BIOMETRICS BASED CRYPTOSYSTEM

ASHOK KUMAR BHATEJA

DEPARTMENT OF ELECTRICAL ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY DELHI, INDIA

OCTOBER 2017

BIOMETRICS BASED CRYPTOSYSTEM

by

ASHOK KUMAR BHATEJA

DEPARTMENT OF ELECTRICAL ENGINEERING

Submitted

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

to the

INDIAN INSTITUTE OF TECHNOLOGY DELHI, INDIA

OCTOBER 2017

CERTIFICATE

This is to certify that the thesis titled "**Biometrics based Cryptosystem**" being submitted by **Ashok Kumar Bhateja** to the Department of Electrical Engineering, 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 our guidance and supervision. In our opinion, 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 to any other university or institute for the award of any degree or diploma.

Prof. Santanu Chaudhury
Department of Electrical Engineering
Indian Institute of Technology Delhi
New Delhi – 110016
&
Director CEERI
Pilani, India

Dr. P.K. Saxena
Scientific Consultant
O/o the Principal Scientific Advisor
to Govt. of India, New Delhi
&
Former Director, SAG
Defence R & D Organization
Metcalfe House, Delhi 110054

To my family

ACKNOWLEDGEMENT

I express hearty thanks and a deep sense of gratitude to Professor Santanu Chaudhury, who gave me an opportunity to undertake this research work. His faith in me is the main thrust behind all the motivation which didn't let me deter. Without his constant guidance, encouragement and creative approach to problem solving this work would not have reached completion.

It's my greatest pleasure to mention the name of Dr. P. K. Saxena whose analytical perceptions molded me towards critical thinking. His blessings, endeavors and technical as well as official support helped me to complete this project.

I am also thankful to Dr. G. Athithan, Distinguished Scientist & Director General (Med and CoS), DRDO Delhi, for providing his valuable comments and suggestions to improve the quality of the work.

Finally, I would like to express my gratitude towards my family members for their love, support and encouragement in all my endeavours.

It would be unfair if I do not appreciate unknown reviewers of my research work who accepted my papers for publication in repudiated journals and conferences.

Ashok Kumar Bhateja

Abstract

In modern communication world, the transmission is secured mainly by transforming the contents of the message to an unintelligible form, using some mathematical transformations, before transmitting it. For securing the contents, a cryptographic algorithm is used which binds the ‘plaintext’ with a ‘Key’ to generate the cipher-text in such a manner that access to cipher-text alone does not lead to recovery of the ‘key’ or the ‘plaintext’ easily using any amount of computational resources. Classical cryptosystems such as Vigenere cipher are not useful for high level of secrecy requirements as some cryptanalytic attacks are feasible in real time. Some evolutionary techniques such as Genetic Algorithm (GA), Particle Swarm Optimization (PSO) etc. are useful in analyzing various classical ciphers. Analysis of Vigenere ciphers using Cuckoo Search is proposed and it is observed that it performs much better as compared to GA and PSO based analysis.

Present day crypto systems are based on more complex crypto primitives having a very large key space. As the secrecy of the ciphers lies mainly in the ‘keys’, maintenance of confidentiality of keys, which need to be exchanged between communicating parties, remains one of the major problems of secure

communication. The keys cannot be remembered because these are large in size and are mostly random. To overcome the difficulties of securing the cryptographic keys, biometrics such as fingerprint, iris patterns, online signatures etc. could be used as these are unique, difficult to guess, cannot be stolen and are more reliable for identification of legitimate person.

Biometric based cryptosystems like fuzzy vault binds the secret (may be key of a cryptosystem) with the biometric templates. In comparison with other biometrics like fingerprint, iris etc. the variability in online signatures is very high therefore fuzzy vault kind of scheme has high false rejection rate. Also, sufficient number of zero crossing or high curvature points may not be available in all kinds of signatures. To overcome these problems a novel scheme for securing a secret or key using online signature of a person has been designed. Weighted back propagation algorithm is developed for training binary classifiers using the features which are consistent in genuine signature and inconsistent in forged signature. AdaBoost algorithm is used to increase the performance of the system. The classifier helps to find the genuine points in the vault for unlocking and extracting the secret. This scheme is highly robust i.e. it works well for all kinds of signatures and it does not depend on the number of zero crossing and high curvature points in the signature.

Fingerprint, iris and online signature biometrics are analysed for extraction of consistent features. A scheme for finding reference point (core point) of fingerprint by maximizing the global gradient matrix of orthogonal matrices of orientation fields and a test function in order to choose a stable reference point is proposed. An efficient and robust iris recognition model based on sparse representation using compressive sensing and *k*-nearest subspace (segments) has been developed.

In fuzzy vault the actual biometric features are also stored in the vault and these points are disguised in a large set of chaff points. The presence of actual biometric features makes the vault vulnerable and the large number of chaff points requires huge storage. A novel scheme of highly secure biometric based cryptosystem which does not require any extra storage (for chaff points) is proposed. The scheme is tested for fingerprint using minutiae point as biometric templates and online signature using high curvature, crossings, and end points as biometric templates.

In biometric cryptosystems, using single biometric as key, the security can be breached if the biometrics of the user gets compromised. To mitigate this threat a biometric cryptosystem which uses more than one biometric trait is used. A scheme for bi-modal biometric based cryptosystem has been proposed

which offer more security over the biometric cryptosystems using single biometric.

Safe Deposit Boxes are used mostly in Banks/Post offices for safe custody of valuable items where two keys namely user key and the master key are used. The user key is required to lock the locker, whereas user key as well as master key is required to unlock it. We have adopted this concept in making an attempt to apply cryptographic techniques and proposing a Safe Deposit Box System which can be used for safely storing secret cryptographic keys of any crypto system or any secret data for that matter. It uses public key cryptographic techniques where locking and unlocking of the Safe Deposit Box can be done in a manner as is being done in the normal Safe Deposit Boxes of Banks, under multiple authority, but using soft keys extracted through biometrics rather than physical keys. As we have used a new biometric based encryption scheme developed, the need to remember or store keys of such Safe Deposit Box System as proposed is avoided.

सार

आधुनिक संचार दुनिया में, प्रसारण मुख्य रूप से संदेश की सामग्री को एक अपरिवर्तनीय रूप में बदलकर, कुछ गणितीय परिवर्तनों का उपयोग करके, उसे ट्रांसमिट करने से पहले सुरक्षित होता है। सामग्री को हासिल करने के लिए, एक क्रिप्टोग्राफ़िक एल्गोरिथ्म का उपयोग किया जाता है जो 'सादा पाठ' को 'कुंजी' के साथ जोड़ता है ताकि सिफर-टेक्स्ट को इस प्रकार बनाया जा सके कि केवल सिफर-पाठ का उपयोग ही 'कुंजी' या 'सादा पाठ' आसानी से किसी भी मात्रा में कम्प्यूटेशनल संसाधनों का उपयोग कर वसूली का कारण न हो। शास्त्रीय क्रिप्टोसिस्टम्स जैसे कि विगीनेर सिफर उच्च स्तर की गोपनीयता आवश्यकताओं के लिए उपयोगी नहीं हैं क्योंकि वास्तविक समय में कुछ क्रिप्टान्टिकल हमलों संभव हैं। कुछ विकासवादी तकनीकों जैसे कि आनुवंशिक एल्गोरिथ्म (जीए), कण झुंड अनुकूलन (पीएसओ) आदि विभिन्न शास्त्रीय सिफरों के विश्लेषण में उपयोगी हैं कोकीन खोज का उपयोग करते हुए वीजेनेर सिफर का विश्लेषण प्रस्तावित है और यह पाया जाता है कि यह जी ए और पी एस ओ आधारित विश्लेषण की तुलना में बेहतर प्रदर्शन करता है।

वर्तमान में क्रिप्टो सिस्टम अधिक जटिल क्रिप्टो प्राइमिटिवों पर आधारित होते हैं जिनमें कुंजी-जगह बहुत बड़ी होती है। चूंकि सिफर की गोपनीयता मुख्य रूप से 'चाबियाँ' में होती है, जो कि चाबियों की गोपनीयता का रखरखाव करती है, जो संचार दलों के बीच आदान-प्रदान करने की आवश्यकता होती है, यह सुरक्षित संचार की प्रमुख समस्याओं में से एक है। चाबियाँ याद नहीं की जा सकतीं क्योंकि ये बड़े आकार में हैं और अधिकतर यादृच्छिक हैं। क्रिप्टोग्राफिक कुंजियों को हासिल करने की कठिनाइयों को दूर करने के लिए, फिंगरप्रिंट, आईरिस पैटर्न, ऑनलाइन हस्ताक्षर आदि जैसी बॉयोमीट्रिक्स का इस्तेमाल किया जा सकता है क्योंकि यह अद्वितीय, अनुमान लगाने में मुश्किल है, चोरी नहीं की जा सकती है और वैध व्यक्ति की पहचान के लिए अधिक विश्वसनीय हैं।

बायोमेट्रिक आधारित क्रिप्टोसिस्टम्स जैसे फ़ज़ी वॉल्ट बायोमेट्रिक टेम्पलेट्स के साथ गुप्त (एक क्रिप्टोसिस्टम की कुंजी हो सकती है) को बांधता है। फिंगरप्रिंट, आईरिस आदि जैसी अन्य बॉयोमीट्रिक्स की तुलना में ऑनलाइन हस्ताक्षर में परिवर्तनशीलता बहुत अधिक है इसलिए फजी वॉल्ट प्रकार की योजना में उच्च झूठी अस्वीकृति दर है साथ ही, सभी तरह के हस्ताक्षरों में पर्याप्त संख्या में शून्य पार या उच्च वक्रता अंक उपलब्ध नहीं हो सकते हैं। इन समस्याओं पर काबू पाने के लिए किसी व्यक्ति के ऑनलाइन हस्ताक्षर का प्रयोग करके गुप्त या कुंजी हासिल करने के लिए एक उपन्यास योजना तैयार की गई है। वेटेड बैक प्रचार एल्गोरिथम को उन सुविधाओं का उपयोग करने वाले द्विआधारी

क्लासिफायरियर को प्रशिक्षण देने के लिए विकसित किया गया है जो वास्तविक हस्ताक्षर में संगत हैं और नकली हस्ताक्षर में असंगत हैं। AdaBoost एल्गोरिथ्म का उपयोग प्रणाली के प्रदर्शन को बढ़ाने के लिए किया जाता है। क्लासिफायरियर गुप्त को अनलॉक करने और निकालने के लिए वॉल्ट में वास्तविक अंक ढूंढने में मदद करता है। यह योजना बेहद मजबूत है क्योंकि यह सभी प्रकार के हस्ताक्षरों के लिए अच्छी तरह से काम करती है और यह हस्ताक्षर में शून्य पार और उच्च वक्रता अंक की संख्या पर निर्भर नहीं करती है।

सुसंगत सुविधाओं के निष्कर्षण के लिए फ़िंगरप्रिंट, आईरिस और ऑनलाइन हस्ताक्षर बॉयोमेट्रिक्स का विश्लेषण किया गया है एक स्थिर संदर्भ बिंदु चुनने के लिए अभिविन्यास क्षेत्रों के ऑर्थोगोनल मैट्रिक्स के वैश्विक ढाल मैट्रिक्स को अधिकतम करके और फिंगरप्रिंट के संदर्भ बिंदु (कोर बिंदु) को खोजने के लिए एक योजना प्रस्तावित है। कॉम्प्रेक्टिव सेंसिंग और कश्मीर के निकटतम सबस्पेस (सेगमेंट) का इस्तेमाल करते हुए विरल प्रतिनिधित्व के आधार पर एक कुशल और मजबूत आईरिस मान्यता मॉडल विकसित किया गया है।

फजी वॉल्ट में वास्तविक बायोमेट्रिक फीचर्स को भी वॉल्ट में जमा किया जाता है और इन बिंदुओं को बड़े पैमाने के ठिकानों में प्रच्छन्न किया जाता है। वास्तविक बायोमेट्रिक सुविधाओं की मौजूदगी से झंडा कमजोर पड़ता है और बड़ी संख्या में भुख़्त अंक के लिए विशाल भंडारण की आवश्यकता होती है। उच्च सुरक्षित बायोमेट्रिक

आधारित क्रिप्टो तंत्र की एक उपन्यास योजना जिसे किसी अतिरिक्त भंडारण की आवश्यकता नहीं है (चफ बिंदुओं के लिए) प्रस्तावित है। बायोमेट्रिक टेम्पलेट्स के रूप में मिनिटियाई पॉइंट का उपयोग करके फिंगरप्रिंट के लिए स्कीम का परीक्षण किया गया है और बायोमेट्रिक टेम्पलेट्स के रूप में उच्च वक्रता, क्रॉसिंग और एंड प्वाइंट का उपयोग करके ऑनलाइन हस्ताक्षर।

बॉयोमीट्रिक क्रिप्टोसिस्टम्स में, कुंजी के रूप में एकल बॉयोमीट्रिक का उपयोग करते हुए, सुरक्षा का उल्लंघन किया जा सकता है अगर उपयोगकर्ता के बायोमेट्रिक्स से समझौता हो जाता है। इस खतरे को कम करने के लिए एक बायोमेट्रिक क्रिप्टोसिस्टम जो एक से अधिक बॉयोमीट्रिक विशेषता का उपयोग करता है का उपयोग किया जाता है। द्वि-मोडल बायोमेट्रिक आधारित क्रिप्टोसिस्टम के लिए एक योजना प्रस्तावित की गई है जो एकल बॉयोमीट्रिक का उपयोग करके बायोमेट्रिक क्रिप्टोसिस्टिम पर अधिक सुरक्षा प्रदान करती है।

सुरक्षित जमा बक्से का उपयोग बहुमूल्य वस्तुओं की सुरक्षित हिरासत में बैंकों / डाकघरों में किया जाता है जहां दो चाबियाँ हैं जिनमें उपयोगकर्ता कुंजी और मास्टर कुंजी का उपयोग किया जाता है। लॉकर लॉक करने के लिए उपयोगकर्ता कुंजी की आवश्यकता होती है, जबकि उपयोगकर्ता कुंजी के साथ-साथ मास्टर कुंजी को इसे अनलॉक करने के लिए आवश्यक है। हमने क्रिप्टोग्राफिक तकनीकों को लागू करने और

एक सुरक्षित जमा बॉक्स सिस्टम का प्रस्ताव देने का प्रयास करने में इस अवधारणा को अपनाया है, जिसका उपयोग किसी भी क्रिप्टो सिस्टम के गुप्त क्रिप्टोग्राफिक कुंजियों या उस बात के लिए किसी गुप्त डेटा के सुरक्षित भंडारण के लिए किया जा सकता है। यह सार्वजनिक कुंजी क्रिप्टोग्राफिक तकनीकों का उपयोग करता है जहां सेफ डिपॉजिट बॉक्स के लॉकिंग और अनलॉक करना एक तरीके से किया जा सकता है जैसा कि बैंकों के सामान्य सेफ डिपॉजिट बॉक्स में किया जा रहा है, कई प्राधिकरणों के तहत, लेकिन भौतिक कुंजियों के बजाय बॉयोमेट्रिक्स के माध्यम से निकाले गए सॉफ्ट कीट का उपयोग करते हुए। जैसा कि हमने एक नया बायोमेट्रिक आधारित एन्क्रिप्शन योजना विकसित की है, प्रस्तावित के रूप में ऐसे सुरक्षित जमा बॉक्स सिस्टम की कुंजी याद रखने या संग्रहीत करने की आवश्यकता है।

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES