جامعة التنمية البشرية
UNIVERSITY OF HUMAN DEVELOPMENT

p-ISSN 2521-4209
e-ISSN 2521-4217

UHD Journal of Science and Technology

A Scientific periodical issued by University of Human Developement

Vol.1 No.(1) June 2017

2017 2717

www.jst.uhd.edu.iq

Kurdistan Regional Government
University of Human Development

UHD Journal of Science and Technology

A periodic scientific journal issued by University of Human Development

Introduction

UHD Journal of Science and Technology (UHDJST) is a semi-annual journal published by the University of Human Development, Sulaymaniyah, Kurdistan Region, Iraq. UHDJST member of ROAD, e-ISSN: 2521-4217, p-ISSN: 2521-4209 and a member of Crossref, DOI: 10.21928/issn.2521-4217. UHDJST publishes original research in all areas of Science, Engineering, and Technology. UHDJST is a Peer-Reviewed Open Access journal with Creative Commons Attribution Non-Commercial No Derivatives License 4.0 (CC BY-NC-ND 4.0). UHDJST provides immediate, worldwide, barrier-free access to the full text of research articles without requiring a subscription to the journal, and has article processing charge (APC). UHDJST applies the highest standards to everything it does and adopts APA citation/referencing style. UHDJST Section Policy includes three types of publications: Articles, Review Articles, and Letters.

By publishing with us, your research will get the coverage and attention it deserves. Open access and continuous online publication mean your work will be published swiftly, ready to be accessed by anyone, anywhere, at any time. Article Level Metrics allow you to follow the conversations your work has started.

UHDJST publishes works from extensive fields including, but not limited to:

- Pure Science
- Applied Science
- Medicine
- Engineering
- Technology

Scope and Focus

UHD Journal of Science and Technology (UHDJST) publishes original research in all areas of Science and Engineering. UHDJST is a semi-annual journal published by the University of Human Development, Sulaymaniyah, Kurdistan Region, Iraq. We believe that if your research is scientifically valid and technically sound then it deserves to be published and made accessible to the research community. UHDJST aims to provide a service to the international scientific community enhancing swap space to share, promote and disseminate the academic scientific production from research applied to Science, Engineering, and Technology.

SEARCHING FOR PLAGIARISM

We use plagiarism detection: detection; According to Oxford online dictionary, Plagiarism means: *The practice of taking someone else's work or ideas and passing them off as one's own.*

Section Policies

No.	Title	Peer Reviewed	Indexed	Open Submission
1	Articles: This is the main type of publication that UHDJST will produce	☑	☑	☑
2	Review Articles: Critical, constructive analysis of the literature in a specific field through summary, classification, analysis, comparison.	☑	☑	☑
3	Letters: Short reports of original research focused on an outstanding finding whose importance means that it will be of interest to scientists in other fields.	☑	☑	☑

PEER REVIEW POLICIES

At UHDJST we are committed to prompt quality scientific work with local and global impacts. To maintain a high-quality publication, all submissions undergo a rigorous review process. Characteristics of the peer review process are as follows:

- The journal peer review process is a "double-blind peer review".
- Simultaneous submissions of the same manuscript to different journals will not be tolerated.
- Manuscripts with contents outside the scope will not be considered for review.
- Papers will be refereed by at least 2 experts as suggested by the editorial board.
- In addition, Editors will have the option of seeking additional reviews when needed. Authors will be informed when Editors decide further review is required.
- All publication decisions are made by the journal's Editors-in-Chief on the basis of the referees' reports. Authors of papers that are not accepted are notified promptly.
- All submitted manuscripts are treated as confidential documents. We expect our Board of Reviewing Editors, Associate Editors and reviewers to treat manuscripts as confidential material as well.
- Editors, Associate Editors, and reviewers involved in the review process should disclose conflicts of interest resulting from direct competitive, collaborative, or other relationships with any of the authors, and remove oneself from cases in which such conflicts preclude an objective evaluation. Privileged information or ideas that are obtained through peer review must not be used for competitive gain.
- Our peer review process is confidential and the identities of reviewers cannot be revealed.

Note: UHDJST is a member of CrossRef and CrossRef services, e.g., CrossCheck. All manuscripts submitted will be checked for plagiarism (copying text or results from other sources) and self-plagiarism (duplicating substantial parts of authors' own published work without giving the appropriate references) using the CrossCheck database. Plagiarism is not tolerated.

For more information about CrossCheck/iThenticate, please visit
http://www.crossref.org/crosscheck.html.

OPEN ACCESS POLICY

This journal provides immediate open access to its content on the principle that making research freely available to the public supports a greater global exchange of knowledge. Open Access (OA) stands for unrestricted access and unrestricted reuse which means making research publications freely available online. It access ensures that your work reaches the widest possible audience and that your fellow researchers can use and share it easily. The mission of the UHDJST is to improve the culture of scientific publications by supporting bright minds in science and public engagement.

UHDJST's open access articles are published under a Creative Commons Attribution CC-BY-NC-ND 4.0 license. This license lets you retain copyright and others may not use the material for commercial purposes. Commercial use is one primarily intended for commercial advantage or monetary compensation. If others remix, transform or build upon the material, they may not distribute the modified material. The main output of research, in general, is new ideas and knowledge, which the UHDJST peer-review policy allows publishing as high-quality, peer-reviewed research articles. The UHDJST believes that maximizing the distribution of these publications - by providing free, online access - is the most effective way of ensuring that the research we fund can be accessed, read and built upon. In turn, this will foster a richer research culture and cultivate good research ethics as well. The UHDJST, therefore, supports unrestricted access to the published materials on its main website as a fundamental part of its mission and a global academic community benefit to be encouraged wherever possible.

Specifically:

- The University of Human Development supports the principles and objectives of Open Access and Open Science
- UHDJST expects authors of research papers, and manuscripts to maximize the opportunities to make their results available for free access on its final peer-reviewed paper
- All manuscript will be made open access online soon after final stage peer-review finalized.
- This policy will be effective from 17th May 2017 and will be reviewed during the first year of operation.
- Open Access route is available at http://journals.uhd.edu.iq/index.php/uhdjst for publishing and archiving all accepted papers,
- Specific details of how authors of research articles are required to comply with this policy can be found in the Guide to Authors.

ARCHIVING

This journal utilizes the LOCKSS and CLOCKSS systems to create a distributed archiving system among participating libraries and permits those libraries to create permanent archives of the journal for purposes of preservation and restoration.

LOCKSS: Open Journal Systems supports the LOCKSS (Lots of Copies Keep Stuff Safe) system to ensure a secure and permanent archive for the journal. LOCKSS is open source software developed at Stanford University Library that enables libraries to preserve selected web journals by regularly polling registered journal websites for newly published content and archiving it. Each archive is continually validated against other library caches, and if the content is found to be corrupted or lost, the other caches or the journal is used to restore it.

CLOCKSS: Open Journal Systems also supports the CLOCKSS (Controlled Lots of Copies Keep Stuff Safe) system to ensure a secure and permanent archive for the journal. CLOCKSS is based upon the open-source LOCKSS software developed at Stanford University Library that enables libraries to preserve selected web journals by regularly polling registered journal websites for newly published content and archiving it. Each archive is continually validated against other library caches, and if the content is found to be corrupted or lost, the other caches or the journal is used to restore it.

PUBLICATION ETHICS

Publication Ethics and Publication Malpractice Statement

The publication of an article in the peer-reviewed journal UHDJST is to support the standard and respected knowledge transfer network. Our publication ethics and publication malpractice statement is mainly based on the Code of Conduct and Best-Practice Guidelines for Journal Editors (Committee on Publication Ethics, 2011) that includes;

- General duties and responsibilities of editors.
- Relations with readers.
- Relations with the authors.
- Relations with editors.
- Relations with editorial board members.
- Relations with journal owners and publishers.
- Editorial and peer review processes.
- Protecting individual data.
- Encouraging ethical research (e.g. research involving humans or animals).
- Dealing with possible misconduct.
- Ensuring the integrity of the academic record.
- Intellectual property.
- Encouraging debate.
- Complaints.
- Conflicts of interest.

ANIMAL RESEARCHES

- For research conducted on regulated animals (which includes all live vertebrates and/or higher invertebrates), appropriate approval must have been obtained according to either international or local laws and regulations. Before conducting the research, approval must have been obtained from the relevant body (in most cases an Institutional Review Board, or Ethics Committee). The authors must provide an ethics statement as part of their Methods section detailing full information as to their approval (including the name of the granting organization, and the approval reference numbers). If an approval reference number is not provided, written approval must be provided as a confidential supplemental information file. Research on non-human primates is subject to specific guidelines from the Weather all (2006) report (The Use of Non-Human Primates in Research).
- For research conducted on non-regulated animals, a statement should be made as to why ethical approval was not required.
- Experimental animals should have been handled according to the highest standards dictated by the author's institution.
- We strongly encourage all authors to comply with the '*Animal Research: Reporting In Vivo Experiments*' (ARRIVE) guidelines, developed by NC3Rs.
- Articles should be specific in descriptions of the organism(s) used in the study. The description should indicate strain names when known.

ARTICLE PROCESSING CHARGES

UHDJST is an Open Access Journal (OAJ) and has article processing charges (APCs). The published articles can be downloaded freely without a barrier of admission.

Address

University of Human Development, Sulaymaniyah-Kurdistan Region/Iraq
PO Box: Sulaymaniyah 6/0778

Contact

Principal Contact

Dr. Aso Darwesh

Editor-in-Chief

University of Human Development – Sulaymaniyah, Iraq

Phone: +964 770 148 5879

Email: jst@uhd.edu.iq

Support Contact

UHD Technical Support

Phone: +964 770 158 4888

Email: jst@uhd.edu.iq

Contents

ORIGINAL RESEARCH ARTICLE UHD JOURNAL OF SCIENCE AND TECHNOLOGY

Intelligent Techniques in Cryptanalysis: Review and Future Directions

Sufyan T. Al-Janabi[1,2], Belal Al-Khateeb[3] and Ahmed J. Abd[3]

[1]*Department of Information Systems, College of CS and IT, University of Anbar, Ramadi, Anbar - Iraq*
[2]*Department of Computer Science, College of Sceince and Technology, University of Human Development, Sulaimaniya, Kurdistan Region - Iraq*
[3]*Department of Computer Science, College of CS and IT, University of Anbar, Ramadi, Anbar - Iraq*

ABSTRACT

In this paper, we consider the use of some intelligent techniques such as artificial neural networks (ANNs) and genetic algorithms (GAs) in solving various cryptanalysis problems. We review various applications of these techniques in different cryptanalysis areas. An emphasis is given to the use of GAs in cryptanalysis of classical ciphers. Another important cryptanalysis issue to be considered is cipher type detection or identification. This can be a real obstacle to cryptanalysts, and it is a basic step for any automated cryptanalysis system. We specifically report on the possible future research direction of using spiking ANNs for cipher type identification and some other cryptanalysis tasks.

Index Terms: Artificial Neural Networks, Cipher Identification, Classical Ciphers, Cryptanalysis, Genetic Algorithms

1. INTRODUCTION

The basic aim of cryptography is to transmit messages from one place to another in a secure manner. To satisfy this, the original message called "plaintext" is encrypted and sent to the receiver as "ciphertext." The receiver decrypts the ciphertext to get the plaintext. This can be done using a cipher which is a tool that hides the plaintext and converts it to the ciphertext (and also can return back the plaintext from the ciphertext). Ciphers make use of (cryptographic) keys that determine the relationship between the plaintext and the ciphertext. Cryptography can be considered as assemble from security and mathematics. It is used to protect important information and ensure that this information arrives to its destination in peace without violations. Ciphers gradually evolved from simple ones which are currently considered to be easily breakable such as Caesar cipher through more complex cipher algorithms such as the data encryption standard (DES) and the advanced encryption standard (AES) [1], [2].

On the other hand, cryptanalysis means trying to break any security system (or cipher) using unauthorized ways to access the information in that system. Thus, cryptanalysis works against cryptography. The cryptanalyst tries to find any weakness in the cryptographic system to get either the source of information (plaintext) or the key used in the encryption algorithm. This process is called an attack. If this attack is successfully applied, then the cryptographic system is said to be broken. Cryptography and cryptanalysis together form the field of cryptology [3], [4].

In the recent decades, cryptography developed quickly because of the development in computational resources which increased the speed and decreased the time of encryption and decryption processes. This moved cryptography from solving by hand to more and more complex computer programs that need considerably long time and sophisticated attack

Access this article online

DOI: 10.21928/uhdjst.v1n1y2017.pp1-10

E-ISSN: 2521-4217
P-ISSN: 2521-4209

Corresponding author's e-mail: saljanabi@fulbrightmail.org

Received: 10-03-2017 Accepted: 25-03-2017 Published: 12-04-2017

techniques to solve. Hence, instead of using the simple Caesar cipher which needs no more than few minutes (or seconds) to be broken using brute force attack (trying every possible solution), we are using now more complex ciphers (AES, triple DES, etc.) that might need hundreds (or thousands) years to break using brute force attack with the current technology.

One important issue to mention is that despite the technological and mathematical complexity, the modern versions of cryptosystems still follow the same classical concepts. Thus, it is still prudent to apply certain attacks on classical ciphers and study their evolution aspects before using them with more complex modern ciphers. This is quite justifiable considering the nature of intelligent techniques such as GAs, artificial neural networks (ANNs), and evolutionary algorithms (EA).

Although several survey works can be found in earlier literature [5]-[7], more work is needed in this direction to shed the light on various aspects of this kind of interdisciplinary research. The aim of this paper is to review various applications of intelligent techniques in cryptanalysis problems and to investigate some possible future research directions.

The remaining of this paper is organized as follows: Section 2 summarizes various types of ciphers and cryptanalysis attacks in a generic way. The intelligent techniques of ANNs, GAs, and evolutionary computation are reviewed and compared to each other in Section 3. Then, Section 4 reviews the application of GAs in cryptanalysis of classical ciphers. The issue of classification or identification of cipher type is considered in Section 5. Next, we present some insights regarding the future direction of using spiking ANNs in cipher classification in Section 6. Finally, the paper is concluded in Section 7.

2. CLASSIFICATION OF CIPHERS AND ATTACKS

Cryptosystems can be classified in multiple approaches depending on various criteria. This can simplify the study of cryptography science and make it easier to understand and implement. At first, if we take in consideration the amount of data that can be encrypted at a time, we can then classify cryptosystems in two classes:[3]

1. Block ciphers, which encrypt block of data at time like DES
2. Stream ciphers, which encrypt single datum (symbol, byte, or bit) at a time like Caesar cipher.

Second, it is also possible to classify cryptosystems according to the key used in encryption and decryption processes. In this case, we can put a cryptosystem under one of the following:

1. Symmetric key ciphers, where the same key is used for encryption and decryption, for example, Vigenere cipher.
2. Public key ciphers, where one key is used for encryption and another one for decryption, for example, Rivest-Shamir-Adleman system.

Third, we can classify cryptosystems depending on the history and time of invention. Thus, we can put cryptosystems under one of the following:

1. Classical ciphers, which are those ciphers used in the past and can be solved by hand. They became now breakable, for example, Caesar cipher
2. Modern ciphers, which are those complex (computerized) ciphers widely used currently and cannot be solved by hand, for example, AES.

Finally, another classification approach is to classify ciphers according to their building blocks. This approach is typically applied for classical ciphers to divide it into:[3]

1. Substitution systems, where every character is replaced by another one, for example, monoalphabetic ciphers
2. Transposition systems, where characters are rearranged rather than replaced, for example, columnar cipher.

It is also possible to further classify both of the main two categories of classical ciphers: Substitution and transposition ciphers. Transposition ciphers can be classified into sub classes:[3], [8]

- Single transposition: This type transposes one letter at a time, for example, the columnar transposition, route transposition, and grille transposition ciphers
- Double transposition: This type transposes more than one letter at a time.

Substitution ciphers can be classified into sub classes as follows:[3], [9]

- Monoalphabetic substitution ciphers: In this type of encryption techniques, one letter of plaintext is represented by one letter in ciphertext, and one ciphertext letter represents one and only one plaintext letter, so it is the simplest form of substitution techniques. Monoalphabetic substitution includes direct monoalphabetic, reversed monoalphabetic, decimated monoalphabetic, and mixed monoalphabetic ciphers
- Polyalphabetic substitution ciphers: In this type of

encryption, one letter of plaintext is represented by multiple ciphertext letters, and one ciphertext letter represents multiple plaintext letters. There are two types of polyalphabetic substitution ciphers: Periodic (where there is a keyword repeating along plaintext like the Vigenere cipher) and non-periodic (where there is no repeating key, e.g., the running key cipher)

- Polygraphic substitution ciphers: In this type of substitution, more than one plaintext letters are encrypted at a time by more than one ciphertext letters. This includes digraphic, trigraphic, and tetragraphic ciphers. Examples of these ciphers are the Playfair cipher and Hill cipher
- Homophonic substitution ciphers: In this type of substitution, one plaintext letter is represented by multiple ciphertext letters or characters, and every ciphertext letters or characters can only represent one plaintext letter, for example, the nomenclator cipher.

Furthermore, it is possible to define combinations of transposition and substitution ciphers to produce more secure systems. Such combinations are used to avoid the weaknesses in pure transposition and pure substitution systems. A classical example of such combined ciphers is when we combine simple substitution with a columnar transposition. In modern cryptography, ciphers are designed around substitution and transposition principles simultaneously. Fig. 1 depicts various types of classical systems.

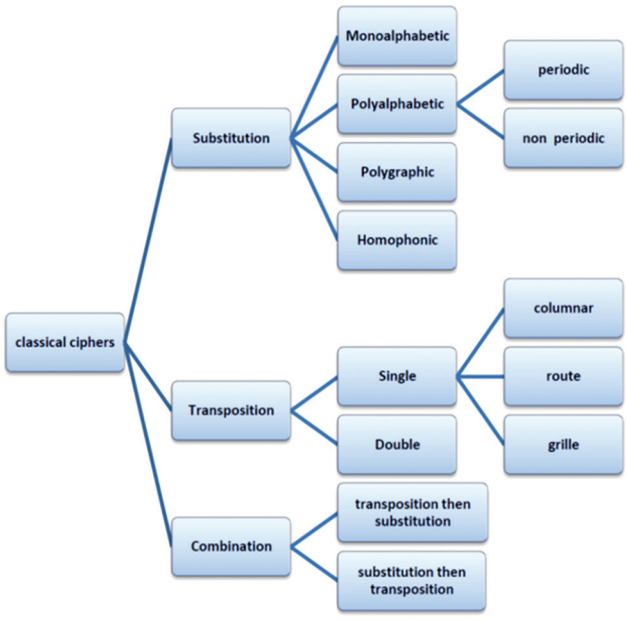

Fig. 1. Most important classical cipher types

Similarly, we can also classify cryptanalysis attacks. Actually, there are many types of such attacks. Some of them can be considered as general types, while others are specific for certain ciphers, protocols, or implementations. Here, we are not going to try to list all attack types rather we are only interested in some generic ways for classifying attacks. It is possible to generically classify attacks based on the amount of information available to the attacker. The amount of information that attacker have is important to make any attack so the cryptanalyst should determine what is available in his hand. Accordingly, we are going to have cipher text only, known plaintext, chosen ciphertext, chosen plaintext, adaptive chosen plaintext, adaptive chosen ciphertext, and related key attacks. Alternatively, we might generically classify attack according to the computational resources (time, memory, and data) required by these attacks [3], [10].

3. INTELLIGENT TECHNIQUES

In this section, we review the relevant intelligent techniques of ANNs, genetic algorithms (GAs), and evolutionary computation. We also give a brief comparison on their characteristics an application scope.

A. ANNs

ANNs are numerical models that use a gathering of basic computational units called neurons that connect with each other to build a network. There are many types of ANNs; each type is suitable for one or more problems depending on the problems itself. Hence, the important thing in ANNs is how to design the topology of ANN that can better describe the problem then solving it using very simple principles to obtain very complex behavior [5], [11]. ANNs can model human brains and use nervous system to solve the problems by learning it with true examples and giving a chance to generalize all solutions. Since the nature of ANNs that simulate the brain and use parallel processing rather than serial computation, we can put ANNs in multiple fields according to the huge capabilities that ANNs can introduce. These fields include classification, approximation, prediction, control, pattern recognition, estimation, optimization, and others.

When using ANN for solving a problem, the following steps should be chosen carefully to make ANN works in an effective way: Design of ANN topology, choosing suitable learning way, and setting the inputs. There are many ANN topologies such as:[12]

- Feed-forward ANNs
- Recurrent ANNs
- Hopfield ANN

- Elman and Jordan ANNs
- Long short-term memory
- Bi-directional ANNs
- Self-organizing map
- Stochastic ANN
- Physical ANN.

There are three generations of neuron models [13]. The first generation of ANNs also called perceptrons, which are composed each of two sections: Sum and threshold. The sum part receives input from a set of weighted synapses. Then, it performs a threshold function on the result of the sum. The input and the output have values that may be equal to either 0 or 1, as shown in Fig. 2.

The second generation of ANNs is composed by two stages:

- Sum of values that are received through weighted synapses
- Sigmoid function evaluator whose input is the result of the sum previously computed. In this generation, the inputs can be any real-valued number, and the output is defined by the transfer function. For example, the sigmoid unit limits outputs to [0; 1], whereas the hyperbolic function produces outputs in the range [1; 1], as shown in Fig. 3.

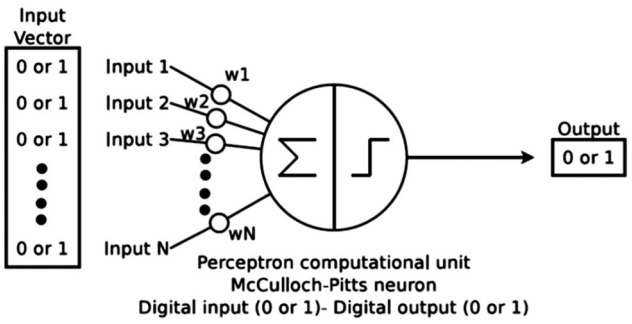

Fig. 2. The first generation of artificial neural networks[13]

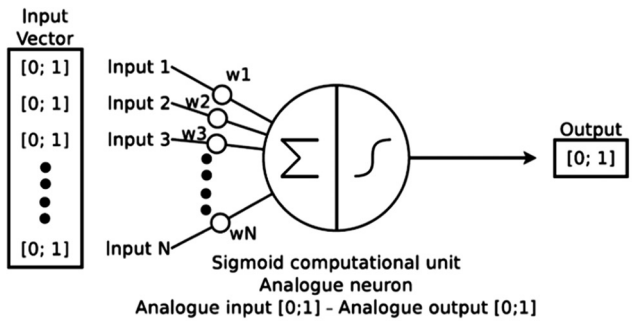

Fig. 3. The second generation of artificial neural networks[13]

The third generation of ANNs is composed by spiking neurons: Neurons which communicate through short signals called spikes. This generation has two main differences when compared with the previous two generation. At first, this generation introduces the concept of time in the simulation, while earlier, the neural networks were based on abstract steps of simulation. Second, such neurons present similarities to biological neurons, as they both communicate using short signals, which in biology are electric pulses (spikes), also known as action potentials, as shown in Fig. 4. The spike train generation can be Gaussian receptive fields [14], Poisson distribution [15], or directed spike generation [16]. Indeed, the applied training algorithm for ANNs is usually the backpropagation [17], while spiking ANNs use Spikeprop [18].

B. GAs

GAs are considered to be one of the best ways to solve a problem, for which there is only a little knowledge. Hence, they work well in any search space. All that is required know is what the solution is needed to be able to do well, and a GA will be able to create a high-quality solution. GAs apply the both principles of selection and evolution to produce several solutions to a given problem [19].

GAs are better applied in an environment in which there is a very large set of candidate solutions and in which the search space is uneven and has many hills and valleys. Although GAs will do well in any environment, they will be greatly outclassed by more situation-specific algorithms in the simpler search spaces. Therefore, GAs are not always the best choice. Sometimes, they can take quite a while to run and are therefore not always feasible for real-time use. However, they are considered to be among the most powerful methods with which to (relatively) quickly create high-quality solutions to a problem. The proper selection of appropriate mutation operators and fitness functions is necessary for implementing a successful attack [19], [20].

In fact, GAs are adaptive heuristic search algorithms based on the evolutionary ideas of natural selection and genetics.

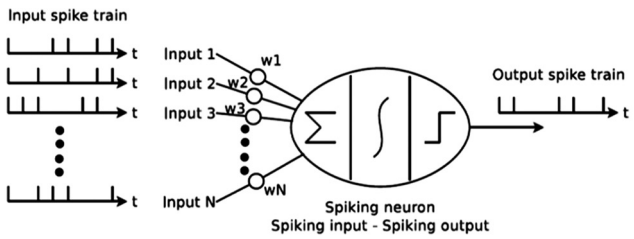

Fig. 4. The third generation of artificial neural networks[13]

Thus, they represent an intelligent exploitation of a random search used to solve optimization problems. They exploit historical information to direct the search into the region of better performance within the search space. The basic techniques of the GAs are designed to simulate processes in natural systems necessary for evolution, especially those follow the principle of "survival of the fittest." This is based on our understanding of nature where competition among individuals for scanty resources results in the fittest individuals dominating over the weaker ones [19].

C. Evolutionary Computation

Simply, evolutionary computation simulates evolution on a computer. The result of such a simulation is a series of optimization algorithms. These are usually based on a simple set of characteristics. Optimization iteratively can improve the quality of solutions to some problem until an optimal (or at least feasible) solution is found. Evolutionary computation is an umbrella term that includes GAs, evolution strategies, and genetic programing [21].

D. Differences Between ANNs, Gas, and Evolutionary Computation

An ANN is a function approximator. To approximate a function, you needs an optimization algorithm to adjust the weights. An ANN can be used for supervised learning (classification and regression) or reinforcement learning and some can even be used for unsupervised learning.

GAs are an optimization algorithm, in supervised learning, a derivative-free optimization algorithm like a GA is slower than most of the optimization algorithms that use gradient information. Thus, it only makes sense to evolve neural networks with GAs in reinforcement learning. This is known as "neuroevolution." The advantage of neural networks like multilayer perceptrons in this setup is that they can approximate any function with arbitrary precision when they have a sufficient number of hidden nodes.

An EA deploys a randomized beam search, which means your evolutionary operators develop candidates to be tested and compared by their fitness. Those operators are usually non-deterministic and you can design them, so they can both find candidates in close proximity and candidates that are further away in the parameter space to overcome the problem of getting stuck in local optima.

EAs are slow because they rely on unsupervised learning: EAs are told that some solutions are better than others but not how to improve them. Neural networks are generally faster, being an instance of supervised learning: They know how to make a solution better using gradient descent within a function space over certain parameters; this allows them to reach a valid solution faster. Neural networks are often used when there is not enough knowledge about the problem for other methods to work.

4. CRYPTANALYSIS OF CLASSICAL CIPHERS USING GAS

There are many approaches and tools that are used in the field of cryptanalysis. One of the successful approaches that achieved promising results is based on GAs. This is mainly due to the nature of GAs that allow reducing the big size of solutions, leading to optimal or likely best solution from this group of solutions. GAs use fitness function to evaluate each solution then select the best one or best group of solutions to generate other children solutions and so on until the cipher is broken. In this section, we report on some interesting aspects of applying GAs in cryptanalyzing classical ciphers.

A. Cryptanalysis of Monoalphabetic Substitution Ciphers

The GA attack on such cipher can be implemented by generated initial keys consisting of permutation of the set of letters. These keys are generated randomly, and after encrypting using each generated key, we can measure the value of fitness of each key. Then, pairs of these keys which have a high fitness value are selected and crossover operation then is used between selected keys to produce new enhancement child keys. After crossover operation is completed, some keys are selected to mutation to enhance the attributes of it by the choice of a random point in a selected key and replacing it with another point. After the two operations are completed, the loop is repeated until the end with suitable stopping [22].

B. Cryptanalysis of Playfair Cipher

For attacking the Playfair cipher using GAs, we should determine the individuals which contain one possible key of the cipher and each individual has its fitness value. One individual is represented as a matrix of 5*5 positions that contain the characters of alphabets distributed randomly. After the generation of the individuals is completed, the selection operation begins according to each individual fitness, so the individual has a highest fitness value that is put in the beginning of the rank. After selection process is completed, the reproduction or crossover operation will begin to produce new children key that may has attribute better than its parents. The crossover operation is implemented by filling

the positions of the child with character of the parents or mutating the child by replacing characters positions locally. The loop continues until meeting the stopping condition.

However, the recovery of the plaintext is not easy to implement usually, for several reasons. One is that words that have double letters may not be counted correctly, due to the fact that the double letters might be split up. Second, because *I* and *J* share a position in the key (typically), all the words that have *I*s and *J*s in them have to be checked using both letters, if the dictionary is fully implemented. Third, the plaintext has no white space to delimit words so being able to tell where words end and begin can be difficult [23].

C. Cryptanalysis of Vernam Cipher

GAs can be used for attacking the Vernam cipher by building a dictionary of words that consist of words that are frequently used in English (e.g., they, the, and when). Then, the fitness value is calculated according to the following steps:[24]

1. Initialize the parameters of the GA and maximum number of iteration
2. Generate random keys which are the population of chromosomes as the 0^{th} generation; each key is a vector with size equal to ciphertext size
3. Decrypt the ciphertext by all generated keys
4. Calculate the fitness function for each chromosome by adding the square value of repeated three letters and four letters which are available in built dictionary. The calculation of fitness function deals with the probability of existing of the three and four letter words in normal English
5. Sort the keys based on decreased fitness values
6. Apply the crossover operator to the parent keys and produce a new generation. Here, a simple two-point crossover can be performed. Furthermore, apply mutation operation by generating two random positions and replace the two letters in these positions by others letters randomly
7. The best key is used to decrypt ciphertext to get the best-decrypted text.

D. Cryptanalysis of Vigenere Cipher

To attack Vigenere cipher using GAs, we should determine the number of attributes that the GA takes as parameters or inputs such as population size, number of individuals tenured per generation, number of random immigrants per generation, number of generations, key length, maximum key length, ciphertext length, known text length, and number of runs per mutation operator combination. These parameters may be used together or some of them might be ignored. The key length parameter is very important, so it must be firstly identified [25].

E. Cryptanalysis of Transposition Ciphers

GAs are very useful to break classical transposition ciphers by finding the sequence of characters that the transposition cipher used. This particular class of algorithms can be used because the automated breaking of such ciphers is very difficult. In spite of that, a number of statistical tools aiding automated breaking have been developed for substitution ciphers, cryptanalysis of transpositions is usually considered to be highly interventionist and demands some knowledge of the likely contents of the ciphertext to give an insight into the order of rearrangement used. Thus, genetic cryptanalyst enables a known plaintext attack to be successfully made, based on only small portion of some plaintext/ciphertext [26].

5. IDENTIFICATION OF CLASSICAL CIPHER TYPE

The typical sequence of steps needs to be followed by cryptanalyst to break any cryptosystems is:[27]

1. The cryptanalyst should determine if the text encrypted by any cipher or it is compressed or generated randomly
2. The cryptanalyst should determine the language of the text
3. The cryptanalyst should determine the type of cipher used in encryption process
4. The cryptanalyst should determine the key used in encryption process
5. The cryptanalyst then uses the key with encrypted data to extract the original data.

When the cryptanalyst wants to identify the cipher type (having just a ciphertext), he/she should extract some features that can lead to estimating the type of cipher. The list below shows a group of features that may help the cryptanalyst in the estimation process:

1. Frequency analysis: Every language has frequency characteristics for its characters such that each character has repeating ratio recognizing it from other characters in normal texts. In English, for example, the letter "*e*" has the greatest frequency ratio (12.70), but the letter "*x*" has the lowest (0.15) [8]. Frequency analysis can be done based on single letter frequency and/or multiple letter frequency (double, triple, etc.). Fig. 5 depicts the typical frequency distribution of single letters in normal English text. Frequency analysis is very useful in differentiating between transposition ciphers and

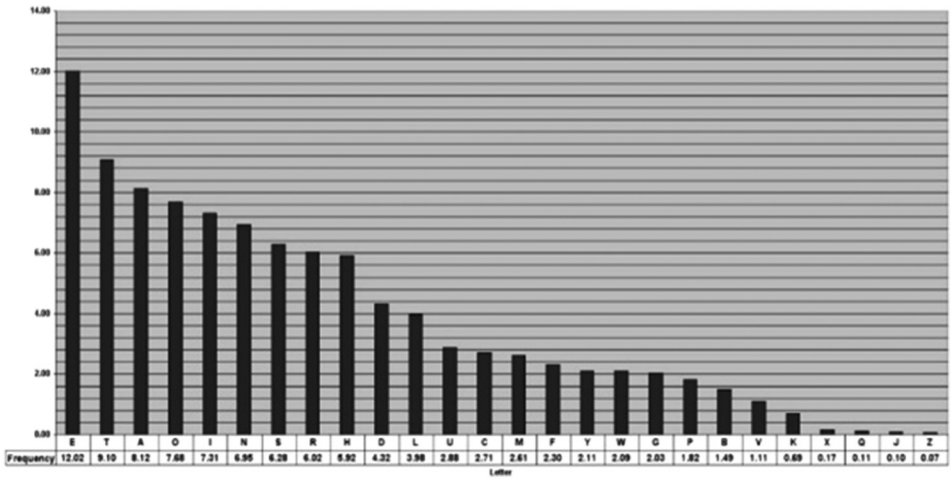

Fig. 5. Frequency distribution of single letters in normal English text[28]

substitution ciphers. Frequency analysis can be used in three main directions:[28]

- The first one is to compute the frequency of ciphertext letters and compare it with the frequency of the original data such that compare the frequency of the letter in ciphertext and natural text and compute the changing in two texts
- The second direction is to compute the frequency of ciphertext letters and find which letters in normal text have the same repeating ratio such that if the letter "*f*" in ciphertext has the same repeating ratio of the letter "*a*" in the original text, we can say the letter "*a*" is encrypted by the letter "*f*."
- Third one is to use frequency analysis to compute if there is any shifting occurs in ciphertext characters such that when the letter "*x*" gives the same ratio of letter "*a*," this indicates that possibly the Caesar cipher which encrypts "*a*" by "*x*" has been used

2. Ciphertext length: The length of ciphertext plays an important role in identification of cipher type where some ciphertext length is exactly divisible by 2 like the Playfair cipher case. Other ciphers (e.g., Hill cipher) can produce ciphertext length divisible by 3, etc.
3. Ciphertext characters number: Some ciphers employee few number of characters such the Baconian cipher which uses just two letters "*a*" and "*b*" in encryption process and the Playfair cipher that uses 25 letters
4. Repeating sections: Periodic polyalphabetic substitution ciphertext has repeating sections with a constant period. This feature can help to identify this type of ciphers [29], [30]
5. AB-BA feature: Ciphertext may contain double sections with its reverse such as "*xy*" and "*yx*." This feature appears in ciphertext produced from Playfair cipher [31]
6. Ciphertext characters type: Some ciphers employee just letters in encryption process another cipher employee letters and numbers [9]
7. Adjacent characters: It can be useful to check if there are any adjacent characters have the same value [28].

6. FUTURE RESEARCH DIRECTIONS

This work lies within a larger team project aiming to design and implement a general cryptanalysis platform for pedagogical purposes. Considering the architectural design of the proposed general cryptanalysis platform, the platform has a number of components or modules including the supervisory module, the crypto-classifier, parallel cryptanalysis modules, feedback and reporting module, graphical analyzer, and the steganography module. Here, we are mainly interested in the crypto-classifier module that is responsible for the identification and classification of the ciphertext type. At least, two levels of classification need to be implemented:[32]

1. Level 1 crypto-classifier: In this module, a first level classification of the considered ciphertext needs to be done so as to decide the general cryptographic category (e.g., classical cipher, block cipher, and public-key cipher) of it. Information obtained from various resource need to be used, and some intelligent classification techniques (such as artificial intelligence, genetics, and neural networks) have to be developed
2. Level 2 crypto-classifier: In the second level of classification, specific algorithm(s) or cipher(s) should

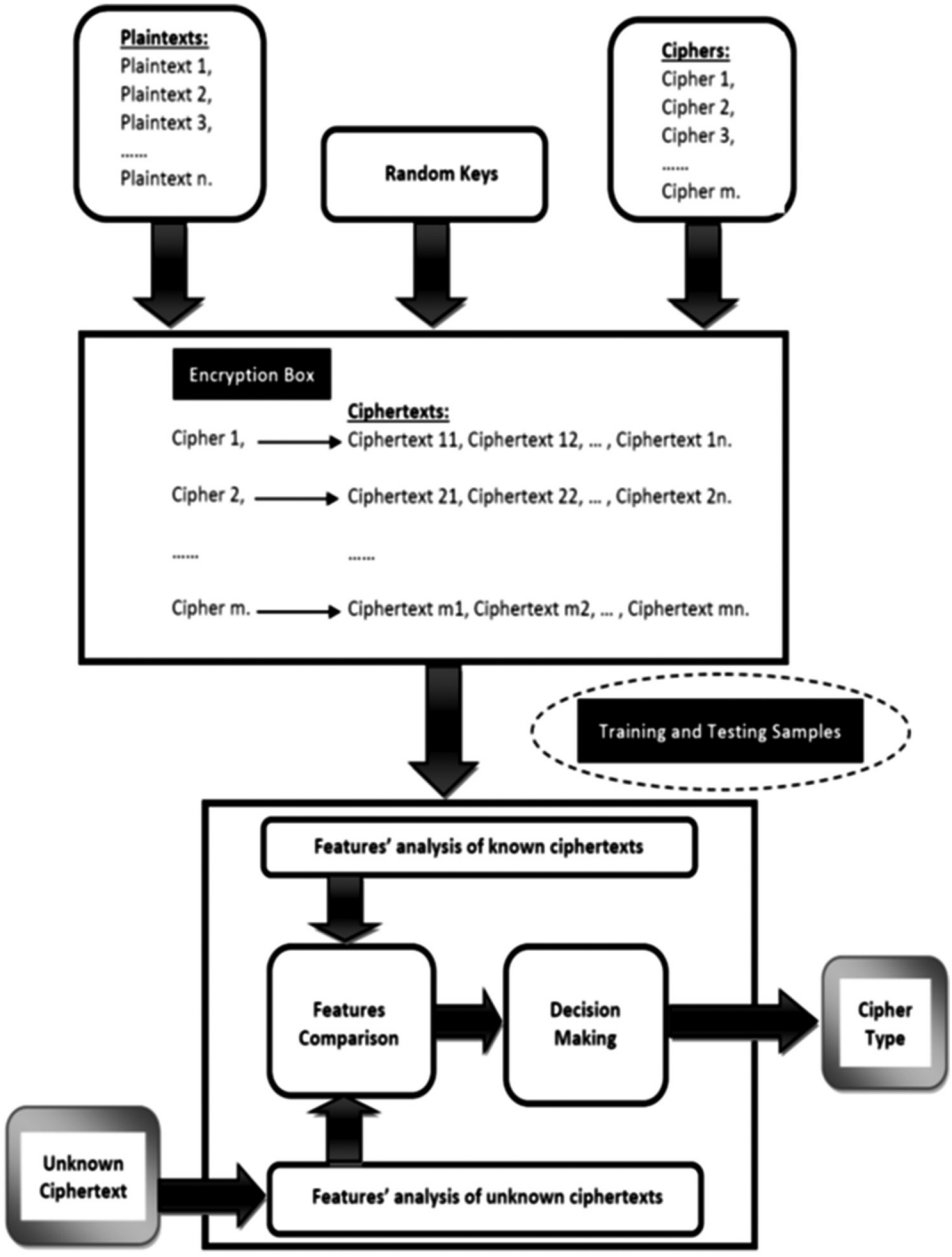

Fig. 6. Data flow of the proposed artificial neural network-based cipher identification process

be assigned for the ciphertext in accordance with the classification done at the first level. For example, if the classifier of level 1 deduced that the ciphertext belongs to the category of block ciphers; level 2 classifier job is to decide which specific block cipher has been used (e.g., DES, AES, and Twofish). Besides the information deduced by different means, some distinguishing characteristics for different ciphers must be known.

Concerning the future research, we are specifically interested in using the estimation capabilities of ANNs to identify the ciphers type. As mentioned previously, ANNs use parallel processing rather than serial computation. This behavior may enable us to move from typical statistical techniques of analyzing any cipher to more powerful generations that provide many solutions at a time. Thus, the analyzing process will depend on how to model ANN

in the correct way and manage the training processes rather than spend the time in mathematical computation of the cipher. Fig. 6 shows the data flow of the proposed estimation process.

The ANN box will have two types of inputs; the first one is a group of training data and the second is a group of testing data. These two groups are managed by ANNs to correct errors produced from estimation process. ANNs would use supervised learning to estimate the cipher type. The number of neurons in the input, hidden, and output layers depend on the number of ciphers used and how much the analyst can extract features from ciphertext.

Several previous works on using ANNs and other techniques for cipher type classification can be found [33]-[37]. However, to the best of authors' knowledge, we could not see specific previous work on using spiking ANNs for this task. Hence, our focus will be directed to this specific application of spiking ANNs. In the first stage, classification of classical ciphers will be considered. In the next stages, other modern cipher types will be taken into consideration also.

7. CONCLUSION

This work is mainly concerned in building automatic tools for various cryptanalysis tasks. This definitely requires the use of suitable intelligent techniques such as GAs and ANNs. The focus here has been on using GAs for cryptanalysis of classical ciphers and adoption of ANNs for cipher type identification. More specific results of cipher classification based on spiking ANNs are going to be presented in a subsequent paper.

REFERENCES

[1] B. Carter, and T. Magoc. "Introduction to classical ciphers and cryptanalysis." A technical report, 11 Sep. 2007. Available: http://www.citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.125.8165. [Feb. 5, 2017].

[2] R. J. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*, USA: John Wiley & Sons, 2010.

[3] W. Stallings. *Cryptography and Network Security Principles and Practice*, 6th ed, Upper Saddle: Pearson Education, Inc., 2014.

[4] M. J. Banks. "A Search-Based Tool for the Automated Cryptanalysis of Classical Cipher." MEng. thesis, Department of Computer Science, The University of York, 2008.

[5] S. Ibrahim, and M. A. Maarof. "A review on biological inspired computation in cryptology." Journal Teknologi Maklumat, vol. 17, no. 1, pp. 90-98, 2005.

[6] S. R. Baragada, and S. Reddy. "A survey of cryptanalytic works based on genetic algorithms." *International Journal of Emerging Trends and Technology in Computer Science (IJETTCS)*, vol. 2, no. 5, pp. 18-22, Sep. Oct. 2013.

[7] H. Bhasin, and A. H. Khan. "Cryptanalysis using soft computing techniques." *Journal of Computer Sciences and Applications*, vol. 3, no. 2, pp. 52-55, 2015.

[8] Department of the Army. *Basic Cryptanalysis*: *Field Manual No. 34-40-2*, *Headquarters*, Washington, DC: Department of the Army, 1990.

[9] F. A. Stahl. "A homophonic cipher for computational cryptography." AFIPS '73 Proceedings of the National Computer Conference and Exposition, New York, pp. 565-568, 4-8 Jun. 1973.

[10] A. K. Kendhe, and H. Agrawal. "A survey report on various cryptanalysis techniques." *International Journal of Soft Computing and Engineering (IJSCE)*, vol. 3, no. 2, May. 2013.

[11] S. Haykin. *Neural Networks and Learning Machines*, 3rd ed, Upper Saddle River, New Jersey: Pearson Education, Inc., 2009.

[12] K. Suzuki. *Artificial Neural Networks-Methodological Advances and Biomedical Applications*, Rijeka, Croatia: InTech, 2014.

[13] S. Davies. "Learning in Spiking Neural Networks." Ph.D. thesis, School of Computer Science, University of Manchester, UK, 2012.

[14] S. M. Bohte, H. La Poutré, and J. N. Kok. "Unsupervised clustering with spiking neurons by sparse temporal coding and multilayer RBF networks." *IEEE Transactions on Neural Networks*, vol. 13, no. 2, pp. 426-435, Mar. 2002.

[15] M. Fatahi, M. Ahmadi, M. Shahsavari, A. Ahmadi, and P. Devienne. "evt_MNIST: A spike based version of traditional MNIST." The 1st International Conference on New Research Achievements in Electrical and Computer Engineering, 2016.

[16] A. Tavanaei, and A. S. Maida. "A minimal spiking neural network to rapidly train and classify handwritten digits in binary and 10-digit tasks." *(IJARAI) International Journal of Advanced Research in Artificial Intelligence*, vol. 4, no.7, pp. 1-8, 2015.

[17] R. Rojas. *Neural Networks*, Berlin: Springer-Verlag, 1996.

[18] S. M. Bohtea, J. N. Koka, and H. La Poutre. "Error-backpropagation in temporally encoded networks of spiking neurons." *Neurocomputing*, vol. 48, no. 1, pp. 17-37, 2002.

[19] D. Goldberg. *Genetic Algorithms*, New Delhi: Pearson Education, 2006.

[20] K. P. Bergmann, R. Scheidler, and C. Jacob. "Cryptanalysis using genetic algorithms." Genetic and Evolutionary Computation Conference GECCO'08, ACM, Atlanta, Georgia, USA, pp. 1099-1100, 12-16 Jul. 2008.

[21] D. B. Fogel. *Evolutionary Computation: Toward a New Philosophy of Machine Intelligence*, 3rd ed, New York: John Wily & Sons, Inc., Publication, 2006.

[22] S. S. Omran, A. S. Al-Khalid, and D. M. Al-Saady. "Using genetic algorithm to break a mono-alphabetic substitution cipher." IEEE Conference on Open Systems, Malaysia, pp. 63-68, 5-7 Dec. 2010.

[23] B. Rhew. "Cryptanalyzing the Playfair cipher using evolutionary algorithms." 9 Dec. 2003. Available: http://www.citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.129.4325. [Jul. 15, 2016].

[24] F. T. Lin, and C. Y. Kao. "A genetic algorithm for ciphertext-only attack in cryptanalysis." *IEEE International Conference on Systems, Man and Cybernetics*, vol. 1, pp. 650-654, 1995.

[25] K. P. Bergmann. "Cryptanalysis Using Nature-Inspired Optimization Algorithms." M.Sc. thesis, Department of Computer Science, The University of Calgary, Alberta, 2007.

[26] R. A. Muhajjar. "Use of genetic algorithm in the cryptanalysis of

transposition ciphers." *Basrah Journal of Scienec A*, vol. 28, no.1, pp. 49-57, 2010.

[27] K. N. Haizel. "Development of an Automated Cryptanalysis Emulator (ACE) for Classical Cryptogram." M.Sc. thesis, Faculty of Computer Science, University of New Brunswick, New Brunswick, 1996.

[28] P. Maheshwari. "Classification of Ciphers." master of technology thesis, Department of Computer Science and Engineering, Indian Institute of Technology, Kanpur, 2001.

[29] M. Nuhn, and K. Knight. "Cipher type detection." Information Sciences Institute, University of Southern California, EMNLP, 2014. Available: https://www.semanticscholar.org/paper/Cipher-Type-Detection-Nuhn-Knight/81e5e15afba9301558a7aaca1400b69e0ddaa027#paperDetail. [Jun. 10, 2016].

[30] K. Pommerening. "Polyalphabetic substitutions." Fachbereich Physik, Mathematik, Informatik der Johannes-Gutenberg-Universit at Saarstraße, Mainz, 25 Aug. 2014. Available: http://www.staff.uni-mainz.de/pommeren/Cryptology/Classic/2_Polyalph/Polyalph.pdf. [Jul. 5, 2016].

[31] G. Sivagurunathan, V. Rajendran, and T. Purusothaman. "Classification of substitution ciphers using neural networks." *IJCSNS International Journal of Computer Science and Network Security*, vol. 10, no. 3, pp. 274-279. Mar. 2010.

[32] S. Al-Janabi, and W. A. Hussien. "Architectural design of general cryptanalysis platform for pedagogical purposes, i-manager's." *Journal on Software Engineering*, vol. 11, no. 1, pp. 1-12, Jul. Sep. 2016.

[33] A. D. Dileep, and C. C. Sekhar. "Identification of block ciphers using support vector machines." International Joint Conference on Neural Networks, Vancouver, BC, Canada, pp. 2696-2701, 16-21 Jul. 2006.

[34] J.G. Dunham, M. T. Sun, and J. C. R. Tseng. "Classifying file type of stream ciphers in depth using neural networks." The 3rd ACS/IEEE International Conference on Computer Systems and Applications, pp. 97, 2005.

[35] S. O. Sharif, L. I. Kuncheva, and S. P. Mansoor. "Classifying encryption algorithms using pattern recognition techniques." IEEE International Conference on Information Theory and Information Security (ICITIS), pp. 1196-1172, 17-19 Dec. 2010.

[36] C. Tan, and Q. Ji. "An approach to identifying cryptographic algorithm from ciphertext." 8th IEEE International Conference on Communication Software and Networks, pp. 19-23, 2016.

[37] W. A. R. de Souza, and A. Tomlinson. "A distinguishing attack with a neural network." IEEE 13th International Conference on Data Mining Workshops, pp. 154-161, 2013.

ORIGINAL RESEARCH ARTICLE UHD JOURNAL OF SCIENCE AND TECHNOLOGY

Application of Artificial Bee Colony Algorithm in Power Flow Studies

Kassim Al-Anbarri and Husham Moaied Naief

Department of Electrical Engineering, Faculty of Engineering, Mustansiriyah University, Bab Al-Muadham Campus, 46049 Baghdad, Iraq

ABSTRACT

Artificial bee colony (ABC) algorithm is one of the important artificial techniques in solving general-purpose optimization problems. This paper presents the application of ABC in computing the power flow solution of an electric power system. The objective function to be minimized is the active and reactive power mismatch at each bus. The proposed algorithm has been applied on typical power systems. The results obtained are compared with those obtained by the conventional method. The results obtained reveal that the ABC algorithm is very effective for solving the power flow problem in the maximum loadability region.

Index Terms: Artificial Bee Colony, Maximum Loadability, Power Flow, Swarm Artificial Technique

1. INTRODUCTION

The power flow analysis is one of the important and extensively used studies in electrical power system engineering. It is considered a fundamental tool for many other power system studies such as stability, reliability, fault, and contingency study. The main objective of a power flow study is to find the bus voltages and the power flow in the transmission system for a particular loading condition. The steady-state performance of an electrical power system is described by a system of non-linear algebraic equations. These equations represent the active and reactive power balance. The inherent difficulty of the power flow problem is the task of obtaining analytical solutions to the power flow equations. An extensive research has been carried out since the latter half of the twentieth century [1], [2] to solve this problem. The solution of power flow problem has been based on numerical technique methods such as Gauss-Seidel [3], Newton-Raphson method [4]-[14], and fast-decoupled method [15]-[18]. Although some of these methods are widely used in power utilities, they are sensitive to the starting (guess) values. In some cases, especially in heavily loaded conditions, they fail to converge. It was found that the factors affecting the convergence of the previous methods are the R/X ratio of the transmission systems and the singularity of the Jacobian matrix for a heavily loaded system. Different attempts have been done to improve the reliability of these methods [19], [20]. Artificial intelligence techniques had been applied to power flow study [21]-[23]. Recently, the fields of swarm intelligence have attracted many researches as a branch of artificial intelligence that deals with the collective behavior of swarms such as flocks of bird, colonies of aunts, schools of fish, and swarm of bees [24], [25]. The important features of swarm intelligence are self-organization, scalability, adaptation, and speed. The swarm intelligence techniques have been applied in many power system studies [26]-[28]. In this paper, the load flow problem is approached as an optimization problem using

Access this article online

DOI: 10.21928/uhdjst.v1n1y2017.pp11-16

E-ISSN: 2521-4217
P-ISSN: 2521-4209

Corresponding author's e-mail: alanbarri@yahoo.com

Received: 10-03-2017 Accepted: 25-03-2017 Published: 12-04-2017

swarm intelligence. The objective function is to minimize the power mismatch. This paper is organized as follows: Section 2 reviews the Newton-Raphson (NR) technique in solving load flow problem. The basics model of artificial bee colony (ABC) is presented in section 3. Section 4 discusses the results obtained by applying the proposed algorithms on a typical system. Finally, section 5 presents the conclusion.

2. POWER FLOW FORMULATION

For N bus electrical power system, the bus power S_i can be expressed by the following equation:

$$S_i=S_{Gi}-S_{Di}$$

$$S_i=P_{Gi}-P_{Di}+j(Q_{Gi}-Q_{Di}) \quad (1)$$

Where P_{Gi} is the active power generation at bus i

P_{Di} is the active power demand at bus i

Q_{Gi} is the reactive power generation at bus i

Q_{Di} is the reactive power demand at bus i

The current balance equation at bus i

$$I_i=\frac{S_i^*}{V_i^*}=\sum_{k=1}^{N}Y_{ik}V_k \quad (2)$$

Where Y_{ik} is the i, k^{th} element of bus admittance matrix

V_k is the bus voltage at bus k.

By substituting (1) into the (2) and resolved the resulting equation into the following two real equations:

$$P_k=\sum_{i=1}^{N}|V_k||V_i||Y_{ki}|\cos(\gamma_{ki}+\delta_i-\delta_k) \quad (3)$$

$$Q_k=\sum_{i=1}^{N}|V_k||V_i||Y_{ki}|\sin(\gamma_{ki}+\delta_i-\delta_k) \quad (4)$$

For N bus power system, there are $2N$ real non-linear algebraic equations similar to (3) and (4). These equations are non-linear function of the state variables ($|V|,\delta$). The conventional technique to solve these equations is using a numerical technique. The most widely used method is NR method. This method is based on expanding the above equations by Taylor series. The compact linearized form of the above equations is as follows:

$$\begin{bmatrix}\Delta P_i\\ \Delta Q_i\end{bmatrix}=\begin{bmatrix}J_{P\delta} & J_{P|V|}\\ J_{Q\delta} & J_{Q|V|}\end{bmatrix}\begin{bmatrix}\Delta\delta_i\\ \Delta|V|_i\end{bmatrix} \quad (5)$$

Where the left-hand side of (5) is the vector of power mismatch, which can be calculated as:

$$\begin{bmatrix}\Delta P_i\\ \Delta Q_i\end{bmatrix}=\begin{bmatrix}P_i^{sp}-P_i^{cal}\\ Q_i^{sp}-Q_i^{cal}\end{bmatrix} \quad (6)$$

The traditional algorithm for obtaining power flow solution is as follows:

1. Assume a guess values for the state variables (flat start $|V|=1.0$ pu; $\delta=0$)
2. Evaluate the vector of power mismatch and the elements of the Jacobian matrix
3. Calculate the vector of state variable disturbance
4. Update the state variables at the end of iteration
5. Check the absolute value of the elements of the vector of power mismatch, if it is less than a specified tolerance; calculate the line flow in each transmission line. Otherwise, go to step 2.

The previous algorithm works reliably in ordinary loading conditions. Unfortunately, it is found in some cases (e.g., heavily loaded conditions and high R/X ratio system) that the above algorithm fails to converge. This is because of singularity of the Jacobian matrix. For this purposes, a swarm intelligence technique is presented to avoid the singularity of the Jacobian matrix.

3. POWER FLOW ALGORITHM USING ABC METHOD

The honey bees foraging behavior, learning, and memorizing characteristics have been attracted many researcher in the area of swarm intelligence. The pioneer work of Karaboga [24] which describes an ABC algorithm based on the behavior of honey bee is first attempt model in this aspect. One of the main features of ABC algorithm is its ability to conduct both global search and local search in each iteration.

According to the ABC algorithm, there are three categories of artificial bees in the colony. These are employed bees, onlookers bees, and scouts bees. The bee colony is divided into two halves, the first half of colony includes employed bees, and the second half includes the onlookers. The onlooker's bees are those waiting on the dance area in hive as a decision-maker for choosing the suitable food source. The employed bees are those collecting the nectar from food

source. While the scout bees are those searching the food sources. The searching cycle in the ABC algorithm consists of the following steps [29]:

- At the initialization step, the bees select a set of food source positions randomly. After determining the nectar amount, the bees come to the hive to share the information with those waiting on the dance area.
- At the second step, the employed bees use the gained information to choose new food sources in neighborhood area after going to the old position, which is visited by themselves previously.
- At the third stage, the onlooker bee chooses a particular area for the food sources depending on the information given by the employed bees on the dance area.

To utilize the ABC algorithm, there are some control parameters that should be set [30]; they are number of variables, lower bound of variables (LB), upper bound of variables (UB), population size (colony size) (nPop), number of onlooker bees (nn Onlooker), maximum number of iterations (MaxIt) (the stopping criteria), abandonment limit parameter (Limit), and acceleration coefficient upper bound (A).

A. Steps of ABC Implementation

The steps of ABC can be outlined as follows [31]:

1. Generate a randomly distributed initial population solutions (food source positions).
2. Evaluate the population which represents the nectar quantity. The population of the positions (solutions) is subjected to iterated cycles, C =1, 2,…, C_{max}, of the search processes of the employed bees, the onlooker bees and scout bees. Based on a probabilistic approach, the artificial employed or onlooker bee makes a change on the position (solution) in her memory for finding a new food source and tests the nectar amount (fitness value) of the new source (new solution).
3. Apply the roulette wheel selection (choose the best fit individuals).
4. Calculate the probability rate (*Pi*) related with solutions;

$$P_i = \frac{fit_i}{\sum_{i=1}^{npop} fit_i} \tag{7}$$

The fitness values (*fit*) are computed by the following expression:

$$fit_i = \begin{cases} \dfrac{1}{1+f_i} & \text{if } f_i \geq 0 \\ 1+\text{abs}(f_i) & \text{if } f_i < 0 \end{cases} \tag{8}$$

Usually, the value of P_i is between {0,1}.

5. Find the new solutions for the onlookers depending on the probability P_i related with the solutions.
6. Reapply roulette wheel selection.
7. Find the abandoned solution if exists, change it with new randomly generated solution.
8. Register the best solution achieved so far.
9. C=C+1 (until maximum cycle number is reached).

B. ABC Implementation for Power Flow Study

ABC optimization is applied to obtain the bus voltage magnitude ($|V_i|$) and voltage phase angle (δ_i) by minimize the following objective function:

$$\min f(\delta, |V|) \tag{9}$$

Where,

$\delta=(\delta_1,\ldots\ldots\ldots\ldots, \delta_n)$

$|V|=(|V_1|,\ldots\ldots\ldots\ldots, |V_n|)$

This objective function is constrained by the inequalities LB and UB.

$LB<|V|<UB$

$LB<\delta<UB$

The optimization process starts with setting the number of solutions (food sources) in ABC algorithm, which represents the number of flowers, the bees will reach to food sources, and then computes the nectar's quantity, the food sources are initialized using a random number generator.

The voltage magnitude and voltage phase angle are limited to the following range:

$0.5<|V_i|<1.05$

$-5<\delta_i<5$

The objective function (*f*) that designed to determine the load flow problem using ABC algorithm is as follows:

$$f = \sqrt{\sum \Delta P_i^2 + \sum \Delta Q_i^2} \tag{10}$$

Where i = 1, 2, 3,… number of buses

In ABC algorithm, the objective function (fitness value) describes the quality of food source (solution). The food

source that has the best quality will be registered in a memory as the best food source (solution) ever found. The neighborhood search process uses to obtain the best fitness value will continue by employed bees and onlookers. The fitness value will be computed for each new solution (food source), and the new solution (food source) that having the best fitness value will be the new reference in memory. The optimization process will continue to looking for the food source near to hive, which depending on the probability that computed previously from fitness value. The new solution (food source) after neighborhood search will be registered if its fitness is better. The optimization process will continue until reach to the best fitness value or reach to the maximum cycle number afterward the solution converges and the mismatch power is close to zero. The flow chart of ABC approach in load flow computation is shown in Fig. 1.

4. RESULTS AND DISCUSSION

The ABC algorithm is being applied to the 6-bus system as follows:

A. Six Bus Test Power System with Normal Load

The ABC method is applied to the 6-bus system with a particular normal loading condition [32]. The test system is shown in Fig. 2 consists of three generating stations and three load stations. After initialize the control parameters of ABC algorithm, each variable was initialized with random number using random number generator. The elements of power mismatch vectors ΔP and ΔQ are computed using Equation 6. The best food source (load flow solution) will be selected by applying roulette wheel selection.

A comparison between the results that obtained from conventional (NR) with that found from ABC algorithm is given in Table I. As shown from these tables, the results obtained are identical. The final objective function value in ABC optimization process after 15000 iterations is 1.5902×10^{-11}. The performance of ABC algorithm to obtain the best solution is clarified by graph that was shown in Fig. 3.

TABLE I
The Bus Voltages using NR Method and ABC Technique

Bus No.	NR-method		ABC algorithm	
	V_i	δ_i	V_i	δ_i
1	1.05	0	1.05	0.0
2	1.05	−3.635	1.05	−3.635016
3	1.07	−4.117	1.07	−4.117675
4	0.989	−4.18	0.989013	−4.180701
5	0.9813	−5.306	0.981364	−5.306448
6	1.004	−5.856	1.004079	−5.856946

ABC: Artificial bee colony, NR: Newton-Raphson

B. Six Bus Test Power System with Heavy Load

To simulate the heavy load condition, the load at bus 4, 5, and 6 is increased as shown in Appendix A. It is found that the conventional NR method is failed to converge. However, when the ABC algorithm is applied, the solution converges as shown in Table II. The final objective function value in ABC optimization process after 5000 iteration is 8.99×10^{-4}. The

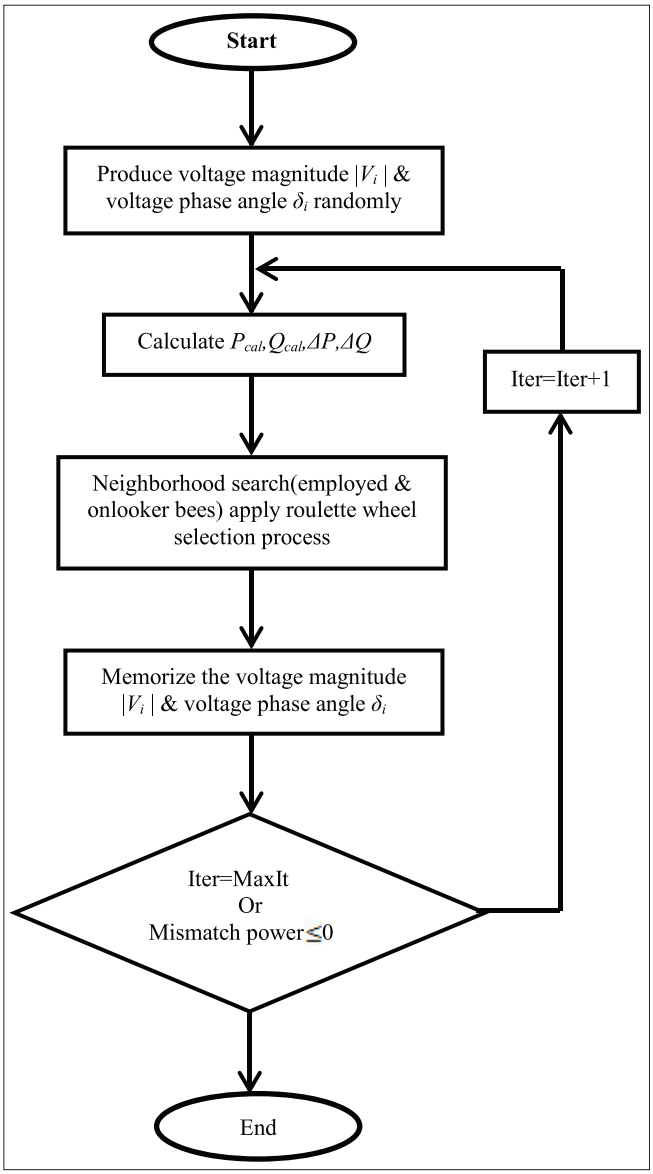

Fig. 1. Flow chart of application of artificial bee colony technique in power flow study

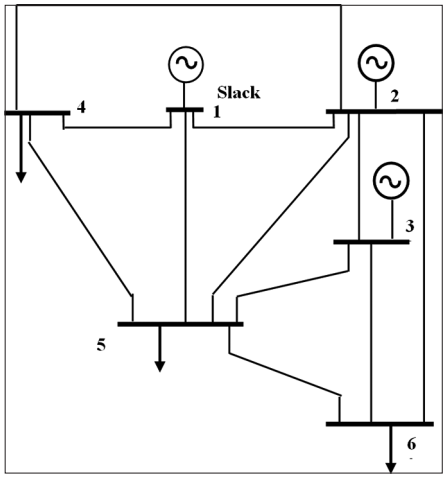

Fig. 2. Six bus test power system

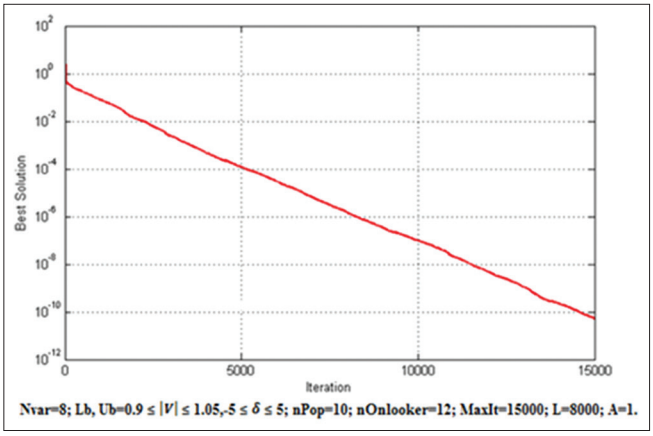

Fig. 3. The performance of artificial bee colony algorithm, best solution versus iteration

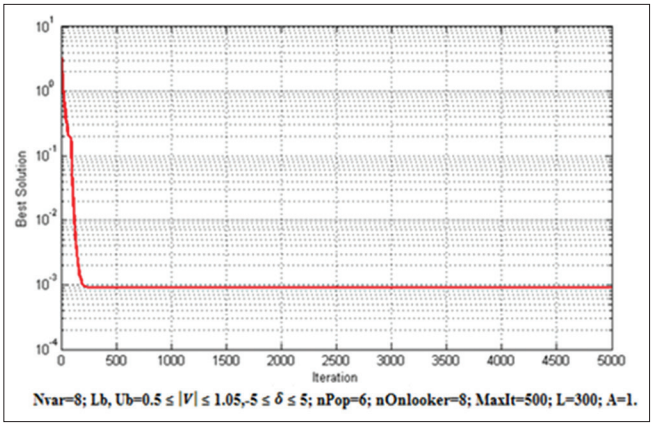

Fig. 4. The performance of artificial bee colony algorithm, best solution versus iteration

performance of ABC method to obtain the best solution is clarified by graph that was shown in Fig. 4.

TABLE II
The Bus Voltages for the Heavily Loaded Case using ABC Technique where the NR Method Fails to Solve

Bus No.	V_i	δ_i
1	1.0500	0
2	1.0500	−52.3630
3	1.0700	−63.0819
4	0.7575	−46.0854
5	0.6721	−58.3285
6	0.8341	−68.0498

ABC: Artificial bee colony, NR: Newton-Raphson

5. CONCLUSION

A meta-heuristic approach to solve power flow problem has been presented. The proposed algorithm is based on ABC technique which is considered to be one of the type of swarm intelligence techniques. The proposed algorithm is applied to the six bus system with different loading conditions, and the results obtained have been compared with the results of (NR) method. The main advantages of ABC algorithm are the flexibility of modeling, accuracy, strong convergence, and reliability, which considered reasonable and acceptable optimization process. In addition, the presented algorithm shows promising results regarding heavily loaded system.

6. ACKNOWLEDGMENT

The author would like to thank the Department of Electrical Engineering, Faculty of Engineering, Mustansiriyah University (www.uomustansiriyah.edu.iq), Baghdad, Iraq, for its support in the present work.

REFERENCES

[1] M. A. Laughton and M. W. H. Davies, "Numerical techniques in solution of power system load flow problems."*Proceedings of the Institution of Electrical Engineers,* vol. 111, No. 9, pp. 1575-1588, Sept. 1964.

[2] L. L. Freris and A. M. Sasson, "Investigation of the load-flow problem." *Proceedings of the Institution of Electrical Engineers*, vol. 115, No. 10, pp. 1459-1465, Oct. 1968.

[3] S. Moorthy, M. Al-Dabbagh and M. Vawser, "Improved phase-coordinate gauss-seidel load flow algorithm."*Electric Power System Research,* vol. 34, pp. 91-95, 1995.

[4] W. F. Tinney and C. E. Hart, "Power flow solution by Newton's method." *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-86, pp. 1449-1460, Nov. 1967.

[5] B. Stott, "Effective starting process for Newton-Raphson load flows." *Proceedings of the Institution of Electrical Engineers*,

vol. 118, no. 8. pp. 983-987, Aug. 1971.

[6] R. G. Wasley and M. A. Shlash, "Newton-Raphson algorithm for 3-phase load flow." *Proceedings of the Institution of Electrical Engineers*, vol. 121, No. 7, pp. 630-638, Jul. 1974.

[7] M. E. El-Hawary and O. K. Wellon, "The ALPHA-modified quasi-second order Newton-Raphson method for load flow solutions in rectangular form." *Proceedings of the Institution of Electrical Engineers*, vol. PAS-101, pp. 854-866, 1982.

[8] A. J. Flueck and H. D. Chiang, "Solving the nonlinear power flow equations with an inexact Newton method using GMRES." *IEEE Transactions on Power Systems*, vol. PWRS-13, No. 2. pp. 267-273, May. 1998.

[9] M. D. Schaffer and D. J. Tylavsky, "A non-diverging polar form Newton based power flow." *IEEE Transactions on Industry Applications,* vol. 24, No. 5, pp. 870-877, 1998.

[10] V. M. da Costa, N. Martins and J. L. R. Pereira, "Developments in the Newton-Raphson power flow formulation based on current injections." *IEEE Transactions on Power Systems,* vol. 14, No. 4, pp. 1449-1456, Nov. 1999.

[11] Y. Xiao and Y. H. Song, "Power flow studies of a large practical power network with embedded FACTS devices using improved optimal multiplier Newton-Raphson method." *European Transaction on Electrical Power*, vol. 11, No. 4, pp. 247-256, Jul. Aug. 2001.

[12] M. Irving, "Pseudo-load flow as a starting process for Newton Raphson algorithm." *International Journal of Electrical Power and Energy Systems*, vol. 32, pp. 835-839, 2010.

[13] T. Kulworawanichpong, "Simplified Newton-Raphson power flow solution method." *International Journal of Electrical Power and Energy Systems*, vol. 32, pp. 551-558, 2010.

[14] S. M. R. Slochanal and K. R. Mohanram, "A novel approach to large scale system load flows Newton-Raphson method using hybrid bus." *Electric Power Systems Research,* vol. 41, pp. 219-223, 1997.

[15] B. Stott, "Decoupled Newton load flow." *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-91, pp. 1955-1959, 1972.

[16] B. Stott and O. Alsac, "Fast decoupled load flow." *IEEE Transactions on Power Apparatus and Systems,* vol. PAS-93, No. 3. pp. 859-869, May. Jun. 1974.

[17] K. Behnam-Guilani, "Fast decoupled load flow: The hybrid model," *IEEE Transactions on Power Systems*, vol. PWRS-3, No. 2, pp. 734-742, May. 1988.

[18] A. V. Garcia and M. G. Zago, "Three-phase fast decoupled power flow for distribution networks." *IEE Proceedings-Generation, Transmission and Distribution*, vol. 143, No. 2, pp. 188-192, Mar. 1997.

[19] S. C. Tripathy, G. D. Prasad, O. P. Malik and G. S. Hope, "Load flow solutions for ill-conditioned power systems by a Newton-like method," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-101, pp. 3648-3657, Oct. 1982.

[20] D. Rajicic and A. Bose, "A modification to the fast decoupled power flow for networks with high R/X ratios." *IEEE Transactions on Power Systems*, vol. PWRS-3, No. 2, pp. 743-746, May. 1988.

[21] X. Yin, "Application of genetic algorithms to multiple load flow solution problem in electrical power systems." Proceedings of the 32nd Conference on Decision and Control, Texas, pp. 3734-3738, 1993.

[22] W. L. Chan, A. T. P. So and L. L. Lai, "Initial applications of complex artificial neural networks to load-flow analysis." *IEE Proceedings-Generation, Transmission and Distribution,* vol. 147, No. 6, pp. 361-366, Nov. 2000.

[23] P. Acharjee and S. K. Goswami, "Simple but reliable two-stage GA based load flow," *Electric Power Components and Systems,* vol. 36, pp. 47-62, 2008.

[24] D. Karaboga, "An idea based on honey bee swarm for numerical optimization," Technical Report-TR06, Erciyes University, Kayseri, Turkey, 2005.

[25] B. Akay and D. Karaboga, "A modified artificial bee colony algorithm for real-parameter optimization" *Information Science*, vol. 1, pp. 120-142, Jun. 2010.

[26] S. J. Huang, X. Z. Liu, W. F. Su, and T. C. Ou, "Application of enhanced honey-bee mating optimization algorithm to fault section estimation in power systems." *IEEE Transaction on Power Delivery*, vol. 28, no. 3, pp. 1944-1951, Jul. 2013.

[27] M. Afzalan and M. A. Taghikhani, "Placement and sizing DG using PSO and HBMO algorithms in radial distribution networks" *International Journal of Intelligent System and Applications*, vol. 4, no. 10, pp. 43-49, Sep. 2012.

[28] N. T. Linh and D. X. Dong, "Optimal location and size of distributer generation in distribution system by artificial bees colony algorithm" *International Journal of Information and Electronics Engineering,* vol. 3, no. 1, pp. 63-67, Jan. 2013.

[29] D. Karaboga and B. Basturk, "A powerful and efficient algorithm for numerical function optimization: Artificial bee colony(ABC) algorithm." *Journal of Global Optimization,* vol. 39, pp. 459-471, 2007.

[30] M. S. Kiran and M. Gündüz, "The analysis of peculiar control parameters of artificial bee colony algorithm on the numerical optimization problems." *Journal of Computer and Communications,* vol. 2, pp. 127-136, Mar. 2014.

[31] K. Al-Anbarri, A. H. Miri, and S. A. Hussain, "Load frequency control of multi-area hybrid power system by artificial intelligence techniques." *International Journal of Computer Applications*, vol. 138, no. 7, Mar. 2016.

[32] A. J. Wood and B. F. Wollenberg, *Power Generation, Operation and Control*, 2nd ed, New York, NY: John Wiley & Sons Ltd., 1996.

APPENDIX A
Buses Data of 6-Bus Case with Heavily Loaded Condition

Bus No.	|V|pu	δ (°)	P_G (MW)	Q_G (MVAR)	P_D (MW)	Q_D (MVAR)
1	1.05	0	0	0	0	0
2	1.05	0	80	0	0	0
3	1.07	0	90	0	0	0
4	1.0	0	0	0	255	130
5	1.0	0	0	0	255	130
6	1.0	0	0	0	255	152

ORIGINAL RESEARCH ARTICLE UHD JOURNAL OF SCIENCE AND TECHNOLOGY

Mathematical Modeling of Sampling, Quantization, and Coding in Sigma Delta Converter using Matlab

Azeez Abdullah Azeez Barzinjy, Haidar Jalal Ismail, and Mudhaffer Mustafa Ameen

Department of Physics, College of Education, Salahaddin University-Erbil, Zanko, Erbil, Iraq

ABSTRACT

The received analog signal must be digitized before the digital signal processing can demodulate it. Sampling, quantization, and coding are the separate stages for the analog-to-digital adaptation procedure. The procedure of adapting an unceasing time-domain signal into a separate time-domain signal is called sampling. While, the procedure of adapting a separate-time, continuous-valued signal into a discrete-time, discrete-valued signal is known as quantization. Thus, quantization error is the mismatch between the unquantized sample and the quantized sample. The method of demonstrating the quantized samples in binary form is known as coding. This investigation utilized Matlab® program to recommend a proper scheme for a wireless-call button network of input signal, normalized frequency, and over-sampling ratio against signal-to-quantization noise ratio. Two vital characteristics of this wireless network design are cost-effective and low-power utilization. This investigation, through reducing the in-band quantization error, also studied how oversampling can enhance the accomplishment of an analog-to-digital adapter.

Index Terms: Analog-to-digital Adapter, Coding, Matlab, Quantization Error, Wireless Network

1. INTRODUCTION

It is not easy to decide precisely when and how the first data converter was established. The most primitive documented binary analog-to-digital adaptor recognized is not electronic at all but hydraulic. To the best of our knowledge, the optimum historical review regarding the analog-to-digital adapters, in general, can be found in the study of Kester *et al.* [1].

The analog domain is unceasing with both time and signal magnitude, while the digital domain is independent on both time and magnitude. A single binary value signifies a variety of analog values in the quantization band nearby its code center point. Analog values that are not precisely at the code center point have an allied amount of quantization error [2].

It can be stated that sigma-delta [3] analog-to-digital adapter is a most common approach of over-sampling analog-to-digital adapter. The map processor of a sigma-delta analog-to-digital adapter is displayed in Fig. 1 [4].

The sigma-delta analog-to-digital adapter can be divided into two lumps, the quantizing and the decimating parts. Essentially, decimation is the act of decreasing the data rate down from the over-sampling rate without losing information. The quantizing part contains the analog integrator, the 1-bit analog-to-digital adapter, and the 1-bit digital-to-analog adapter [5]. The task of the quantizing part is to adapt the data in the analog input into digital shape. The input-output relationship of the sigma-delta quantizer is

Access this article online

DOI: 10.21928/uhdjst.v1n1y2017.pp17-22

E-ISSN: 2521-4217
P-ISSN: 2521-4209

Corresponding author's e-mail: azeez.azeez@su.edu.krd

Received: 10-03-2017 Accepted: 25-03-2017 Published: 12-04-2017

non-linear; nevertheless, the capacity of frequency depression for the analog input, explicitly $x(t)$, might be retrieved from the quantizer yield, namely, $y[n]$ as shown in Fig. 1. $y[n]$ is a restricted order with sample values equivalent to −1 or +1. $y[n]$ may just stay restricted if the output collector, $w[n]$, is bounded similarly. As a result, the typical value of $y[n]$ is needed to be equivalent to the mean value of the input $x(t)$. Accordingly, the authors have been capable of solving $w[n]$ to obtain the constant of $x(t)$ [6].

This investigation suggests a 1-bit analog-to-digital converter which can be utilized as an alternative of a more costly multi-bit analog-to-digital converter. This can be done through studying two divergent procedures that permit a 1-bit analog-to-digital converter to attain the enactment of a multi-bit analog-to-digital converter. The authors will also investigate the superiority and drawbacks of both these procedures. Relying on this exploration, one of the two procedures is selected for our data radios.

2. THEORY

$x_a(t)$ is an analog signal ant it behaves similar to the input to an analog-to-digital adapter. Equations 1 and 2 describe $x_a(t)$ and the average power in $x_a(t)$, correspondingly [7].

$$x_a(t) = \frac{A}{2}\cos \omega t \tag{1}$$

$$\sigma_x = \frac{1}{T}\int_0^T [x_a(t)]^2 dt = \frac{A^2}{8} \tag{2}$$

To prototype this analog signal, assume a b-bit analog-to-digital adapter. Conditionally, if the analog signal possesses

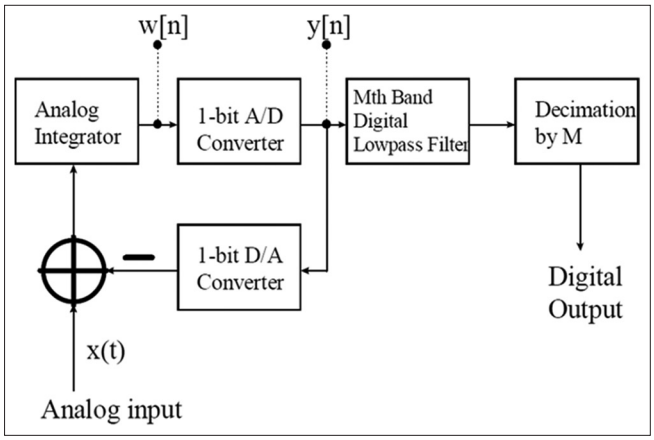

Fig. 1. Sigma-delta analog-to-digital converter

peak-to-peak amplitude of A, and subsequently, the minimum potential step, ΔV, by means of b bits is given by Equation 3:

$$\Delta V = \frac{A}{(2^b - 1)} \cong \frac{A}{(2^b)} \tag{3}$$

Quantization noise, or quantization error, is a unique restricting parameter for the effective range of an analog-to-digital adaptor [8]. This error is essentially the "round-off" error that happens when an analog signal is quantized.

A quantized signal may be different as of the analog-signal by just about $\pm(\Delta V/2)$. Supposing a quantization error is equivalently distributed ranging from $-\Delta V/2$ to $\Delta V/2$, then the root mean square of the quantization noise power, σ_e, is identified by Equation 4 [9].

$$\sigma_e^{\,2} = \frac{(\Delta V)^2}{12} = \frac{A^2}{\left(2^{2b}\right)12} \tag{4}$$

Using Equations 2 and 4, the signal-to-quantization noise ratio (SQNR) for our b-bit analog-to-digital converter might be assessed [10] as follows:

$$SQNR = \frac{\sigma_x}{\sigma_e} = \frac{3}{2}2^{2b} \tag{5}$$

The SQNR in decibels is assumed through Equation 6 [11].

$$SQNR(\text{dB}) = 10\ log_{10} SQNR = 1.76 + 6.02b \tag{6}$$

Equation 6 is an illustration of the SQNR of an analog-to-digital adaptor which rises through almost 6 dB per every single added bit.

One can realize that the assessed signal through the analog-to-digital adaptor is at baseband. Thus, a uniform spectrum in the frequency ranges from 0 to $F_s/2$ is the characteristic of the root mean square quantization noise power, σ_e. The noise power for each unit of bandwidth can be assumed using Equation 7.

$$N_o = \frac{\sigma_e}{(F_s/2)} = \frac{A^2}{\left(2^{2b}\right)6F_s} \tag{7}$$

The Nyquist frequency, which termed after Harry Nyquist, is basically twice the input signal bandwidth F_m. Recalling that F_m for a baseband signal expands from 0 to F_m [12]. The entire quantization noise power in the concerned band or the in-band noise is specified through Equation 8.

$$N_o(F_m)=\frac{A^2}{\left(2^{2b}\right)6F_s}(F_m)=\frac{A^2}{\left(2^{2b}\right)6}\left(\frac{F_m}{F_s}\right) \quad (8)$$

Equation 8 might be examined to classify which limits disturb the in-band quantization error in analog-to-digital adaptor. Where A is the amplitude of the signal and F_m is half Nyquist frequency, both of them are relying on signal, while the analog-to-digital adaptor has no dominance above these. Nevertheless, the available analog-to-digital bits number, b, and the specimen frequency, F_s, are organized through the analog-to-digital adaptor scheme [13].

The act of sampling the input signal at frequencies considerably higher than the Nyquist frequency is called oversampling.

By means of Equation 8, a correlation might be resulting for the over-sampling segment, $M = F_s/2F_m$, like that the two analog-to-digital adaptors offer an identical in-band error power [14]. After allowing $F_s = 2F_m$, Equation 8 becomes:

$$\frac{A^2}{\left(2^{2b}\right)6}\left(\frac{F_m}{F_s}\right)=\frac{A^2}{\left(2^{2\beta}\right)12} \quad (9)$$

By means of Equation 9, one can acquire Equation 10.

$$(\beta-b)=+\frac{1}{2}\log_2(M) \quad (10)$$

$(\beta-b)$ means the additional determination bits which are in consequence gained out of a b-bit adaptor by means of oversampling. The above equation, also, indicates that each duplication of the over-sampling proportion rises the actual bits at the Nyquist frequency by 0.5 [15].

$$H(z)=\frac{1-z^{-M}}{1-z^{-1}} \quad (11)$$

Mitra [16] relates the enactment of a sigma-delta analog-to-digital adaptor through that of a linear over-sampling analog-to-digital adaptor. The enhancement in enactment achieved by means of a sigma-delta analog-to-digital adaptor is illustrated in Equation 10 [17].

$$Enhancement(M)=-5.1718+20\log_{10}(M) \quad (12)$$

The power spectral density, $S_x(f)$, is the strength of the variations as a function of frequency. For an arbitrary time signal $x_a(t)$, the power spectral density can be given by Equation 13.

$$S_x(f)=\lim_{T\to\infty}E\left\{\frac{1}{2T}\left|\int_{-T}^{T}x(t)e^{-i\omega t}dt\right|^2\right\} \quad (13)$$

Power spectral density computation can be made straightforwardly through the fast Fourier transform method.

3. RESULTS AND DISCUSSIONS

A. Power Spectral Density

A first-order integrator which might be demonstrated as a collector has been utilized by the straightforward sigma-delta quantizer [18]. The Matlab® program imitates the occupied first-order sigma-delta adaptor. The power spectral density, Equation 13, of the stimulus signal can be illustrated in Fig. 2. In addition, the stimulus signal has been over sampled at a level of 50 times Nyquist. It can be notice in Fig. 2 indicated that the normalized frequency is schemed against power spectral density possessing a range from 0 to 1 knowing that 1 indicating 50 Nyquist frequency [19].

Analogous tendency has been obtained by Belitski *et al.* [20] which indicates that the proposed model is appropriate for sampling, quantization, and coding in sigma-delta converter.

$y[n]$ is the digital signal characterized by means of 1-bit. The power spectral density of $y[n]$ is plotted in Fig. 3 against the normalized frequency.

Fig. 3 shows the noise forming aptitudes of the sigma-delta analog-to-digital converter. As stated previously, a straightforward over-sampling analog-to-digital converter is capable to diffuse the overall quantization error power

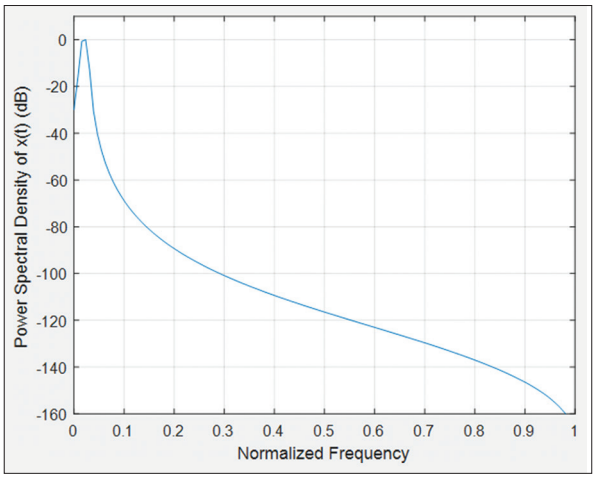

Fig. 2. Power spectral density of input signal after oversampling

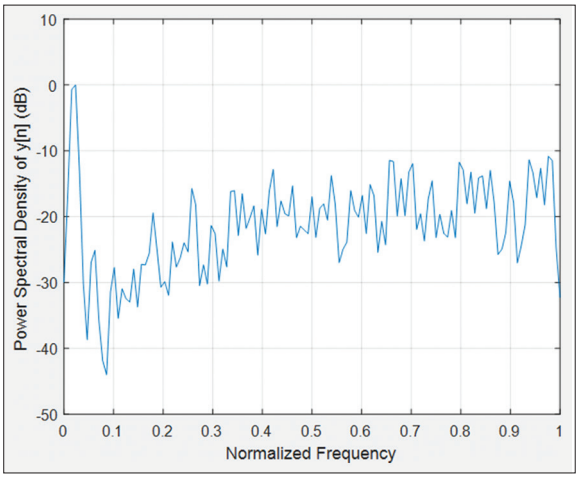

Fig. 3. Power spectral density of *y*[*n*] versus normalized frequency

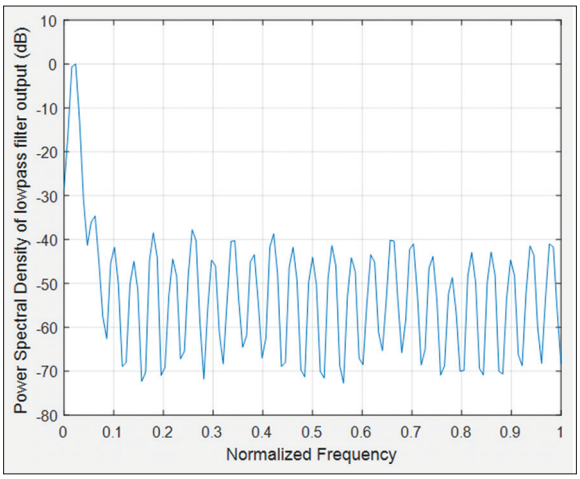

Fig. 4. Power spectral density versus normalized frequency of low-pass filter output

above a longer band, thus reducing the in-band error power. Alternatively, Overney *et al.* [21] utilize Josephson voltage standard to achieve logical description of higher level resolution analog-to-digital adaptor. Their method might be used in many metrological applications for different analog-to-digital adaptors with frequencies up to a few kHz. In addition, Posselt *et al.* [22] utilized a reconfigurable analog-to-digital converter which was suggested with aptitudes of digitalizing completely related wireless facilities for vehicular usage with frequency ranging from of 600 MHz to 6 GHz.

In addition, sigma-delta adaptors are normally capable to achieve error modeling just like that the error power is centralized in upper frequencies [23]. Fig. 3 demonstrated that the bottom error is significantly sophisticated at upper frequencies and rather beneath the concern band. Furthermore, the signal $y[n]$ is the quantizer yield and is low pass clean by means of a M^{th} band low-pass filter, where $M = 50$ is the over-sampling ratio. The transmission function, H(z), of the M^{th} band low-pass filter is known from Equation 10. The power spectral density of the clarified yield is shown in Fig. 4.

Fig. 5 displays the power spectral density of the real analog-to-digital converter production. It can be obvious that, at this point, the signal has been downsampled to the Nyquist frequency once again.

Taking into consideration that for the sigma-delta adaptor, exhibited in the Matlab® program, the utilized over-sampling ratio, *M*, was 50. It can be realized that, through Equation 12, a sigma-delta adaptor might offer an enhancement of about 29 dB once likened through a straight over-sampling adaptor that similarly works at 50 times Nyquist frequency.

B. SQNR

The SQNR generated using a 1-bit sigma-delta adaptor can be linked through Fig. 6 with the SQNR of a straight over-sampling analog-to-digital converter at numerous over-sampling ratios.

Moreover, it can be noticed that from Fig. 6 when the over-sampling ratio is 15, then the SQNR is just round 20 dB. Accordingly, the Nyquist frequency for an analog signal modulator utilizing a binary phase shift keying and conveying 80 Kbps of data will be 160 KHz. On the other hand, oversampling in 15 would necessitate sampling at 2.4 MHz. Otherwise stated, considering the present digital signal processing, which can treat samples at an order of nearly 2.4 MHz, one might be capable to carry out a regulate over-sampling analog-to-digital adaptor. In similar work, Brooks *et al.* [24] stated that their analog-to-digital converter works at a 20 MHz and it attains a signal-to-noise ratio of about 90 dB exceeding a 1.25 MHz signal bandwidth. Fig. 7 displays a scheme of the extra accuracy bits achieved against the over-sampling percentage.

Fig. 7 indicates that for a 10 dB corresponded input, once the signal-to-quantization error ratio of the analog-to-digital adaptor is 20 dB, and the digitized output possesses a signal-to-noise ratio of approximately 9.5 dB. This, perhaps, shows that using a SQNR of 20 dB, the digitizing process solely increases the bottom error by 0.5 dB. The bottom error is increased by even below 0.5 dB if the equivalent contribution's signal-to-noise ratio is less than 10 dB. Accordingly, the first and the last goal behind this study was directing over-sampling analog-to-digital adaptor to possess

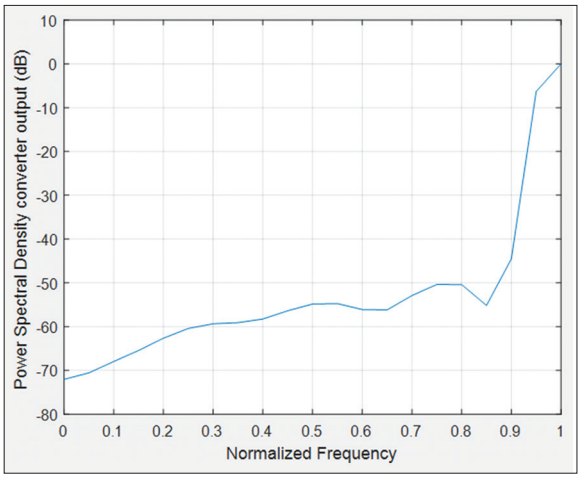

Fig. 5. Power spectral density of analog-to-digital converter output signal

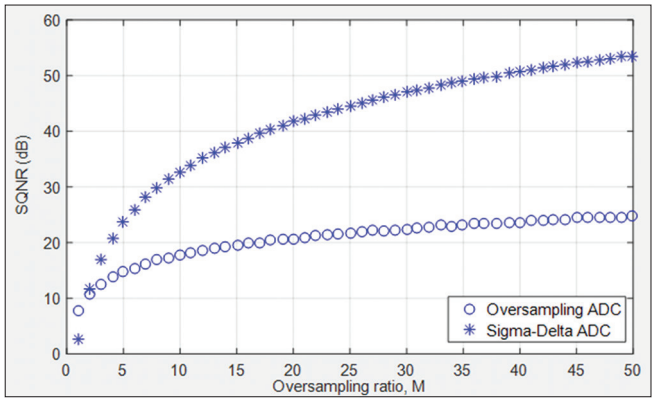

Fig. 6. Over-sampling ratio versus signal-to-quantization noise ratio

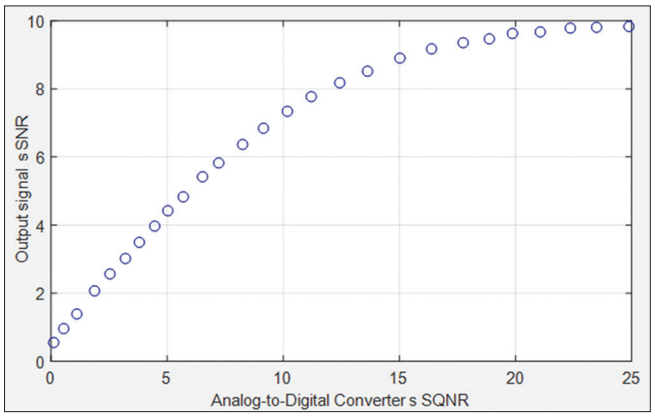

Fig. 7. Analog-to-digital adaptor yield's signal-to-noise ratio (SNR) (with contribution's SNR = 10 dB)

a SQNR of 20 dB or less. Fujimori *et al.* [25], alternatively, stated that in their study, no signal-to-noise ratio decay caused by numerical swapping error has been inspected, showing the strength of the error combination avert methods in combination with the low master clock of 20 MHz.

4. CONCUSSION

Running the analog-to-digital adaptor beyond the input signal's Nyquist frequency enhances the improvement of a low accuracy analog-to-digital adaptor. This is the evidence behindhand the operating of continuous over-sampling analog-to-digital converters. The quantization noise addition to the analog-to-digital adaptation procedure supplementary enhances enactment. Sigma-delta analog-to-digital adaptors apply both noise affecting and oversampling. Sigma-delta analog-to-digital converters propose significantly superior enactments than uninterrupted over-sampling adaptors. Nevertheless, it has been recommended that a straightforward sampling adaptor be utilized due to the difficulty of a sigma-delta analog-to-digital adaptor. Similarly, it has been observed that a straight over-sampling analog-to-digital converter can be utilized without any kind of signal humiliation.

5. ACKNOWLEDGMENT

The authors would like to extend their sincere acknowledgement to the Salahaddin University for supporting them with available tools. If anyone who needs the Matlab codes please contact the corresponding author for any additional help.

REFERENCES

[1] W. A. Kester. "Analog devices," in *Data Conversion Handbook*, Burlington, MA: Elsevier, 2005.

[2] K. Fowler. "Part 7: Analog-to-digital conversion in real-time systems." *IEEE Instrumentation and Measurement Magazine,* vol. 6, No. 3, pp. 58-64, 2003.

[3] R. Schreier and G. C. Temes. *Understanding Delta-Sigma Data Converters*, vol. 74. Piscataway, NJ: IEEE Press, 2005.

[4] J. M. de la Rosa and R. Río. *CMOS Sigma-Delta Converters: Practical Design Guide*, Hoboken, NJ: Wiley, 2013.

[5] M. Pelgrom. *Analog-to-Digital Conversion*, Switzerland: Springer International Publishing, 2016.

[6] J. Keyzer, J. Hinrichs, A. Metzger, M. Iwamoto, I. Galton and P. Asbeck. "Digital generation of RF signals for wireless communications with band-pass delta-sigma modulation." in Microwave Symposium Digest, IEEE MTT-S International, 2001.

[7] J. J. Wikner and N. Tan. "Modeling of CMOS digital-to-analog converters for telecommunication." *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, vol. 46, no. 5, pp. 489-499, 1999.

[8] J. Kim, T. K. Jang and Y. G. Yoon. "Analysis and design of

voltage-controlled oscillator based analog-to-digital converter." *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 57, no. 1, pp. 18-30, 2010.

[9] B. S. Song. *MicroCMOS Design*, Hoboken, NJ: Taylor & Francis, 2011.

[10] J. G. Proakis and D. G. Manolakis. *Digital Signal Processing: Principles, Algorithms, and Applications*, New Jersey, USA: Prentice Hall, 1996.

[11] G. J. Foschini and M. J. Gans. "On limits of wireless communications in a fading environment when using multiple antennas." *Wireless Personal Communications*, vol. 6, no. 3, pp. 311-335, 1998.

[12] K. Sudakshina. *Analog and Digital Communications*, Singapore: Pearson Education India, 2010.

[13] J. S. Chitode. *Principles of Communication*, Pune: Technical Publications, 2009.

[14] D. R. Morgan, Z. Ma, J. S. Kenney, J. Kim and C. R. Giardina. "A generalized memory polynomial model for digital predistortion of RF power amplifiers." *IEEE Transactions on Signal Processing*, vol. 54, no. 10, pp. 3852-3860, 2006.

[15] B. Le, T. W. Rondeau, J. H. Reed and C. W. Bostian. "Analog-to-digital converters." *IEEE Signal Processing Magazine,* vol. 22, no. 6. pp. 69-77, 2005.

[16] S. K. Mitra and S. K. Mitra. *Digital Signal Processing: A Computer-based Approach*, New York: McGraw-Hill, 2011.

[17] V. Mladenov, P. Karampelas, G. Tsenov and V. Vita. "Approximation formula for easy calculation of signal-to-noise ratio of sigma-delta modulators*." ISRN Signal Processing,* vol. 2011, Article ID: 731989. pp. 7, 2011.

[18] K. Francken and G. G. Gielen. "A high-level simulation and synthesis environment for/spl Delta//spl Sigma/modulators." *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,* vol. 22, no. 8. p. 1049-1061, 2003.

[19] B. E. Bammes, R. H. Rochat, J. Jakana, D. H. Chen and W. Chiu. "Direct electron detection yields cryo-EM reconstructions at resolutions beyond 3/4 Nyquist frequency." *Journal of Structural Biology*, vol. 177, no. 3, p. 589-601, 2012.

[20] A. Belitski, A. Gretton, C. Magri, Y. Murayama, M. A. Montemurro, N. K. Logothetis, S. Panzeri. "Low-frequency local field potentials and spikes in primary visual cortex convey independent visual information." *Journal of Neuroscience,* vol. 28, no. 22, pp. 5696-5709, 2008.

[21] F. Overney, A. Rufenacht, J. P. Braun and B. Jeanneret. "Josephson-based test bench for ac characterization of analog-to-digital converters." in Precision Electromagnetic Measurements (CPEM), 2010 Conference on IEEE, 2010.

[22] A. Posselt, D. Berges, O. Klemp, B. Geck. "Design and evaluation of frequency-agile multi-standard direct RF digitizing receivers for automotive use." in Vehicular Technology Conference (VTC Spring), IEEE 81st, IEEE, 2015.

[23] P. M. Aziz, H. V. Sorensen and J. van der Spiegel. "An overview of sigma-delta converters." *IEEE Signal Processing Magazine*, vol. 13, no. 1, pp. 61-84, 1996.

[24] T. L. Brooks, D. H. Robertson, D. F. Kelly, A. Del Muro and S. W. Harston. "A cascaded sigma-delta pipeline A/D converter with 1.25 MHz signal bandwidth and 89 dB SNR." *IEEE Journal of Solid-State Circuits*, vol. 32, no. 12, pp. 1896-1906, 1997.

[25] I. Fujimori, L. Longo, and A. Hirapethian. "A 90-dB SNR 2.5-MHz output-rate ADC using cascaded multibit delta-sigma modulation at 8/spl times/oversampling ratio." *IEEE Journal of Solid-State Circuits,* vol. 35. no. 12. pp. 1820-1828, 2000.

ORIGINAL RESEARCH ARTICLE UHD JOURNAL OF SCIENCE AND TECHNOLOGY

Utilization of Solar Water Heaters to Reduce Residential Electrical Load

Majid S. Al-Hafidh[1], Mudhafar A. Al-Nama[2] and Azher S. Al-Fahadi[3]

[1]Department of Electrical Engineering, Mosul University, Mosul, Iraq
[2]Department of Computer Engineering and Technology, Al Hadbaa University, Mosul, Iraq
[3]Department of Electrical Engineering, Mosul University, Mosul, Iraq

ABSTRACT

Residential electrical load in Iraq can be divided into five components, lighting, home appliances, heating, cooling, and water heating. Water heating component represents the largest residential electric load component in Iraq. The current research aims to test the possibility of using solar water heaters to supply hot water to residential units. Solar water heaters were added to a number of residential units in Mosul city, with the addition of a small electrical heater to provide supplementary heating. The readings of the total energy consumed, the energy consumed in the supplementary heating, the amount of water consumed and the water temperature in the solar heated tank, were recorded each day for a full year. The results were analyzed and compared with the case without the addition of solar heaters. The addition of solar water heater with supplementary heating leads to the reduction of the total consumption up to one-fifth of the total energy (19.19%).

Index Terms: Iraqi Residential Electrical Load, Residential Electrical Load, Solar Energy, Solar Water Heaters

1. INTRODUCTION

Electrical loads can be divided into several categories, including residential, industrial, commercial, and government. These components vary in the electrical system depending on the economic, political, social state of the country, etc.

In previous research, diversity factor was been studied in the Iraqi electricity distribution system. The study shows that household electrical loads have grown at high rates exceeded the standard values for stable systems [1]. Another study conducted aims to use artificial neural network technology to guess household electrical loads [2].

Access this article online	
DOI: 10.21928/uhdjst.v1n1y2017.pp23-26	**E-ISSN:** 2521-4217 **P-ISSN:** 2521-4209

Residential loads represent biggest components in the Iraqi electrical systems, due to low industrial and commercial loads components. Residential electrical loads consist of many components, household appliances, lighting, space heating, cooling, and water heating. A previous field survey study was conducting in the city of Mosul to specify these components. The study found that the water heating component was the largest component, 32.29% [3].

The current research aims to test the possibility of using solar water heaters to supply hot water in the housing units. Solar water heaters were added with low rating electrical heater to provide supplementary heating for a number of residential units in Mosul city. The total energy consumed, the energy consumed in the supplementary heaters, the amount of water consumed, and the water temperature in the solar heater tank registration were recorded. Readings recorded daily for 1 full year. The readings were analyzed to find the percentage of water heating component. Furthermore, the change with the months of the year is compared with the previous

Corresponding author's e-mail: el_noor2000@yahoo.com

Received: 10-03-2017 Accepted: 25-03-2017 Published: 12-04-2017

study (without solar heated). The results, the analysis, and comparison are listed in the following paragraphs.

2. THEORETICAL BASIS

Renewable energies represent suitable alternatives to solve the problems resulting from high energy consumption rates (especially electricity). Renewable energies (wind energy, solar energy, hydropower, etc.) can be used to generate thermal energy, kinetic energy, electrical energy, etc.

Many researchers have been conducted to study the solar energy falling in different areas in Iraq. The studies included which study all Iraqi areas and gave illustrations of solar energy for different seasons of the year [4]. Other studies Al-Salihi *et al.* and Ali have been conducted to certain areas in Iraq such as Baghdad, Mosul and Kirkuk, Ramady, etc. [5], [6].

Solar energy has been used for water heating in many developing countries. Mohammed, *et al.*, 2011, study the possibility of using solar energy to heat water for the use of 25 people in Baghdad using a solar panels collectors of 10 m^2 capacity and a storage tank of 600 L capacity [7]. The study concluded the possibility of using solar energy to provide 69% of the hot water using solar heaters, by providing more than 60% in the winter, and more than 70% in the summer. It is well known that in summer no hot water is needed (June, July, August, and September).

Another study uses TRNSYS software to model and verify a direct solar water heating system in Baghdad, Iraq. The study aims to meet the demand of hot water for 25 persons using 10 m^2 of a flat plate collector and 600 L storage tank [7].

3. RECORDING READINGS

A group of houses (8 homes) was selected in the technical institute's foundation. A solar water heater has been added for each residential unit. A low rating electrical heater of 1 kW is used to provide supplementary heating. Fig. 1 shows one of the solar water heating systems used in the study. The system consists of two flat plate collectors each of the dimension 80 cm × 150 cm and storage tank of hot water with a capacity of 180 L. The flat plate collector and the storage tank capacity can be changed to match the consumers hot water demand.

Each solar water heater was equipped with a set of meters. The meters measure the energy consumed in the supplementary heaters, the amount of hot water consumed, and the water temperature in the storage tank. The supplementary heating energy and hot water consumed were recorded, once every 2 days.

Fig. 1. One of the solar water heating systems used in the study

Furthermore, an ammeter is used to measure the current drawn in the house units. The current and the water temperature in the storage tank readings have been registered at three different times at the morning, afternoon, and at night. As well as the total energy consumption in the residential units reading was recorded. Total energy reading was recorded, once every 2 days.

Previous readings were recorded for the entire year. Recorded readings were used in the analysis to get the results described in the following paragraphs. Calculations can be performed based on the distribution of the foundations weekly or monthly. The calculations discussed in the results based on a semimonthly period, as well as monthly.

4. RESULTS AND ANALYSIS

Electrical load in Iraq is strongly influenced by weather climate changes where the high temperature in the summer leads to increase the electrical load as a result of using the cooling devices. Furthermore, the low temperature in winter leads to increase electrical load as a result of using space heating and water heating whereas mild temperatures in spring and autumn lead to a reduction of electrical load, which represents the lowest throughout the year.

In general, a large amount of solar energy falls on Iraq, and especially in Mosul city. It is clear that the amount of solar energy falling vary with seasons, where maximum energy

falls in the summer. The minimum fallen energy is winter. The statistics show that the hours of solar brightness in Iraq, during the winter is represented 50-60% of daylight hours. Lowest rate happens to solar brightness hours in the month of January with 4.87 h. While the hours of solar brightness in summer represents 90% of the daylight hours, with a maximum brightness of the sun hours in the month of July 12.31 h. Fig. 2 shows the average daily solar energy falling and the rate of solar brightness hours versus months of the year in the city of Mosul. Less solar energy occurs in the month of January and reaches 7.22 MJ/m^2-day. The maximum solar fallen in the month of June and reach 26.32 MJ/m^2-day (Iraqi Air Adversity 1989).

Supplementary heating energy changes with temperature in the proportion of different seasons, as well as with the intensity of incoming solar radiation changes. Therefore, the need for supplementary energy heating in winter becomes the highest in the whole year. Fig. 3 illustrates the monthly supplementary rated heating in the year. It shows that there is no need for supplementary heating during summer. As well as it decreases in spring and autumn.

The supplementary heating energy rate was calculated for a period of semimonthly to compare it with the energy consumed in the water heating (without the addition of solar heated). Fig. 4 shows the energy consumed in the water heating with and without solar water heating. It is clear from the figure the great difference between the amount of supplementary heating energy used with solar water heater and the case without using it. Also the times in which maximum benefits of adding solar heater is achieved. As well as there is no need to heat the water the majority of the summer. The maximum reduction ratio result during the spring and autumn. While reduction rates are less during winter than in the case of spring and autumn.

Table I summarizes the percentage of water heating component with the addition of solar water heaters and without them. The table includes the amount of the proportion of water heating component for the case of high consumption, the average consumption and the low

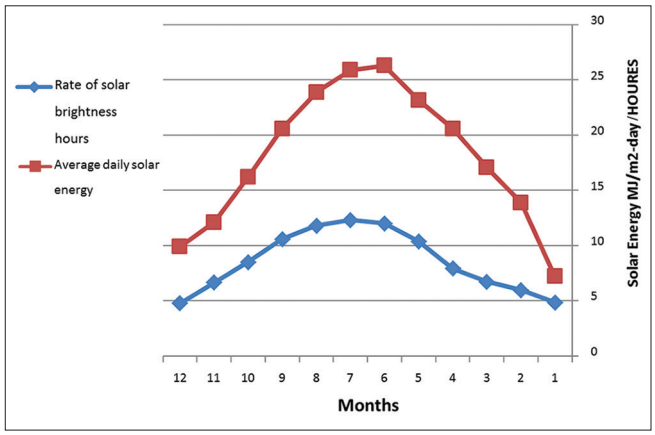

Fig. 2. Average daily solar energy falling and the rate of solar brightness hours versus months of the year in the city of Mosul

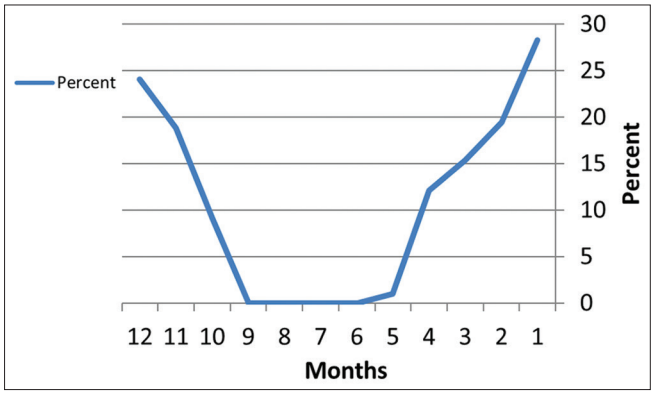

Fig. 3. Supplementary heating rate of the months of the year

TABLE I
Percentage of the Components of Household Electrical Load and the Amount of Little and Average Total and High Consumption

Case	Rate %	Consumption		
		Low %	Average %	High %
With solar heater	13.1	13.1	9.85	11.61
Without solar heater	32.3	32.29	13.39	30.4

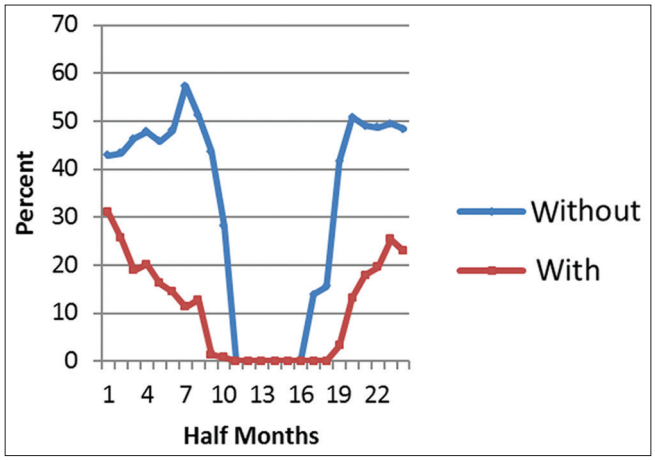

Fig. 4. Energy consumed in the water heating with and without solar water heating

consumption, in addition to the average consumer. Evidenced by the average value of the added solar water heater leads to a reduction in the total consumption by 19.19%.

5. CONCLUSION

The current research shows a reduction in water heating component in residential units electrical load using solar water heaters. A solar water heater was added to a number of residential units in the city of Mosul in northern Iraq. A small rating heater was added to the solar water heaters to provide supplementary heating. The percentage of supplementary heating component compared with total electrical energy consumption in each housing units was calculated. As well as the percentage of supplementary heating component compared with total electrical energy consumption in all housing units. The results illustrate the possibility of obtaining a holistic reduced by 19.19%.

The solar water heaters used have a standard specifications, while the hot water needs of the residential units vary as a result of differing ages and number of occupants (consumer), etc. Which must leads to change some specifications of the solar water heaters, such as solar heater flat plane area and hot water storage volume. The solar water heaters specification can be studied to get a further reduction in the supplementary heating component.

6. FUTURE WORK

The registered readings of the water consumed can be used to find a general model for hot water demand for different houses units. This general model can be used to design the suitable heating system to meet the hot water demand for any consumer.

Furthermore, the water temperature of the storage tank can be used to wake a general model for heat transfer for the heating system. This model can be used to improve the system efficiency.

7. THANKS AND APPRECIATIONS

The researchers express their deep gratitude and thanks to the administration and the engineers of the general management for north region electrical distribution for their valuable help and cooperation throughout this work and fruitful discussion and suggestions made among the different study stages.

REFERENCES

[1] M. A. Al-Nama, M. S. Al-Hafid and A. S. Al-Fahadi. "Estimation of the diversity factor for the Iraqi distribution system using intelligent methods." *Al-Rafidain Engineering, Mosul*, vol. 17, no.1, pp. 14-21, 2009.

[2] M. A. Al-Nama, M. S. Al-Hafid and A. S. Al-Fahadi. "Estimation of the consumer peak load for the Iraqi distribution system using intelligent methods." *Iraqi Journal for Electrical and Electronic Engineering*, vol. 7, no. 2, pp. 180-184, 2011.

[3] M. S. Al-Hafid, M. A. Al-Nama and A. S. Al-Fahadi. "Determination of Residential Electrical Load Components in Iraqi North Region." Iraqi Journal for Electrical and Electronic Engineering, Basra, Iraq: Sent for Publication.

[4] M. Z. Mohammed, M. A. Al-Nema and D. A. Al-Nema. "Seasonal distribution of solar radiation in Iraq." Proceeding of the Conference on the Physics of Solar Energy. Arab Development Institute, Special Publication, Tripoli, 1977.

[5] A. M. Al-Salihi, M. M. Kadum and A. J. Mohammed. "Estimation of global solar radiation on horizontal surface using routine meteorological measurements for different cities in Iraq." *Asian Journal of Scientific Research,* vol. 3, no. 4, pp. 240-248, 2010.

[6] F. A. Ali. "Computation of solar radiation on horizontal surface over some Iraqi cities." *Engineering and Technical Journal*, vol. 29, no.10, pp. 2026-2042, 2011.

[7] M. N. Mohammed, M. A. Alghoul, K. Abulqasem, A. Mustafa, K. Glaisa, P. Ooshaksaraei, M. Yahya, A. Zaharim and K. Sopian. "TRNSYS simulation of solar water heating system in Iraq." *Recent Researches in Geography, Geology, Energy, Environment and Biomedicine*, pp. 153-156, Jul. 2011.

ORIGINAL RESEARCH ARTICLE UHD JOURNAL OF SCIENCE AND TECHNOLOGY

The Future of Technology-based Classroom

Mazen Ismaeel Ghareb[1] and Saman Ali Mohammed[2]

[1]Department of Computer Science, College of Science and Technology, University of Human Development, Iraq
[2]Department of English, College of Language, University of Human Development, Iraq

ABSTRACT

In recent years, Information Technology has turned out to be a standout among the most essential social practices of the Iraqi society. Technology has developed in many areas in Iraq, yet the internet and computer technology is not implemented in every classroom in most of Iraqi universities. The aim of this paper is to question: Why technology is not executed in the classroom of the universities? The point of this contextual analysis is to recognize the difficulties that face university organizations from executing computer technology in every classroom with support of ministry of higher education. Another question is: How popular or effective could the application of computer communication or computer application in the classrooms of our graduate students be when it comes to education? This study wants to uncover the underlying issues and reasons for the in capabilities in using technology. To examine this, the researchers inspected cases of teaching where technologies used in the classrooms as a lived experience and as an apparatus for encouraging direction while instructing in the universities. The outcomes show that the country's current educational and telecommunications infrastructure is weak and the ministry of higher education and universities need to manufacture the framework limit of schools, and furthermore to enhance educator preparing programs at all levels.

Index Terms: E-classroom, Information Technology, Internet in Education, Iraq Education, Online Learning Applications

1. INTRODUCTION

The Iraqi population consists of several ethnic gatherings, including Arab Muslim Shiite, Arab Muslim Sunnis, Kurds, Assyrian, Turkoman, Chaldean, Armenian, Yazidi, Sabean, and Jews. Arabic is the language used in many regions and Kurdish is the official language in Kurdistan [1], and overall designing a curcuilm of using technology will help each ethnic group to express their culture globally with using technology; the key is to be a technology-based classroom context where each individual can work and develop ideas. Thus, technology-based classroom can bring together this melting pot in a diverse country such as Iraq with diverse students in the university. MIT professor Seymour Papert had presented among great debate that the kids were to use computer in their learning. What was all the more shocking was the progressive route in which he led his classes, in open investigation of learning and information that exemplified the general population's PC development of the 1960s. This scene summed up the significance of the change of training and a move in pondering training that fits so well for a fates approach [2].

Thus, could a similar case be witnessed in Kurdistan and/or Iraq? Lei and different researchers demonstrate the significance of utilizing computer technology in learning and profitability. Furthermore, innovation is utilized as a part of instructing and learning techniques in many nations. However, not all the university organizations in Iraq utilize technologies in their classrooms. This review has taken a subjective research approach to examine this issue and recognize the reasons of why the technological tools are not utilized to encourage the procedure of correspondence,

Access this article online

DOI: 10.21928/uhdjst.v1n1y2017.pp27-32

E-ISSN: 2521-4217
P-ISSN: 2521-4209

Corresponding author's e-mail: mazen.ismaeel@uhd.edu.iq

Received: 20-03-2017 Accepted: 30-03-2017 Published: 12-04-2017

improve the strategies for instructing, and enhance the students' learning skills in Iraqi colleges and personnel [3].

2. LITERATURE REVIEW

A. Technology and Information Age

During the previous 50 years, electronic devices (radio, TV, PCs, satellite, and so forth) were the focal instruments and correspondence advances in assisting with transmitting the information to the individuals [4]. The information age has brought new challenges since 1950 where individuals might want to have multimedia sources accessible for them to utilize. The term is used to describe a cybernetic society, which relies upon computer and information transmission.

The commonplace casing of understanding a modern culture depends on the human work and the machines they use to deliver products. In the light of the consistent changes over decades, geographic hindrances are being broken down, and the connection between the employees and their working environment is evolving quickly. New data Information Technology (IT) and types of correspondence have developed to take care of issues and set new bearings for issues that have been around for quite a while. If we take education, for example, we will see that individuals can read, compose, sort, and print by utilizing computer literacy [5]. In many societies, the nature and capacity of technology have changed using computerized advancements in correspondence and in keeping people in general educated on matters of open significance [6].

IT is the reason for changes for the dominant part of businesses. IT is a strategic tool, and without information and technologies, changes are unrealistic especially in a modern age. In the recent years, a large portion of the enterprises everywhere worldwide utilized telecommunicated systems of computers at the center of information systems and communication processes. The development of new technologies makes educating and correspondence all the more effective and less demanding. Technologies do not take care of the social issues, but rather a crucial instrument for improvement and creativity in education in society [7]. Research has demonstrated that the utilization of innovation serves massively crucial by encouraging the learning process where it associates workforce and students with the world. In addition, technology can offer assets and encounters that books are not ready to offer. Computer technology can likewise help with data analysis. They can encourage the administration of vast volumes of information and empower staff, students, or analysts to find, mark, and gather distinctive mixes of portions of literary information [8].

B. The Futures of Educations

The use investigating the morally stable points of UNESCO's Educating process for a Sustainable Future [9], or the Global Challenges training and learning uncovers the principal and effectiveness of human association with instruction and the importance of training as an extensive advancement apparatus for social monetary change, that is repeated solidly [10]. Training in this regard is one of the problems needs to be addressed when tending to change and what's to come. It is clear that the educational systems do not set us up for the rising pluralistic, interconnected, and complex world. They unquestionably do not set us up for apparently interminable change, insecurity, or more all, instability [11].

Educators and education structures, then need to address this issue of managing ceaseless change and its complexities, new establishments for training. Hicks and Gidley maintain that if teachers do not help youngsters to feel engaged in connection to their future and future change, then, it can be contended, they will have bombed in their obligation to the present era of learners [12]. Thus, these are heated words that place the future eras at the wheel of education and its key approach, as the experience of instruction will shape them, in their expert capacity as well as in their exceptional character, as the Finnish instruction service shows that training basically constructs personality. The moral and good obligation in view of future lives and personalities then could not be as vital or as esteem driven.

C. Education in Iraq

Iraq government requires all qualified matured kids to go to grade school. This helped establish the framework for a standout among the most created and proficient populaces in the area. Amid the times of 1970-1984, a period some recognize as the country's "Brilliant years," education system increased huge initiative acknowledgment in Middle East. Today, the Ministry of Education (MOE) and Ministry of Higher Education and Scientific Research (MOHESR) and Ministry of Higher education of Kurdistan Region Government (MOH-KRG) deal with the Iraqi instruction framework [13]-[15].

D. Computers in the Classroom

In a presentation on education and learning in 1990, Seymour paper questioned what specialists, futurists, and prophets are asking - what will it resemble? What kind of a world will it be? Furthermore, he states that these could be wrong

sort of things to ask, as they are all wrong, he said that "the question is definitely not What will the computer do to us?" The question is "The thing that we will make of the computer?" The fact of the matter is defined not to foresee the computer future [16]. The substance of this is the vital position in which training ought to be viewed as proactive and authoritative, that diagram two distinctive perspectives of education, one that is repetitive knowledge based, and the other that is an experience based learning. That the adjustments in our condition do not simply happen to us and impact us, however, we likewise play a part in influencing them. This fits extremely well for a prospect's point of view and helps in exploring moral issues managing technology and education.

On account of this we can get better engagement with kids as dynamic learners and their enabling perspective of training that is exploratory in nature. The landing of the computer in the classroom, blended up with solid moral inquiries regarding the significance of information, educating, and discovering till the present time serves as a key issue that raises key inquiries, for and against technology. We can see this sort of viewpoint today in moral discourses about kids bringing individual innovations such as Mobile smart phones into the classroom. One proposed enactment for instance, announced in the news as of late, recommended that they ought to confiscate smart-phones since they would be a diversion to learn, or that students were tricked in some way, which in particular moral cases are genuine issues confronted for conventional education learning settings [16]. Embracing childhood and youth as engaged through digital media, and consequently for instructive arrangement reflects their strengthening. It recognizes the requirement for a "quiet revolution" in education that saddles the impressive limits of youngsters and youngsters to take part in and coconstruct conceivable future [17].

E. Internet Revolution in Iraq

In recent years, the Internet technology as methods for communication and its users have been growing drastically. The number of users in Iraq increased after the 2003 war because there were rules feeding using internet [18].Currently, the Internet circumstance is enhanced significantly as there are presently there are many [19]. The last information gathered in regards to non-military personnel access to the Internet was in 2017 and around then roughly 6.381 million Iraqis had home web, positioning 87th for Internet access globally [19]. While this is a an improvement, individuals get to independent companies, educational institutions, and government framework and keep on crippling Iraq in turning out to be globally competitive. The United States (US) government welcomed the financial specialists and enormous organization to invest in Iraq to begin the procedure of the country's reconstruction. In 2004, the United Nations Development Group Iraq Trust Fund (UNDG ITF) began in Iraq. UNDG ITF is one of the International Reconstruction Fund Facility for Iraq (IRFFI). The Iraqi government counseled with the United Nations and the World Bank to plan the IRFFI and open the entryways for contributors and global sources to bolster Iraq's reconstruction activities including technology implementation projects [20].

F. Social Media in Iraq

Researchers have been inspecting the part that web-based social networking plays in the higher education classroom. A portion of the work has highlighted the full of feeling results of Social Network Sites coordination. A couple thinks about examined learning results and understudy accomplishment in relating to the instructive utilization of online networking in school courses. While the lion's share of studies detailed positive evidence, there was proof of downsides too. Education system does tend toward investigating and developing technologies as new or enhanced apparatuses to upgrade instruction and learning.

Web-based social networking has developed as a profoundly valuable individual correspondence technology. Although the foundation to bolster web-based social networking's nearness exists in many colleges today, teachers have been moderate in receiving the instrument as an instructive one.

A few, obviously, are not willing to acknowledge the apparatus unlimited power favoring theoretical or pragmatic reasons for an implementation [21]. Adding to that there are many students and undergraduates who spent a lot of time on social network, making many groups of study. Many lecturers also have been interacting about the subjects, assignments, and courses on social media guiding and giving the students instructions [22].

3. METHODOLOGY

The aim of this research is to recognize the difficulties that face the universities administrations from implementing the computer technology in every classroom. This study attempts to answer the accompanying research question: Why the technology is not implemented yet in the classroom settings in the Iraqi and KRG colleges? This review takes after a qualitative research way to examine the issue.

G. The Iraqi Education System

The models in country risk analysis, for example, the Economic Intelligence Unit, Business Environment Risk Intelligence, and Euro money help organizations and their administrations see well which nation is a decent market for speculation and which one is not to maintain a strategic distance from misfortunes to their organizations. These models function as a hazard appraisal to help firms in settling on market passage choices, operations principles, and leave procedure choices. These models and strategies incorporate essential data on Iraq's political circumstance, legal, investment overview, social, cultural, environmental, and geological dangers of the nation. The reports on Iraq from these models were not positive which make it harder for the Iraqi government to move quickly with the innovation execution extends in the scholarly organizations. In spite of the fact that the utilization of computer technology in classroom settings can help in encouraging the educating and enhancing the student's learning aptitudes, the classrooms in Iraqi universities still do not have the accessibility of this technology because of a few difficulties that the nation faces. These difficulties will be clarified in the accompanying sections.

4. RESULTS AND DISCUSSIONS

We as the researchers of this paper, have been observing some English and computer teaching classes in some of Kurdistan universities such as University of Human Development as a private one and Sulimanya university as the state University in Iraq. The English training in Iraq depends on conventional instructional strategy and generally the class size is extensive. The quantity of students is around 30-50 in each class. The technique in which the understudies learn English is an educator focused. Perusing understanding takes a substantial piece of class time and linguistic use is essential. Talking and listening appear to be disregarded in showing English as an outside dialect in Iraq. Moreover, little gathering work, which is common with the communicative teaching method (the strategy more generally acknowledged by remote language instructors these days), is disregarded in the Iraqi classroom, which is also teacher-centered instead of student-centered. Regarding the programming teaching, Mazen experienced the lack of infrastructure for students to publish their software product and no support from government as small business projects [23]. As interview with several professors, they do not use the computer technologies to encourage learning through online talk bunches, watching the recordings and clasps inside the classroom, talking and recordings, and so on because of the absence of language laboratories or computer technology in classrooms. This issue is as yet present in Iraq till now the same number of my associates who still sit-in Iraq told me of these ongoing problems.

Getting to online instructional materials and the utilization of Blackboard apparatuses in Iraqi organizations is as yet not accessible to all public and private universities in Iraq. However, University of Human development uses Moodle tool. Moodel is used as an open source for our teaching using online forums, assignments, and online quizzes. In addition, we have experience using social media for group working as an effective method in learning process [24]. The Iraqi and the US governments have been attempting to modernize the instructional framework and to improve online instructive libraries. This incorporates building instructive organizations among Iraqi and US schools, trade projects and going by researchers, and supporting Iraqi understudies and instructor to examine or to get prepared in the US foundations. In spite of the fact that this support is exceptionally useful, the overall progress is very slow [25].

5. CONCLUSIONS AND RECOMMENDATIONS

The research findings show that if country risk analysts contrast Iraq's education, technological status with other developed countries such as the USA, they can see that getting to online instructional materials in Iraqi establishments is still not of that high quality, and the nation's current educational and media communications infrastructure is weak. In addition, Iraq confronts various difficulties after the 2003 war. One of these difficulties was to recover the unmistakable quality that its instruction framework once held in the Middle East, the need to construct the foundation limit of schools, and furthermore to enhance instructor preparing programs at all levels [26].

In view of the unsecure circumstance and the political instability in Iraq, it is difficult to execute technology in all schools in a short time. Therefore, the alternatives recognized are to have a PC laboratory, technology tools, and the internet in each school as an initial step to encourage learning and instructing. Having such a lap is an essential official unit unlike Smartphone. Having Internet café undergrad and graduate students to use for their class study and research. Since so many students have Smartphone and tablets, the use of internet and the technology-based classroom becomes easy if there are adopted mechanisms. The recommendations outlined in this research are as follows: The universities must

have a correct time span for finishing the outline and the cost of their technology-based systems, classrooms, and project. It ought to likewise determine which schools that can profit by the technology implementation. There ought to likewise be a political strength and security in the nation to ensure the specialists and associations that will take the venture and play out the business. The universities have likewise to empower Iraqi lecturers and students to go to workshops and gatherings to acquire information and improvement. MOE and MOHESR may contract worldwide staff and personnel to help with the educational development process and technology used in classrooms. Sending Iraqi students to consider in foreign countries will be an advantage for the country once they come back to exchange with the nearby staff their own experiences and knowledge. We recommend the other public and private university using new technological tools for their educational process. For instance, university of Human Development has used Moodle tool as an open source for their students which has positively affected the capabilities of interact with the students and teaching activities in university and later outside the university [24]. This system is upgrade to Google applications and all the students have their own university account and it will be configured to Google class next year. Furthermore, students can use many social media applications for educational communication such as Facebook, Viber, and many more.

6. ACKNOWLEDGMENT

We would like thanks University of Human Development for usual support to conduct this research, and for all students and lectuere that support us during analysis data of this study.

REFERENCES

[1] J. Ainsworth, Ed. *Sociology of Education: An A-to-Z Guide*. Thousand Oaks, CA: Sage Publications, 2013.

[2] D. C. Hoyles and R. Noss. "Visions for mathematical learning: The inspirational legacy of seymour papert (1928-2016)." *EMS Newsletter*, vol. 3, no. 103, pp. 34-36, 2017.

[3] J. Lei, J. Shen and L. Johnson. "Digital technologies and assessment in the twenty-first-century schooling." in *Assessing Schools for Generation R (Responsibility)*, Netherlands: Springer, 2014, pp. 185-200.

[4] M. M. Teixeira, C. D. de Aquino, M. B. C. Leão, H. V. L. Souza, R. F. F. de Oliveira, L. Miranda, R. Neves and E. Medeiros. "Mass media in teaching and learning: Circumstances in higher education." in Information Systems and Technologies (CISTI), 2016 11th Iberian Conference on IEEE, 2016, Jun. pp. 1-5.

[5] T. Gillespie, P. J. Boczkowski and K. A. Foot. *Media Technologies: Essays on Communication, Materiality, and Society*. Cambridge, Massachusetts: MIT Press, 2014.

[6] J. Jordan-Meier. "*The Four Stages of Highly Effective Crisis Management: How to Manage the Media in the Digital Age*." Boca Raton: CRC Press, 2016.

[7] L. S. Sidhu and J. Sharma. "Information, globalization through research and social development." *COMPUSOFT, An International Journal of Advanced Computer Technology*, vol. 4, no. 5, pp. 1760, 2015.

[8] T. A. Schwandt. "*The Sage Dictionary of Qualitative Inquiry*." Thousand Oaks, CA: Sage Publications, 2014.

[9] A. E. Wals. "Sustainability in higher education in the context of the UN DESD: A review of learning and institutionalization processes." *Journal of Cleaner Production,* vol. 62, pp. 8-15, 2014.

[10] E. Unterhalter. "Measuring education for the millennium development goals: Reflections on targets, indicators, and a post-2015 framework." *Journal of Human Development and Capabilities,* vol. 15, no. 2-3, pp. 176-187, 2014.

[11] A. Montuori. "Creative inquiry: Confronting the challenges of scholarship in the 21st century. *Futures,* vol. 44, no. 1, pp. 64-70, 2012.

[12] D. Hicks and J. Gidley. "Futures education: Case studies, theories and transformative speculations." *Futures,* vol. 44, no. 1, pp. 1-3, 2012.

[13] J. H. Issa and H. Jamil. "Overview of the education system in contemporary Iraq." *European Journal of Social Sciences,* vol. 14, no. 3, pp. 360-386, 2010.

[14] S. Al-Husseini and I. Elbeltagi. "Knowledge sharing practices as a basis of product innovation: A case of higher education in Iraq." *International Journal of Social Science and Humanity*, vol. 5, no. 2, pp. 182, 2015.

[15] N. Kaghed and A. Dezaye. "Quality assurance strategies of higher education in Iraq and Kurdistan: A case study." *Quality in Higher Education, vol.*15, no. 1, pp. 71-77, 2009.

[16] A. Taylor. "Technology in the classroom-the ethical futures of a transforming education." *Coolest Student Papers at Finland Futures Research Centre*, vol. 2015-2016, pp. 15, 2016.

[17] A. Craft. "Childhood in a digital age: Creative challenges for educational futures." *London Review of Education*, vol. 10, no. 2, pp. 173-190, 2012.

[18] K. M. Wagner and J. Gainous, J. "Digital uprising: The internet revolution in the middle east." *Journal of Information Technology and Politics,* vol. 10, no. 3, pp. 261-275, 2013.

[19] R. W. Abedalla, L. S. Escobar and D. A. Al-Quraishi. Accessing information technology-social media in Iraq." *International Journal of Scientific and Research Publications,* vol. 4, pp. 32, 2014.

[20] UNESCO Institute for Statistics. "*Global Education Digest 2010: Comparing Education Statistics across the World.*" Montreal, Quebec: UNESCO-UIS, 2010.

[21] P. A. Tess. "The role of social media in higher education classes (real and virtual)-a literature review." *Computers in Human Behavior*, vol. 29, no. 5, pp. A60-A68, 2013.

[22] M. I. Ghareb and H. O. Sharif. "Facebook effect on academic performance and social life for undergraduate students of university of human developments." *International Journal of Multidisciplinary and Current Research*, vol. 3, pp. 811-820, 2015.

[23] M. I. Ghareb and S. A. Mohammed. "The effect of e-learning and the role of new technology at university of human development." *International Journal of Multidisciplinary and Current Research*, vol. 4, pp. 299-307, 2016.

[24] M. I. Ghareb and S. A. Mohammed. "The role of e-learning in producing independent students with critical thinking." *International Journal of Multidisciplinary and Current Research,* vol. 4, pp. 299-307, 2016.

[25] A. D. Andrade and B. Doolin. "Information and communication technology and the social inclusion of refugees." *Mis Quarterly*, vol. 40, no. 2, pp. 405-416, 2016.

[26] A. G. Atiya and M. Vrazhnova. "Higher education funding in Iraq in terms of the experience of particular developed countries." *International Journal of Advanced Studies*, vol. 6, no. 1, pp. 8-17, 2017.

ORIGINAL RESEARCH ARTICLE UHD JOURNAL OF SCIENCE AND TECHNOLOGY

Advanced Methods for Detecting Pelviureteric Junction Dilatation by Two Dimensional Ultrasound

Heamn Noori Abduljabbar and Sardar Yaba Perxdr

Department of Physics, College of Education, Shaqlawa Slahaddin University, Erbil, Iraq

ABSTRACT

Pelviureteric junction (PUJ) obstruction is a condition frequently encountered in both adult and pediatric patients. Congenital abnormalities and crossing lower-pole renal vessels are the most common underlying pathologies in both men and women. There are different methods for detecting it the most usual, safe, and easy one is by ultrasound scanning. The aim of this study is how to improve the image quality of two dimensional (2D) ultrasound screening of detecting PUJ dilatation using image processing software, image enhancement, and different types of filters, then making comparison which filter is the best to improve the image quality, that helps the medical doctors, and sonographers to make the correct decision and diagnosis. 1357 patients scanned by ultrasound in Harer general hospital for general abdominal scanning, 987 cases among them have detected as urinary tract infection cases among this 987 case there were 73 case of them with PUJ dilatation. The 2D ultrasound images saved, after making image enhancement and using different types of filters (HE, ADH, CLAHE, and Wiener) to enhance four 2D ultrasound images of abnormal kidneys, the result was in each type of filters there were some advantages and disadvantages, so that the best type of filters are (HE and ADH) because the PUJ and pelvis is much more clear and easy to define after using these kinds of filters.

Index Terms: ADH, CLAHE, HE, Image Enhancement, Image Processing, Pelviureteric Junction, Wiener

1. INTRODUCTION

Ultrasound imaging regarded as a boon to study the internal tissues of a human body for different purposes, especially for the pregnant women because of its several advantages as comparing with computed tomography (CT), magnetic resonance imaging (MRI), and positron emission technology (Ransley 1990). However, it is consider as one of the best methods of diagnostic scanning tools but the presence of multiplicative speckle noise which is difficult to model in real time that affects the visual quality of the ultrasound images, especially in two dimensional (2D) ultrasound. The extensive research done by the researchers at device level led to the introduction of the three dimensional and four dimensional [3]. Ultrasound scanning is one of the best methods for detecting many diseases related to the internal organs, one of the most important defects that can be diagnosed clearly by ultrasound scanning is pelviureteric junction (PUJ) dilatation. Congenital and acquired (PUJ) obstruction can be treated with balloon dilatation, using a Fogarty/Gruntzig catheter introduced through the cystoscope in children.

Mahant *et al.* [4] stated that PUJ dysfunction is one of the common causes of renal hydronephrosis. Other causes, which are usually associated with hydroureter as well hydronephrosis, include bladder pathology vesicoureteric

Access this article online

DOI: 10.21928/uhdjst.v1n1y2017.pp33-37

E-ISSN: 2521-4217
P-ISSN: 2521-4209

Corresponding author's e-mail: heamn.abduljabbar@su.edu.krd

Received: 10-03-2017 Accepted: 25-03-2017 Published: 12-04-2017

obstruction and vesicoureteric reflux. Common causes of PUJ dysfunction include intrinsic stenosis is indicated in patients with pain, infection or hematuria, fever, back pain, dysuria, and hypertension in severe cases. Surgery may be performed open or laparoscopically.

2. ANATOMY

A. Location

Kidneys are located on the posterior abdominal wall, with one on either side of the vertebral column and perirenal space. Kidneys normally are lie on the quadratus lumborum muscles, the long axis of the kidney is parallel to the lateral border of the psoas muscle, and can be visualized in the first trimester by transabdominal scan at 12-13 weeks. In addition, the kidneys lie at an oblique angle, that is the superior pole is more medial and anterior than inferior renal pole. Right kidney usually lies slightly lower than left kidney due to the right lobe of the liver (Bems 2014).

B. Structure

Renal shape looks like a bean-shaped with a superior and an inferior pole. The mid portion of the kidney is often called the midpole. In adults, each kidney is normally weighs 150-260 g and 10-15 cm in length, 3-5 cm in width. The left kidney is usually slightly larger than right. Moreover, kidney has a fibrous capsule, which is surrounded by pararenal fat. The kidney itself can be divided into renal parenchyma, consisting of renal cortex and medulla, and the renal sinus containing renal pelvis, calyces, renal vessels, nerves, lymphatics, and perirenal fat. Renal parenchyma consists of two layers: Cortex and medulla. Renal cortex lies peripherally under the capsule while the renal medulla consists of 10-14 renal pyramids (renal filters), which are separated from each other by an extension of renal cortex called renal columns. Urine is produced in the renal lobes, which consists of the renal pyramid with associated overlying renal cortex and adjacent renal columns. Each renal lobe drains at a papilla into a minor calyx, four or five of these unite to form a major calyx. Each kidney normally has two or three major calyxes, which unite to form the renal pelvis, furthermore proximal ureter is connecte or started from renal pelvis which make a PUJ. The renal hilum is the entry to the renal sinus and lies vertically at the anteromedial aspect of the kidney. It contains the renal vessels and nerves, fat and the renal pelvis, which typically emerges posterior to the renal vessels, with the renal vein being anterior to the renal artery. Renal function is removing excess water, salts, and wastes of protein metabolism from the blood.

Diagnostic imaging of kidney:

- X-ray
- MRI
- CT scan
- Ultrasound.

3. METHODOLOGY

Ultrasound is used to detect urinary tract infections (UTI), one of the most important renal diseases is PUJ dilatation which can be defined by ultrasound clearly if the image quality is high, in this study 2D ultrasound used for scanning, the scanning procedure starts using convex probe (transducer), with 3.5 MHz frequency, time gain compensation total gain compensator should be adjusted according to each patient, then applying translucent gel to the patient abdominal skin who requested to be in supine position.

Scanning point for the kidneys starts from both sides of the abdomen, which called also upper loin, scanning windows should be from three points as general, anterioposterily, lateromedially, and posteriomedially. With oreintations and angulations to obtain the best image in which PUJ should be clearly defined. 1357 patients scanned by ultrasound in Harer general hospital/Erbil/Kurdistan/Iraq for general abdominal scanning, 987 cases among them have detected as UTI cases among this 987 case there were 73 case of them with PUJ dilatation. The 2D ultrasound images saved and transmitted to a computer to be processed by applying different types of filters to improve image quality, and finally comparing between filters types to choose the best type with best image quality of detecting PUJ dilatation. Different types of filters (HE, ADH, CLAHE, and Wiener) used to enhance 2D ultrasound images of (4) abnormal kidneys making image enhancement.

The contrast enhances techniques performed through some operations such as point operations are referred to as gray-level transformations or spatial transformations. They can be expressed as:

$$g(x,y) = T[f(x,y)] \quad (1)$$

Where g(x,y) is the processed image, f(x,y) is the original image, and T is an operator on f(x,y). Since the actual coordinates do not play any role in the way the transformation function processes the original image, equation (1) can be rewritten as:

$$s = T[r] \quad (2)$$

Where r is the original gray level of a pixel and s is the resulting gray level after processing.

Point transformations may be linear (e.g., negative), piecewise linear (e.g., gray-level slicing), or nonlinear (e.g., gamma correction).

Contrast adjustment is one of the most common applications of point transformation functions (also known by many other names such as contrast stretching, gray-level stretching, contrast adjustment, and amplitude scaling). One of the most useful variants of contrast adjustment functions is the automatic contrast adjustment (or simply autocontrast), a point transformation that—for images of class uint 8 in MATLAB—maps the darkest pixel value in the input image to 0 and the brightest pixel value to 255 and redistributes the intermediate values linearly. The autocontrast function can be described as follows:

$$S=\frac{L\text{-}1}{r_{max}-r_{min}}(r-r_{min}) \quad (3)$$

Where r is the pixel value in the original image (in the [0, 255] range), r_{max} and r_{min} are the values of its brightest and darkest pixels, respectively, s is the resulting pixel value, and L-1 is the highest gray value in the input image (usually L = 256). MATLAB has a built-in function imadjust to perform contrast adjustments.

Power law (gamma) transformations is given by the following transformation function:

$$s = c \bullet r^{\gamma} \quad (4)$$

Where r is the original pixel value, s is the resulting pixel value, c is a scaling constant, and γ is a positive value.

Histogram equalization is one of the well-known enhancement techniques. In histogram equalization, the dynamic range and contrast of an image is modified by altering the image such that its intensity histogram has a desired shape. This is achieved using cumulative distribution function as the mapping function. The intensity levels are changed such that the peaks of the histogram are stretched and the troughs are compressed. If a digital image has *N* pixels distributed in L discrete intensity levels and n_k is the number of pixels with intensity level i_k and then the probability density function of the image is given by equation (5). The cumulative density function is defined in equation (6):

$$f_i(i_k)=\frac{n_k}{N} \quad (5)$$

$$F_k(i_k)=\sum_{j=0}^{k} f_i(i_j) \quad (6)$$

Although this method is simple, since the gray values are physically far apart from each other in the image. Due to this reason, histogram equalization gives very poor result images (Sasi and Jayasree, 2013).

Adaptive Histogram Equalization (AHE) is a method of contrast enhancement. It is different from ordinary histogram equalization. In adaptive method, many histograms are computed where each histogram corresponds to a different section of image. Hence, AHE improves the local contrast of an image and more details can be observed. With this method, information of all intensity ranges of the image can be viewed simultaneously. There are many ordinary display devices that are not able to depict the full dynamic intensity range. This method brings a solution to this problem. Other advantages include that it is automatic (i.e., no manual intervention is required) and reproducible from study to study [DOI, Kunio 1996] (DOI 1996).

Apart from the advantage of local enhancement, AHE method has some limitations also. This method works too slowly on a general purpose computer although it works correctly. As enhancement is carried out in a local area, AHE tends to over enhance the noise content (Gupta and Kaur, 2014).

4. RESULT AND DISCUSSION

Four different types of filters used to enhance the images which are (HE, ADH, CLAHE, and Wiener) after image processing completed results showed that (HE, and ADH) is the best method to be used for detecting this renal problem as in (HE) filter PUJ, renal cortex, and renal pelvis is very clear to be defined in all of the images, furthermore using (ADH) PUJ, renal cortex and renal pyramids can be clearly defined. While pictures that used (CLAHE), and (Wiener) types of filter shows poor quality of the PUJ borders, and somewhat blurring with more noises compared with (HE and ADH). As the figures show in Fig. 1-8.

5. CONCLUSION

Image processing is a revolution in imaging as general, especially in the medical imaging due to the options that

Fig. 1. Original two-dimensional ultrasound image shows simple (mild) pelviureteric junction dilatation

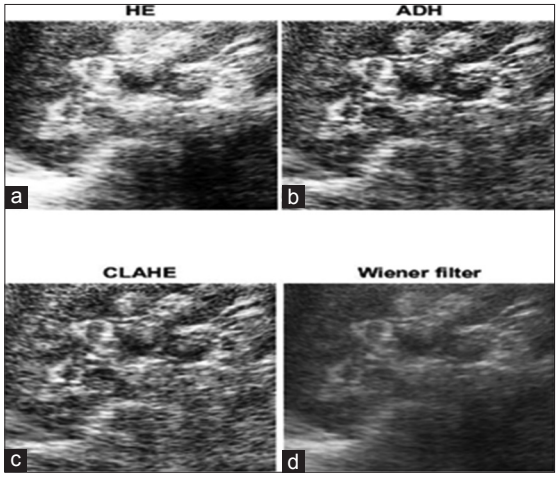

Fig. 2. (a-d) Image treated with the four filter types

Fig. 3. Original two-dimensional ultrasound image shows mild–moderate dilatation in pelviureteric junction

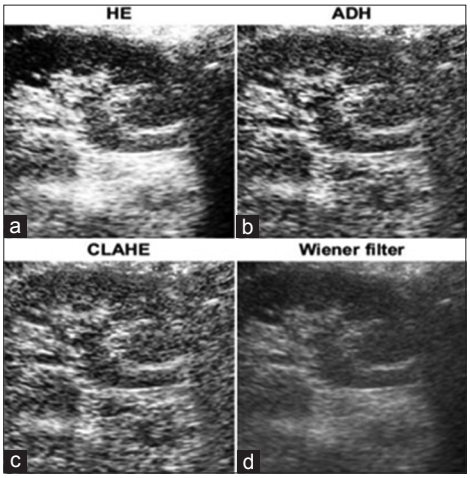

Fig. 4. (a-d) Image treated with the four filter types

Fig. 5. Original two-dimensional ultrasound image shows moderate dilatation of pelviureteric junction

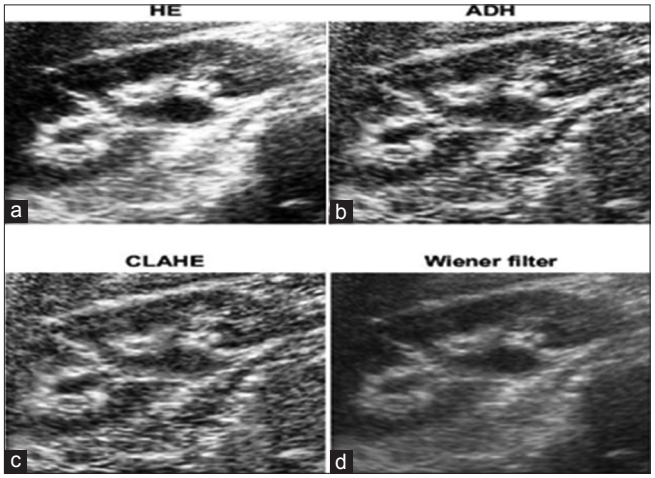

Fig. 6. (a-d) Image treated with the four filter types

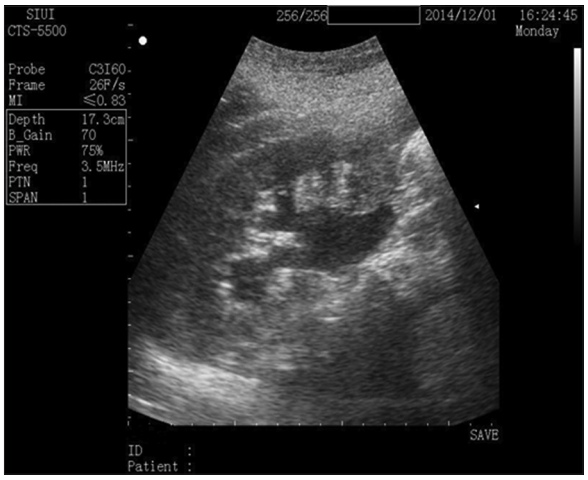

Fig. 7. Original two-dimensional ultrasound image shows sever dilatation in the pelviureteric junction

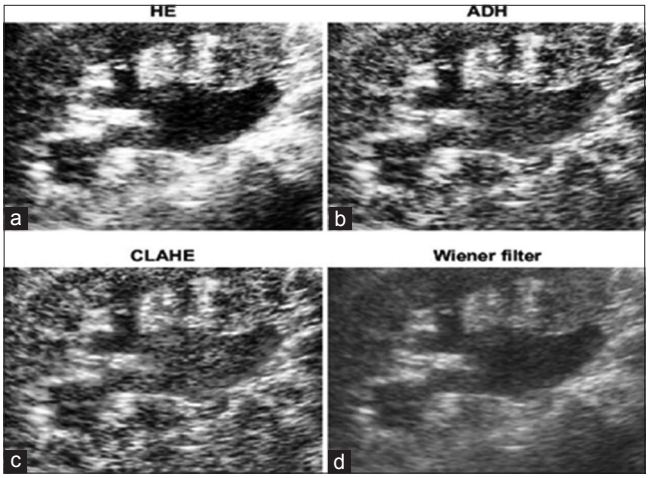

Fig. 8. (a-d) Image treated with the four filter types

provides to medical doctors and sonographers, so that in this study after saving 2D ultrasound images, different types of filters used to enhance those images, and improve its quality to be easier for diagnosis four different abnormal images of PUJ dilatation selected from all the patients who scanned, each case with different level of dilation from mild to moderate and sever.

REFERENCES

[1] J. R. Lindner, J. Song, F. Xu, A. L. Klibanov, K. Singbartl, K. Ley and S. Kaul. "Noninvasive ultrasound imaging of inflammation using microbubbles targeted to activated leukocytes." *Circulation*, vol. 102. No. 22, pp. 2745-2750, 2000.

[2] P. G. Ransley, H. K. Dhillon, I. Gordon, P. G. Duffy, M. J. Dillon and T. M. Barratt. "The postnatal management of hydronephrosis diagnosed by prenatal ultrasound." *The Journal of Urology*, vol. 144, pp. 584-587, 1990.

[3] T. D. Brandt, H. L. Neiman, M. J. Dragowski, W. Bulawa and G. Claykamp. "Ultrasound assessment of normal renal dimensions." *Journal of Ultrasound in Medicine*, vol. 1. no. 2, pp. 49-52, 1982.

[4] S. Mahant, J. Friedman and C. MacArthur. "Renal ultrasound findings and vesicoureteral reflux in children hospitalised with urinary tract infection." *Archives of Disease in Childhood*, vol. 86. No. 6, pp. 419-420, 2002.

[5] J. S. Berns, D. H. Ellison, S. L. Linas and M. H. Rosner. "Training the next generation's nephrology workforce." *Clinical Journal of the American Society of Nephrology*, vol. 9. No. 9, pp. 1639-1644, 2014.

[6] A. P. Barker, M. M. Cave, D. F. Thomas, R. J. Lilford, H. C. Irving, R. J. Arthur and S. E. Smith. "Fetal pelvi-ureteric junction obstruction: Predictors of outcome." *British Journal of Urology*, vol. 76. no. 5, pp. 649-652, 1995.

[7] R. Aviram, A. Pomeranz, R. Sharony, Y. Beyth, V. Rathaus and R. Tepper. "The increase of renal pelvis dilatation in the fetus and its significance." *Ultrasound in Obstetrics and Gynecology*, vol. 16. No. 1, pp. 60-62, 2000.

[8] H. P. Duong, A. Piepsz, K. Khelif, F. Collier, K. de Man, N. Damry, F. Janssen, M. Hall and K. Ismaili. "Transverse comparisons between ultrasound and radionuclide parameters in children with presumed antenatally detected pelvi-ureteric junction obstruction." *European Journal of Nuclear Medicine and Molecular Imaging*, vol. 42. no. 6, pp. 940-946, 2015.

[9] P. Masson, G. De Luca, N. Tapia, C. Le Pommelet, A. Es Sathi, K. Touati, A Tizeggaghine and P. Quetin. "Postnatal investigation and outcome of isolated fetal renal pelvis dilatation." *Archives de Pediatrie*, vol. 16. no. 8, pp. 1103-1110, 2009.

[10] C. Hong-Lin. "Surgical indications for unilateral neonatal hydronephrosis in considering ureteropelvic junction obstruction." *Urological Science*, vol. 25. no. 3, pp. 73-76, 2014.

[11] N. A. Patel and P. P. Suthar. "Ultrasound appearance of congenital renal disease: Pictorial review." *The Egyptian Journal of Radiology and Nuclear Medicine*, vol. 45. no. 4, pp. 1255-1264, 2014.

[12] K. Doi. "Current status and future potential of computer-aided diagnosis in medical imaging." *The British Journal of Radiology*, vol. 78. no. 1, pp. S3-S19, 2014.

[13] K. Doi. "Current research and future potential of computer-aided diagnosis (CAD) in radiology: Introduction to overviews at five institutions around the world." *Medical Imaging Technology*, vol. 14. no. 6, pp. 621, 1996.

ORIGINAL RESEARCH ARTICLE UHD JOURNAL OF SCIENCE AND TECHNOLOGY

Estimation of Nanopore Size Using Image Processing

Haidar Jalal Ismail, Azeez Abdullah Azeez Barzinjy, and Kadhim Qasim Jabbar

Department of Physics, College of Education, Salahaddin University-Erbil, Zanko, Erbil, Iraq

ABSTRACT

Nanopores, which are nanometer-sized holes, have been utilized in apparatus that point toward sensing a range of molecules such as DNA and RNA and single proteins The important factor for sensing molecules is diameters of nanopores which can be found through a substantial process called segmenting for nanopores of scanning electron microscope (SEM) images. In this investigation, four segmentation methods, namely, threshold, bilateral filter, k-means, and expectation maximization-Gaussian mixture model (EM-GMM) which has been utilized to segment three SEM images of nanopores efficiently. The quality of segmentation evaluated objectively through computing Rand index among them. Consequently, the nanopore size of Al_2O_3 films computed by means of SEM images. This study found that EM-GMM segmenting method gives promising results among other examined methods. It is for their high R-index, minimum adjustment parameters (just one variable which set usually 2), and low consuming time. Hence, it can be used efficiently for computing nanopore count and size.

Index Terms: Feature Extraction, Image Segmentation, Nanopore, Segmentation Evaluation

1. INTRODUCTION

Biosensors can sense single molecule through using nanopores. They may sense unlabeled biopolymers such as DNA and RNA and single proteins. The sensing takes place when ion currents reduced largely due to blocking pores by passing molecules [1]. The nanopore diameter is very important for sensing molecules. The main step for finding that is through using segmenting of them from scanning electron microscope (SEM) image.

Image segmentation defined as dividing images into multiple parts that have homogeneity in pixel intensity, color, or texture [2]. One of the simple, sometimes useful, segmenting methods is threshold technique. However, it is time-consuming for its strategy based on trial and error method, and for sometimes, a single threshold value does not work well, especially, for a series of image frames of video data. Akhtaruzzaman *et al.* [3] used an automated threshold detection on a video which is a series of image frames of human walking to segment human lower limbs. They applied automated threshold detection to convert the image frames into grayscale image, line fill algorithm to smoothing the edges of object, and remove background to get out the object.

In general, image enhancing through denoising is an important previous step before segmenting objects. One of the denoising filters is bilateral filter which reduces noise with remaining sharp edges of the objects. Besides, Nguyen *et al.* [4] denoised specific artifacts and segmented the full body bone structure by employing 3D bilateral filter and 3D graph-cut, respectively. On the other hand, Sahadevan *et al.* [5] increased the accuracy of super vector machine classifier using a bilateral filter which merges spatial contextual information to spectral domain.

Access this article online

DOI: 10.21928/uhdjst.v1n1y2017.pp38-44

E-ISSN: 2521-4217
P-ISSN: 2521-4209

Corresponding author's e-mail: haidar.ismail@su.edu.krd

Received: 10-03-2017 Accepted: 25-03-2017 Published: 12-04-2017

Another method of segmentation is K-means which put the image into multi cluster of pixels according to factors such as their intensities. Chen *et al.* [6] propose a semiautomatic segmentation method, using K-means, to determine object's mean temperature and variance through segmenting contours of thermal images taken by the optical camera.

Fu and Wang [7] applied expectation maximization-Gaussian mixture model (EM-GMM) on color images to segmenting them, and their results approve the power of it. The EM-GMM and fuzzy-C-means (FCM) methods are widely used in image segmentation. However, they have a major drawback for their sensitivity to the noise. Kalti and Mahjoub [8] proposed a variant of these methods to resolve this problem. Their results showed improvement compare to standard version of EM-GMM and FCM.

Several researches work to find geometrical structures of nanopores. Alexander *et al.* [9] computed nanopore size, perimeter, and some other geometric features using histogram equalization, morphological, and statistical operations. In another work, that done by Phromsuwan *et al.* [10], size of nanopores of SEM images obtained through using morphological and Canny edge detector techniques. Parashuram and Vidyasagar [11] used morphological and global thresholding for obtaining nanopore diameter and statistical features. Same authors with Muralidhara [12] using same operations to obtain perimeter of the nanopores. It can be realized that all above methods using methods that need trial and error parameters to give proper results.

This work aims to find semiautomatic algorithm to find diameter of nanopores of SEM images through examine four segmenting techniques. The performance will be evaluated objectively, and the average of nanopore's diameter will be computed.

2. MATERIALS AND METHODS

Three SEM images of the nanopores anodic alumina film [13] used in this study for segmenting by our segmenting techniques and compute their diameters and number of pores. They consist of three SEM images with different widening times, namely, 0, 10, and 20 minutes as shown in Fig. 1.

The images segmented by four methods. The simple method is thresholding method that used here as ground truth images for objective evaluating of other segmenting methods. The second and third segmenting methods utilize bilateral filter, k-means, as the first step and using region selector as the second step. The fourth one is segmenting images using EM-GMM (Fig. 2).

Thresholding is a technique of selecting optimum gray level value which separates the region of interest from other regions. Thresholding produced binary images from gray level by making pixels lower or greater than a gray level value to zero and other remaining pixels to one. If g(x, y) is threshold output of an input f(x, y) at specific input gray level value T, it can be described as [14] follows:

$$g(x,y)=\begin{cases}1 & f(x,y)>T\\ 0 & \text{otherwise}\end{cases} \quad (1)$$

K-means method divides pixels into a number of separate clusters. It's algorithm consists of two steps. First, it finds k centroid (k number of clusters) for pixels of the image, and second, relate each pixel to a centroid through using different methods of computing distance between them. Euclidean distance may be used to measure distance, and it defined as follows:

$$d=||p(x,y)-c_k|| \quad (2)$$

Where p(x, y) is an input pixel to be cluster and c_k is the cluster centers. After grouping pixels into k sets (i.e. clusters), new Euclidean distance evaluated between each center and pixels, so pixels assigned to the minimum Euclidean distance [15].

The bilateral filtering is a technique for smoothing and sharpening edges of an image. It obtained by applying one Gaussian filter for obtaining the spatial domain and another one for intensity domain. The filter output of s pixel is given by following equation:

$$J(s)=\frac{1}{K(s)}\sum_{p\in\varnothing}(p-s)(I_p-I_s)I_p \quad (3)$$

Where K(s) is normalization expression:

$$K(s)=\sum_{p\in\varnothing}f(p-s)g(I_p-I_s) \quad (4)$$

Where f and g are Gaussian, in the spatial domain and in the intensity domain, which represents the range filter, respectively [16].

Region selector method uses roicolor command in Matlab which select wanted region according to color or intensity levels in grayscale image.

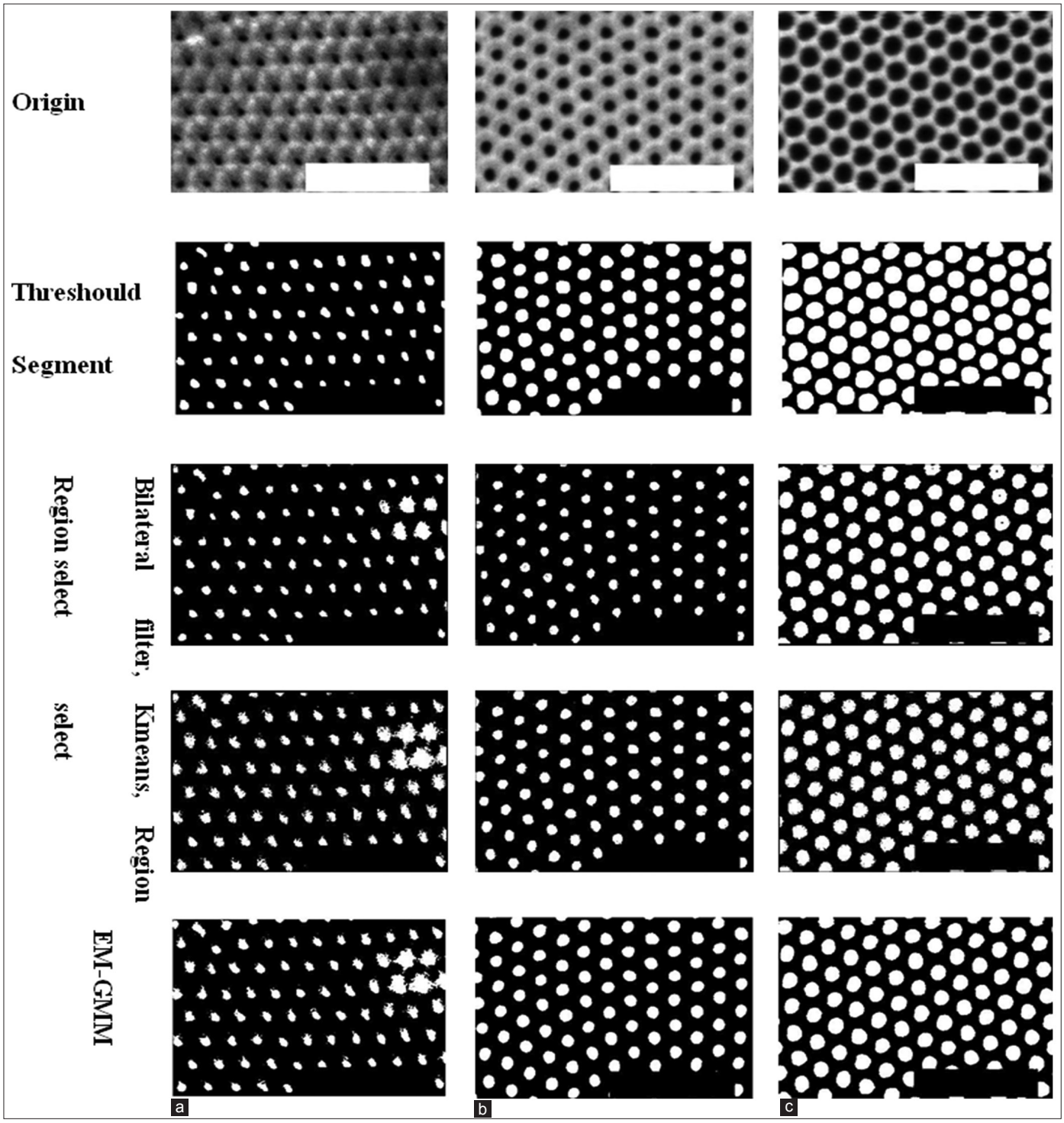

Fig. 1. Four segmentation methods for three scanning electron microscope images with pore widening times: (a) 0 min, (b) 10 min, and (c) 20 min (Scale bar = 500 nm) [13]

The GMM consists of Gaussian distributions that defined as follows:

$$f(x_n) = \sum_{k=1}^{K} p_k N(x_n \mid Q_k) \quad (5)$$

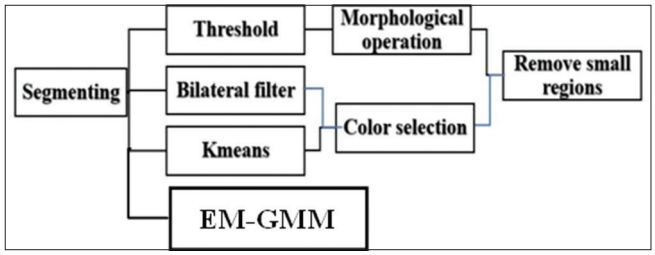

Fig. 2. Image processing steps for different segmentation methods

Where every component of function $N(x_n|\Theta_k)$ is a Gaussian distribution which, for a D-dimensional vector x, defined as follows:

$$N(x|\Theta)=\frac{1}{(2p)^{D/2}}\frac{1}{|S|^{1/2}}\exp\left\{-\frac{1}{2}(x-m)^T\Sigma^{-1}(x-m)\right\} \quad (6)$$

Where μ and Σ are a D-dimensional average vector and a D × D covariance matrix, respectively. The prior distribution π_k defines the probability of noticing x_n that belongs to the k^{th} class Ω_k. It is unrelated to the observation x_n. Moreover, π_k must possess these restrictions:

$$0\le\pi_k\le 1,\sum_{k=1}^{K}\pi_k;\qquad k=1,....,K \quad (7)$$

After finding the density function for an observation, the log-likelihood function of N observations is as follows:

$$L(\Theta)=\sum_{n=1}^{N}\log(\sum_{k=1}^{K}\pi_k N(x_n|\Theta_k) \quad (8)$$

According to Equations 5 and 8, the major feature of the GMM is that its form is too simple and it needs few variables. Moreover, when GMM used in image segmentation, the correct results obtained if they unrelated to each other. To find the variables (π_k, μ_k, and Σ_k), the EM step is usually applied to get the upper limit of the log-likelihood function in Equation 8. The last probability for expectation stage of EM obtained as follows:

$$p^t(\Theta_k|x_n)=\frac{\pi_k N(x_n|\Theta_k)}{\sum_{j=1}^{K}\pi_j N(x_n|\Theta_j)} \quad (9)$$

In the maximization step of EM, the parameters (π_k, μ_k, and Σ_k) are changed iteratively through the following formulas:

$$\pi_k^{t+1}=\frac{\sum_{n=1}^{N}p^t(\Theta_k|x_n)X_n}{\sum_{n=1}^{N}p^t(\Theta_k|x_n)} \quad (10)$$

$$\Sigma_k^{t+1}=\frac{\sum_{n=1}^{N}p^t(\Theta_k|x_n)(x_n-m_k)(x_n-m_k)^T}{\sum_{n=1}^{N}p^t(\Theta_k|x_n)} \quad (11)$$

$$\pi_k^{t+1}=\frac{\sum_{n=1}^{N}p^t(\Theta_k|x_n)}{N} \quad (12)$$

Where t denotes the iteration value. The loop is stopped in the convergence condition. The value from Equation 9 for maximum posterior criterion used to get the class label for each pixel [17].

A. Rand Index

The Rand index, which founded by William Rand, used for the comparison of two arbitrary segmentations using pair-wise label relationships. It obtained by division of the number of pixel pairs that have the same label relationship in both segmentations. The n_{uv} is the number of points labeled u in S and that labeled v in S'. The labeled points u in the first part of S, and labeled points v in second part S' are termed as $n_{u\blacksquare}$ and $n_{\blacksquare v}$, respectively. Afterward:

$$n_{u\blacksquare}=\sum_v n_{uv} \qquad n_{\blacksquare v}=\sum_u n_{uv} \quad (13)$$

Clearly $\sum_u n_{u\blacksquare}=\sum_v n_{u\blacksquare}=N$ is the entire data points. Hence, the Rand index is as follows:

$$R(S,S')=1-\frac{\frac{1}{2}\left(\sum_u n_u^2+\sum_v n_u^2\right)-\sum_{u,v}n_{uv}^2}{N(N-1)/2} \quad (14)$$

The R-index is 1 when both segmentations have total similarities and 0 for zero ones. This type of similarity measurements takes small running time when unique labels in S and S' are smaller than total data numbers N [18].

3. RESULTS AND DISCUSSION

All three SEM images segmented using threshold technique obtained after a large number of trial and error for optimize threshold intensity pixel value, morphological operation, and removing small objects. They considered as ground truth images through visual perception to objective evaluating other segmenting methods (Fig. 1). The results of other segmenting methods are shown in same figure too.

Fig. 1a shows SEM that suffers from some noise effect. The Wiener filter and adaptive histogram equalization used

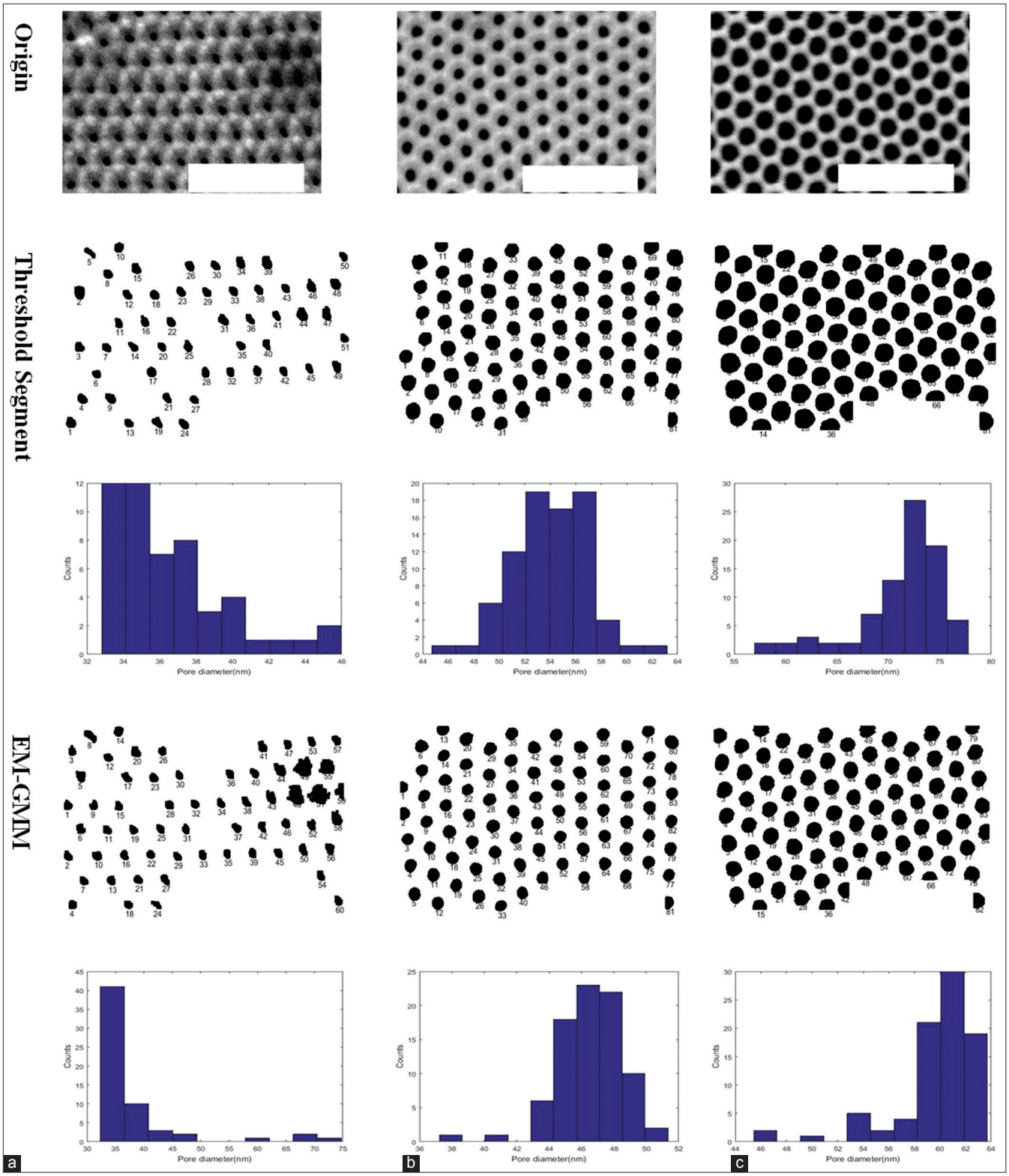

Fig. 3. (a-c) Total counting nanopores and distribution of nanopore sizes for threshold segmenting (ground truth image) and expectation maximization-Gaussian mixture model (higher R index) for all three scanning electron microscope types

TABLE I
Time Consuming, Rand Index, Nanopore Diameter and Nanopore Counts for all SEM Images Segmented by the Four Techniques

Nanopore	Threshold segment	Bilateral filter, region selector	K*means, region selector	EM-GMM
a				
Time (s)	1.31	29.21	15.51	19.96
Rand index	-	0.781	0.757	0.91
Diameter (nm)	36.7±10.4	-	-	39.3±19.5
Pore count	51	-	-	60
b				
Time (s)	1.28	30.44	20.07	11.24
Rand index	-	0.599	0.592	0.870
Diameter (nm)	54.2±11.9	-	-	46.6±9.1
Pore count	81	-	-	83
c				
Time (s)	1.36	30.35	14.79	13.68
Rand index	-	0.503	0.503	0.755
Diameter (nm)	71.8±15.9	-	-	59.8±12.7
Pore count	83	-	-	84

SEM: Scanning electron microscope, EM-GMM: Expectation maximization-Gaussian mixture model

for denoising and contrast enhancement before segmenting by threshold technique. Nevertheless, it still effects on segmenting by other methods.

Fig. 1b and c show good segmenting for all segmenting methods. Fig. 3 presents all three images that segment by threshold, ground truth image, and EM-GMM, higher R index, that number labeled each pore. Furthermore, the distribution of pore size which mentioned showed in same figure. They can be fitted mainly as Gaussian distribution as appear charts of Fig. 3 and that in agreement with what in results of Macias *et al.* [13].

The time consuming for running code, Rand index, number, and diameter of nanopores for segmenting methods and for all three SEM images presented in Table I. The obtained results for diameter of nanopores are in a good agreement with Macias *et al.* [13] results for threshold segmenting and smaller for EM-GMM segmenting. The method of analysis SEM images in mentioned reference is unknown. The EM-GMM is semiautomatic method, with high R index, and relatively smaller time consuming is better than other segmenting methods studied here.

4. CONCLUSION

Four different segmenting methods are applied on three SEM images with various time widening pores 0, 10, and 20 minutes. It can be noticed that the threshold segmenting possesses good results, but perhaps, it needs a large number of trial and error for choosing optimum threshold pixel intensity and needs also morphological operation and removing small objects. The authors also concluded that the EM-GMM is superior than bilateral filter and K-means with region selector, since it has higher R index than them. Consequently, their segmenting results used for pore counting and computing their diameters. Likewise, it has relatively small time consuming of running. Accordingly, EM-GMM can be used professionally for segmenting SEM images and finding number of pores and their diameters.

5. ACKNOWLEDGMENT

The authors would like to express their acknowledgment to the Salahaddin University for supporting him with available tools.

REFERENCES

[1] C. Raillon, P. Granjon, M. Graf, L. J. Steinbock and A. Radenovic, "Fast and automatic processing of multi-level events in nanopore translocation experiments." *Nanoscale,* vol. 4, no. 16, pp. 4916, 2012.

[2] M. Ahmed, S. Abd El-attySoliman and J. Adamkani. "Performance study of innovative and advanced image segmentation techniques." *Singaporean Journal of Scientific Research,* vol. 7, no. 12015, pp. 320-326, 2014.

[3] M. Akhtaruzzaman, A. A. Shafie and R. Khan. "Automated threshold detection for object segmentation in colour image. *ARPN Journal of Engineering and Applied Sciences,* vol. 11, no. 6, pp. 4100-4104, 2016.

[4] C. Nguyen, J. Havlicek, Q. Duong, S. Vesely, R. Gress,

L. Lindenberg, P. Choyke, J. H. Chakrabarty and K. Williamset. “An automatic 3D CT/PET segmentation framework for bone marrow proliferation assessment.” 2016 IEEE International Conference on Image Processing (ICIP), Phoenix, AZ, 2016, pp. 4126-4130.

[5] A. S. Sahadevan, A. Routray, B. S. Das and S. Ahmad. “Hyperspectral image preprocessing with bilateral filter for improving the classification accuracy of support vector machines.” *Journal of Applied Remote Sensing,* vol. 10, no. 2, pp. 025004, Apr. 2016.

[6] Y. Y. Chen, W. S. Chen and H. S. Ni. “Image segmentation in thermal images.” 2016 IEEE International Conference on Industrial Technology (ICIT), Taipei, 2016, pp. 1507-1512.

[7] Z. Fu and L. Wang. “Color image segmentation using gaussian mixture.” in *Multimedia and Signal Processing: Second International Conference, CMSP 2012*, Shanghai, China, 2012.

[8] K. Kalti and M. Mahjoub. “Image segmentation by Gaussian mixture models and modified FCM algorithm.” *The International Arab Journal of Information Technology,* vol. 11, no. 1, pp. 11-18, 2014.

[9] S. Alexander, R. Azencott, B. Bodmann, A. Bouamrani, C. Chiappini, M. Ferrari, X. Liu and E. Tasciotti. “SEM image analysis for quality control of nanoparticles.” in Computer Analysis of Images and Patterns, Springer, Berlin, Heidelberg, 2009. pp. 590-597.

[10] U. Phromsuwan, Y. Sirisathitkul, C. Sirisathitkul, P. Muneesawang and B. Uyyanonvara. “Quantitative analysis of X-ray lithographic pores by SEM image processing.” *MAPAN-Journal of Metrology Society of India*, vol. 28, no. 4, pp. 327-333, 2013.

[11] P. Bannigidad and C. Vidyasagar. “Effect of time on anodized Al2O3 nanopore FESEM images using digital image processing techniques: A study on computational chemistry.” *International Journal of Emerging Trends and Technology in Computer Science (IJETTCS)*, vol. 4, no. 3, pp. 15-22, 2015.

[12] C. Vidyasagar, P. Bannigidad and H. Muralidhara. “Influence of anodizing time on porosity of nanopore structures grown on flexible TLC aluminium films and analysis of images using MATLAB software.” *Advanced Materials Letters,* vol. 7, no. 1, pp. 71-77, 2016.

[13] G. Macias, J. Ferré-Borrull, J. Pallarès and L. Marsal. “Effect of pore diameter in nanoporous anodic alumina optical biosensors.” *The Analyst*, vol. 140, no. 14, pp. 4848-4854, 2015.

[14] M. H. J. Vala and A. Baxi. “A review on Otsu image segmentation algorithm.” *International Journal of Advanced Research in Computer Engineering and Technology,* vol. 2, no. 2, pp. 387-389, 2013.

[15] N. Dhanachandra, K. Manglem and Y. Chanu. “Image segmentation using K-means clustering algorithm and subtractive clustering algorithm.” *Procedia Computer Science,* vol. 54, pp. 764-771, 2015.

[16] S. Agarwal and P. Kumar. “Denoising of a mixed noise color image through special filter.” *International Journal of Signal Processing, Image Processing and Pattern Recognition,* vol. 9, no. 1, pp. 159-176, 2016.

[17] T. Xiong, L. Zhang and Z. Yi. “Double Gaussian mixture model for image segmentation with spatial relationships.” *Journal of Visual Communication and Image Representation*, vol. 34, pp. 135-145, 2016.

[18] R. Unnikrishnan and M. Hebert. “Measures of similarity.” Application of Computer Vision, 2005. WACV/MOTIONS ‘05. vol. 1. Seventh IEEE Workshops on, Breckenridge, CO., 2005, pp. 394.

p-ISSN 2521-4209
e-ISSN 2521-4217

جامعة التنمية البشرية
UNIVERSITY OF HUMAN DEVELOPMENT

UHD Journal of Science and Technology

A Scientific periodical issued by University of Human Developement

Vol.1 No.(1) June 2017

2017 2717

e.mail:jst@uhd.edu.iq