# MUHAMMAD USAMA

R-458 Rafi Bungalows Malir City Karachi
**Email:** Usama.khanzada@hotmail.com
**Cell#** (+92-321) 230-0205

## Education

**Bahria Institute of Management and Computer Science (BIMCS)**
Karachi, Pakistan www.bimcs.edu.pk

**Degree:** MS Software Engineering
**CGPA**: 3.45
**Thesis Topic:** "Classical and Chaotic Encryption Techniques for the Security of Satellite Images."[1]

**Bahria Institute of Management and Computer Science (BIMCS)**
Karachi, Pakistan www.bimcs.edu.pk

**Degree:** BS Software Engineering
**CGPA:** 3.57
**Final Year Project:** "Interactive Parallel Visualization of Protein Analysis using Cluster of Workstations (IPVPAC)."[1]

## Professional Experience

**Prince Muqrin Chair (PMC) for IT Security**
**King Saud University, Riyadh, Kingdom Saudi Arabia**

**Position Held:** Researcher

**Duration:** Feb 2010 to till date

**About KSU:** King Saud University, the premier institution of higher education in the Kingdom of Saudi Arabia, was established in 1957 to enhance the nation's growth and well-being. Through strong government support and many highly-qualified professionals and administrators, KSU has supplied the Saudi people and market with years of invaluable service, and served as a traditional source of skilled professionals and academics needed to meet the nation's growing needs in the areas of medicine, engineering, agriculture, science and development, the humanities and language.

**Responsibilities:**
- Identify research questions and gaps in literature.
- Develop research design, procedures, seek funding and implement the procedures.
- The management and conduct of the project.
- The proper allocation of research funds and sound financial management.
- Human resource management including the supervision of employees and students.
- Conducting research in collaboration with students and other research colleagues.
- Ensuring a safe working environment.

[1] Please Refer Annexure – 1 for details of each paper.

- Ensuring compliance with the University's policies and procedures governing the management and conduct of research.
- Ensuring compliance with the terms and conditions governing the grant.
- Disseminate in peer-reviewed scholarly journal
- Promotion and tenure are largely dependent upon publishing in top notch scholarly journals.

**Major Work:**
- Project based research and development of satellite image encryption system.
- Refinement and Implementation of the Essential Information Security Controls of ISO 27001.
- Research and development Identity-based Signature and Authentication techniques.

**PAKISTAN SPACE & UPPER ATMOSPHERE RESEARCH COMMISSION (SUPARCO)** (www.suparco.gov.pk)

**Position Held:** Assistant Manager (RS & GIS)

**Duration:** July 2007 to Feb 2010

**About SUPARCO:** SUPARCO is the National Space Agency of Pakistan. The division in which I am currently working is Remote Sensing (RS) and Geographical Information System (GIS) Division. RS & GIS Division's major involvement involve in Satellite Remote Sensing, Image Processing & GIS Based Solution Development for various National & International companies. It has a history of almost 3 decades working in these fields.

**Responsibilities:**
My responsibilities at SUPARCO mainly includes:

**Management:** My primary role and responsibility is to assist the top management in all management duties such as sales & marketing, coordination, billing, procurement, employees training, deliver presentations and manage business partner through various technologies e.g. remote Sensing, GIS, satellite imagery, GPS, Satellite & GSM Communications.

**Software Engineering and Technical:**
1. Manage Software lifecycle development.
2. Designing, coding and debugging applications.
3. Software analysis, code analysis, requirements analysis, software review, identification of code metrics, system risk analysis, software reliability analysis
4. Software modeling, simulation and front-end GUI design.
5. Software testing and quality assurance.
6. Performance tuning, improvement, balancing, usability, automation.
7. Support, maintain and document software functionality.
8. Integrate software with existing systems.
9. Evaluate and identify new technologies for implementation.

**Major Projects:**
- Development of J2ME based Navigation & Tracking System.
- Establishment and development of SUPARCO online catalog system for Satellite Imagery.
- Establishment of Water Management Spatial Database System for Monitoring of

Watercourse Improvement. Work in the Punjab and NWFP provinces for National Program on Improvement of Watercourses (NPIW), Pakistan. [2]

- Development of GPS/GIS Based Fleet Management & Vehicle Tracking System for Geo-Informatics, Sri Lanka, MegaTech, Pakistan, K&N's food limited, Pakistan and Punjab Highway Patrol Posts (PHPP), Pakistan. [2]
- Development of Thematic analysis reporting software & PDA based software system K&N's food limited, Pakistan. [2]

**COMPASS PARTNERS CONSULTANTS IN PROCESS EXCELLENCE (SIGMAFLOW) Pakistan (http://www.sigmaflow.com)**

**Position Held:** Software Engineer

**Duration:** July 2006 to July 2007

**About SigmaFlow:** SigmaFlow was founded in 2001 to develop the premier software solution for Six Sigma, Process Management and other initiatives. SigmaFlow provides enterprise and desktop level software solutions for capturing and implementation for the best practices, and uniquely aggregates data from multiple projects into a central repository for result analysis and reporting.

**Responsibilities:** Job responsibility included full software development life cycle from architecture designing down to implementation and provide support for SigmaFlow Coach [Best practice Templates, Roadmaps & tools] on operating systems Windows in Microsoft Visual Studio 2003, VB.Net language.

## Research Publication

1. Muhammad Usama, Muhammad Khurram Khan, Khaled Alghathbar, Changhoon Lee, **"Chaos-based Secure Satellite Imagery Cryptosystem"**, In Press, Journal of Computer and Mathematics with Applications (CMA), Elsevier Science, 2010. [ISI SCI-E]
2. Fahad Bin Muhaya, Muhammad Usama, Muhammad Khurram Khan, **"Modified AES using Chaotic Key Generator for Satellite Imagery"**, ICIC 2009, Lecture Notes in Computer Science (LNCS), Springer-Verlag Germany, pp. 1014-1024, vol. 5754, 2009.
3. Muhammad Usama Khanzada, Muhammad Khurram Khan, **"Satellite Imagery Security Application (SISA)"**, 12th IEEE International Multitopic Conference INMIC, pp. 232-238, 23-24 December 2008.
4. **"AINAN: Collaborative Application for Protein Visualization & Analyses"**, snpd,pp.171-175, 2008 Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2008.
5. Muhammad Usama Khanzada, Muhammad Khurram Khan, **"Classical and Chaotic Encryption Techniques for the Security of Satellite Images"**, IEEE International Symposium on Biometrics & Security Technologies (ISBAST), 23-24 April, 2008.

[2] Please Refer Annexure – 2 for details of each project.

## Professional Skills

- **Programming Languages**
  Microsoft C# & VB .Net, Java, J2ME and C/C++.
- **Databases**
  Microsoft SQL Server 2000/2005, Microsoft Access and Oracle
- **GIS Customization and Modeling**
  ERDAS Image Web Server, Arc GIS Desktop (Arc Catalog, Arc Map, Arc Globe, Arc SDE) & Arc GIS Engine 9.2, MapInfo, MapXtreme and MapX Mobile.

## Achievements & Other Activities

- First prize winner at Bahria University Software Competition in 2006, for developing a project "A Collaborative application for Protein Visualization & Analyses, AINAAN".
- Participate in Soft-Tec programming Competition at Lahore, Pakistan in Years 2004, 2005, and 2006.
- Participate in KRL Software Competition Islamabad 2005.

## Personal Information


| | |
|---|---|
| **Address:** | R-458 Rafi Bungalows Malir City Karachi 75050, Pakistan |
| **Phone #:** | (+92-21) 451-6127 |
| **Mobile #:** | (+92-321) 230-0205 |
| **Email:** | usama.khanzada@hotmail.com |
| **Date of Birth**: | 5th Aug, 1984 |
| **Office:** | Prince Muqrin Chair (PMC) for IT Security<br>Computer Science department<br>King Saud University<br>Riyadh P.O Box 2459<br>Kingdom of Saudi Arabia |
| **Mobile #:** | (+966-598) 66-2047 |

# ANNEXURE – 1
# [Academic Publications ‘‘Bahria University Karachi’’]

**Title** **Chaos-based Secure Satellite Imagery Cryptosystem**

**Abstract** With the large-scale development in satellite and network communication technologies, there is a great demand to preserve the secure storage and transmission of satellite imagery over internet and shared network environment. This brings new challenges to protect sensitive and critical satellite images from unauthorized access and illegal usage. In this paper, we address aforementioned issues and develop techniques to eliminate the associated problems. To achieve this, we propose a new chaos-based symmetric-key encryption technique for satellite imagery. This scheme utilizes multiple chaotic maps e.g. Logistic, Henon, Tent, Cubic, Sine and Chebyshev for enhancing the key-space, robustness and security of satellite imagery. We perform key sensitivity, statistical and performance analysis experiments to determine the security, reliability, and speed of our algorithm for satellite imagery. The proposed algorithm presents several interesting features, such as a high level of security, large enough key-space, pixel distributing uniformity and an acceptable encryption speed as compare to AES, 3-DES, and DES.

**Title** **Modified AES Using Chaotic Key Generator for Satellite Imagery Encryption**

**Abstract** In this paper, we propose a new modified version of Advanced Encryption Standard (AES) using chaotic key generator for satellite imagery security. We analyze and examine the Modified AES and chaotic key generator to enhance the key space and sensitivity, performance, and security level for reducing the risk of different attacks. The chaotic key generator utilizes multiple chaotic maps named as Logistic, Henon, Tent, Cubic, Sine and Chebyshev. The proposed algorithm presents numerous interesting and attractive features, such as a high level of security, large enough key-space with improved key sensitivity, pixel distributing uniformity and an acceptable encryption and decryption speed. The presented algorithm is ideal for real-time applications to deal with redundant, bulky, complex and stubborn satellite imagery.

**Title** **Satellite Imagery Security Application (SISA)**

**Abstract** With the large-scale research and development in space sciences, space technologies and network communication technologies, there is a great demand of satellite imagery security system for providing secure storage and transmission of satellite imagery over Internet and/or shared network environment. This brings new challenges to protect sensitive and critical satellite imagery from unauthorized access and illegal use, in order to keep the storage and transmission process secure and reliable. Therefore there is strong need of satellite imagery encryption and decryption application for security. Satellite Imagery Security Application (SISA) is an information security application developed for satellite imagery. The application supports new and modified version two most

popular data encryption standards named as Data Encryption Standard (DES) and Advanced Encryption Standard (AES). This paper investigates the security and performance level of the new modified version DES and AES for satellite imagery. The method of application of DES and AES on the satellite imagery in each case is explained. The application provides conventional tools of measurement and analysis such as key sensitivity, statistical and performance analysis to determine the level of security, reliability and performance.

**Title** **AINAAN: A COLLABORATIVE APPLICATION FOR PROTEIN VISUALIZATION & ANALYSES**

**Abstract** AINAAN is a collaborative application developed for molecular visualization and analysis with multiple view points. The application allows multiple users to view and manipulate single and multiple representations of molecular structures. Network sessions can be initiated by any user over the network. Members over the network can join the session, and the initiator owns the activities of the session. The application provides conventional molecular visualization facilities like rendering, rotation, with different views, along with the usage of protein network stores. Protein store is the repository of the protein structures, alignment results, and movies maintained by each user, which can be shared over the network. Sequence and structural analysis algorithms are also supported in AINAAN. Sessions can be saved by recording events and alignment results for future reference. Large scale study of protein molecular structures will need network views support for comparative analysis.

**Title** **Classical and Chaotic Encryption Techniques for the Security of Satellite Images**

**Abstract** In this paper, we will provide an overview of the mechanisms used in image protection, especially Chaos-based encryption techniques available today. We will see how previously proposed methods such as Data Encryption Standard (DES), Triple Data Encryption Standard (Triple-DES), and International Data Encryption Algorithm (IDEA) have been applied in image protection domain and how new concepts of Chaos-based encryption techniques are superior to traditional methods. The chaotic system is rich in significance and in implication because of sensitivity to change initial conditions, control parameters, ergodicity, random-like behavior, repeated processing and very high diffusion and confusion properties that are desirable for cryptography.

# ANNEXURE – 2
# [Major Projects in ‘‘SUPARCO’’]

**Title** **SUPARCO Online Catalog System for Satellite Imagery**

**Description** The objective of the system is to provide access to end-users and applications of SUPARCO satellite imagery repository. The present prototype version provides a simple Web-based interface to an archive of imagery data which is stored on a RAID array. The web interface provides tools to select and view multiple images and perform searching and analysis. In this project **ERDAS Image Web Server** has been used to serve satellite imagery and for complimenting and integrating with SUPARCO GIS and business systems which contains large amounts of satellite imagery data. This project is developed in Microsoft ASP.Net, Java script and Microsoft SQL Server 2005. The project is initially deployed in SUPARCO.

**My Role** System analysis, design, development, testing & implementation of the project.

**Client**
- SUAPRCO

**Title** **Development of J2ME based Navigation & Tracking System.**

**Description** The core objective of the project was to develop a General Mobile based client/server system for navigation & tracking of Mobiles, vehicles, pets, persons etc. The monitoring and controlling of data collection is done using tracking device having a GPS so that the track could be mapped and analyzed with respect to its geography. This project is developed in J2ME, Microsoft .Net, Microsoft SQL Server 2005. In this project Google Static Maps API has been customized keeping in view their need and performance in Mobile Handsets. The project was initially designed for SUPARCO Vehicles however after its successful implementation in SUPARCO; the application is ready for its commercial implementation. The project has been successfully deployed at many client sites.

**My Role** System analysis, design, development, testing & implementation of the project.

**Client**
- SUAPRCO
- V-Track Tracker, Pakistan

**Title** **Establishment of Water Management Spatial Database System for Monitoring of Watercourse Improvement.**

**Description** The project was a part of president’s special program on Improvement of Watercourses in which all watercourses are to be lined for reducing water losses. The project is about the digitization of complete irrigation network from channels to watercourses command areas and collection of data related to watercourses from field & pooling the same over GSM network with the database inventory in their headquarters. The field data collection is done on a PDA having a GPS so that the collected data could be mapped, archived, retrieved & analyzed with respect to its geography. This project is developed in VB.net using Arc GIS engine and SQL Server 2005. In this project Arc GIS tools have been customized keeping in view their need in irrigation system. The Irrigation system is

digitized using Arc GIS desktop with the help of satellite imagery and Topographic maps.

**My Role** System analysis, design, development, testing & implementation of the project.

**Client** Agriculture Department, Punjab for NPIW, Pakistan

**Title** **Development of GPS/GIS based Fleet Management & Vehicle Tracking System.**

**Description** The project was initially designed for SUPARCO fleet of vehicles however after its successful implementation in SUPARCO; the application was ready for its commercial implementation. The project has been successfully deployed at many client sites including Srilanka and Saudi Arabia.

**My Role** I worked as software programmer and system analyst for development and implementation of this project.

**Clients**

- SUAPRCO
- Geo-Informatics, Sri Lanka
- Punjab Highway Patrol Posts [PHPP], Pakistan
- Pakistan Rangers Sindh
- MegaTech Tracker, Pakistan
- Syndustria (Pvt) Limited, Pakistan

**Title** **Establishment of Geo-Database Software and Tracking System for the NWFP Province.**

**Description** The project was a part of president's special program on Improvement of Watercourses in which all watercourses are to be lined for reducing water losses. The project was about collection of data related to watercourses from field & pooling the same over GSM network with the database inventory in their headquarters. The field data collection is done on a PDA having a GPS so that the collected data could be mapped, archived, retrieved & analyzed with respect to its geography.

**My Role** Project system analysis & design, development, field testing & implementation of the project.

**Client** Agriculture Department, NWFP for NPIW, Pakistan

**Title** **K&N's Sales and Management System**

**Description** The core objective of the project was to develop a PDA based client/server system for identifying new trends in context to geography for sales and management high level decision.

**My Role** System analysis & design, development, field testing & implementation of the project.

**Client** K&N's Food (Pvt) Limited, Pakistan

**Title** **Parking Monitoring and Management System**

**Description** The core objective of the project was to develop a PDA based client/server monitoring and management system for Parking Lots. The project was about collection of data related to Parking-Meters, Parking Stands, Inspectors and Vehicles.

**My Role** System analysis & design, development, field testing & implementation of the project.

**Client** City District Government of Lahore (CDGL), Pakistan

# ANNEXURE – 3
# [Major Academic Projects]

**Title** **Interactive and Parallel Visualization of Protein Analysis using Cluster**

**Description** A complete application that performs protein sequence and structure analysis on cluster of workstations. We have designed and implemented cluster using message passing interfaces (MPI).The main features of cluster are dynamic scheduling and task monitoring which is scalable to supercomputer. We used OpenGL and Java based programming components for implementing protein visualization module on shared network environment.

**Tools**
- For developing cluster we used MPI-Java ,J2SDK and XML
- OpenGL is used for visualization of proteins.
- Java Socket programming for interactive and collaborative visualization of proteins.

**Semester** Eight

**Title** **CMM assessment of AVANZA Karachi**

**Description** AVANZA is a growing software house in Pakistan. The objective of this assessment is to understand the CMM model by applying it in actual environment. (It's a voluntary effort for AVANZA Solution.)

**Semester** Eight

**Title** **Client Management System**

**Description** This application provides complete sales and purchase system for shop.

**Tools**
- C#.NET (Win forms, Windows Services, Assemblies etc).
- SQL Server2000 as back end database.

**Semester** Eight

**Title** **Character Reorganization**

**Description** This application is used to recognize the ANSI Characters using Neural network algorithm named as "Back propagation".

**Tools** Java Virtual Machine (SDK), J2SDK1.4

**Semester** Eight

**Title** **Implementation of Data Encryption algorithms**

**Description** I have Implemented the AES, DES, and RSA data encryption algorithms for providing security in data communication.

**Tools** Java Virtual Machine (SDK), J2SDK1.4

**Semester** Seven

**Title** **Bahria University Time-Table Generator**

**Description** This software generates the Bahria University Time-Table for all Classes and It resolves the time collision between teachers and checks the availability of class-rooms.

**Tools**
- Java Virtual Machine (SDK), J2SDK1.4.
- Oracle 8i as back-end database.

**Semester** Six

**Title** **SQL Statement Recognizer**

**Description** I have designed and implemented SQL statement Recognizer that can parse Select, Insert, Delete and update statements.
**Tools** Java Virtual Machine (SDK), J2SDK1.4
**Semester** Six

**Title** **Directory Server**
**Description** I have designed and implemented the directory server that maintain directory of many servers and its services for multiple clients.
**Tools** Java Virtual Machine (SDK), J2SDK1.4
**Semester** Six

**Title** **Bahria University Transcript Management System**
**Description** This application enables to record the examination results of all students and generate their transcripts.
**Tools**
- Java Virtual Machine (SDK), J2SDK1.4
- Oracle 8i as back end database.

**Semester** Five

**Title** **Chatting software**
**Description** TCP/IP protocol based chatting software which enables users to interact and chat with each others.
**Tools**
- Java Virtual Machine (SDK), J2SDK1.3.
- Java TCP/IP Sockets Programming API.

**Semester** Four

**Title** **GUI Based Student Record System**
**Description** This application stores and retrieves the data of students
**Tools** C language (it is completely GUI based software).
**Semester** Second