DESIGN AND ANALYSIS OF IMAGE ENCRYPTION SCHEMES

AMIT ARORA

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY, DELHI
JUNE 2023

DESIGN AND ANALYSIS OF IMAGE ENCRYPTION SCHEMES

by

AMIT ARORA

Department of Mathematics

Submitted

in fulfillment of requirements of the degree of Doctor of Philosophy

to the

Indian Institute of Technology Delhi
June 2023

Dedicated to
Almighty and My Family

Certificate

This is to certify that the thesis entitled **"Design and Analysis of Image Encryption Schemes"** submitted by **"Mr. Amit Arora"** 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 and guidance. 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.

Dr. R. K. Sharma
Professor
Department of Mathematics
Indian Institute of Technology Delhi
New Delhi, 110016

New Delhi
June 2023

Acknowledgments

Lifelong learning is a challenge. As a society, we value knowledge and recognize intellectual development as a key to sustainability. This thesis embodies the quest for knowledge made possible by the support of an academic community of dedicated educators. Reaching major milestones in one's life does not happen without the assistance of great many people, and for each one of them I am truly blessed and grateful.

First and foremost, I would like to thank almighty God, late B K Laxman and B K Sundari for giving me strength, ability and opportunity to undertake this research work and complete it successfully.

I would like to express my deepest gratitude to my supervisor, Prof. R. K. Sharma, for his endless encouragement, valuable suggestions, good understanding and above all for his friendly behavior. Dr. Sharma always gave me the freedom to pursue my own interests and provided me with insightful suggestions and support in developing independent thinking and research skills. He has been an exceptional mentor and I appreciate both our professional and personal conversations over the years. The knowledge and wisdom I have gained from him will forever guide me in education and in life.

I would like to give special thanks to my SRC (Student Research Com-

mittee) members Prof. Amit Priyadarshi, Prof. Ritumoni Sarma, and Prof. Arun Kumar Varshney for their valuable time, suggestions, cooperation and support during all the time of my research work. I am greatly indebted to IIT Delhi authorities and all faculty members of Department of Mathematics for their cooperation, support, and providing me the necessary facilities.

I appreciate all my seniors for making me comfortable in the department and motivating in the initial days of my research. I would like to give my heartily thanks to my friends, Dr. Sachin Kumar, Dr. Arun Kumar, Dr. Gaurav Bhatnagar and S N Shadangi for their unconditional love and support. A discussion with them always seems like a discussion with my elder brothers. I am highly thankful to my colleagues and friends, Sandeep, Hariom, Soniya, Pooja, Neha, Abhinay, Divay, Sachin, Gyanendra, Praveen and Astha for encouraging me and creating joyful environment in this duration. I am highly indebted to Sandeep, Hariom and Sachin for their support whenever I approached them for the same. It appears almost impossible to thank each one of my friends here individually, but I would like them to know that the happy memories of my friendship with them always remains in the deepest corner of my heart.

Words cannot completely express my love and gratitude to my family who have supported and encouraged me through this journey. I would like to thank my parents, Krishna and Suresh Arora for their life-long support, love, and sacrifices, which sustained my interest in research and motivated me towards the successful completion of this study. No words can be ever enough to thank my wife Neha 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 lovable daugh-

ter Nishka extended during this study is really heart rending as sometimes I could not able to complete her tiny demands. I thanks to my brother Sunny, sister-in-law Deepti, Sisters Seema and Ashu, brother-in-laws Ravi and Gulshan and their children Bhumika, Shivam, Akshat, Sanu, Sparsh and Shubh for their love and continued encouragement. I would also thank my in-laws family for their support and confidence in my ability to succeed.

New Delhi *Amit Arora*

June 2023

Abstract

In the last few years, multimedia and network technology has grown up very rapidly. Due to this development the transfer of multimedia data, such as images, audio and video over the networks, has been increased. Some multimedia data especially related to military, medical, banking, and other critical sectors is required to be protected from access by unauthorized users. To achieve the security of data over the networks, cryptography and steganography is widely used. In steganography, data is concealed in a cover medium such as image, audio, or video. Many methods have been developed for hiding the data and work in different domains such as compression, spatial, transform and encryption [31, 32]. In cryptography, plain data is converted into unintelligible data by some method and vice-versa. Many methods have been developed to protect the data in cryptography. For example:- Advanced Encryption Standard (AES), International Data Encryption Algorithm (IDEA), Rivest Cipher (RC5), and Blowfish algorithm etc. These algorithms are not appropriate for image data encryption as image data has some inherent features such as large size, the correlation among neighboring pixels, and high redundancy etc. Therefore, various encryption schemes have been developed specifically to encrypt the images in the last decade. These schemes are based

on different design techniques and primitives with an edge over the other as per the requirement of their applications. Hence, this area has emerged as an important field of research and has been enthusiastically pursued by many researchers.

In this thesis, we have analysed some of the recently published Image Encryption (IE) schemes. In addition, we have modified these schemes in such a manner that they resist existing attacks and maintain the merits of the original schemes.

In 2019, Deb et al. [15] proposed an IE scheme based on the Logistic map, Arnold transformation, and word-oriented feedback shift register (wfsr). As per the scheme, firstly plain image is randomized and scrambled with the help of a Logistic map and Arnold transformation. Then, the pixels of an intermediate image are bit-wise XORed with output of the wfsr to obtain the cipher image. Designers claim that the scheme is secure against brute force and other existing cryptanalytical attacks. We have applied Chosen Plaintext Attack (CPA) on this scheme and found that the scheme is not secure against CPA. In addition, we have modified the original scheme in such a way that it resists CPA and maintains the qualities of the original scheme.

In 2018, Essaid et al. [21] improved the randomness of the Skew Tent Map (STM) and proposed a new IE scheme based on this Enhanced Skew Tent Map (ESTM). The authors claim that their scheme is secure against brute force and all the known attacks. We have analysed their scheme and found that this scheme is not secure against Known Plaintext Attack (KPA). We have cryptanalysed this scheme with the help of only one known plain-cipher image pair. The plain image is recovered from the cipher image successfully in real-time. In addition, we have modified the original scheme so that it is

secure against KPA. The modified scheme also maintains the qualities of the original scheme.

In 2021, Khalil et al. [33] proposed an IE scheme that uses 2D sine-cosine cross chaotic map for scramble the image as a confusion phase. For diffusion phase, designers use a 1D Logistic-Tent chaotic map to generate a chaotic self-diffusion matrix that is bit-wise XORed with the scrambled image to produce the final cipher image. Authors claim that the proposed algorithm combines the merits of both 1D and 2D chaotic maps and the algorithm has a promising security performance and has a high ability to resist statistical and differential attacks. We have analysed the proposed scheme and found that the scheme is vulnerable against CPA. We have cryptanalysed this scheme with the help of only one chosen and five known plain-cipher image pairs in real-time. Further, we have found the cause of vulnerability and refined the scheme in such a manner that it resists CPA, and also maintains the merits of original scheme.

सार

पिछले कुछ सालों में मल्टीमीडिया और नेटवर्क टेक्नोलॉजी का काफी तेज़ी से विकास हुआ है। इस विकास के कारण मल्टीमीडिया डेटा जैसे इमेजेज, ऑडियो और वीडियो का नेटवर्क पर स्थानांतरण बढ़ गया है। कुछ मल्टीमीडिया डेटा को, जोकि विशेष रूप से सैन्य, चिकित्सा, बैंकिंग और अन्य महत्वपूर्ण क्षेत्रों से संबंधित है, अनाधिकृत उपयोगकर्ताओं द्वारा प्रयोग करने से रोकने की आवश्यकता है। नेटवर्क पर डाटा की सुरक्षा के लिए मुख्य रूप से क्रिप्टोग्राफ़ी और स्टेग्नोग्राफी का उपयोग किया जाता है। स्टेग्नोग्राफ़ी में, डेटा को एक आवरण माध्यम में छुपाया जाता है जैसे इमेज, ऑडियो या वीडियो। छिपाने के लिए कई तरीके विकसित किए गए हैं जो विभिन्न कार्यक्षेत्रों में कार्य करते हैं जैसे कम्प्रेशन, स्पाटिअल, ट्रांसफॉर्म और एन्क्रिप्शन [३१, ३२]। क्रिप्टोग्राफी में, किसी विधि द्वारा प्लेन डेटा को साइफर डेटा में परिवर्तित किया जाता है और इसके विपरीत साइफर डेटा को प्लेन डेटा में परिवर्तित किया जाता है। क्रिप्टोग्राफी में डेटा की सुरक्षा के लिए कई तरीको को विकसित किया गया है। उदाहरण के लिए:- एडवांस एन्क्रिप्शन स्टैण्डर्ड (ए.ई.एस.), इंटरनेशनल डेटा एन्क्रिप्शन एल्गोरिथम (आई.डी.ई.ए.), रिवेस्ट साइफर (आर.सी.)-5, और ब्लोफिश एल्गोरिथम आदि। ये एल्गोरिदम इमेज डेटा एन्क्रिप्शन के लिए उपयुक्त नहीं हैं क्योंकि इमेज डेटा में कुछ अंतर्निहित विशेषताएं हैं- जैसे बड़ा आकार, पड़ोसी पिक्सेल के बीच संबंध और उच्च रीडनडेंसी आदि। इसलिए पिछले दशक में विशेष रूप से इमेजेज को एन्क्रिप्ट करने के लिए विभिन्न एन्क्रिप्शन योजनाएं विकसित की गई हैं। ये योजनाएं अलग-अलग डिजाइन तकनीकों और क्रिप्टोग्राफिक प्रिमीटिव्स पर आधारित हैं जो उनके उपयोग की आवश्यकता के अनुसार दूसरी योजनाओ से बेहतर डिज़ाइन की गयी है। इसलिए यह क्षेत्र अनुसंधान के एक महत्वपूर्ण क्षेत्र के रूप में उभरा है और कई शोधकर्ताओं द्वारा उत्साहपूर्वक इसका अनुसरण किया गया है ।

इस थीसिस में हमने हाल ही में प्रकाशित कुछ इमेज एन्क्रिप्शन (आई.ई.) योजनाओ का विश्लेषण किया है। इसके अलावा हमने इन योजनाओं को इस तरह संशोधित किया है कि वे मौजूदा हमलों का विरोध करती हैं और मूल योजनाओ के गुणों को भी बनाये रखती हैं।

सन २०१९ में, देब. एट. अल. [१५] ने लॉजिस्टिक मैप, अर्नोल्ड ट्रांसफॉर्मेशन, और वर्ड-बेस्ड फीडबैक शिफ्ट रजिस्टर (डब्ल्यू.एफ़.एस.आर.) के आधार पर आई.ई. योजना प्रस्तावित की। योजना के अनुसार, सबसे पहले प्लेन इमेज को लॉजिस्टिक मैप और अर्नोल्ड ट्रांसफॉर्मेशन की मदद से रेनडमाइज़ड और स्क्रैम्बल किया जाता है। फिर साइफर इमेज प्राप्त करने के लिए मध्यवर्ती इमेज को डब्ल्यू.एफ़.एस.आर. के आउटपुट के साथ बिट-वाइज एक्स.औ.आर. किया जाता है। डिजाइनरों का दावा है कि यह योजना ब्रूटफोर्स और अन्य मौजूदा क्रिप्टैनालिटिकल हमले के खिलाफ सुरक्षित है। हमने इस योजना पर चूजन प्लेनटेक्स्ट अटैक (सी.पी.ए.) लगाया

और पाया कि यह योजना सी.पी.ए के खिलाफ सुरक्षित नहीं है। इसके अलावा हमने मूल योजना में इस तरह से संशोधन किया है कि यह सी.पी.ए. का विरोध करती है और मूल योजना के गुणों को बनाए रखती है।

सन २०१८ में, एस्सैड. एट. अल. [२१] ने स्कीउ टेंट मैप (एस.टी.एम.) की रेनडमनेस में सुधार किया और इस उन्नत स्कीउ टेंट मैप (ई.एस.टी.एम.) के आधार पर एक नई आई.ई. योजना प्रस्तावित की। लेखकों का दावा है कि उनकी योजना ब्रूटफोर्स और सभी ज्ञात हमलो के विरुद्ध सुरक्षित है। हमने उनकी योजना का विश्लेषण किया और पाया कि ज्ञात प्लेनटेक्स्ट अटैक (के.पी.ए.) के खिलाफ यह योजना सुरक्षित नहीं है। हमने केवल एक ज्ञात प्लेन-साइफर इमेज की जोड़ी की सहायता से इस योजना का क्रिप्टविश्लेषण किया है और साइफर इमेज से प्लेन इमेज वास्तविक समय में सफलतापूर्वक पुनर्प्राप्त की है। इसके अलावा हमने मूल योजना को संशोधित भी किया है ताकि यह के.पी.ए. के खिलाफ सुरक्षित हो। संशोधित योजना मूल योजना के गुणों भी को बनाए रखती है।

सन २०२१ में, खलील. एट. अल. [३३] ने एक आई.ई. योजना प्रस्तावित की जो कनफ्उसन चरण में इमेज को स्क्रैम्बल करने के लिए २-डी साइन-कोसाइन क्रॉस कयोटिक मैप का उपयोग करती है। डिफ्उसन चरण में, डिजाइनर कयोटिक सेल्फ-डिफ्उसन मैट्रिक्स उत्पन्न करने के लिए १-डी लॉजिस्टिक-टेंट कयोटिक मैप का उपयोग करते हैं जो कि साइफर इमेज प्राप्त करने के लिए स्क्रैम्बल इमेज के साथ बिट-वाइज़ एक्स.औ.आर. की जाती है। लेखकों का दावा है कि प्रस्तावित एल्गोरिथम १-डी और २-डी दोनों कयोटिक मैप्स की खूबियों को जोड़ता है और एल्गोरिथ्म में एक होनहार सुरक्षा प्रदर्शन और स्टैटिस्टिकल एंड डिफ़्फेरनेटियल हमलो का विरोध करने के लिए एक उच्च क्षमता है। हमने प्रस्तावित योजना का विश्लेषण किया है और पाया है यह योजना सी.पी.ए. के प्रति संवेदनशील है। हमने इस स्कीम का केवल एक चुने हुए और पांच ज्ञात प्लेन-साइफर इमेज जोड़ो की मदद से वास्तविक समय में क्रिप्टएनालिसिस किया है। इसके अलावा, हमने भेद्यता का कारण ढूंढा है और इस योजना को इस तरह से परिष्कृत किया है कि यह सी.पी.ए. का प्रतिरोध करती है, और मूल योजना के गुणों को भी बनाए रखती है।

Contents

List of Figures

List of Tables

List of Symbols

Symbol	**Meaning**
$\mathbb{N}$	the set of natural numbers
$=$	is equal to
$\neq$	is not equal to
$<$	less than
$>$	greater than
$\leq$	less than or equal to
$\geq$	greater than or equal to
$\lll$	left circular shift
$\lfloor x \rfloor$	greatest integer less than or equal to x
$\cup$	set union
$\oplus$	bitwise XOR
$\forall\ x$	for all x
$\circ$	composition of functions
$x \in X$	x belongs to X
$x \notin X$	x does not belong to X
F_2	finite field with elements 0 and 1

F_{2^m}	extension field of F_2 with 2^m elements
$F_{2^m}^n$	vector space over the field F_{2^m} whose elements are n-tuples
I_m	identity matrix of size $m \times m$ over F_2
$M_m(F_2)$	ring of all metrics of size $m \times m$ with entries in F_2
$M_m(F_2)[x]$	ring of polynomial in x with coefficient in $M_m(F_2)$
$0x$	prefix to indicate hexadecimal