http://www.icact.org/journal.asp

ICACT-TACT JOURNAL

Transactions on Advanced Communications Technology

Volume 3 Issue 3, Mar 2014, ISSN: 2288-0003

Editor-in-Chief
Prof. Thomas Byeongnam YOON, PhD.

Global IT
Research Institute

Volume. 3 Issue. 2

Globalization and ICT Innovation Policy: Absorption Capacity in developing Countries

Ayesha SALEEM, Kiyohide HIGUCHI

Graduate School of Global Information and Telecommunication Studies, Waseda University, Tokyo, Japan

dua@fuji.waseda.jp, higuchi@waseda.jp

***Abstract*— This paper is about the new role of academic institutions in the economic development of developing countries. Educational institutes are significant in propelling economic development as they are the powerful drivers, technology centres, developers and investors. Universities can affect the economic growth of developing countries. The purpose of this new role of academic institutions is to touch virtually every aspect of daily lives and the prosperity of the communities living in rural areas. At a larger scale it aims to initiate a process of policy learning, exchange between countries in different stages of economic development and knowledge sharing with their universities research students. The study identifies the current technology innovation in the field of education and analyzes the case of developing and developed countries. To demonstrate, we do an in-depth study of Pakistan's education system.**

This paper explores strategic decision by using game theoretical analysis. The paper constructs a game model subject to preferential policy between Government and Universities. It offers three games that give the overview of the role of the government to promote the quality of education. The paper finds the equilibrium of the game under three specific conditions. The result shows that better policies lead to quality education that foster the development of the country. It clearly shows that having an autonomous body to regulate the education policies can promote the innovation and technology adoption. This study is two-fold; it provides the insight of university-government interaction as well universities' interaction among themselves.

***Keyword*— ICT, Innovation Policy, Role of Universities, ICT education, Technology catch-up/transfer, Game Theory**

I. INTRODUCTION

THIS research focus on Pakistan, officially the Islamic Republic of Pakistan covers an area of 796,096 square kilometres. Pakistan has a very high growth rate and is the sixth most populous country in the world with an estimated population of 184.3 million in 2012-13. Almost 70% of the its population (i.e. 110 million) lives in rural areas. Adult literacy rate (10 year and above) is 58 %, literacy is higher in urban areas (74%) than in rural areas (49%), Public spending on education as percentage of GDP is 2.1 %. According to Labour Force Survey of 2010-11, 44.9 % of the total workforce is employed in agriculture sector, 13.02 % in manufacturing, 6.62% in Construction, 5.23% in Transport, 13.66 % in services and 0.1 % in others. Whatever progress Pakistan has made, most of its gain is not shared in the rural area. In rural area, structural changes and improvement in factor of production is very low. Human Development Indicators are also low. [1][2]

Most of the rural areas of Pakistan are similar with respect to their infra structure, economy and resources and are diverse in nature at the same time by their socio cultural conditions. Rural areas are generally backward in every aspect. There is a need to educate people, improve their healthcare services and to create job opportunities; there are many fields to develop like a considerable number of developmental project are being implemented by World Bank, ADB and NGOs. However all such projects have adopted the progressive approach for development which takes time. If we follow the same pattern that has been adopted by the OECD countries then it will take the same time which they took to be in the present position. They follow the same traditional pattern. If we start to educate all the children from a village, it will take 30 years for that village for all children to be educated and use their knowledge for the growth of their village. The other point is to provide health care services which also have a long term affect on the economic development.

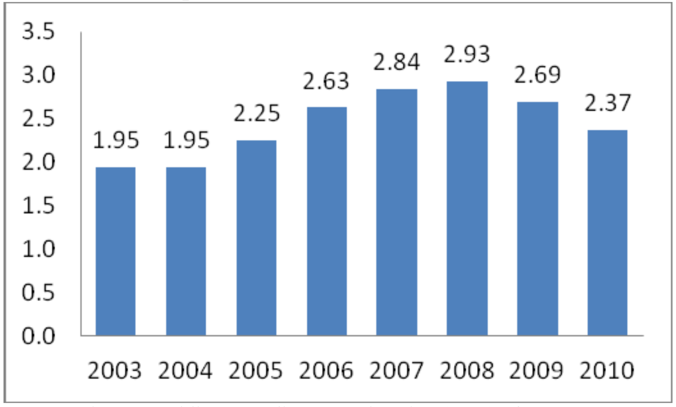


Figure1: Public Expenditure on education (as %) of GDP [2]

Many Universities around the globe have started comprehensive reviews of the curricula and introduced new strategies to transform the university learning and teaching approach. However, the quality of higher education in Pakistan is way below. Pakistan has 138 Universities including six new

Manuscript received September 27, 2013.

Ayesha Saleem is PhD student in Graduate School of Global Information and Telecommunication Studies, Waseda University, Tokyo, Japan (corresponding author phone: +81-80-3240-5875;+33-758-200-164 e-mail: dua@fuji.waseda.jp; Ayesha.saleem@OECD.org).

Kiyohide Higuchi is Professor of Graduate School of Global Information and Telecommunication Studies, Tokyo, Japan (email: higuchi@waseda.jp)

universities established in 2010-11. There is a pressing need to re-assess the current curriculum with the hope of adjusting its standard. Many universities have regarded understanding Information Technology (IT) and mastering the basic skills and concepts of IT as part of the core of education, alongside reading, writing and numeracy. In order to enhance the global competence by universities is the latest proposal for the developing countries like Pakistan.[3][4][5]

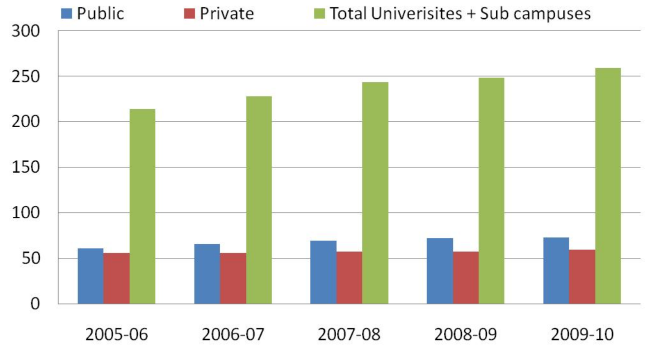


Figure2: Universities/Degree Awarding Institutions in Pakistan [3]

II. LITERATURE REVIEW

Internationalization is not only about learning elsewhere, but it is also about learning to solve local problems or address local issues within an international context; or learning to address international or global issues within a local context. Globalization is constantly changing the employment prospects of our workforce. Universities can do this by providing employers with graduates who are not only technically knowledgeable, but globally competent, as well.

Now the question arise who is responsible to take initiative and how it is possible. According to OECD share of private expenditure on educational institution is highest in Chile, United Kingdom, Korea, Japan and United States respectively. It is important policy aspect to balance the share of public and private financing of education and currently it is an important issue in many OECD countries.

There we discuss some challenges to overcome for promoting the technology adoption capacity with the help of universities.

A. *Globalization and Change of Technology*

The world has changed, it has become flat, more facilities are available, new techniques has developed. Thomas L. Friedmans's in his book discuss with the help of examples that how and why globalization has now shifted into wrap drive [6].

Growth is not the process of simple replication. It reflects a never ending flow of inventions, innovations and technological advancements leading to improvement in the production possibilities. Technology and the process of production have changed, and new products and services has introduced. Innovation has enabled doing things in different yet more efficient and cost effective ways.

Before 20 years, there was no computer, no concept of the internet no search engine, telecommunication was not available. These technologies were not used for the economic development. There are new conditions for future prospects, hyper growth is possible, and mobility of the resources is also possible. Use of new techniques changed the life and sudden change towards modernization can be possible.

The author discussed the entry condition in the world market for catching up has changed and is entirely different from 50 or 100 years ago. He grouped the countries on the basis of the patterns of economic growth as innovator, 19th century followers, 19th century cases of stumbling back, underdeveloped and stay behind, Learner or 20th century followers, 20th century cases of stumbling back. Pakistan is included in Group IV that refers to the country "underdeveloped and staying behind". [7][8]

In the era of global competition it is recognized that changes in technology and competition have diminished many of the traditional roles of location. Yet clusters, or interconnected companies with in the same area, are a striking feature of virtually every national, regional, state, and even metropolitan economy, especially in more advanced nations. The prevalence of clusters shows important insights about the microeconomics of competition and the role of location in competitive advantage. In the globalized world the old purposes for clustering have diminished, it has new impacts of clusters on knowledge-based and dynamic economy. Clusters represent a new way of thinking about national, state, and local economies, and they necessitate new roles for companies, government, and other institutions in enhancing competitiveness [9].

B. *Internationalization of Higher Education*

"Innovation involves getting new ideas accepted and new technologies adopted and used. The introduction of new technologies, methodologies or content into a university IT course can thus be considered as an example of innovation."[10].

"Internationalization of Higher Education is the process of integrating an international/intercultural dimension into the teaching, research and service functions of the institution".[11] With the economic rationale as a backdrop to internationalizing the higher education, the term "internationalizing the curriculum" is proposed as a strategy for internationalization. Internationalization has been discussed as the relevance and importance of student outcomes, teaching strategies and knowledge content and inclusive curricula and pedagogy.[12][13][14]

Numerous researchers emphasize the centrality of the curriculum and the internationalization of the curriculum, teaching and learning processes as critical elements of internationalization. Knight describes the curriculum as "the backbone of the internationalization process". Other researchers concur, emphasizing the importance of an internationalized curriculum in providing a student-centered learning experience for all students and in preparing students to be successful in today's increasingly interdependent global society.

Indian IT industry has advantage on the other Ireland because of focused on English language skills for engineers and higher quantities of quality engineers. [15]

C. University–industry links

University links with the industry can enhance the performance of the faculty [16]. Institutional policy regarding University Industries links can build institutional direction as well give clear and explicit regulations for understanding relationships [17].

In the post war period Japan University Industry cooperation was established. Industries contacted the universities for hiring the skilled labors. As a result Japan industries achieved world class status in 1980's. The Ministry of International Trade and Industry (MITI) was mostly responsible for policies related to the manufacturing sector and financially supported a number of R & D projects.

A legal framework was established in Japan to promote university- industry technology transfer [18][19].

In Pakistan during 1990s first time Government formulate the trade liberalization and privatization policies. Scientists at the Pakistan Council for Scientific and Industrial Research and the Pakistan Atomic Energy Commission collaborated with the Universities. But there were no collaboration between Public R &D institutions and private industry. The GDP growth rate was not sufficient for large population growth rate [20].

III. UNIVERSITIES ROLE

In Japan the higher education sector R & D expenditure is growing fast. University has new role in the science and technology policies. Universities reforms considered the part of transformation of Japanese research and innovation system since 1990s. Legal government structure of the national universities changed to "corporate status" for better efficiency and increased independence. From 2001 to 2004 educational reform were accelerated towards economic and industrial policy objectives [21].

The universities financial system was also reformed by introducing the "black grant system". The budget for the universities substantially increased in the past few years with the objective of having world top level of research universities.

Ministry of Economy, Trade and Industry (MITI) in Japan proposed a plan for reforming universities as part of the national industries policy. After that MEXT released "Toyama Plan" for basic principles for structural reforms on Universities. In the plan three changes i.e. reorganization of national universities including merger of some institutions; introduction of business methods to national universities through the process of "incorporatization" and introduction of competitive mechanism into the university sector, including national, public and private universities.

In developing countries Industry University and Research Institution coordination can reduce the gap and create better environment for the research and development of the technology and its adoption.

A value chain model is suggested in which… "a central agency will play the role of helping in national intellectual property (IP) system in promotion and encouragement of local inventions and innovation. It will facilitate creation and management of IP assets in Institutions of Higher Learning, especially in assisting researchers on how to identify patentable inventions and take appropriate action to safeguard them from exploitation. Also it will facilitate in commercialization of R&D results and innovation. This includes the process involving business strategies and techno-entrepreneur's development that need to be implemented so as to reap best possible returns from R&D investment. Most importantly it will address significant issues as how to obtain financing for development of innovations via government and private venture capital funds for the commercialization of new and indigenous technology"[22].

Therefore, there should be new role of universities. The knowledge sharing by the universities is a way to achieve development, because the World has changed it is not the same as it was 20 years earlier. A strategy should be evolved with collaboration of research universities and stakeholders of rural area.

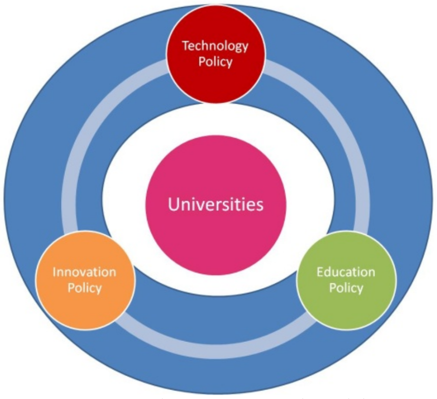


Figure3: Proposed Model

A. Globalized Trend of Internationalization of Higher Education

As espoused in the abovementioned literature, internalization of higher education curriculum is vital towards economic development of a country to prepare students for careers that are potentially international and contribute to local economic development and competitiveness. Recent years have seen a tremendous expansion of ways in which higher education goes 'international". As well, international trends and developments taking place beyond national boundaries impact more easily on higher education policy at institutional and national levels, thus creating additional inter-connections between various changes. Consequently, it is not only difficult to keep track of the various concepts and terms used to describe new processes in the international aspects of higher education, it is also difficult to capture these interconnections. An additional challenge comes from the fact that innovations and changes are on-going and thus the field is evolving constantly.

University curricula in Information Communication Technology (ICT) necessarily require frequent changes, updating and even complete revision due to advancements in technologies and changes in how people and organizations make use of computers. The increased focus on achieving economic benefits and the technological advancement demands higher education policies on internationalization of ICT education. The most important reasons for integrating international topics into the ICT curriculum are:

1. To identify key issues, trends and area of growth and to elaborate policy statement that call for change and improvement.
2. Results in a more global orientation on part of students.
3. Sensitizes students to differentiate between countries in technologies.
4. Results in more interesting class discussions, and
5. Makes students more desirable in the marketplace. [11]

In effect, countries can be able to match other countries, such as India, in producing this 'raw material' of university-educated professionals in high enough quality and quantity it can become a 'Services-export Tiger' rivaling the growth rates of the fastest growing Asian economies. This, however, should not be seen as a case of 'picking the latest fad' but rather an example of one opportunity where investment in higher education could yield very high economic returns.

Acknowledging the growing needs to better prepare students for living and working in an increasingly culturally diverse and socially complex world, universities should develop new teaching and learning strategies to attain an internationalized curricula. Likewise, there is a need for a customized national curriculum in order to cope with the global world that could ultimately lead to the future production of quality graduates for job opportunities within and outside of the country, and be at par with other universities.

B. Model Universities

In this respect the University may introduce an internship program for the students for duration of six months. This should be made as a requirement of their study program. The student will have to spend that time in rural area of countries and then work to solve the rural area problems. They will be working as "Brain Circulation". That will affect the living status of the village. People of the rural area don't have facilities so even their own person after getting education don't want to come back to the place. The highly qualified people from different universities will work there, share their knowledge and will see the real situation to solve their problem. Education should begin from home.

People of the rural area of the developing countries should provided with free internet and mobile phone. That will not be a high cost. After implementing this strategy the social inclusion, gender equity, reaching remote areas and regional imbalances/disparities will be eliminated. The experiment and prototype manufacturing and the use of that prototype in the live environment will change the economic condition.

In many analyses it proves that universities play an important role for innovation because R & D is the key aspect of the innovation. So doing this initiative it is the knowledge investment in the rural area. Universities, public research institution and Science Park play important role in the innovation. Economic Development of the rural sector is strongly related to technological and scientific specialization and innovation. From the traditional process the developing country has to face painful transition process towards techno economic system.

C. Innovation Universities Example

An example of how a university can undertake its new role in different ways to enhance innovation explained in RMIT's initiatives in the East Gippsland region. In consultation between RMIT and the local community, RMIT questioned about the issues confronting the region and find out the way how best it might assist. They had a report on degradation of the ecological systems which had identified problems but there had been little follow-up. They recruited nineteen post-graduate students to follow up the initial report and identify solutions. Their research is being conducted in the region, and with those affected by the problems they seek to solve. They will report progressively on their results, reducing the normal dissemination time-cycle. They will have access to local, often informal or undocumented data, available only on the spot. This exemplifies a new way of working in collaboration and partnership with others and identification of research agendas by others.

A research university is one of the necessary conditions for economic restructuring. Research universities play a important role to provide scientific knowledge, technical expertise, and skilled workforce for implementation in the field. While in industrial growth we have successful examples of Silicon Valley in California, Route 128 in Massachusetts, and Research Triangle area in North Carolina are all close to major research universities, and this fact has been perceived as instrumental in positioning these areas on new growth trajectory.

John Hopkins Institute for Policy Studies in Baltimore offers service to the community through graduate and undergraduate student internships, seminars and briefings, and volunteer activities, each year the Institute's first-year students research a policy issue of particular interest to the City of Baltimore, and present their findings and recommendations to city leaders, community activists, local business owners, and concerned citizens, among others. [23]

Massachusetts Institute of Technology (MIT) has a program for International Development "D-Lab". The purpose is to foster the development of appropriate technologies and sustainable solutions within the framework of international development. In India M S Swaminathan Research Foundation (MSSRF) a Centre for Research on Sustainable Agriculture and Rural Development has established to harness the power of ICT in the knowledge, skill, economic and social empowerment of rural families based on the principle of reaching the unreached and voicing the voiceless. The MSSRF has collaboration with the D-Lab program. [24][25]

D. Initiative in Pakistan

Namal college is the initiative to trigger innovation for the benefit of the society with collaboration of University of Bradford, UK and LUMS, Pakistan. Namal Knowledge City is built in Mianwali a small district of Pakistan. Project building consisting of Computer Science, Software Engineering and Electrical Engineering departments with their laboratories has now been completed.

The development of Namal Knowledge City (NKC) is planned in three phases. The Phase-1 short certificate courses, diploma in higher education programmes and undergraduate degree programmes has established, after that it will offer postgraduate degree programme in various disciplines. One of the main planned activities of Phase-2 is Namal College staff development and establishment of links with industrial partners to promote knowledge transfer at local and national level. Phase 3 will establish Technology Park, enterprises and commercial. [26].

In Pakistan Higher Education Commission is the primary regulator. Higher education commission is the autonomous body and is responsible for higher education policy, quality assurance, degree recognition, development of new institutions and uplift of existing institutions. Higher education commission program "Program for Collaborative Research" (PPCR). The objective of this program to involve the experts from foreign universities in developing curriculum, updating laboratory techniques, and provide guidance to post graduates students in universities of the Pakistan. This program encourages the community of foreign experts to develop joint-research programs with local faculty and to enhance expertise for the overall development of concerned departments. On the other hand Higher education commission is building the Nation Innovation policy for the university industry collaboration to promote the innovation. Nation Innovation policy preparation has started with the creation of an Innovation Strategy Working Group (I-SWOG) in May 2009. The members of the working group were the government, private sector and academia. Two workshops also organized in Karachi and Lahore. The CSF Karachi workshop released a Draft Strategy document "Pakistan Innovation Initiative: Towards Strategy and Implementation". This document has sound base for making the innovation policy.

IV. ANALYSIS

Game theory has become a cross- disciplinary study of great importance for the mathematical social sciences. It offers the tool- kit applicable to decision problems in which the consequences of one decision may depend on the decisions of others, previous decisions creating the conditions for current decisions, simultaneous and subsequent decision. Game theory analysis is used to analyze that where the structural flaws lie and begs the question, "Can fix those flaws? The reasons to think where rules don't apply in particular case?" Understanding of game theory is vital to technology prioritization. It is also an important thing to evaluate for the think tank that was their predictions correct?

It has been argued that "operational characteristics of economic models, and in particular stability considerations, point strongly toward an equilibrium concept for dynamic dominant player models which implies that the players determine their best decisions depending on the current state of the system and the decisions of the other players, and rationally expecting that equilibrium decisions will be chosen in the future. This solution is called the feedback solution. It has the property that the original plan is consistent under replanning. The difference between the solutions in this regard does not depend on the presence of uncertainty. Because of this property, the feedback solution is the only one that seems likely to be stable in the sense that decision makers grouping for equilibrium decision rules will converge on these decision rules" [25].

As Aumann has observed "those two aspects of game theory are really not two separate disciplines; they are part of the same whole". For the purpose of the public policy, though it is not enough that cooperative and non- cooperative analysis are complementary, as Aumann observes. Rather we need analysis of given models that are linked, drawing on cooperative and non- cooperative approaches. This reflects the different roles of cooperative and non- cooperative models in the pragmatic project of the public policy, in that it is commonly the non-cooperative models that identify the problems, so that cooperative analysis of the same example is necessary in order to propose solutions [27][28].

Game theory concept has been used in solving problem of education [29][30][31]. However, this paper is using a new approach between Government and University role for adopting the technology.

Therefore, this paper uses this tool "Game Theory" for the solution of issue "How do the Government interact with the university to promote and adopt the technology and innovative integral process for the development of the country".

Now we construct the following game between the government and University. The game is simultaneous game. There are two players, Government and university. The players also have two strategies.

Players:

Government and University.

Sequence of events:

Sequential decision by government and then University

Strategies:

(1) Government don't take any action in case when Universities are self aware.

(2) Government strategy is to take action and provide latest technology in the form of machinery/equipment, staff and investment.

(3) Government strategy is to make integral policies for the industry university collaboration.

Payoffs:

C1 = Government's cost to do action.

C2 = University's Investment cost

α = University extra cost to do action for adopt of technology the in the absence of Government support.

Pg = Government probability to provide subsidy

Pg- 1= Government probability for no subsidy

Pu = University probability to do action

Pu-1 = University probability not to do action.

S= Social Benefit

K = Technology

K1= New Technology

Y= Output Y=y(K+K1)

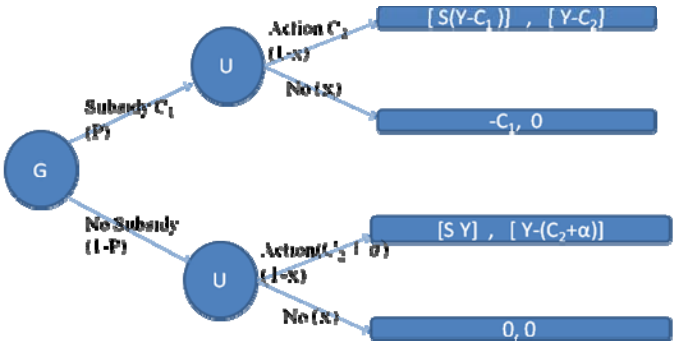


Figure 4 : Government University Game

If
$Y-(C2+\alpha)\geqslant 0$ then the University should do action

$Y-(C2+\alpha)\leqslant 0$ then Government should do action or better policy.

Government Pay off:
Government provide technology /integrated policy

$=[Pg.Pu(S.Y-C1)]+[Pg(1-Pu)(-C1)]$
$=[PgPu.SY-PgPu.C1]+[Pg-PgPu(-C1)]$
$=Pg.Pu.SY-PgPu.C1-Pg.C1+PgPu.C1$
$=PgPu.Sy-Pg.C1$
$=Pg(Pu.SY-C1)$

Government do not provide technology /integrated policy
$=[(1-Pg)Pu\ S.Y]+[(1-pg)(1-Pu)(0)]$
$=[(1-Pg).Pu.SY]$

University Pay off:
Government provide technology /integrated policy
$=[Pg.Pu(Y-C2)]+pg(1-Pu)(0)$
$=[PgPu.Y-PgPu.C2]$
$=[PgPu(Y-C2)]$
Government do not provide technology /integrated policy
$=[(1-Pg).Pu(Y-(C2+\alpha)]+ [(1-Pg)(1-Pu)(0)]$
$=(1-Pg).Pu.Y-(1-Pg)Pu(C2+\alpha)$
$=(1-Pg).Pu(Y-(C2+\alpha)$

It is clear that Government payoff is greater if don't do action and university do it by them self.
$Pg(Pu.SY-C1)<[(1-Pg).Pu.SY]$
In other case
$PgPu(Y-C2)>(1-pg).Pc(Y-(C2+\alpha))$

Now the decision of action base on the probability of the University if the probability of the university to do action Pu is near to zero such as Pu= 0.01, the government should provide the technology in the first stage of the game. The University's probability will increase. We construct the repeated game. In the second stage when the University's probability will increase to take action such as near to 1 Pu= 0.9 then government should not do action.

The government's aim is to provide preferential support to University's for the taking action and encourages them. As a result the government's pay off revenue increase in the form of increased social benefit of countries.

The game process on adoption of the technology and government role to provide preferential support to the Universities is explained in game tree and with the help of equation. The game has three strategies for government and Universities. Government takes action to provide preferential support for adoption of technology. The government will manage some expert to evaluate the technology for its effectiveness and make policy and process to adopt that technology. These expenses are shown as "C1". The Government provides new technology or implements a integrated policy which is the investment cost. Then University adopts new technology or in other case follow the integrated policy as a result the increased output in the form of human capital. The government social welfare increases. If government does not take any action then University will not be able to do action due to risk factor, less intensive and funds. The University has two strategies to adopt the technology and not to adopt. We use the Backward Induction game to take the decision of government bases on Univesity's strategies. As this game has both cases symmetric and asymmetric information game, in symmetric information both players clearly understand their strategies and asymmetric Information when only government aware of the strategy.

A. *Case 1: Government University Non Cooperation Game*

The institution is the backbone of the country, credibility of the education system is very important. Therefore, to keep the high standard in education, government should have information. Government should evaluate the education system and their capability. In case Government gets information that Universities has capability to do action and University is self aware and decides to do action by investing cost C2, University has more resources than government. In this case government plays not to do action as government has constrained to play A (action) because government has limited fund and the university plays action. The government gets 3 and the university 2. We assume in this case that both players are rational and the structure of the game is common knowledge. The university self awareness is the way to achieve to quality of education and improve the role of university. University hire competent faculty, improve the research and development facilities and collaborate with the industry. The government is likely to choose N with other players being better off and government save the fund for the other development projects.

The payoffs are intuitive. This is the government best strategy, as the government plays no action to the university and saves costs. The government knows that the university will take the right approach for the greater good by drawing upon its comparative advantage in the creation and transmission of knowledge. The government gets worst payoff of 0, as the university could not produce skilled human resource in all fields and that will not be able to cope with the current economic situation.

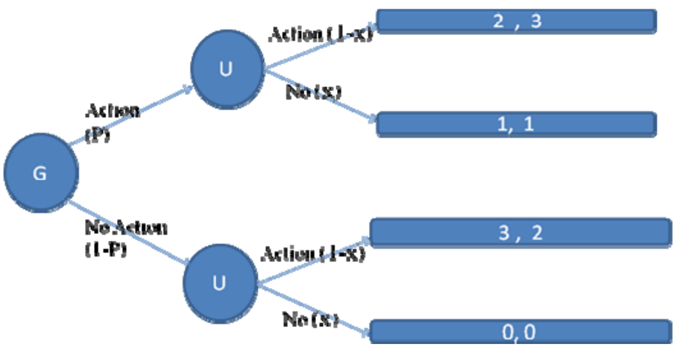


Figure 5: Government University Non Cooperative Game

While at (2, 3) the university obtains its best payoff of 3 in this one-shot game. For the government, (2, 3) is ranked next to the best, with a payoff of 2, as the government is playing role. On the point (1, 1) the university gets q. In the game the university has dominant strategy (2, 3) if the government plays A then university is better off playing A as well, and if the government plays N, the university is better off playing A. Thus, no matter what the government plays, the university is better off playing A. So the government would play N to get 3 instead of A and get payoff 2. The strategy pair (N, A) emerges as the unique equilibrium of the game yielding a payoff of (3, 2). In the first phase the universities do actions and in the second phase it revised simultaneous game is played. The strategy is (N, A) is a good outcome.

B. Government University Cooperation Game

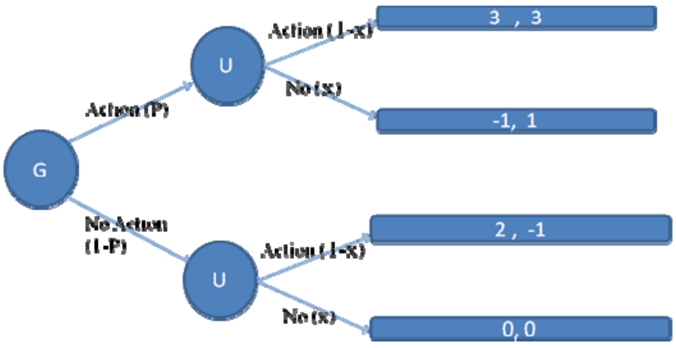


Figure 6: Government University Cooperative Game

In this case we assume that Universities don't have capability to do action and don't have information and resources. Then the new game is mentioned in Figure. If government unable to do this practices that result the failure of the expected outcome. This case assumes that the government has fund, therefore able to do actions and adopt the strategy A. The university's new dominant strategy is to follow that action. The equilibrium of the revised game would be (3,3) at which the government gets its best payoff of 3, and the university gets its payoff of 3. The new equilibrium is also Pareto optimal in the sense that no player can be made better off without making the other worse off. It is also the case that the university would find its way to do action what the government says under (A, A). The self awareness is a strategic move, a move that induces the other player to choose in one's favor. It constrains the other player's choice by affecting his expectations. So in this game as the Government strategic move to do action and change its payoffs encourage universities to do action government's expectation that the university would also play A.

C. Case 3: Government University Cooperation Game with Policy

In this case universities assume that there are integration policies that stimulate the university to play A. The policy imposes rule and is a game changer. The new game is represented in Figure. Now university has a dominant strategy to play A and (A, A) is the dominant strategy equilibrium. The policy induces cooperation such that the universities and Government are better off.

In this case all other payoffs remain the same. The new equilibrium is also Pareto optimal in the sense that no player can be made better off without making the other worse off. They are both better off because they play (A, A) and get 3 each. Therefore, it is perfect cooperation because Government does effort in the form of policy and University also use it resources to follow the policy.

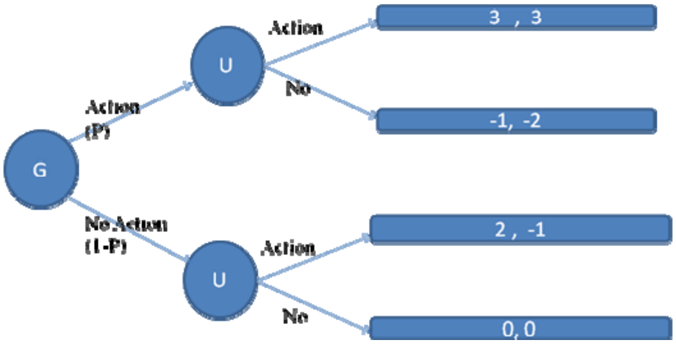


Figure 7: Government University Non Cooperative Game with policy

The following conclusion seems evident. Universities with the ability to compete and having the means to play A while the government implement and enforce policies. It is obvious that once the policies are implemented, the universities follow the rule and will be better off. The policy will change the role of university; universities with the new role will be part of the Government towards the development. The government of the developing countries does not have funds and do not want to implement such policies. Therefore, is still gearing up to implement policies. Credible commitment to swift and effective implementation of the policies is thus critical. There is pressing need to improve the policies for the quality of education and to make well defined policies for the development of the country.

V. Conclusion

In essence, this study is proposing a new role of universities for economic development of the country. It is concluded that to transfer or catch up technology to developing countries, new universities should be established in the rural areas with the Internationalization of ICT curriculum. The highly qualified people from different universities will work there, share their knowledge and will see the real situation to solve their problems. This study would not only be significant to the developing countries but also to universities in other developed countries that need to upgrade higher education system to compete with the globalized world.

The role of the government is to initiate and promote the technology by the effective policies and rules. Government can do action by providing the technology or by effective integral policies for the better control of Universities. There is need to design the mechanism that specify the institutions, procedures and the rules of the game with a desired outcome in mind. The mechanism should consider the all the stake holders and the communication system. The desired outcome can be achieved if the players of the game have full information about the game. While in education system it would be fatal to relay on the universities only because moral hazard is a serious issue and is likely to be misused. It also does not seem wise to keep the education in the government sector under direct control of the politicians. The wise option is education system should be under the autonomous body like Higher education commission (HEC) in Pakistan to deal with policy formulation as well as policy implementation. The commission should formulate policy on a continuing basis, analyze real-time data for mid-course correction, and prosecute cases against unscrupulous providers of education.

REFERENCES

[1] Government of Pakistan. Federal Bureau of Statistics (FBS) Pakistan Statistical Year Book 2011, http://www.pbs.gov.pk/content/pakistan-statistical-year-book-2011

[2] Economic Survey 2012-13 http://www.finance.gov.pk/survey_1213.html

[3] Higher Education Commission Pakistan Annual Report 2010-11

[4] State of the Economy Annual Report 2010-11, http://www.sbp.org.pk/reports/annual/arFY12/Anul-index-eng-12.htm

[5] Khawaja Amjad Saeed. (2006). The Economy of Pakistan . Karachi: Oxford University Press

[6] Thomas L Friedman. The World Is Flat: A Brief History of the Twenty-First Century (4th updated and expanded). New York: The Washington post, 2007.

[7] Claes Brundenius, Bo Goransson and Jan Agren (2008).The Role of Academic Institutions in the National System of Innovation and the Debate in Sweden, (UniDev Discussion Paper Series paper no. 9). Retrieved May 08, 2010, from http://developinguniversities.blogsome.com

[8] Convergence of Productivity: Cross-National Studies and Historical Evidence by William J. Baumol, Richard R. Nelson and Edward N. Wolff (Jun 30, 1994) Oxford University Press, USA. Staying Behind, Stumbling back, Sneaking up, Soaring ahead: Late Industrialization in Historical perspective, Takashi Hikono, Alice H. Amsden

[9] Michael E.Porter (1998). Clusters and the New Economics of Competition. Harvard Business Review (Nov- Dec 1998)

[10] Tatnall, A & Davey, B. (2004). Improving the Chances of Getting your IT Curriculum Innovation Successfully Adopted by the Application of an Ecological Approach to Innovation. Informing Science Journal, volume 7, 2004.

[11] Knight, J. (1999). Internationalisation of Higher Education. Quality and Internationalisation in Higher Education, OECD.

[12] Rizvi, F. (1999). Internationalization of Curriculum: RMIT Teaching and Learning Strategy. RMIT. Retrieved March 2, 2003, from http://www.pvci.rmit.edu.au/ioc/back/icpfr.pdf

[13] Gayle, F. (1997). Where does Australian higher education need to go from here? In E. J. Sharpham and G.Harman (Eds.), Australia's Future Universities. University of New England, NSW.

[14] IDP Education Australia (1995). Curriculum Development for Internationalisation: Australian Case Studies and Stocktake. Canberra: DEETYA.

[15] S. Sadagopan, "IT in India," IT Professional, vol. 14, pp. 14-17, 2012.

[16] Gulbrandsen, M., & Smeby, J. C. (2005). Industry funding and university professors' research performance. Research Policy, 34(6), 932-950.

[17] Debackere, K., & Veugelers, R. (2005). The role of academic technology transfer organizations in improving industry science links. Research policy, 34(3), 321-342.

[18] Yamamoto, K. (2004), Corporatization of National Universities in Japan: Revolution for Governance or Rhetoric for Downsizing?. Financial Accountability & Management, 20: 153–181.

[19] Fukuda, K.; Watanabe, M.; Korenaga, M.; Seimaru, K.; , "The progress of the strategic technology roadmap of METI (Ministry of Economy, Trade and Industry of Japan): Practical business cases and sustainable manufacturing perspective," Management of Engineering & Technology, 2008. PICMET 2008. Portland International Conference on , vol., no., pp.2102-2114, 27-31 July 2008

[20] [20] Chaojung Chen, Chihiro Watanabe, Charla Griffy-Brown (2007).The co-evolution process of technological innovation—An empirical study of mobile phone vendors and telecommunication service operators in Japan, Technology in Society, Volume 29, Issue 1, January 2007.

[21] Khawaja Amjad Saeed. (2006). The Economy of Pakistan . Karachi: Oxford University Press

[22] K. Ahmad and A. Hassan, "Policy Implications for Government and Higher Education in Pursuing Innovation," in Technology Management for the Global Future, 2006. PICMET 2006, 2006, pp. 957-966.

[23] Maryann P. Feldman, The University and Economics Development: The Case of Johns Hopkins University and Baltimore. Economics Development Quarterly, Vol. 8 No. 1, February 1994 67-76, 1994.

[24] D Lab: http://d-lab.mit.edu/

[25] M S Swaminathan Research Foundation (MSSRF) a Centre for Research: http://www.mssrf.org/

[26] Namal College of Pakistan http://www.namal.edu.p

[27] Fudenberg, D., & Tirole, J. (1991). Game theory. 1991: MIT Press.

[28] Hart, S., (2006), Robert Aumann's Game and Economic Theory, Scandanavian Journal of Economics 108, 185-211

[29] Alex Baker, Emily Oh Navarro, and Andr´e van der Hoek.Problems and Programmers: an Educational Software Engineering Card Game. In ICSE '03: Proceedings of the 25th International Conference on Software Engineering, pages 614–619,Washington, DC, USA, 2003. IEEE Computer Society.

[30] Emily Oh Navarro and Andr´e van der Hoek. SimSE: an Educational Simulation Game for Teaching the Software Engineering Process. In ITiCSE '04: Proceedings of the 9th annual SIGCSE conference on Innovation and technology in computer science education, pages 233–233, New York,NY, USA, 2004. ACM Press.

[31] W. Bian, A. I. Wang, J. E. Strom, and T. B. Kvamme, "An Evaluation of Using a Game Development Framework in Higher Education," in Software Engineering Education and Training, 2009. CSEET '09. 22nd Conference on, 2009, pp. 41-44.

[32] Roger A. McCain (2009). Game Theory and Public Policy. Edward Elgar Cheltenham, UK. Northampton, MA, USA

[33] Yong Cao; Sakai, H.; Xie-lin Liu; Nagahira, A.; Iguchi, Y.; , "Technology Catch-Up in China Compared with Japan: A New Development Model," Technology Management for the Global Future, 2006. PICMET 2006 , vol.3, no., pp.1030-1039, 8-13 July 2006

[34] Steenhuis, H.-J.; de Bruijn, E.J.; , "Innovation and technology based economic development: Are there short-cuts?," Management of Innovation and Technology, 2008. ICMIT 2008. 4th IEEE International Conference on , vol., no., pp.837-841, 21-24 Sept. 2008

[35] Robertson, S. et al. (2007). Globalisation, Education and Development: Ideas, Actors and Dynamics, Department for International Development, University of Bristol.

[36] Christian Aid (2004) The Politics of Poverty: Aid in the New Cold War, London: Christian Aid.

[37] Fasih Uddin & M Akram Swati, Pakistan's Economic Journey, Need for New Paradigm,Institute for Policy Studies, Islamabad, 2006

[38] Ladha, Krishna K. (2012), "Strategic Opportunities for Quality in Higher Education in India", IIM Kozhikode Society Management Review, Vol. 1 No. 2, July 2012, pg. 65-74.

[39] Khadria, Binod (2010), “The future of South Asian migration: a look at India, Pakistan and Bangladesh”, OECD Journal: General Papers, Vol. 2009/4.

[40] W. Dong, "Preliminary analysis on international business negotiation strategy in a game with incomplete information," in Information Management and Engineering (ICIME), 2010 The 2nd IEEE International Conference on, 2010, pp. 363-365.

[41] Ayesha Saleem, Kiyohide Higuchi (2012)“Globalization and ICT Innovation Policy: Absorption Capacity in developing Countries” IEEE the 14th International Conference on Advanced Communication Technology ICACT 2012, February 19-22, 2012, PyeongChang, Korea.

Ayesha Saleem has done Masters of Science in Information Technology. She had been awarded with the Gold Medal in Master of Information Technology after securing 1st Position. She has done Masters in Public Policy as well, from National Graduate Institute for Policy Studies (GRIPS), Japan. She is also certified Project Management Professional by Project Management Institute USA. She is doing PhD in GITS (Graduate School of Global Information and Telecommunication Studies), Waseda University, Tokyo, Japan.

She had been working in a World Bank’s Project titled “Land Records Management Information Systems” (LRMIS) in the capacity of Project Manager. She also has experience to work as section leader & team leader of configuration management/Software quality assurance Department in multinational software houses. These days, she is working as trainee in the Directorate for Science, Technology and Industry (DSTI), Economic Analysis and Statistics (EAS), Organization for Economic Co-operation and Development (OECD), Paris.

Kiyohide Higuchi is PhD in Economics from Graduate School of Economics, Waseda University. He had been Professor of School of Science & Engineering of Waseda University and Meikai University, Japan. Currently he is Professor of Graduate School of Global Information and Telecommunication Studies of Waseda University and Graduate School of International Culture and Communication of Waseda University, Japan.

He has published many books and research paper as author and co-author. His latest publications are: (1)"The way of new information and communications market-status and trends of information and communication in major countries and international organizations", International Telecommunication Union and the World Trade Organization (WTO) Sixth chapter PP.299-305(co-author)(foundation), International Communication Economic Research Institute Reviews, February 2004. (2) “The IT business strategy in open- platform era” second chapter representative “public policy outsourcing as IT Business” PP.12-22(co-author)(foundation), International Communication Economic Research Institution Reviews. March 2005. (3) “Fairness and effect of tolls”, Japan Transport Policy study Group Series A-418, 2006.

Robust Digital Image Cryptosystem Based on Nonlinear Dynamics of Compound Sine and Cosine Chaotic Maps for Private Data Protection

Sarun Maksuanpan, Tanachard Veerawadtanapong, Wimol San-Um

Intelligent Electronics Systems Research Laboratory

Faculty of Engineering, Thai-Nichi Institute of Technology, Patthanakarn Rd., Suanlaung, Bangkok, Thailand

sarun.maksuanpan@gmail.com, tanachad.p@gmail.com, and wimol@tni.ac.th

***Abstract*—this paper presents a digital image cryptosystem based on nonlinear dynamics of a compound sine and cosine chaotic map. The compound sine and cosine chaotic map is proposed for high-degree of chaos over most regions of parameter spaces in order to increase high-entropy random-bit sources. Image diffusion is performed through pixel shuffling and bit-plane separations prior to XOR operations in order to achieve a fast encryption process. Security key conversions from ASCII code to floating number for use as initial conditions and control parameters are also presented in order to enhance key-space and key-sensitivity performances. Experiments have been performed in MATLAB using standard color images. Nonlinear dynamics of the chaotic maps were initially investigated in terms of Cobweb map, chaotic attractor, Lyapunov exponent spectrum, bifurcation diagram, and 2-dimensional parameter spaces. Encryption qualitative performances are evaluated through pixel density histograms, 2-dimensional power spectral density, key space analysis, key sensitivity, vertical, horizontal, and diagonal correlation plots. Encryption quantitative performances are evaluated through correlation coefficients, NPCR and UACI. Demonstrations of wrong-key decrypted image are also included.**

***Keyword*— Digital Image Processing, Cryptosystem, Chaotic Map, Encryption, Decryption, Nonlinear Dynamics**

Manuscript received March 7, 2013. This work was financially supported by Research and Academic Services Division, Thai-Nichi Institute of Technology.

Sarun Maksuanpan is with computer engineering program, Faculty of Engineering, Thai-Nichi Institute of technology, Bangkok, Thailand. (E-mail: sarun.maksuanpan@gmail.com).

Tanachard Veerawadtanapong is with Computer Engineering Program, Faculty of Engineering, Thai-Nichi Institute of technology, Thailand. (E-mail: tanachad.pong@gmail.com).

Wimol San-Um is with the Intelligent Electronics Systems Research Laboratory, Faculty of Engineering, Thai-Nichi Institute of Technology, Bangkok, Thailand, Fax: (+662) 7632700, Tel: (+662) 7632600 Ext. 2926, (E-mail: wimol@tni.ac.th).

I. INTRODUCTION

RECENT advances in communications have led to great demand for secured image transmissions for a variety of applications such as medical, industrial and military imaging systems. The secured image transmissions greatly require reliable, fast and robust security systems, and can be achieved through cryptography, which is a technique of information privacy protection under hostile conditions [1]. Image cryptography may be classified into two categories, i.e. (1) pixel value substitution which focuses on the change in pixel values so that original pixel information cannot be read, and (2) pixel location scrambling which focuses on the change in pixel position. Conventional cryptography such as Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), and RSA algorithm may not be applicable in real-time image encryption due to large computational time and high computing power, especially for the images with large data capacity and high correlation among pixels [2].

Recently, the utilization of chaotic systems has extensively been suggested as one of a potential alternative cryptography in secured image transmissions. As compared to those of conventional encryption algorithms, chaos-based encryptions are sensitive to initial conditions and parameters whilst conventional algorithms are sensitive to designated keys. Furthermore, chaos-based encryptions spread the initial region over the entire phase space, but cryptographic algorithms shuffle and diffuse data by rounds of encryption [3]. Therefore, the security of chaos-based encryptions is defined on real numbers through mathematical models of nonlinear dynamics while conventional encryption operations are defined on finite sets. Such chaos-based encryption aspects consequently offer high flexibility in encryption design processes and acceptable privacy due to vast numbers of chaotic system variants and numerous possible encryption keys.

Chaos-based encryption algorithms are performed in two stages, i.e. the confusion stage that permutes the image pixels and the diffusion stage that spreads out pixels over the entire space. Most existing chaos-based encryptions based on such two-stage operations employ both initial conditions and control parameters of 1-D, 2-D, and 3-D chaotic maps such as Baker map [4,5], Arnold cat map [6,7], and Standard map [8, 9] for secret key generations. Furthermore, the combinations of two or three different maps have been suggested [10, 11] in order to achieve higher security levels. Despite the fact that such maps offer satisfactory security levels, iterations of maps require specific conditions of chaotic behaviors through a narrow region of parameters and initial conditions. Consequently, the use of iteration maps has become typical for most of proposed ciphers and complicated techniques in pixel confusion and diffusion are ultimately required.

This paper therefore presents an alternative chaos-based digital image cryptosystem with three main aspects. First, the compound sine and cosine chaotic maps, which potentially offers high-degree of chaos over most regions of parameter spaces, is proposed through nonlinear dynamics analyses and is consequently exploited as high-entropy random-bit sources for encryption. Second, image confusion and diffusion processes are performed through uncomplicated pixel shuffling and bit-plane separations prior to XOR operations in order to achieve a fast encryption process. Last, security key conversions from ASCII code to floating number for use as initial conditions and control parameters are also presented in order to enhance key-space and key-sensitivity performances.

II. PROPOSED ENCRYPTION ALGORITHMS

A category of trigonometric functions, involving sine and cosine maps, have potentially offered rich dynamic behaviours as described in a simple forms as [12] $x_{n+1}=\sin(ax_n)$ and $x_{n+1}=\cos(bx_n)$ where the constants a and b can be considered as the parameters associated the frequencies of sine and cosine functions, respectively. Although such sine and cosine maps offers relatively high complexity in terms of nonlinear dynamics, the chaotic regions in the bifurcation diagram is still insufficient due to periodic characteristics. This paper therefore considers an enhancement of sine and cosine maps through the combination between sine and cosine maps, i.e.

$$x_{n+1} = \cos(ax_n) + \sin(bx_n) \qquad (1)$$

As will be seen later, such a compound sine and cosine map in (1) offers high-degree of chaos over most regions of parameter spaces. As a nature of chaotic maps, the initial conditions and control parameters can be used as internal security keys that entirely set the encryption characteristics. The proposed cryptography technique attempts to achieve simple-but-highly-secured image encryption and decryption algorithms in a category of chaos-based cryptosystems. Fig.1 shows the proposed encryption and detection algorithms using compound sine and cosine maps. Three major procedures are summarized as follows;

First, the original image is prepared for diffusion. The original color image with $M \times N$ image size is initially converted into three sets of sub-images with RGB components containing pixels in grey scale levels. Each sub-image will subsequently be converted into binary matrix in which each pixel is represented by 8-bit binary numbers. For example, the pixel $p(1,1)$ contains the binary number p_0-p_7. Each pixel will then be separated into eight planes corresponding to binary bits p_0 to p_7. As a result, there are 24 sets of bit plane images represented in matrix forms with a single binary number in each pixel, which is ready for further Excusive-OR (XOR) operations.

Second, the input security keys from users which is represented in ASCII code with arbitrary 16 alphanumeric characters defined as $A=A_1A_2A_3,...,A_{16}$ will form two main sets of ASCII codes, i.e X_m and Y_m, for setting the initial conditions and the control parameters, respectively, where m = 1, 2, 3,...,8

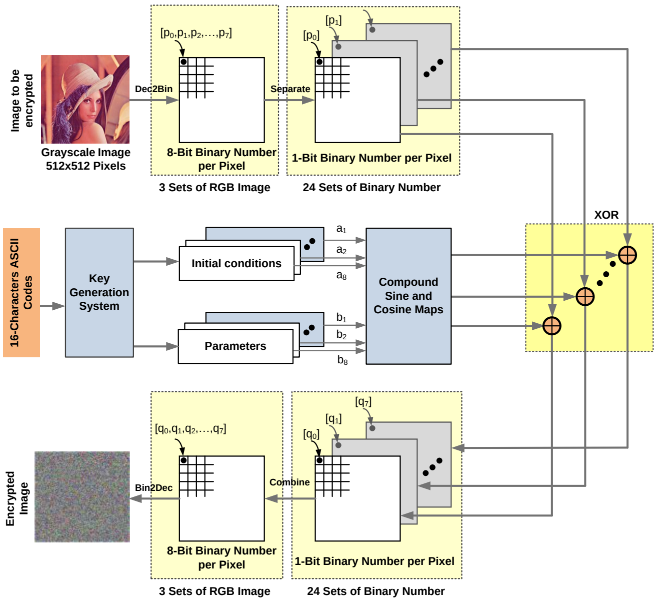


Fig. 1. Proposed pncryption algorithms using compound sine and consine chaotic maps.

TABLE I
SUMMARY OF 16-CHARACTERS INPUT ASCII CODES FOR SETTING INITIAL CONDITIONS AND CONTROL PARAMETERS

ASCII code X_m for Setting initial conditions		ASCII code Y_m for setting control parameters	
X_1	: $A_1A_4A_7A_{10}A_{13}A_{16}$	Y_1	: $A_1A_3A_5A_7A_9A_{11}$
X_2	: $A_2A_5A_8A_{11}A_{14}A_1$	Y_2	: $A_2A_4A_6A_8A_{10}A_{12}$
X_3	: $A_3A_6A_9A_{12}A_{15}A_2$	Y_3	: $A_3A_5A_7A_9A_{11}A_{13}$
X_4	: $A_4A_7A_{10}A_{13}A_{16}A_3$	Y_4	: $A_4A_6A_8A_{10}A_{12}A_{14}$
X_5	: $A_5A_8A_{11}A_{14}A_1A_4$	Y_5	: $A5A_7A_9A_{11}A_{13}A_{15}$
X_6	: $A_6A_9A_{12}A_{15}A_2A_5$	Y_6	: $A_6A_8A_{10}A_{12}A_{14}A_{16}$
X_7	: $A_7A_{10}A_{13}A_{16}A_3A_6$	Y_7	: $A_7A_9A_{11}A_{13}A_{15}A_1$
X_8	: $A_8A_{11}A_{14}A_1A_4A_7$	Y_8	: $A_8A_{10}A_{12}A_{14}A_{16}A_2$

as summarized in Table 1. Such two sets X_m and Y_m will be converted into 48-bit binary representations denoted by B_{X1} to B_{X48} and B_{Y1} to B_{Y48}, respectively. The real numbers are subsequently formed by converting the binary representation as follows;

$$R_{Xm} = (B_{X1} \times 2^0 + B_{X1} \times 2^1 + ... + B_{X48} \times 2^{47}) / 2^{48} \quad (2)$$

$$R_{Ym} = (B_{Y1} \times 2^0 + B_{Y1} \times 2^1 + ... + B_{Y48} \times 2^{47}) / 2^{48} \quad (3)$$

As a result, the initial conditions and the control parameters can be achieved by

$$a_m = (R_{Xm} \times R_{Ym}) \bmod 1 \quad (4)$$

$$b_m = (R_{Ym} \times R_{Ym+1}) \bmod 1 \quad (5)$$

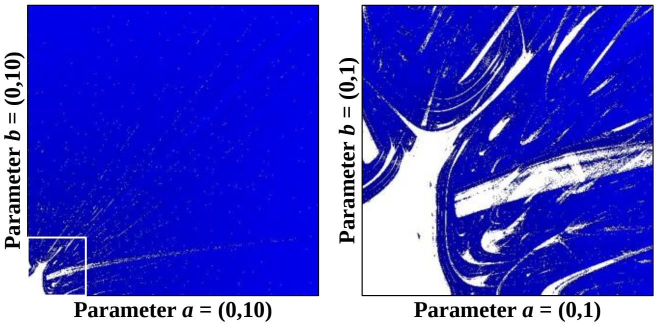
It is apparent that the values of a_m and b_m are in the region of (0,1) and are ready for use as internal security keys in the encryption algorithms. The design algorithm realizes eight chaotic maps based on (1) as follows;

$$x_{m,n+1} = \cos(b_m 10\pi x_n) + \sin(b_{m+1} 10\pi x_n) \quad (6)$$

It is seen in (4) that the constant 10π has been include in order to sustain the parameters a and b described in (1) in the region of (0, 10) which is sufficient to acquire chaos. The values of m are circularly shifted with 1 to 8, i.e. if the operation round reaches m+1=8 then the next value is 1. As results, a total 16 keys are employed as security keys in the encryption process. Such keys are used to generate chaotic signal from the compound sine and cosine chaotic maps. The output signals are adjusted to the binary number through the zero thresholds for the subsequent XOR operations.

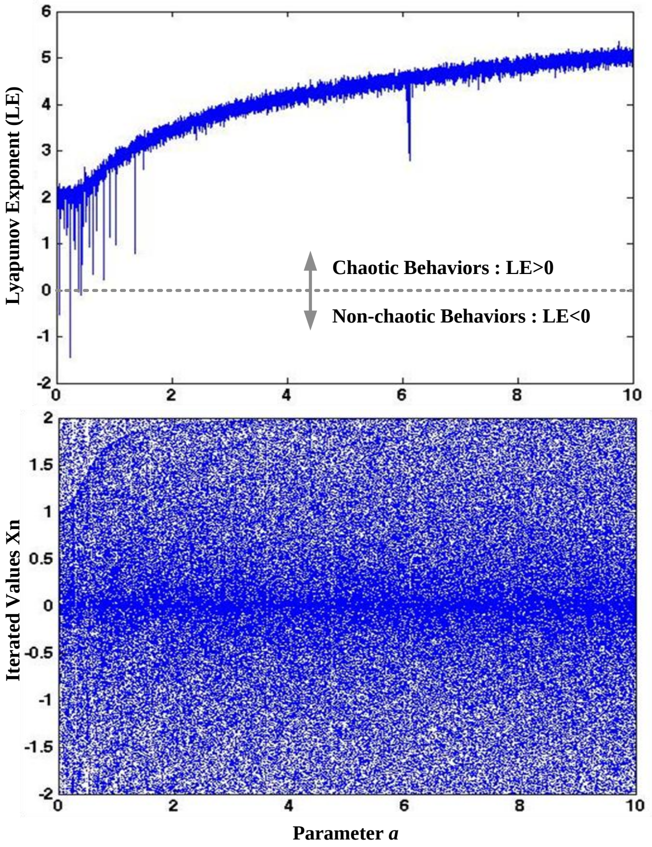
Last, the XOR operations diffuse the generated chaotic bit and the 24 binary images in parallel process. The XOR operation yields bit "1" if the two input bits are different, but yields bits "0" if the two inputs are similar. The results obtained from such XOR operations are 24 matrices with single binary number in each pixel. All the 24 matrices are combined into three RGB matrices of a single 8-bit matrix in which each pixel is represented by [b_0-b_7]. As a result, the encrypted image can be achieved. The decryption process also follows the encryption process in a backward algorithms as long as the security keys are known. It is seen in (4) that the constant 10π has been include in order to sustain the parameters a and b described in (1) in the region of (0, 10) which is sufficient to acquire chaos. The values of m are circularly shifted with 1 to 8, i.e. if the operation round reaches m+1=8 then the next value is 1. As results, a total 16 keys are employed as security keys in the encryption process. Such keys are used to generate chaotic signal from the compound sine and cosine chaotic maps. The output signals are adjusted to the binary number through the zero thresholds for the subsequent XOR operations.

Last, the XOR operations diffuse the generated chaotic bit and the 24 binary images in parallel process. The XOR operation yields bit "1" if the two input bits are different, but yields bits "0" if the two inputs are similar. The results obtained from such XOR operations are 24 matrices with single binary number in each pixel. All the 24 matrices are combined into



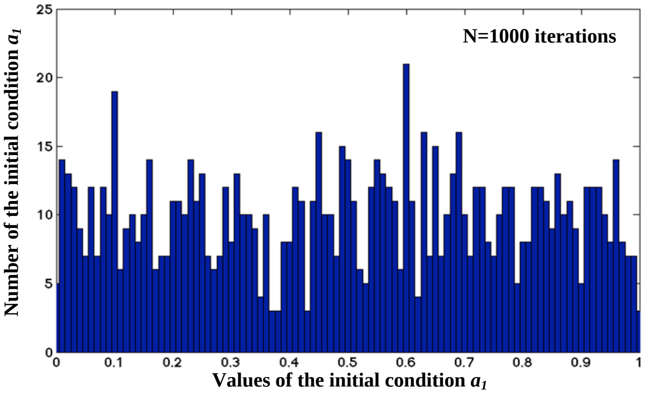
(a) (b)

Fig. 2. Plots of 2-D Lyapunov Exponent bifurcation structure between parameters a and b over the parameter space; (a) (0,10) and (b) the zoomed in region (0,1).



(b) (b)

Fig. 3. Plots of the Lyapunov exponent spectrum and the bifurcation diagram of parameters a over the parameter space (0,10) when the parameter b is fixed at 0.5.



(c) (b)

Fig. 4. Histrogram of numbers of initial conditions a_1.

three RGB matrices of a single 8-bit matrix in which each pixel is represented by [b_0-b_7]. As a result, the encrypted image can be achieved. The decryption process also follows the encryption process in a backward algorithms as long as the security keys are known.

III. Experimental Results

Experimental results have been performed in a computer–aid design tool MATLAB. Nonlinear dynamics of a compound sine and cosine map was initially simulated and encryption and decryption security performances were subsequently evaluated.

A. Nonlinear Dynamics of Compound Sine and Cosine Map

Since chaotic behaviors of the compound sine and cosine maps determine overall performance of the cryptosystem, Lyapunov exponent (LE) has been realized as a quantitative measure of chaoticity. The LE is defined as a quantity that characterizes the rate of separation of infinitesimally close trajectories and is given by

$$\mathrm{LE} = \lim_{n\to\infty} \frac{1}{N} \sum_{n=1}^{N} \log_2 \frac{dX_{n+1}}{dX_n} \qquad (7)$$

where N is the number of iterations. Typically, the positive LE indicates chaotic behaviors. The larger value of LE results in higher degree of chaos. Fig.1 shows the plots of 2-imensional Lyapunov Exponent bifurcation structure between parameters *a* and *b* over the parameter space (0, 10) and the zoomed in region (0, 1) where the chaotic region is represented by the dark blue color while the non-chaotic region is represented in the white region. It is shown in Fig.1 that the chaotic behaviors of the compound sine and cosine map occupy most of parameter spaces, leading to a very robust chaos for secret key generations. Nonetheless, the zoomed in region at small values of parameters *a* and *b* contain some non-chaotic regions, which represent quasi-chaotic or periodic behaviors. The proposed key generation system has been designed to potentially generates secret keys potentially since the nonchaotic signals will ultimately be LE spectrum and the bifurcation diagram of parameters *a* over the parameter space (0, 10) when the parameter *b* is fixed at 0.5. It is apparent in Fig.2 that the LE spectrum is greater than zero and growing to infinity. In addition, the bifurcation diagram shows dense area of the maximum values of X_n over the entire range. As for a particular example, Fig.3 shows the histograms of the numbers of the secret key a_1 for 1,000 iterations. It can be seen from Fig.3 that the nonlinear dynamics of the compound sine and cosine maps provide the random secret keys that distribute over the region (0, 1) randomly. Such characteristics have also found in other secret keys. The simulations have been ensured that the proposed compound the nonlinear dynamics of the compound sine and cosine maps and the key generation systems can potentially provide truly random values for diffusion process in the proposed cryptosystem.

B. Key Space Analysis

The encryption and decryption realizes the 16-character ASCII code “ABCDEFG012345678” as an input key and the wrong key changes the last character to 5. The resulting eight initial conditions and eight parameters, i.e. a total of 16 keys, are represented by 8-digit floating-point numbers. Considering each key in the form $S\times 2^E$ where *S* is a significand and *E* is an exponent, the keys that represented by 8 digits of a floating-point number ($\sim 3.4028\times 10^{38}$) results in 128 uncertain digits, which is greater than the minimum requirement of the 56-bit data ($\sim 7.2057\times 10^{16}$) encryption standard (DES) algorithm [23].

C. Histograms and 2D Power Spectral Analysis

The image histogram is a graph that illustrates the number of pixels in an image at different intensity values. In particular, the histogram of a color image can be separated into three sub-images with Red (R), Green (G), and Blue (B) components. Each sub-image has 256 different grey intensity levels, graphically displaying 256 numbers with distribution of pixels amongst these grayscale values. In addition, the 2D power spectrum that shows the power of image intensity can be obtained through a Discrete Fourier Transform (DFT) analysis and the algorithm is given by [24]

$$F(u,v) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y)\exp(-j(2\pi/M)ux)\exp(-j(2\pi/N)vy) \qquad (8)$$

where *x* and *y* are a coordinates pair of an image, M and N are the size of image, *f*(*x*, *y*) is the image value at the pixel (*x*, *y*). Fig.4 shows the histograms of three R, G, B components and 2D power spectrums of original image, encrypted image, decrypted image, and decrypted image with wrong keys. As for a particular demonstration, the original image is Lena image with 256×256 image size. It can be seen from Figs.4 that the intensities of all original images in the histogram are contributed with different values in a particular shape and the power spectrum is not flat having a peak of intensity in the

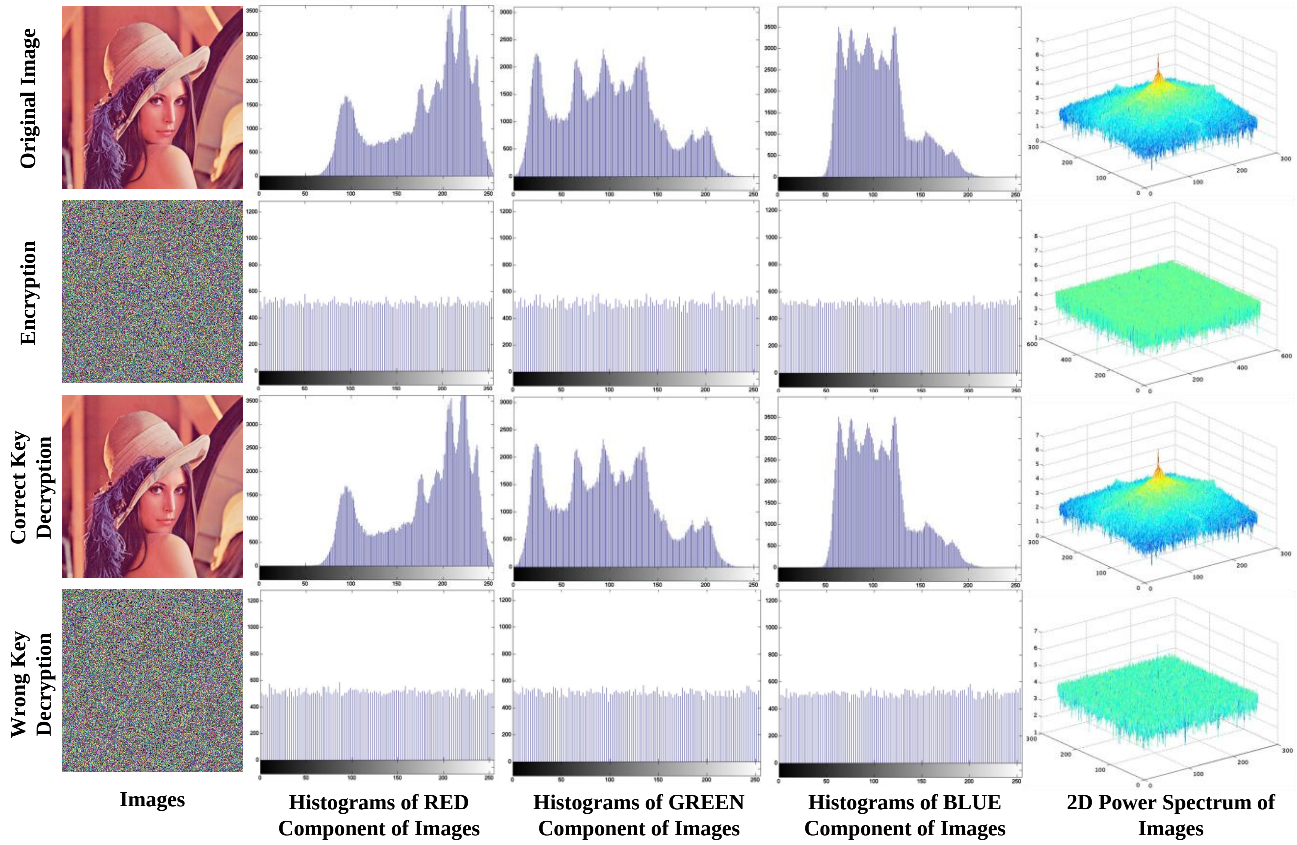


Fig.5. Histograms and 2D power spectrums of original image, encrypted image, decrypted image, and decrypted image with wrong keys.

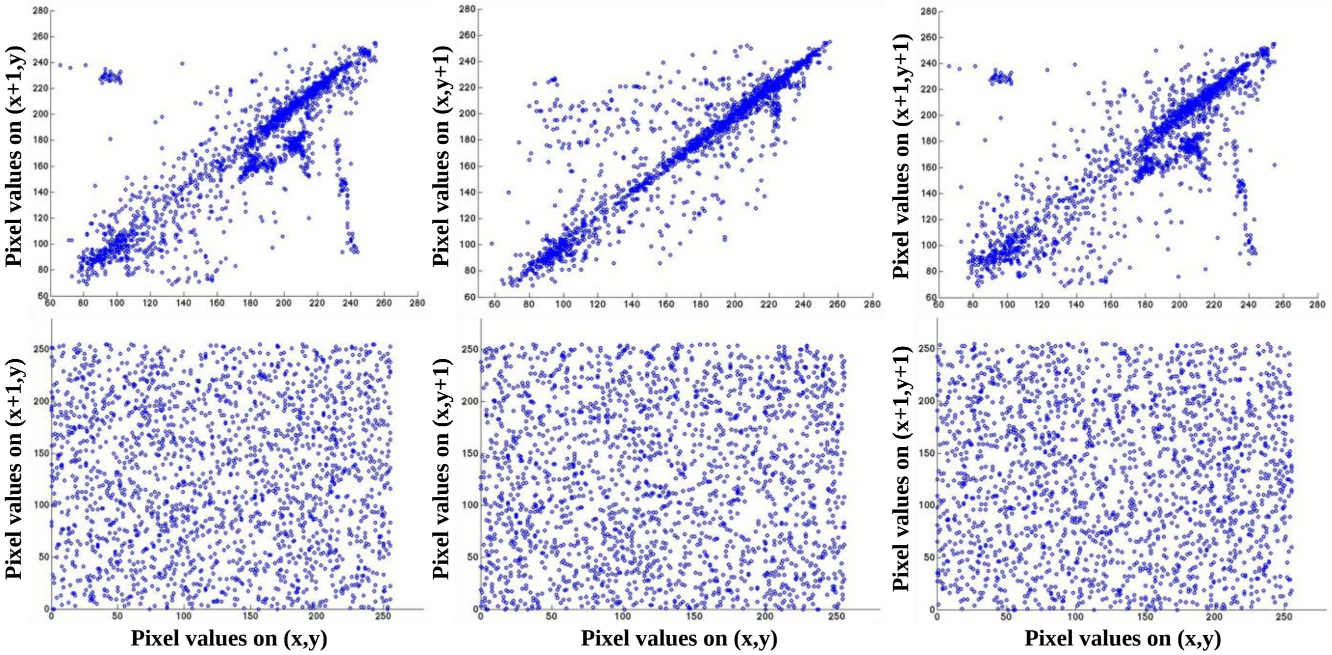
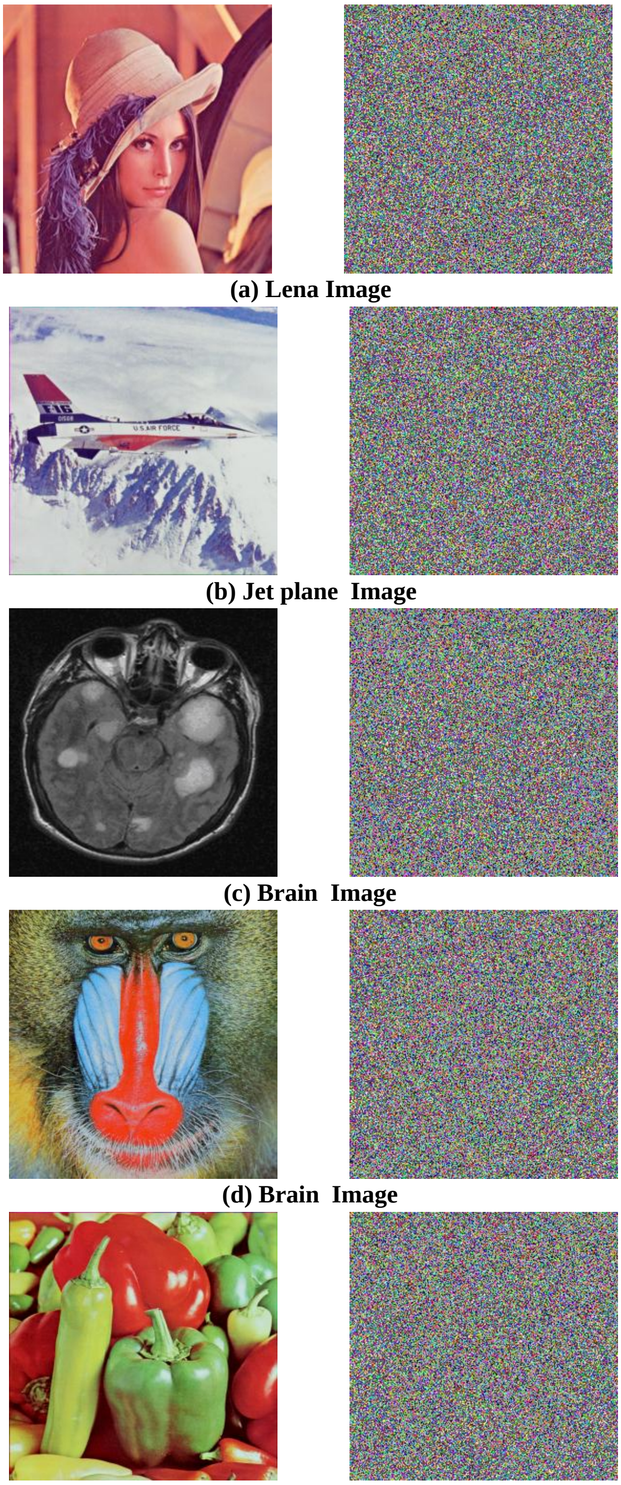


Fig.6. Image correlation tests in original and encrypted images, including horizontally, vertically, and diagonally adjacent pixels.

middle. The encrypted image has a flat histogram and power spectrum, indicating that the intensity values are equally contributed over all the intensity range and the original images are completely diffused and invisible. The decrypted images with right keys provide similar characteristics of the original images while the decrypted images with wrong keys are still diffused and the original images cannot be seen. These results qualitatively guarantee that the image is secured.



(a) Lena Image

(b) Jet plane Image

(c) Brain Image

(d) Brain Image

(e) Peppers Image

Fig. 7. Original and cipher images of five images for the experiments.

D. *Correlation Coefficient Analysis*

In order to quantify the encryption performance and key sensitivity analysis, correlation between image pairs, which is a measure of relationships between two pixels intensities of two images, of the three realized images have been analyzed. The covariance C_v and the correlation coefficient γ_{xy} can be obtained as follows [16-17];

$$\mathrm{C}_v(x,y)=\frac{1}{\mathrm{N}}\sum_{i=1}^{N}(x_i-\mathrm{E}(x))(y_i-\mathrm{E}(y)) \tag{9}$$

$$\gamma_{xy}=\frac{\mathrm{cov}(x,y)}{\sqrt{\mathrm{D}(x)}\sqrt{\mathrm{D}(y)}} \tag{10}$$

where the functions $E(x)$ and $D(x)$ are expressed as

$$\mathrm{E}(x)=\frac{1}{\mathrm{N}}\sum_{i=1}^{N}x_i \quad \text{and} \quad \mathrm{D}(x)=\frac{1}{\mathrm{N}}\sum_{i=1}^{N}(x_i-\mathrm{E}(x))^2 \tag{11}$$

and the variables x and y are grey-scale values of pixels in corresponding pixels in different images or two adjacent pixels in the same image. Typically, the value of γ_{xy} is in the region [-1, 1]. In other words, the values of γ_{xy} in the region (-1,0) and (0,1) respectively indicate positive and negative relationships, while the larger number close to 1 or -1 have stronger relationships. Using a random selection of 2,048 pairs of pixels, Fig.5 shows image correlation tests in original and encrypted images, including horizontally, vertically, and diagonally adjacent pixels. It can qualitatively be considered from Figs.5 that the adjacent pixels of all encrypted images are highly uncorrelated as depicted by scatters plots of correlations.

For the quantitative measures, the correlations between pairs of original images and corresponding encrypted images through the computation of correlation coefficient between RGB components of the original images and corresponding encrypted images have been analyzed. Table 2 summarizes correlation coefficients of 2,048 pixels of each image pair. It can be seen in Table 3 that the correlation coefficients are very small closing to zero, indicating that each pair of images are completely independent of each other. Fig.7 shows the original and cipher images of five images for the experiments, including Lena, Jet plane, Brain, Baboon and Peppers images. As for investigations of other images with different characteristics, comparisons of correlation coefficients of four standard images in MATLAB shown in Fig.7 are also studied. Table 3 summarizes correlation coefficients of 2,048 pixels of each pair of images shown in Fig.7. Apparently, the correlation coefficients are also very small. These results quantitatively guarantee that the image is secured.

E. *Original Image Sensitivity Analysis*

One minor change in the plain image causes significant changes in the encrypted image then such differential analysis may become inefficient, and therefore much difference between encrypted forms is expected in order to maintain high security level. NPCR (Net Pixel Change Rate) and UACI (Unified Average Changing Intensity) are two most common measures. NPCR concentrates on the absolute number of pixels which changes value in differential attacks while the UACI focuses on the averaged difference between two paired encrypted images

TABLE II
COMPARISONS OF CORRELATION COEFFICIENTS OF LENA IMAGE AT DIFFERENT SIZES.

Image Sizes	C_{RR}	C_{RG}	C_{RB}	C_{GR}	C_{GG}	C_{GB}	C_{BR}	C_{BG}	C_{BB}
256×256	0.00312	0.00298	-0.00406	0.00195	0.00061	-0.00267	0.00052	-0.00061	-0.00419
512×512	-0.00306	-0.00325	-0.00099	-0.00421	-0.00211	-0.00153	-0.00367	-0.00060	-0.00108
1024×1024	0.00181	-0.00081	0.00033	0.00113	-0.00056	-0.00053	0.00077	0.00008	-0.00063

TABLE III
COMPARISONS OF CORRELATION COEFFICIENTS OF DIFFERENT IMAGE WITH 256×256 IMAGE SIZE.

Images	C_{RR}	C_{RG}	C_{RB}	C_{GR}	C_{GG}	C_{GB}	C_{BR}	C_{BG}	C_{BB}
Brain	0.00259	-0.00123	-0.00270	0.00259	-0.00121	-0.00271	0.00261	-0.00128	-0.00269
Mandril	-0.00044	0.00735	-0.00606	0.00265	0.00657	-0.00625	0.00340	0.00194	-0.00613
Peppers	0.00429	-0.00456	-0.00240	0.00524	-0.00076	-0.00152	0.00129	-0.00378	-0.00152
Jet Plane	-0.00111	-0.00588	-0.00644	-0.00087	-0.00347	-0.00601	-0.00126	-0.00362	-0.00488

TABLE IV
SUMMARY OF NPCR AND UACI OF DIFFERENT IMAGE WITH 256×256 IMAGE SIZE.

Images	$NPCR_R$	$NPCR_G$	$NPCR_B$	$UACI_R$	$UACI_G$	$UACI_B$
Lena	99.2020	98.4085	99.2020	33.4107	33.4309	33.5449
Brain	99.2048	98.4956	99.3125	33.4488	33.3952	33.3707
Mandril	99.5102	99.0132	99.4123	33.5100	33.3507	33.4846
Peppers	99.4262	99.2144	99.2314	33.4387	33.3085	33.5637
Jet Plane	99.2436	98.9485	99.3345	33.4456	33.3845	33.4562

[17]. For the two encrypted images in which the corresponding original images have only one pixel difference are denoted by C^1 and C^2. Label the greyscale values of the pixels at pixel (i,j) in C^1 and C^2 by C^1(i,j) and C^2(i,j), respectively. Define a bipolar array *D*, with the same size as images C^1 and C^2. Consequently, *D*(i,j) is determined by C^1(i,j) and C^2(i,j), if C^1(i,j) =C^2(i,j) then *D*(i,j)=1, otherwise, *D*(i,j)=0. The NPCR [21] is defined as

$$NPCR = \frac{\sum_{i,j} D(i,j)}{T} \times 100\% \tag{12}$$

$$UACI = \left(\frac{\sum_{i,j} D(i,j)}{T} \right) \times 100\% \tag{13}$$

where *T* denotes the total number pixels in the encrypted image, *F* denotes the largest supported pixel value compatible with the cipher image format, and |.| denotes the absolute value function. Table 4 summarizes the values of NPCR and UACI for different image with the sizes of 256×256. It can be seen that the NPCR are relatively close to 100% and the UACI are also in the acceptable region of approximately 33%.

F. Information Entropy Analysis

The entropy *H*(*s*) is one of important characteristics of the randomness and can be found by

$$H(s) = \sum_{i=0}^{2^M - 1} P(S_i) \log_2 \frac{1}{P(S_i)} \tag{12}$$

where *P*(S_i) represents the probability of symbols *i*. In the case where a purely random source producing 2*M* symbols, the entropy is given by *H*(*s*)=*M*. If the output of a cipher image produces the number of symbols with the entropy value of less than *M*, there is a certain degree of predictability which intimidates its security. Table 5 summarizes the results of information entropy of those five standard images in Fig.7. The values obtained are very close to the theoretical value of *M*=8, indicating that information leakage during encryption process is negligible and the encryption system is secure against the entropy attack.

TABLE V
RESULTS OF INFORMATION ENTROPY OF FIVE STANDARD IMAGES

Images	Entropy H(s)
Lena	7.99915
Brain	7.99924
Mandril	7.99910
Peppers	7.99896
Jet Plane	7.99923

CONCLUSION

A robust digital image cryptosystem based on nonlinear dynamics of a compound sine and cosine chaotic map has been presented. The compound sine and cosine chaotic map has been proposed for high-degree of chaos over most regions of parameter spaces in order to increase high-entropy random-bit sources. Image diffusion has been performed through pixel shuffling and bit-plane separations prior to XOR operations in order to achieve a fast encryption process. Security key conversions from ASCII code to floating number for use as initial conditions and control parameters were also presented to enhance key-space and key-sensitivity performances. Nonlinear dynamics of the chaotic maps have been investigated in terms of chaotic attractor, Lyapunov exponent spectrum, bifurcation diagram, and 2-dimensional parameter spaces. Encryption qualitative performances were evaluated through pixel density histograms, 2-dimensional power spectral density, key space analysis, key sensitivity, vertical, horizontal, and diagonal correlation plots. Encryption quantitative performances were evaluated through correlation coefficients, NPCR and UACI. Demonstrations of wrong-key decrypted image are also included. The proposed cryptosystem offers a potential alternative to private data protection systems.

REFERENCES

[1] M. Philip, "An Enhanced Chaotic Image Encryption" International Journal of Computer Science, Vol. 1, No. 5, 2011.

[2] G.H. Karimian, B. Rashidi, and A.farmani, "A High Speed and Low Power Image Encryption with 128- bit AES Algorithm", International Journal of Computer and Electrical Engineering, Vol. 4, No. 3, 2012.

[3] G. Chen, Y. Mao, C.K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps", Chaos, Solitons and Fractals, Vol. 21, pp. 749-761, 2004.

[4] X. Tong, M. Cui, "Image encryption scheme based on 3D baker with dynamical compound chaotic sequence cipher generator", Signal Processing, Vol. 89, pp. 480-491, 2009.

[5] J.W. Yoon, H. Kim,"An image encryption scheme with a pseudorandom permutation based on chaotic maps", Commun Nonlinear Sci Number Simulation, Vol. 15, pp. 3998–4006, 2010.

[6] X. Ma, C. Fu, W. Lei, S. Li, "A Novel Chaos-based Image Encryption Scheme with an Improved Permutation Process", International Journal of Advancements in Computing Technology, Vol. 3, No. 5, 2011.

[7] K. Wang, W. Pei, L. Zou, A. Song, Z. He, "On the security of 3D Cat map based symmetric image encryption scheme", Physics Letters A, Vol. 343, pp. 432–439, 2005.

[8] K. Wong, B. Kwok, and W. Law, "A Fast Image Encryption Scheme based on Chaotic Standard Map", Physics Letters A, Vol. 372, pp. 2645-2652, 2008.

[9] S. Lian, J. Sun, Z. Wang, "A block cipher based on a suitable use of the chaotic standard map", Chaos, Solitons and Fractals, Vol. 26, pp. 117–129, 2005.

[10] K. Gupta, S. Silakari, "New Approach for Fast Color Image Encryption Using Chaotic Map", Jour. of Information Security, pp. 139-150, 2011

[11] F. Huang, Y. Feng, "Security analysis of image encryption based on two-dimensional chaotic maps and improved algorithm", Front. Electr. Electron. Eng. China, Vol. 4, No. 1, pp. 5-9, 2009.

[12] G.Lee and N. H. Farhat , "Parametrically Coupled Sine Map Networks" ,Electrical Engineering Department, University of Pennsylvania, Philadelphia, PA, USA,15 December 2000

[13] F.Sun, S. Liu , Z. Li , Z. Lu , "A novel image encryption scheme based on spatial chaos map",College of Control Science and Engineering, Shandong University, Jinan , PR China , pp. 631–640 , 2008

[14] Q. Gong-bin, J. Qing-feng,Q. Shui-sheng, "A new image encryption scheme based on DES algorithm and Chua's circuit", Imaging Systems and Techniques, pp. 168 – 172, 2009.

[15] Z. Peng, T.B. Kirk, "Two-dimensional fast Fourier transform and power spectrum for wear particle analysis", Tribology International, Vol. 30, Issue. 8, pp. 583-590, 1997.

[16] A. Yahya and A. Abdalla, "A Shuffle Image-Encryption Algorithm", J. Comput. Sci,pp.999-1002

[17] Y.Wu, Joseph P. Noonan, S.Agaian, "NPCR and UACI Randomness Tests for Image Encryption", Department of Electrical and Computer Engineering Tufts UniversityMedford, MA ,USA

Sarun Maksuanpan was born in Samutsakorn Province, Thailand in 1991. He received B.Eng. in Computer Engineering from Computer Engineering Department, Faculty of Engineering, Thai-Nichi Institute of Technology (TNI). Currently, he is also a research assistant at Intelligent Electronic Research Laboratory. His research interests include information security systems, cryptosystems, artificial neural networks, and digital image processing.

Tanachard Veerawadtanapong was born in Bangkok, Thailand in 1992. He received B.Eng. in Computer Engineering from Computer Engineering Department, Faculty of Engineering, Thai-Nichi Institute of Technology (TNI). Currently, he is also a research assistant at Intelligent Electronic Research Laboratory. His research interests include Ad Hoc mobile network, cryptosystems, and chaos theory.

Wimol San-Um was born in Nan Province, Thailand in 1981. He received B.Eng. Degree in Electrical Engineering and M.Sc. Degree in Telecommunications in 2003 and 2006, respectively, from Sirindhorn International Institute of Technology (SIIT), Thammasat University in Thailand. In 2007, he was a research student at University of Applied Science Ravensburg-Weingarten in Germany. He received Ph.D. in mixed-signal very large-scaled integrated circuit designs in 2010 from the Department of Electronic and Photonic System Engineering, Kochi University of Technology (KUT) in Japan. He is currently with Computer Engineering Department, Faculty of Engineering, Thai-Nichi Institute of Technology (TNI). He is also the head of Intelligent Electronic Systems (IES) Research Laboratory. His areas of research interests are chaos theory, artificial neural networks, control automations, digital image processing, secure communications, and nonlinear dynamics of chaotic circuits and systems.

DVB-RCS: Efficiently Quantized Turbo Decoder

Sherif Welsen Shaker

University of Nottingham, Ningbo Campus, P.R. China

welsen@ieee.org

***Abstract*—Turbo codes have been incorporated into many important wireless communication standards including the satellite return channel in DVB-RCS standards. According to their iterative nature, the computational complexity of turbo decoder is much higher than that of convolutional FEC decoders. From the hardware implementation point of view, the complexity can be reduced by using quantized decoder. For DVB-RCS turbo coding, there are many block sizes and different code rates. In order to realize the DVB-RCS turbo decoder efficiently, an algorithm should be developed for the best computation of quantization range for each code rate and at different signal-to-noise ratios. This paper investigates the decoder input quantization of low complexity decoding algorithm and proposes an algorithm for efficient decoder quantization by introducing a scaling factor into the decoding algorithm, aiming to achieve significant improvement in the hardware implementation of the decoder architecture.**

***Index Terms*— DVB-RCS; Max-log-MAP; Quantization; Turbo Decoder; Reduced Complexity**

I. Introduction

FOUNDED by the European Telecommunications Standards Institute (ETSI) in 1993, the Digital Video Broadcasting (DVB) project intended to standardize the digital television services. DVB-S was the initial standard of digital television with satellite delivery, that used a concatenation of an outer (204,188) byte shortened Reed Solomon code and an inner constraint length 7, variable rate (r ranges from 1/2 to 7/8) convolutional code [1]. DVB-S was a widely accepted standard in the forward link of broadband satellite communications. The second generation DVB-S2 includes the transmission of multimedia contents and a variety of uni-cast and multicast services. Internet over DVB-S is a natural competitor against cable modem and DSL technology, and its universal coverage allows even the most remote areas to be served. Because DVB-S only provides a downlink, an uplink is also needed to enable interactive applications such as web browsing. The uplink and downlink need not be symmetric, since many Internet services require a faster downlink.

Transmitting an uplink signal back to the satellite over the same antenna used for receiving the downlink signal, rather than using a telephone modem, became an attractive alternative for the subscriber equipment. . DVB-RCS standards have been approved for Return Channel via Satellite; it provides two-way, full IP, asymmetric communications via satellite. In this way not only the service can be quickly deployed, but the cost of the service and the quality are independent of the distance between the terminal and access point. This makes the service provided via the satellite a strong competitor in those cases where cable modems are not economically possible. However, given the small antenna aperture and requirement for a low-cost, low-power amplifier, there is very little margin on the uplink. Therefore, strong FEC coding is desired. Turbo codes have shown great performance among forward error correction (FEC) codes; they have been used by many standards like Wideband CDMA, and Third Generation Partnership Project (3GPP) for IMT-2000. For its major advancement in channel coding area, convolutional turbo code are well-suited for mobile satellite broadcasting applications and it has been chosen for DVB-RCS standards [2]. The big advantage of turbo codes is their data transmission reliability within a half decibel of Shannon Limit.

DVB-RCS standards are open to provide interactive broadband access over satellite. It allows a central gateway or hub to broadcast IP date on the forward link in the DVB/MPEG2 format to large number of small terminals with date rates up to 48 Mbit/s. Satellite terminals can send return signals to the hub on the forward link. Twelve frame sizes are supported ranging from 12 bytes to 216 bytes, including 53 byte frame compatible with ATM and a 188 byte frame compatible with both MPEG-2 and the original DVB-S standard. The return link supports data rates from 144 kbps to 2 Mbps and is shared among terminals by using multi-frequency time-division multiple-access (MF-TDMA) and demand-assigned multiple-access (DAMA) techniques. DVB-RCS turbo code was optimized for short frame sizes and high data rates; it supports seven code rates, 1/3, 2/5, 1/2, 2/3, 3/4, 4/5, and 6/7. The outstanding coding performance of those codes requires the investigation of hardware implementation issues. For portable radio terminal, low power consumption is a key implementation issue. Decoding algorithm simplification and quantization are very important issues leading to reduction of power consumption. In the past, several algorithms have been used in order to simplify the decoding process of turbo codes.

Manuscript received July, 27 2013.

S.W. Shaker, is with EEE Dpt., Faculty of Science and Engineering, University of Nottingham Ningbo, P. R. China (Tel: +86 147 149 175 34; e-mail: welsen@ieee.org).

The penalty paid for those algorithms which aim to reduce the complexity is small error rate performance degradation as compared to the performance achieved in case of using the optimal algorithm. An additional correction term is required to be added in order to minimize the performance degradation.

In this paper, our intention is to apply a simplified decoding algorithm for DVB-RCS turbo codes. It is our objective to investigate the impact of the decoder quantization on the requirement of the decoder performance. The paper proposes an algorithm for efficient decoder quantization that can be applied on different DVB-RCS code rates and block sizes in order to achieve a reduced decoder complexity. The structure of DVB-RCS turbo encoder followed by a brief review of turbo decoding algorithms is introduced, for interested reader, in section II. The structure of DVB-RCS turbo decoder is then highlighted for the Duobinary case. The quantized decoder is discussed in section III. In section IV, simulation results are presented for different frame lengths and code rates of DVB-RCS turbo codes. The effect of quantized decoder is then investigated, and the algorithm for efficient decoding quantization is proposed and tested.

II. DVB-RCS TURBO CODES

DVB-RCS turbo encoder is composed of two identical Recursive Systematic Convolutional (RSC) encoders along with Log-MAP or Max-log-MAP decoding [3]. If the encoder begins and ends at a known state, such as the all-zeros state, the decoder for each constituent code performs better. One alternative to do this is by independently terminating the trellis of each encoder with a tail, which forces the encoder back to the all-zeros state. However, forcing the encoder to a known state at the end of the encoding stage by adding tail bits, presents two major drawbacks: First, the minimum free distance dfree is no longer equal to the original minimum free distance for all information data. Second, the spectral efficiency of the transmission is degraded specially for small frame lengths supported by DVB-RCS [4]. The other alternative to terminate the trellis of the code is done by using Circular Recursive Systematic Convolutional (CRSC) encoding [5]. CRSC start the encoding at the circular state Sc, and end the encoding in the same state without the aforementioned drawbacks.

DVB-RCS turbo code uses duobinary constituent encoders defined over GF(4) instead of using binary encoders defined over GF(2). The double binary turbo codes have several benefits compared with classical turbo codes, which use RSC single binary codes, [6]: (a) Reducing the correlation effects between the component decoders, improves the performance. (b) Introducing periodic disorder in the symbols increases the minimum free distance. (c) Duobinary codes are less sensitive to puncturing than the single binary codes; hence puncturing can be used to increase the code rate and data rate. (d) The trellis contains half as many states as a binary code of identical constraint length (but the same number of edges), and therefore needs half as much memory, and the decoding hardware can be clocked at half the rate as a binary code. (e) Suboptimal but efficient Max-log-MAP algorithm at a cost of only about 0.1-0.2 dB relative to the optimal log-MAP algorithm can be used to decode the duobinary code; this is in contrast with binary codes, which lose about 0.3-0.4 dB when decoded with the Max-log-MAP algorithm [7]. Additionally, duobinary codes are less impacted by the uncertainty of the starting and ending states when using tail biting, and perform better than their binary counterparts when punctured to higher rates.

A. DVB-RCS Encoder Structure

The block diagram of the turbo encoder that is used by DVB-RCS is shown in Figure 1, and the CRSC constituent encoder is shown in Figure 2 as described in the standardized DVB-RCS. The encoder is fed blocks of k message bits which are grouped into N = k/2 couples. The number of couples per block can be N ∈ {48, 64, 212, 220, 228, 424, 432, 440, 752, 848, 856, 864}. The number of bytes per block is N/4. In Figure 2, A represents the first bit of the couple, and B represents the second bit. The two parity bits are denoted W and Y [8].

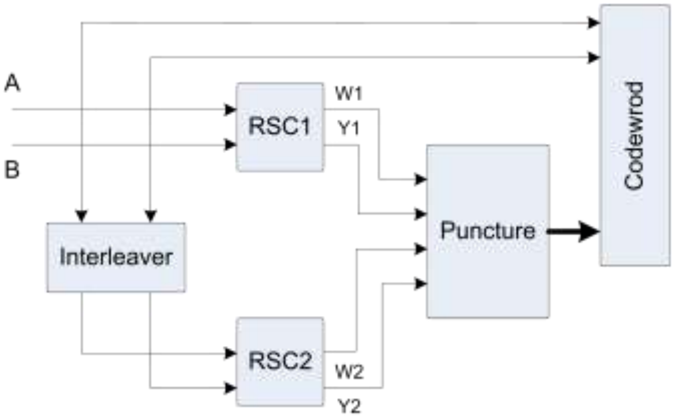


Fig. 1. Block diagram of DVB-RCS Turbo encoder.

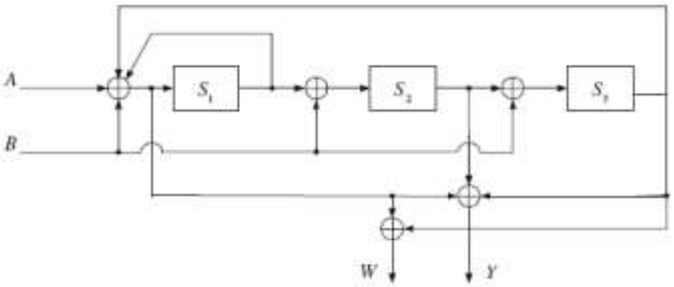


Fig. 2. Duobinary CRSC constituent encoder used by DVB-RCS.

The block must be encoded twice by each constituent encoder because of the tail biting nature of the code. First, the encoder is initialized to the all-zeros state, $\mathbf{S}_0 = [0\ 0\ 0]$. After the block is encoded, the final state of the encoder $\mathbf{S}_N$ is used to derive the circulation state. The circulation state $\mathbf{S}_c$ is given by:

$$\mathbf{S}_c = (\mathbf{I} + \mathbf{G}^N)^{-1}\mathbf{S}_N \tag{1}$$

where

$$G = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \tag{2}$$

In practice, the circulation state $\mathbf{S}_c$ can be found from $\mathbf{S}_N$ by using a lookup table [2]. Once the circulation state is found, the data is encoded again. This time, the encoder is set to start in state $\mathbf{S}_c$ and will be guaranteed to also end in state $\mathbf{S}_c$.

B. Turbo Decoding Algorithms

In a typical turbo decoding system, two decoders operate iteratively and pass their decisions to each other after each iteration. These decoders should produce soft-outputs to improve the decoding performance. Such a decoder is called a soft-input soft-output (SISO) decoder [9]. Each decoder operates not only on its own input, but also on the other decoder's incompletely decoded output, which resembles the operation principle of turbo engines. Generally, we assume that the encoded information sequence, X_k, is transmitted over an additive white gaussian noise (AWGN) channel, and a noisy received sequence, Y_k, is obtained. In binary case, each decoder calculates the log-likelihood ratio (LLR) for the k^{th} data bit d_k, as follows:

$$L(d_k) = \log\left[\frac{P(d_k = 1 \mid Y)}{P(d_k = 0 \mid Y)}\right] \quad (3)$$

The LLR can be decomposed into three independent terms as:

$$L(d_k) = L_{apri}(d_k) + L_c(d_k) + L_e(d_k) \quad (4)$$

where $L_{apri}(d_k)$ is the a priori information of d_k, $L_c(d_k)$ is the channel measurement, and $L_e(d_k)$ is the extrinsic information exchanged between the constituent decoders. LLR computations can be performed by using one of the two main turbo decoding algorithms: Soft Output Viterbi Algorithm (SOVA) [10] and Maximum A posteriori Probability (MAP) [3]. The difference between the two algorithms is that, MAP algorithm seeks for the most likely data sequence, while SOVA seeks for the most likely connected trellis path. MAP algorithm is superior to SOVA specially at low SNR at the expense of implementation complexity.

1) MAP Algorithm

MAP is the optimal but computationally complex algorithm. According to this algorithm, LLR values for each information bit can be calculated as:

$$L(d_k) = \ln\left[\frac{\sum_{S_k}\sum_{S_{k-1}}\gamma_1(S_{k-1}, S_k)\alpha(S_{k-1})\beta(S_k)}{\sum_{S_k}\sum_{S_{k-1}}\gamma_0(S_{k-1}, S_k)\alpha(S_{k-1})\beta(S_k)}\right] \quad (5)$$

where α is the forward state metric, β is the backward state metric, γ is the branch metric, and S_k is the trellis state at time instant k. At state k, the forward state metric, $\alpha_k(S_k)$ is given by:

$$\alpha_k(S_k) = \sum_{j=0}^{1}\alpha_{k-1}(S_{k-1})\gamma_j(S_{k-1}, S_k) \quad (6)$$

The backward state metric, $\beta_k(S_k)$ is given by:

$$\beta_k(S_k) = \sum_{j=0}^{1}\beta_{k+1}(S_{k+1})\gamma_j(S_k, S_{k+1}) \quad (7)$$

The branch metric for each possible transition can be calculated as:

$$\gamma_i(S_{k-1}, S_k) = A_k P(S_k \mid S_{k-1})\exp\left[\frac{2}{N_o}(y_k^S x_k^S(i) + y_k^p x_k^p(i, S_{k-1}, S_k))\right] (8)$$

where A_k is a constant, x_k^S and x_k^p are the transmitted systematic data and parity bits at the transmitter side, and y_k^S, y_k^p are the received noisy bits at the receiver side, respectively.

2) Log-MAP Algorithm

It is a simplified version of MAP algorithm to avoid the mathematical computations complexity. Log-MAP performs the calculations in the logarithmic domain by replacing the exponential and logarithm by the max* operator as follows:

$$\max{}^*(x, y) = \ln(e^x + e^y) = \max(x, y) + \log(1 + e^{-|y-x|}) \quad (9)$$

where the term log $(1+e^{-|y-x|})$ is a correction function that can be calculated by using look-up table.

3) Max-Log-MAP algorithm

It approximates the computation of max* operator in Log-MAP algorithm for the sake of simplicity by omitting the correction term, log $(1+e^{-|y-x|})$ to become as follows:

$$\ln(e^x + e^y) \approx \max(x, y) \quad (10)$$

From the hardware implementation point of view, the complexity is reduced at the expense of decoder performance degradation [7]

C. DVB-RCS Decoder Structure

The decoding process of turbo codes involves the iterative exchange of extrinsic information between the two component decoders. In binary case, only two types of transmitted symbols are possible, 0 or 1. In the decoding process of DVB-RCS code, the case is duobinary which is more complicated. In this case, four types of transmitted symbols are possible, (00, 01, 10, or 11). The corresponding likelihood ratios are as follows:

$$\frac{P(d_k = 00/y)}{P(d_k = 00/y)} = \frac{P(d_k = 00/y)\cdot P(d_k = 00)}{P(d_k = 00/y)\cdot P(d_k = 00)} \quad (11)$$

$$\frac{P(d_k = 01/y)}{P(d_k = 00/y)} = \frac{P(d_k = 01/y)\cdot P(d_k = 01)}{P(d_k = 00/y)\cdot P(d_k = 00)} \quad (12)$$

$$\frac{P(d_k = 10/y)}{P(d_k = 00/y)} = \frac{P(d_k = 10/y)\cdot P(d_k = 10)}{P(d_k = 00/y)\cdot P(d_k = 00)} \quad (13)$$

$$\frac{P(d_k = 11/y)}{P(d_k = 00/y)} = \frac{P(d_k = 11/y)\cdot P(d_k = 11)}{P(d_k = 00/y)\cdot P(d_k = 00)} \quad (14)$$

where, d_k represents the transmitted symbol at time instant k, and y is the received continuous valued noisy symbol.

Performing the decoding in the log-domain is more preferred than in the probability domain since the low complexity Max-log-MAP algorithm can then be applied [3]. Unlike the decoder for a binary turbo code, which can represent each binary symbol as a single log-likelihood ratio, the decoder for a duobinary code requires three log-likelihood ratios. For example, the likelihood ratios for message couple (A_k, B_k) can be represented in the form:

$$\Lambda_{a,b}(A_k, B_k) = \log \frac{P(A_k = a, B_k = b)}{P(A_k = 0, B_k = 0)} \qquad (15)$$

where (a, b) can be (0, 1), (1, 0), or (1, 1).

Figure 3 shows the iterative decoder that can be used to decode the DVB-RCS turbo code. $\{\Lambda_{a,b}^{(i)}(A_k, B_k)\}$ denotes the set of LLRs corresponding to the message couple at the input of the decoder and $\{\Lambda_{a,b}^{(o)}(A_k, B_k)\}$is the set of LLRs at the output of the decoder. The input LLR values are provided to each decoder along with the received values of the parity bits generated by the corresponding encoder (in LLR form). The decoder can produce the updated LLRs $\{\Lambda_{a,b}^{(o)}(A_k, B_k)\}$ at its output by using these inputs and the knowledge of the code constraints. As with binary turbo codes, extrinsic information is passed to the other constituent decoder instead of the raw LLRs. This prevents the positive feedback of previously resolved information. Extrinsic information is found by simply subtracting the appropriate input LLR from each output LLR, as indicated in Figure 3.

It is fairly straightforward to extend the log-MAP and max-log-MAP algorithms [3] to the duobinary case. Each branch must be labeled with the log-likelihood ratios corresponding to the systematic and parity couples associated with that branch. Because QPSK modulation is orthogonal, the LLR of message couple (A,B) can be initialized prior to being fed into the first decoder as $\Lambda_{a,b}^{(i)}(A_k, B_k) = a\,\Lambda(A_k) + b\,\Lambda(B_k)$, where $\Lambda(C) = \log[P(C = 1)/P(C = 0)]$. Since the extrinsic information about the parity bits is not exchanged, the parity bits can always be decomposed in a similar manner. However, for the systematic bits, the three likelihood ratios defined in (15) must be calculated during each iteration and exchanged between the decoders.

Now let $\gamma_k(\mathbf{S}_i \rightarrow \mathbf{S}_j)$ denote the branch metric corresponding to state transition $\mathbf{S}_i \rightarrow \mathbf{S}_j$ at time k. The branch metric depends on the message and parity couples that label the branch along with the channel observation and extrinsic information at the decoder input. In particular, if transition $\mathbf{S}_i \rightarrow \mathbf{S}_j$ is labelled by $(A_k, B_k, W_k, Y_k) = (a, b, w, y)$ then the branch metric $\gamma_k(\mathbf{S}_i \rightarrow \mathbf{S}_j)$ is given by:

$$\gamma_k(S_i \rightarrow S_j) = \Lambda_{a,b}^{(i)}(A_k, B_k) + w\Lambda(W_k) + y\Lambda(Y_k) \qquad (16)$$

Now Let $\alpha_k(\mathbf{S}_i)$ denote the normalized forward metric at trellis stage k and state $\mathbf{S}_i$, while $\alpha'_{k+1}(\mathbf{S}_j)$ is the forward metric at trellis stage k + 1 and state $\mathbf{S}_j$ prior to normalization. The forward recursion is given by:

$$\alpha'_{k+1}(S_j) = \max_{S_i \rightarrow S_j}{}^{*}\{\alpha_k(S_i) + \gamma_k(S_i \rightarrow S_j)\} \qquad (17)$$

The forward metrics are normalized with respect to the metric stored in state zero after computing the forward recursion for all $\mathbf{S}_j$ at time k+1as follows:

$$\alpha_{k+1}(S_j) = \alpha'_{k+1}(S_j) - \alpha'_{k+1}(S_0) \qquad (18)$$

Again, let $\beta'_{k+1}(\mathbf{S}_j)$ denote the normalized backward metric at trellis state k+1 and state $\mathbf{S}_j$ and $\beta'_k(\mathbf{S}_i)$ denote the backward metric at trellis state k and state $\mathbf{S}_i$ prior to normalization. The backward recursion is given by:

$$\beta'_k(S_i) = \max_{S_i \rightarrow S_j}{}^{*}\{\beta_{k+1}(S_j) + \gamma_k(S_i \rightarrow S_j)\} \qquad (19)$$

The backward metrics are normalized with respect to the metric stored in state zero after computing the backward recursion for all $\mathbf{S}_i$ at time k as follows:

$$\beta_k(S_i) = \beta'_k(S_i) - \beta'_k(S_0) \qquad (20)$$

The sets of forward and backward metrics are then stored and used to find the LLR values according to (15). For each branch the likelihood ration can be computed as follows:

$$Z_k(S_i \rightarrow S_j) = \alpha_k(S_i) + \gamma_k(S_i \rightarrow S_j) + \beta_{k+1}(S_j) \qquad (21)$$

For message pair (A_k, B_k) = (a, b) the likelihood is calculated as:

$$t_k(a,b) = \max_{S_i \rightarrow S_j:(a,b)}{}^{*}\{Z_k\} \qquad (22)$$

And the possible values for (a,b) are 01, 10, or 11. At the decoder output, the LLR value is given by:

$$\Lambda_{a,b}^{(o)}(A_k, B_k) = t_k(a,b) - t_k(0,0) \qquad (23)$$

After the iteration process is completed, either by fixed number of iterations or based on some convergence criterion, the LLR of each bit in the couple (A_k, B_k) is computed to take the final decision by comparing them to threshold:

$$\Lambda(A_k) = \max{}^{*}\left\{\Lambda_{1,0}^{(o)}(A_k, B_k), \Lambda_{1,1}^{(o)}(A_k, B_k)\right\} - \max{}^{*}\left\{\Lambda_{0,0}^{(o)}(A_k, B_k), \Lambda_{0,1}^{(o)}(A_k, B_k)\right\} \qquad (24)$$

$$\Lambda(B_k) = \max{}^{*}\left\{\Lambda_{0,1}^{(o)}(A_k, B_k), \Lambda_{1,1}^{(o)}(A_k, B_k)\right\} - \max{}^{*}\left\{\Lambda_{0,0}^{(o)}(A_k, B_k), \Lambda_{1,0}^{(o)}(A_k, B_k)\right\} \qquad (25)$$

where $\Lambda_{0,0}^{(o)}(A_k, B_k) = 0$.

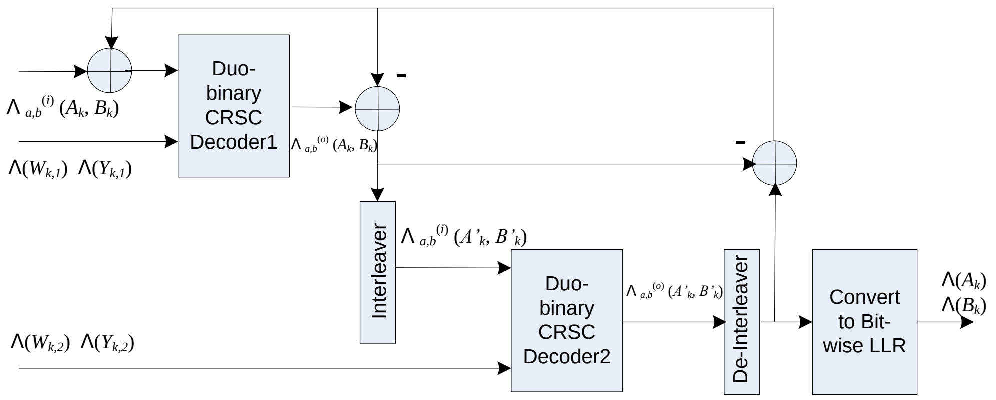

$\Lambda_{a,b}^{(i)}(A_k, B_k)$
$\Lambda(W_{k,1})$ $\Lambda(Y_{k,1})$
Duo-binary CRSC Decoder1
$\Lambda_{a,b}^{(o)}(A_k, B_k)$
-
-
Interleaver
$\Lambda_{a,b}^{(i)}(A'_k, B'_k)$
$\Lambda(W_{k,2})$ $\Lambda(Y_{k,2})$
Duo-binary CRSC Decoder2
$\Lambda_{a,b}^{(o)}(A'_k, B'_k)$
De-Interleaver
Convert to Bit-wise LLR
$\Lambda(A_k)$
$\Lambda(B_k)$

Fig. 3. A decoder for the DVB-RCS code.

III. DVB-RCS Finite Precision Turbo Decoder

In the design phase of turbo codes, good results can be achieved through floating-point software simulations. On the other hand, the efficient hardware implementation of DVB-RCS turbo decoder means, achieving the best performance in terms of area, speed, and low power consumption without loss of error correction capability. The decoding of turbo codes is an iterative process and each iteration needs a lot of processing and calculations. This adds challenge for hardware implementation including huge processing and storage requirements. There is always a tradeoff between hardware complexity and decoder capability in order to achieve the most efficient implementation of the decoder. At different abstraction levels, some design modifications have to be done including algorithmic, architecture, and circuit levels. Fixed point representation might be realizable and preferable for this reason, during hardware implementation phase; circuits then can process the data in finite precision. Finding a fixed point model that has all bit-widths as small as possible under the condition of an acceptable degradation in coding performance is the primary goal when implementing quantized decoder [11]. In terms of speed, area and power consumption the smaller the bit-width of quantization, the better is the decoder performance. In the same time the performance of the decoder is also affected, for this reason, the quantization should be optimized to control the complexity of the implementation.

For the decoding of turbo codes as it was mentioned before, at the algorithmic level also, a lot of modifications have been done already on decoding algorithms [7]. Avoiding the numerical problems of MAP decoding algorithm, additions instead of multiplications can be used in calculating the extrinsic metric of Log-MAP decoding algorithm. For the sake of more complexity reduction, quantized Max-Log-MAP decoding algorithm can be implemented.

IV. Simulations and Results

The performance of the floating-point simulation of DVB-RCS turbo codes is first evaluated using matlab computer based simulation. The performance has been evaluated in terms of bit error rate (BER) against bit energy E_b in an additive white Gaussian noise (AWGN) channel, having single-sided power spectral density N_o. All the block lengths stated by the standards ranging from 48 to 864 message couples have been included in this simulation. The modulation type is quadrature phase shift keying (QPSK). At the receiver side, a maximum of ten decoding iterations have been performed. Figure 4 shows the influence of the block size on the BER curve at code rate 1/3 while Figure 5 and Figure 6 show the influence of the code rate on the BER curve for two different frame lengths of 48, 212 message couples on the BER. Results are shown for all seven code rates when the block sizes are N = 48 and 212 message couples, respectively, and ten iterations of Max-Log-MAP decoding are performed.

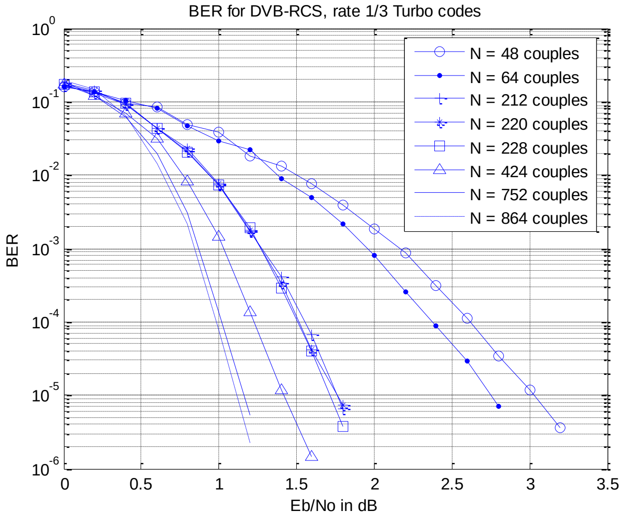


Fig. 4. Influence of block size on the BER performance.

To evaluate the performance of the quantized decoder, another matlab computer based simulation has been driven to compare the performance of the quantized decoder with the floating point representation. The simulation was run on different ranges of 4-bit quantized decoder's LLR input for different coding rates. Results showed that for 4-bit quantization, the performance is getting worst as the range is increased. The maximum and minimum of input LLR values are observed at different points of SNR, and it was observed that the input LLR values are linearly increasing with the SNR. This observation helped in the estimation of the quantization range. Better estimate of the quantization range can be made based on the SNR values using that observation by introducing SNR-dependent variable factor and multiplying that factor with the LLR input values before the decoding process. As the SNR increases, that multiplier factor should be smaller. The decoding process is then applied on the input LLR values after the multiplying process.

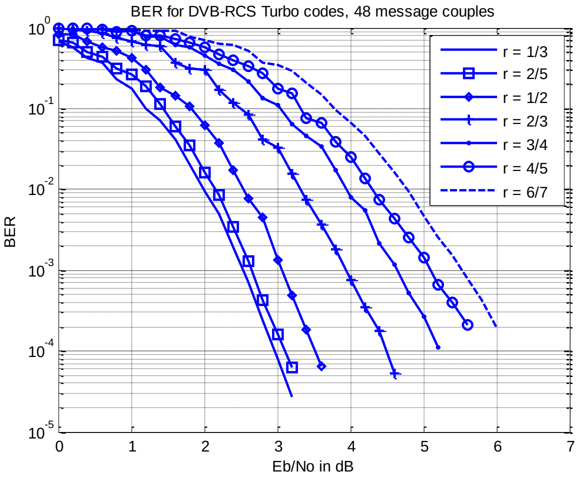


Fig. 5. Influence of block size on the BER performance.

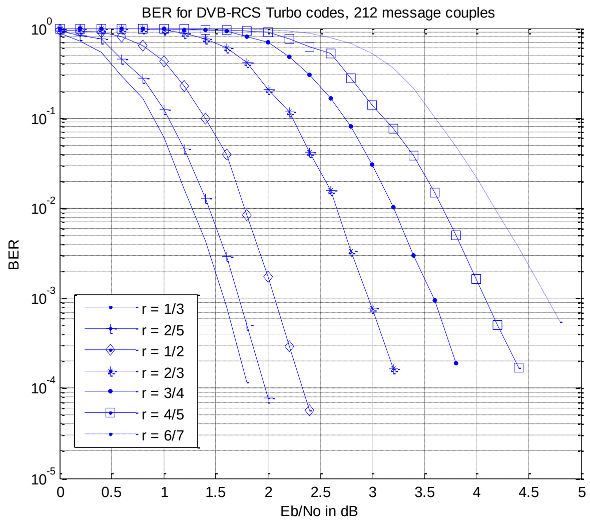


Fig. 6. Influence of block size on the BER performance.

As it was mentioned before, Max-Log-MAP simplifies the Log-MAP algorithm by omitting the correction factor. A lot of researches have been done aiming to reduce the complexity of the decoding algorithm by approximating the correction factor with different methods. Table I presents the most important reduced complexity turbo decoding algorithms. In our research, we have tried also another technique to estimate the appropriate quantization range by introducing a scaling factor in the decoding process. The input LLR values fed to the decoding routine are scaled by multiplying them with that scaling factor first. The max* operator within the Log-MAP decoding scheme is then computed by introducing a constant correction factor. It should be noticed that the computation of the max* operator in the decoding algorithm constitute a significant portion of the decoding complexity [12].

The estimate of the correction factor in our simulation is based on [16]. The computation of the max* operator considering that correction factor is given by:

TABLE I
REDUCED COMPLEXITY ALGORITHMS FOR TURBO DECODING

Decoding Algorithm	Correction factor, $f_c(\lvert y\text{-}x\rvert)$
MAX-Log-MAP [3]	0
Constant Log-MAP [13]	$\begin{cases} 3/8, if \lvert y-x \rvert < 2 \\ 0, otherwise \end{cases}$
Linear Log-MAP [14]	$\max(0, \ln 2 - 0.5^* \lvert y-x \rvert, 0)$
Average Log-MAP [15]	$\begin{cases} \ln 2 + 0.5^*(y+x), if \lvert y-x \rvert < 2^* \ln 2 \\ 0, otherwise \end{cases}$

$$\max{}^*(x,y) = \max(x,y) + f_c(|y\text{-}x|) \qquad (26)$$

where x and y, are the LLR input values, and fc(|y-x|), is the correction function. For Log-MAP algorithm, the max* operator can be computed as:

$$\max{}^*(x, y) \approx \max(x, y) + \begin{cases} 0, if \ |y-x| > T \\ C, if \ |y-x| \leq T \end{cases} \qquad (27)$$

where C is the correction factor and T is a threshold value, C = 0.5, T = 1.5 based on [16].

To measure the performance of the decoding algorithm with constant correction factor for the scaled LLR input values, another matlab code was built to study the effect of the scaling. It was observed that a better performance for the decoding process can be achieved when multiplying the correction factor with the same scaling factor in the decoding process. Accordingly, we propose a change in the approximation of the max* operator computed by (26), to become as follows:

$$\max{}^*(x, y) \approx \max(x, y) + \begin{cases} 0, if \ |y-x| > T \\ K, if \ |y-x| \leq T \end{cases} \qquad (28)$$

where, $K = k \,.\, C$.

The same operation has been done but this time on different code rate. Figure 7 shows the performance of the quantized 212 blocks of rate 6/7 compared with the floating-point BER. It was found that as SNR increases, the performance of the quantized code worsen. It has also been observed from the calculations that the input LLR values for the code rate 6/7 are higher than those of rate 1/3. This is an indication that varying the input

LLR range as a function of SNR gives good results, but the best performance could be obtained when the code rate is also considered. Therefore, the quantization range should be scaled by a factor including both the SNR and code rate. In the same time, fixed quantization range couldn't give the best performance for all code rates.

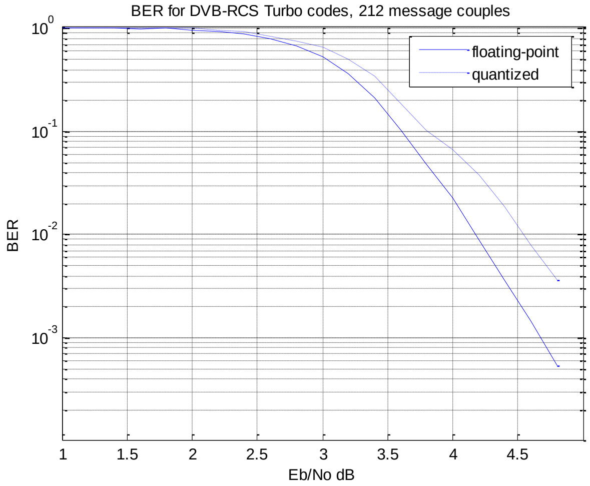


Fig. 7. Floating-point vs. quantized decoder at rate 6/7.

From the hardware implementation point of view, there is a tradeoff between the performance and resolution. For a given code rate, smaller decoder input range affects the decoder performance, while higher range affects the resolution. Based on the fact that the decoder performance of the quantized code is affected by both of the code rates and the value of SNR, we develop an algorithm to estimate the efficient quantization of DVB-RCS turbo decoder. Figure 8 shows a flow-chart of our proposed algorithm for the decoder quantization.

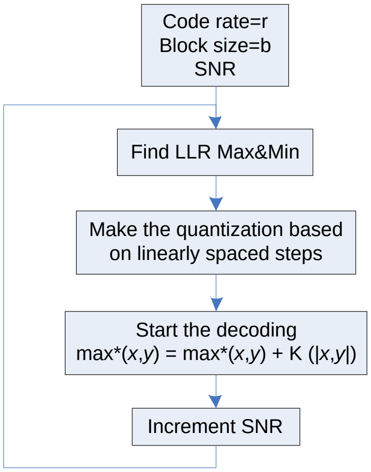

Code rate=r
Block size=b
SNR
Find LLR Max&Min
Make the quantization based on linearly spaced steps
Start the decoding
max*(x,y) = max*(x,y) + K (|x,y|)
Increment SNR

Fig. 8. Proposed algorithm for efficient decoder quantization.

The performance comparison between variable-rate floating-point codes and quantized version of those codes is shown in Figure 9. The simulation was run on blocks of 212 message couples for both of floating point codes and quantized codes using our proposed algorithm. We considered all the possible different codes rates supported by DVB-RCS standards, ranging from r = 1/3 to r = 6/7. For each code rate, the maximum and minimum LLR input values have been calculated at different SNR points. Uniform quantization has been made by using 4-bits. After that, we applied the modified MAX-Log-MAP decoding algorithm based on the proposed modification in this paper. A fixed scaling factor of 0.75 was used to perform this simulation. The performance has been evaluated in terms of bit error rate (BER) against bit energy Eb in an additive white Gaussian noise (AWGN) channel, having single-sided power spectral density No. The modulation type is QPSK. At the receiver side, a maximum of ten decoding iterations have been performed. It can be noticed that the difference in the performance between the floating-point codes and the quantized codes using the proposed algorithm in this paper is less than 0.1 dB. This gives better performance compared with [17] in which the authors obtained 0.4 dB improvement over the standard Max-Log-Map algorithm at BER of 10-4 for code rate 1/3.

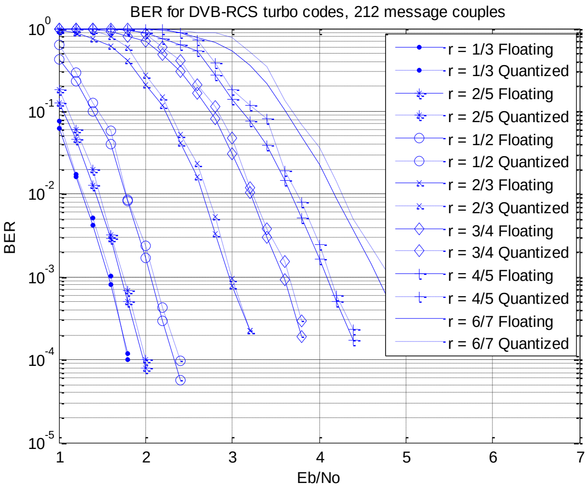


Fig. 9. Influence of quantization on variable rate DVB-RCS Turbo codes.

V. Conclusion

In this paper, an algorithm that computes the quantization range for an efficient decoder quantization has been proposed. The algorithm efficiently estimates decoder quantization of DVB-RCS turbo coding that reduces the complexity of the decoder and overall power consumption in the realization of DVB-RCS radios. The algorithm is based on the modification that improves the BER performance of Max-Log-MAP for fixed point decoder. Performance simulation for different supported code rates of such codes has been presented, and results showed that the quantized decoder essentially matches the performance of the floating point decoder.

References

[1] *Digital broadcasting system for television, sound, and data services*, European Telecommunications Standards Institute, ETSI 200 421, 1994.

[2] *Digital video broadcasting (DVB); interaction channel for satellite distribution systems*, European Telecommunications Standards Institute. ETSI EN 301, 790 V1.5.1, May 2009.

[3] P. Robertson, P. Hoeher, and E. Villebrun. "Optimal and sub-optimal maximum a posteriori algorithms suitable for turbo decoding," *European Trans. On Telecommun.*, 8(2):119–125, Mar./Apr. 1997.

[4] C. Douillard, M. Jezequel, and C. Berrou, "The turbo code standard for DVB-RCS," *Proc. 2^{nd} Int. Symp. Turbo codes*, pp. 551-554, Sept. 2000.

[5] C. Berrou, C. Douillard, and M. Jezequel, "Multiple parallel concatenation of circular recursive systematic convolutional (CRSC) codes," *Annals of Telecommunication*, 54(3-4):166–172, Mar.-Apr. 1999.

[6] Papaharalabos, S.; Benmayor, D.; Mathiopoulos, P.T.; Pingzhi Fan; , "Performance Comparisons and Improvements of Channel Coding Techniques for Digital Satellite Broadcasting to Mobile Users," *Broadcasting, IEEE Transactions on*, vol.57, no.1, pp.94-102, March 2011.

[7] M. C. Valenti and J. Sun. "The UMTS turbo code and an efficient decoder implementation suitable for software defined radios," *Int. J. Wireless Info. Networks*, 8:203–216, Oct. 2001.

[8] S.W. Shaker, "Reduced complexity DVB-RCS turbo decoder," *Advanced Communication Technology (ICACT), 2012 14th International Conference on*, vol., no., pp.444-448, 19-22 Feb. 2012.

[9] B. Sklar, *Digital Communications: Fundamentals and Applications*, 2nd ed. Fundamentals of Turbo Codes. 2001, NJ: Prentice Hall.

[10] Bera, D.; Sen, J., "SOVA based decoding of double-binary turbo convolutional code," *Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology*, 2009. Wireless VITAE 2009. 1st International Conference on, vol., no., pp.757-761, 17-20 May 2009.

[11] Shaker, S.W., "DVB-S2 LDPC finite-precision decoder," *Advanced Communication Technology (ICACT)*, 2011 13th International Conference on , vol., no., pp.1383-1386, 13-16 Feb. 2011.

[12] Papaharalabos, S.; Mathiopoulos, P.; Masera, G.; Martina, M., "On optimal and near-optimal turbo decoding using generalized max operator," *Communications Letters, IEEE*, vol.13, no.7, pp.522-524, July 2009.

[13] Gross, W.J.; Gulak, P.G., "Simplified MAP algorithm suitable for implementation of turbo decoders," *Electronics Letters, IEEE*, vol.34, no.16, pp.1577-1578, 6 Aug 1998.

[14] Jung-Fu Cheng; Ottosson, T., "Linearly approximated log-MAP algorithms for turbo decoding," *Vehicular Technology Conference Proceedings, 2000. VTC* 2000-Spring Tokyo. 2000 IEEE 51st , vol.3, no., pp.2252-2256 vol.3, 2000.

[15] Classon, B.; Blankenship, K.; Desai, V., "Channel coding for 4G systems with adaptive modulation and coding" *Wireless Communications, IEEE, 2000*. vol.9, no.2, pp.8-13, April 2002.

[16] Y. Ould-Cheikh-Mahmedou, P. Guinand, and P. Kabal, "Enhanced Max-Log-MAP and Enhanced Log-APP Decoding for DVB-RCS," *Proc. Int. Symp. Turbo Codes*, Brest, France, pp. 259–262, Sept. 2003.

[17] Taskaldiran, M.; Morling, R.C.S.; Kale, I., "A comparative study on the modified Max-Log-MAP turbo decoding by extrinsic information scaling," *Wireless Telecommunications Symposium*, 2007. WTS 2007, vol., no., pp.1-5, 26-28 April 2007.

Dr. Sherif Welsen Shaker, university of Nottingham Ningbo, China, Faculty of Science and Engineering. Sherif Welsen is currently a teaching fellow in the department of Electrical and Electronics Engineering. He obtained his Masters degree of science in Electronics and Telecommunications Engineering from the Arab Academy for Science and Technology and Maritime (AAST), Cairo, Egypt. He then joined Ain-Shams University, where, he got his PhD in Electronics and Electrical Communications engineering in Jan 2010. His research was focusing on Software Defined Radios in wireless communication and in particular on "generic low power FPGA implementation of coding schemes for emerging wireless standards". Dr. Welsen worked as research fellow at Kuang-Chi Institute of Advanced Technology, Shenzhen, Guangdong, China from 2011 to 2013, and as assistant professor at Modern Academy of Engineering and Technology from 2004 to 2010. He was part-time research professor at Ain-Shams University, Cairo, Egypt from 2010 to 2011 in the project "DVBT-2 Systems and Cognitive Radio Networks Sharing the Same Frequency Band". He was the founder of many labs in the academia including microprocessors, FPGAs, and wireless communications. He is involved in Cognitive radios, SDRs, Coding Theory, Digital VLSI, VHDL, FPGA and Digital Signal Processing research.

Volume 3 Issue 3, Mar 2014, ISSN: 2288-0003

ICACT-TACT
JOURNAL

GIRI Global IT
Research Institute

1713 Obelisk, 216 Seohyunno, Bundang-gu, Sungnam Kyunggi-do, Republic of Korea 463-824
Business Licence Number : 220-82-07506, Contact: secretariat@icact.org Tel: +82-70-4146-4991