जबकि कुछ अध्याय सार्वजनिक कुंजी-क्रिप्टोसिस्टम के माध्यम से डेटा की सुरक्षा प्रदान करते हैं। इस प्रकार, इस थीसिस में कार्य केंद्रित है आरजीबी छवि डेटा और वीडियो डेटा की सुरक्षा का उपयोग करते हुए:

(i) सममित-कुंजी-सुरक्षा प्रणाली, और

(ii) सार्वजनिक-कुंजी-सुरक्षा प्रणाली।

मानक उदाहरणों पर प्रायोगिक परिणाम और सुरक्षा विश्लेषण प्रस्तुत सुरक्षा प्रणाली के आरजीबी छवियों और वीडियो के लिए प्रस्तावित क्रिप्टो तंत्रों की मजबूती के औचित्य कथन के लिए दिए गए हैं। संभवतः इन पद्धतियों या एल्गोरिदम का उपयोग डिजिटल आरजीबी इमेज प्रोसेसिंग में, छवि डेटा और वीडियो डेटा जैसे दो आयामी डेटा के सुरक्षित और उचित संचरण एक सिरे से (प्रेषक) दूसरे छोर (रिसीवर) तक के लिए होंगे।

Contents

List of Figures

List of Tables