

Volume 6 ▪ Issue 2 ▪ April 2012

Editor-in-Chief  
Professor João Manuel R. S. Tavares

INTERNATIONAL JOURNAL OF

# BIOMETRICS AND BIOINFORMATICS (IJBB)

ISSN : 1985-2347

Publication Frequency: 6 Issues / Year

CSC PUBLISHERS  
<http://www.cscjournals.org>

# **INTERNATIONAL JOURNAL OF BIOMETRICS AND BIOINFORMATICS (IJBB)**

**VOLUME 6, ISSUE 2, 2012**

**EDITED BY  
DR. NABEEL TAHIR**

ISSN (Online): 1985-2347

International Journal of Biometrics and Bioinformatics (IJBB) is published both in traditional paper form and in Internet. This journal is published at the website <http://www.cscjournals.org>, maintained by Computer Science Journals (CSC Journals), Malaysia.

IJBB Journal is a part of CSC Publishers

Computer Science Journals

<http://www.cscjournals.org>

# **INTERNATIONAL JOURNAL OF BIOMETRICS AND BIOINFORMATICS (IJBB)**

Book: Volume 6, Issue 2, April 2012

Publishing Date: 16-04-2012

ISSN (Online): 1985-2347

This work is subjected to copyright. All rights are reserved whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication of parts thereof is permitted only under the provision of the copyright law 1965, in its current version, and permission of use must always be obtained from CSC Publishers.

IJBB Journal is a part of CSC Publishers

<http://www.cscjournals.org>

© IJBB Journal

Published in Malaysia

Typesetting: Camera-ready by author, data conversion by CSC Publishing Services – CSC Journals, Malaysia

**CSC Publishers, 2012**

## EDITORIAL PREFACE

This is the second issue of volume six of International Journal of Biometric and Bioinformatics (IJBB). The Journal is published bi-monthly, with papers being peer reviewed to high international standards. The International Journal of Biometric and Bioinformatics is not limited to a specific aspect of Biology but it is devoted to the publication of high quality papers on all division of Bio in general. IJBB intends to disseminate knowledge in the various disciplines of the Biometric field from theoretical, practical and analytical research to physical implications and theoretical or quantitative discussion intended for academic and industrial progress. In order to position IJBB as one of the good journal on Bio-sciences, a group of highly valuable scholars are serving on the editorial board. The International Editorial Board ensures that significant developments in Biometrics from around the world are reflected in the Journal. Some important topics covers by journal are Bio-grid, biomedical image processing (fusion), Computational structural biology, Molecular sequence analysis, Genetic algorithms etc.

The initial efforts helped to shape the editorial policy and to sharpen the focus of the journal. Starting with volume 6, 2012, IJBB appears in more focused issues. Besides normal publications, IJBB intend to organized special issues on more focused topics. Each special issue will have a designated editor (editors) – either member of the editorial board or another recognized specialist in the respective field.

The coverage of the journal includes all new theoretical and experimental findings in the fields of Biometrics which enhance the knowledge of scientist, industrials, researchers and all those persons who are coupled with Bioscience field. IJBB objective is to publish articles that are not only technically proficient but also contains information and ideas of fresh interest for International readership. IJBB aims to handle submissions courteously and promptly. IJBB objectives are to promote and extend the use of all methods in the principal disciplines of Bioscience.

IJBB editors understand that how much it is important for authors and researchers to have their work published with a minimum delay after submission of their papers. They also strongly believe that the direct communication between the editors and authors are important for the welfare, quality and wellbeing of the Journal and its readers. Therefore, all activities from paper submission to paper publication are controlled through electronic systems that include electronic submission, editorial panel and review system that ensures rapid decision with least delays in the publication processes.

To build its international reputation, we are disseminating the publication information through Google Books, Google Scholar, Directory of Open Access Journals (DOAJ), Open J Gate, ScientificCommons, Docstoc and many more. Our International Editors are working on establishing ISI listing and a good impact factor for IJBB. We would like to remind you that the success of our journal depends directly on the number of quality articles submitted for review. Accordingly, we would like to request your participation by submitting quality manuscripts for review and encouraging your colleagues to submit quality manuscripts for review. One of the great benefits we can provide to our prospective authors is the mentoring nature of our review process. IJBB provides authors with high quality, helpful reviews that are shaped to assist authors in improving their manuscripts.

### **Editorial Board Members**

International Journal of Biometric and Bioinformatics (IJBB)

## **EDITORIAL BOARD**

### **EDITOR-in-CHIEF (EiC)**

**Professor João Manuel R. S. Tavares**  
University of Porto (Portugal)

### **ASSOCIATE EDITORS (AEiCs)**

---

**Assistant Professor. Yongjie Jessica Zhang**  
Mellon University  
United States of America

**Professor. Jimmy Thomas Efird**  
University of North Carolina  
United States of America

**Professor. H. Fai Poon**  
Sigma-Aldrich Inc  
United States of America

**Professor. Fadiel Ahmed**  
Tennessee State University  
United States of America

**Professor. Yu Xue**  
Huazhong University of Science and Technology  
China

**Associate Professor Chang-Tsun Li**  
University of Warwick  
United Kingdom

**Professor. Calvin Yu-Chian Chen**  
China Medical university  
Taiwan

### **EDITORIAL BOARD MEMBERS (EBMs)**

---

**Assistant Professor. M. Emre Celebi**  
Louisiana State University  
United States of America

**Dr. Ganesan Pugalenth**  
Genome Institute of Singapore  
Singapore

**Dr. Vijayaraj Nagarajan**  
National Institutes of Health  
United States of America

**Dr. Wichian Sittiprapaporn**  
Mahasarakham University  
Thailand

**Dr. Paola Lecca**  
University of Trento  
Italy

**Associate Professor. Renato Natal Jorge**  
University of Porto  
Portugal

**Assistant Professor. Daniela Iacoviello**  
Sapienza University of Rome  
Italy

**Professor. Christos E. Constantinou**  
Stanford University School of Medicine  
United States of America

**Professor. Fiorella SGALLARI**  
University of Bologna  
Italy

**Professor. George Perry**  
University of Texas at San Antonio  
United States of America

**Assistant Professor. Giuseppe Placidi**  
Università dell'Aquila  
Italy

**Assistant Professor. Sae Hwang**  
University of Illinois  
United States of America

**Associate Professor Quan Wen**  
University of Electronic Science and Technology  
China

**Dr. Paula Moreira**  
University of Coimbra  
Portugal

**Dr. Riadh Hammami**  
Laval University  
Canada

**Dr Antonio Marco**  
University of Manchester  
United Kingdom

**Dr Peng Jiang**  
University of Iowa  
United States of America

**Dr Shunzhou Yu**

General Motors Global R&D Center  
United States of America

**Dr Christopher Taylor**

University of New Orleans  
United States of America

**Dr Horacio Pérez-Sánchez**

University of Murcia  
Spain

## TABLE OF CONTENTS

Volume 6, Issue 2, April 2012

### Pages

- 38– 46      A Computational Drug Designing from Active Product of Herbal Plant *Ochna Squarrosa* to Relieve Menstrual Complexities  
*Aubhishek Zaman, Md. Arafat Hossain Khan*
- 47 – 57      An Integrated Algorithm Supporting Confidentiality and Integrity for Secured Access and Storage of DICOM Images  
*Suresh Jaganathan, Arun Fera M*
- 58 – 67      Estimation of Age Through Fingerprints Using Wavelet Transform and Singular Value Decomposition  
*Gnanasivam P, Dr. S. Muttan*

# A Computational Drug Designing From Active Product of Herbal Plant *Ochna Squarrosa* to Relieve Menstrual Complexities

**Aubhishek Zaman**

Department of Genetic Engineering and Biotechnology  
University of Dhaka  
Dhaka-1000, Bangladesh

*aubhishek@gmail.com*

**Md. Arafat Hossain Khan**

Department of Computer Science and Engineering  
Jagannath University,  
Dhaka, Bangladesh

*sagar\_buet@yahoo.com*

---

## Abstract

*Ochna squarrosa* (Golden Champak), a Bangladeshi herbal plant known locally as Sheuri, has for long been used for treating menstrual complexities. Although root decoction of the related species variants has been reported to contain active compound Ochnaflavone- a derivative of isoflavone- this chemical's presence in *O. squarrosa* was far from confirmed. Furthermore, the molecular mechanism of action of the chemical is yet to be identified. Here, we report the presence of Ochnaflavone in the plant. Moreover, our computational study reveals a plausible target protein where the active compound binds. This study confirms the basis of the traditional herbal practice and can be useful for further developing a synthetic drug. This in return, we hope, will shift the current use of Ochnaflavone as 'observational medicine' to 'evidence based medicine'.

**Keywords:** *Ochna Squarrosa*, Estrogen Receptor, Isoflavone, Molecular Docking.

---

## 1 INTRODUCTION

Estrogen receptors bind hormone estrogen, alternatively known as 17 $\beta$ -estradiol. There are two distinct forms of the estrogen receptor- they are referred to as  $\alpha$  and  $\beta$ . Each of these forms is encoded by a separate gene (*ESR1* and *ESR2*, respectively). Hormone-activated estrogen receptors form dimers and since the two forms are coexpressed in many cell types, the receptors may form ER $\alpha$  ( $\alpha\alpha$ ) or ER $\beta$  ( $\beta\beta$ ) homodimers or ER $\alpha\beta$  ( $\alpha\beta$ ) heterodimers (Li X *et al.* 2004) [1] Estrogen receptor alpha and beta show significant overall sequence homology and both are composed of five domains.

The N-terminal domain can activate gene transcription in the absence of bound ligand (e.g., the estrogen hormone). While this region is able to activate gene transcription without ligand, this activation is weak and more selective compared to the activation provided by the E domain. The C domain, which is actually the DNA-binding domain, binds to estrogen response elements in DNA. The D domain works as a hinge region that connects the C and E domains. The E domain contains the ligand binding cavity as well as binding sites for coactivator and corepressor proteins. The E-domain in the presence of bound ligand is able to activate gene transcription. The C-terminal F domain function is not entirely clear and is variable in length (Ascenzi P *et al.* 2000, Bourguet W *et al.* 2006) [2][3].

The ER's helix 12 domain plays a crucial role in determining interactions with coactivators and corepressors and, therefore, the respective agonist or antagonist effect of the ligand (Ascenzi P 2000, Bourguet W 2006) [2][3].

Isoflavones comprise a class of organic compounds, often naturally occurring, related to the isoflavonoids (Kaufman PB *et al.* 1997, Heber D *et al.* 2008) [4][5]. Many act as phytoestrogens in

mammals. Being phytochemicals, they are able to be termed antioxidants because of their ability to trap singlet oxygen. Some isoflavones, in particular soy isoflavones, when studied in populations eating soy protein, have indicated that there is a lower incidence of breast cancer and other common cancers because of its role in influencing sex hormone metabolism and biological activity through intracellular enzymes, protein synthesis, growth factor actions, malignant cell proliferations, differentiation and angiogenesis (Heber D *et al.* 2008) [5]. Isoflavones are produced almost exclusively by the members of the *Fabaceae* (that is *Leguminosae*, or bean) family.



**FIGURE 1: *Ochna squarrosa* plant.** The plant is found abundantly in Chittagong Hill Tracts (CHT) and in the northern zone of Mymensingh district in Bangladesh. Although plants from both the location seems to be similar, slight variations in phenotype may well be subject to further investigation. In Bangladesh varieties of the plant, if any, is not well classified.

*Ochna squarrosa* (**FIGURE 1**) is small sub-deciduous tree. The tree is popularly known as Sheuri in local language. Leaves of the plant are alternate, 6-12 cm long, obovate, elliptic, sharply serrate. Flower of the plant is fragrant and it shoots from the ends of short, lateral branches or scars of fallen leaves in corymbose racemes. Plant contains fruit of 3-6 drupes, 6 mm long, oblong-ovoid, black, surrounded by the persistent calyx. The plant is found in the forests of Chittagong, Chittagong Hill Tracts, Cox's Bazar, Sylhet, Mymensingh.

PatchDock (<http://bioinfo3d.cs.tau.ac.il/PatchDock/>) is a computational tool for determining protein ligand or protein protein interaction. Its algorithm is based on object recognition and image segmentation techniques used in Computer Vision. It actually mimics human vision and extracts image data from protein structure files such as in .pdb file extension. Docking can be compared to assembling a jigsaw puzzle. When solving the puzzle it is tried to match two pieces by picking one piece and searching for the complementary one (Mashiach E *et al.* 2010) [6]. A puzzle-solver concentrates on the patterns that are unique for the puzzle element and look for the matching patterns in the rest of the pieces. PatchDock employs a similar technique. Given two molecules, their surfaces are divided into patches according to the surface shape. These patches correspond to patterns that visually distinguish between puzzle pieces. Once the patches are identified, they can be superimposed using shape matching algorithms (Schneidman-Duhovny D *et al.* 2003, Duhovny D NR *et al.* 2002) [7][14]. The algorithm has three major stages:

- Molecular Shape Representation - in this step PatchDock compute the molecular surface of the molecule. Next, it applies a segmentation algorithm for detection of geometric patches (concave, convex and flat surface pieces). The patches are filtered, so that only patches with 'hot spot' residues are retained.

- Surface Patch Matching - PatchDock applies a hybrid of the Geometric Hashing and Pose-Clustering matching techniques to match the patches detected in the previous step. Concave patches are matched with convex and flat patches with any type of patches.
- Filtering and Scoring - the candidate complexes from the previous step are examined. It discards all complexes with unacceptable penetrations of the atoms of the receptor to the atoms of the ligand. Finally, the remaining candidates are ranked according to a geometric shape complementarity score.

Pocket-Finder (<http://www.modelling.leeds.ac.uk/pocketfinder/>), an online computational tool to predict active site within a structure, is based on the Ligsite algorithm written by Hendlich *et al.* (1999) [8]. Pocket-Finder was written to compare pocket detection with our new ligand binding site detection algorithm Q-SiteFinder.

## 2. METHOD

### 2.1 Preparation of Root Decoction

*Ochna squarrosa* root decoction was collected from local herbal vendors. The root preparation was prepared using the standard isolation procedure. A very traditional approach was followed to prepare the root decoction. Local *Kabiraj* and *Homeopathic* physicians have been following the same procedure for ages. At first, the dry herbal ingredients was put in an earthenware or stainless steel pot and cold water was added until the water level is 3–4 cm above the herbs. The herbs were left to soak in the water for at least 1 hour. A pot on the cooker was placed and strong heat was applied to bring it to the boil. Once the liquid is boiling, heat was turned down and the herbs were simmered for 20 minutes, and then the decoction was strained from the pot into a receptacle. Another 200 ml of cold water was poured onto the herbs in the pot and cook for a further 20 minutes. The resulting liquid was strained into the receptacle holding the first decoction, thus mixing the two decoctions together. The total liquid obtained was about 200–250 ml. Finally, the decoction was divided into two or three doses and was taken these over the course of the day, warming each dose before drinking it.

### 2.2 Proof of Presence of Isoflavone

It is widespread in literature that isoflavone is responsible for relieving the menstrual complexity (Kennelly EJ *et al.* 2002) [9]. Presence of Isoflavone in species phylogenetically and phenotypically similar plants prompted us to isolate this active compound from the root decoction. After the root extract was purified, the presence of isoflavone as an active compound in the extract was predicted using chemical confirmation tests.

### 2.3 Computational Prediction

The 3D isoflavone structure was generated and was subsequently docked to protein 3D structure of Estrogen receptor. Protein Data Bank (PDB) (<http://www.pdb.org/>) file of Oyster estrogen receptor (PDB id: 3LTX) was collected from PDB database. The estrogen binding residues were conserved among Human and Oyster estrogen receptor- both the enzyme contains Asn and Gln in its active site. Estrogen receptor showed significantly positive results for receptor-ligand type interaction.

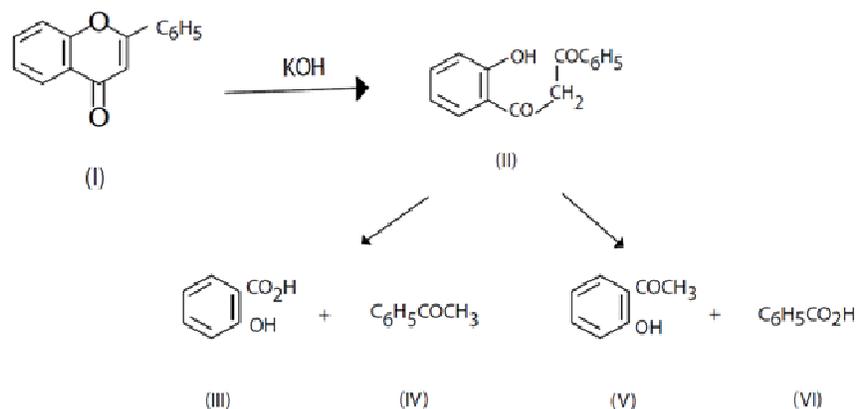
## 3. RESULTS

### 3.1 Proof of Presence of Isoflavone

The extract was purified using column chromatography and filtration. Purity of the product was fairly good for carrying out the chemical tests carried out later on. Isoflavone gave positive tests for its characteristic presumptive tests (S. F. Dyke *et al.* 1961) [10].

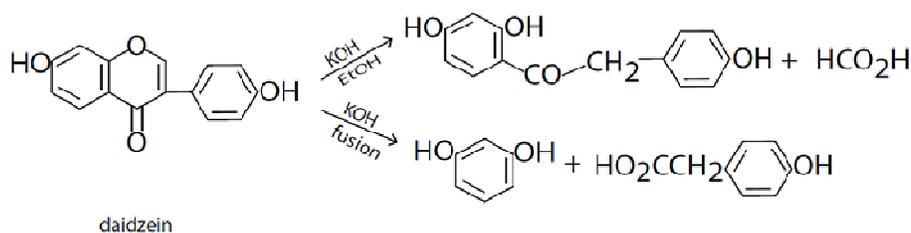
Flavone and isoflavone are structurally similar. So, presumptive tests for Isoflavone were carried out for portion common to both the structure. When boiled with concentrated potassium hydroxide solution, flavones (I) gave a mixture of four products- salicylic acid (III), acetophenone (IV), o-

hydroxyacetophenone (V) and benzoic acid (VI) (**FIGURE 2**). These products arise in pair- III and IV, and V and VI together (J.B. Harborne 1965, J.B. Harborne 1967) [11][12][19]. Both of them has a common precursor, a diketone, when the flavones pyrone ring opens to produce o-hydroxydibenzoylmethane (II). The products (III to VI) were individually identified by their characteristic chemical reactions.



**FIGURE 2: Confirming Flavone in root decoction.** Purified root decoction containing flavones was treated with potassium hydroxide which splitted the compound in two possible way. (See text for detail).

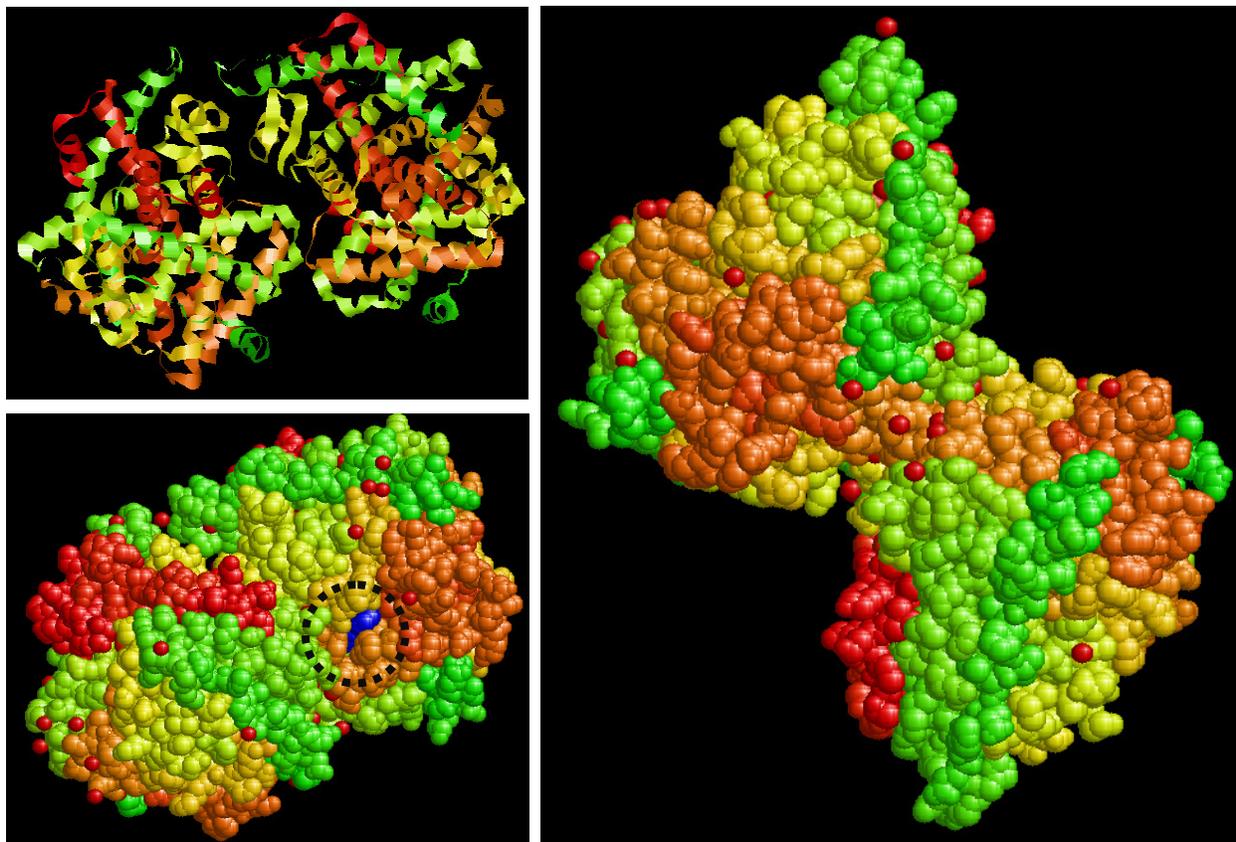
Isoflavone gives similar reaction. Fusion with potassium hydroxide breaks down the molecule in two fragments- one of them is resorcinol (**FIGURE 3**). An additional step to hydrolyze it with ethanolic potassium hydroxide permits the intermediates.



**FIGURE 3: Confirming Isoflavone in root decoction.** Daidzein has similar structure to isoflavone. Isoflavone gives similar reaction to that of flavone's one (See text for detail).

### 3.2 Computational Prediction

Computational drug designing has become one of the most effective ways to screen a ligand's ability as a drug. In biological terms, ligands are small molecules that interact with a protein. Isoflavone is a small molecule that mimics the structure of estrogen. Estrogen, a steroid hormone, is helps to alleviate menstrual cramps and other complexities. Estrogen binds to Estrogen receptor intracellularly and relay a signal by binding straight to DNA response elements (Paul S. Cooke *et al.* 1998) [13]. Isoflavone shows remarkable similarity to the bound state intermediate of the estrogen-estrogen receptor complex. When we computationally docked isoflavone to estrogen receptor (Figure-4), the binding affinity was very high and it bound at the same site where estrogen binds indicating the fact that it can work as a synthetic activator for the receptor (**FIGURE 4**). Isoflavone, as an estrogen agonist, can even induce estrogen action in the absence of its usual ligand, that is estrogen, and thereby relieve menstrual pain.

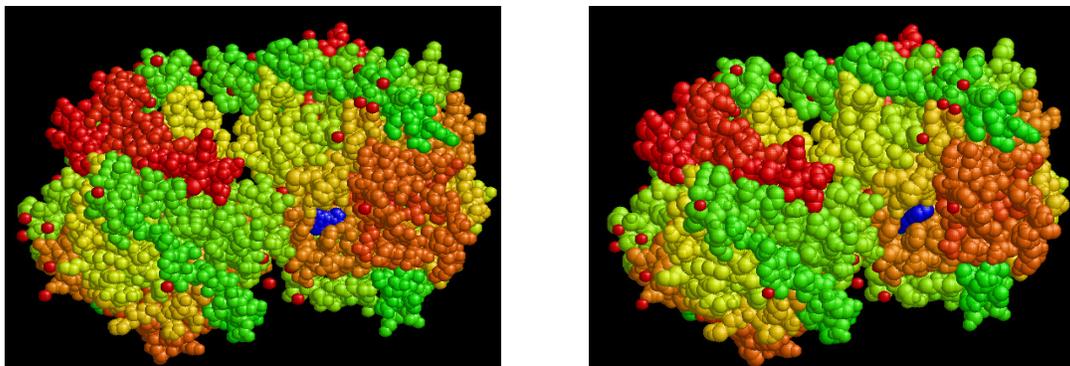


**FIGURE 4: Estrogen receptor complexed with isoflavone.** Top left and right figure shows Estrogen receptor without its ligand bound. Bottom left figure shows Estrogen receptor with Isoflavone bound tightly in the groove (circled with dotted black line) created by the active site.

PatchDock is a computational tool that we used to measures binding affinity between the protein and the small molecule/ligand Isoflavone. The patchDock results were compared to control ligand (Estradiol) and the following results were found-

Ligand type	Score	Area	ACE	Transformation
Isoflavone	4442	502.90	-118.88	1.56, 0.18, 2.63, 49.94, -7.63, 3.63
Estradiol (control)	2912	302.30	-304.04	0.79 1.04 -1.06 28.22 8.47 -2.88

**TABLE 1:** PatchDock results for Isoflavone-Estrogen receptor binding

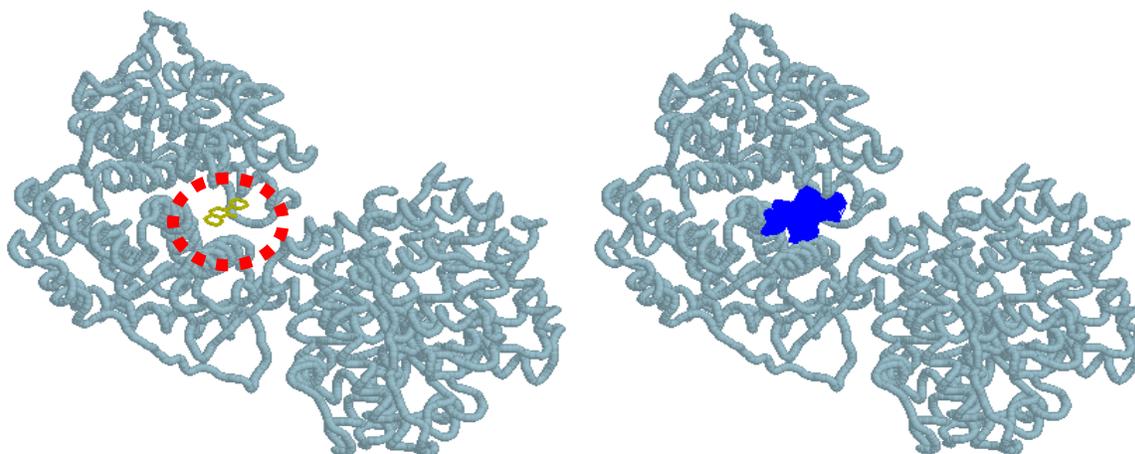


**FIGURE 5: Juxtaposition of control and predicted drug binding.** The figure on the left shows binding for natural substrate (marked in blue) and the right one shows binding of isoflavone.

Parameters analyzed in PatchDock computational tool are as follows-

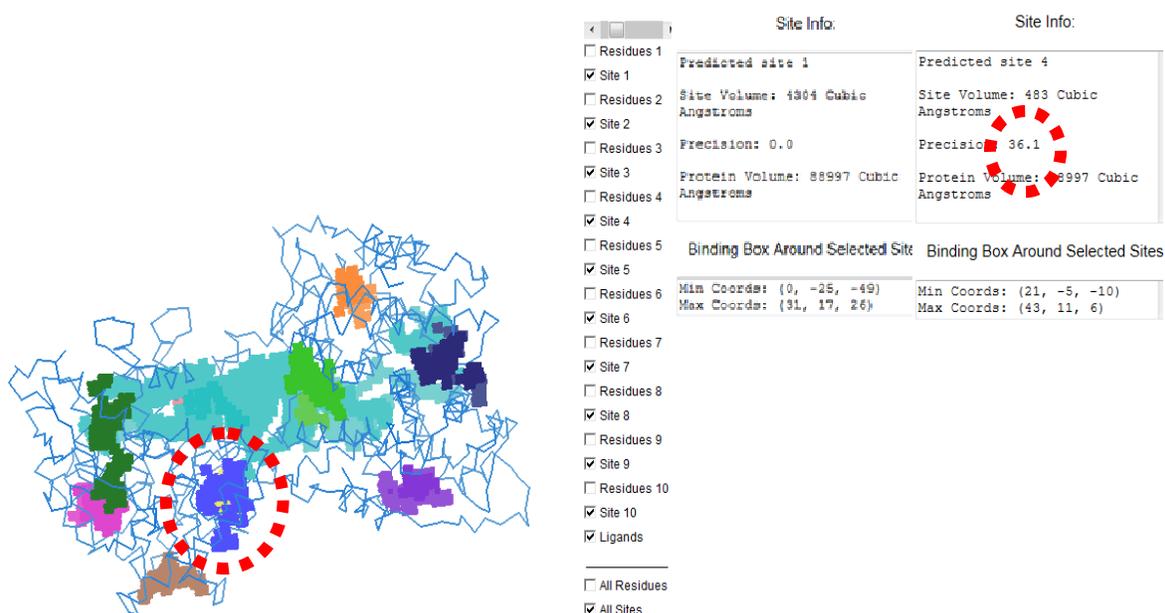
- Score: Geometric shape complementarity score (Duhovny D NR *et al.* 2002) [15]. The solutions are sorted according to this score.
- Area: Approximate interface area of the complex.
- ACE: Atomic contact energy according to Zhang *et al.* 1997 [16].
- Transformation: 3D transformation on the ligand molecule. 3 rotational angles and 3 translational parameters.

PocketFinder computational tool was used to find active site within the protein structure. Although the tool gives positive results for few potential active site, only the predicted site 4 (**Figure-7**) shows significance within confidence interval. The active site correlates excellently to the one cleft where isoflavone binds (**FIGURE-6**).. Thus, it confirms tight binding of isoflavone in the exact groove where estrogen binds in its receptor.



**FIGURE 6: Pocket-Finder results for surface cleft identification.** Binding site of the ligand Isoflavone (Left), as predicted by the tool. The right figure shows binding cleft for natural substrate Estrogen.

Amino acids residues interacting at the active site are- Gln371, Gln374, Asn375, Arg428, His429, Ala432, Val433, Leu435, His439, Val391, Asn392, Ala393, Glu394, Val395, Arg396, Leu398, Tyr401, Phe405, Gln408, Gln409.



**FIGURE 7:** Pocket-Finder results for cleft verification. The results show that for predicted cleft 1 (marked with Cyan patch) the precision was 0.00 whereas for surface cleft 4 (marked with blue patch, circled with dotted red line) the precision was 36.1 which fits well in the range of the confidence interval.

#### 4. DISCUSSION

Herbal plants have been one of the most important natural sources of isolating new active products. *Ochna squarrosa* has for long been identified to decrease menstrual pain, bleeding and muscle cramp (Vissandjee B *et al.* 1997) [18]. Here, our results show that the *O. squarrosa* has an active product which is Isoflavone (or its derivative) and it binds to estrogen receptor as an agonist which in result binds to gene regulatory elements responsible for alleviating the menstrual pain.

Although, a counter-current chromatography could have doubtlessly proved the presence of the active product (Renmin Liu *et al.* 2004) [17], our chemical evidences were sufficient enough for proving the presence of Isoflavone or its derivative conclusively. Besides, case studies of the closely related species such as *Ochna jabotapita* reveal the presence of similar active product.

Distinguishing between energy and binding parameters between agonist and antagonist has been the Holy Grail in structure based drug designing. However, based on the phenotypic effect it is clear that the herbal extract must enhance the effect of the receptor instead of reducing it. This is even clearer from our score data in **TABLE 1** where the score of the small molecule is fairly larger than the natural ligand.

The shape similarity between isoflavone ligand and estrogen was remarkable which gave us an initial indication about the ligand's target protein. The score for docked ligand and the estrogen receptor was significant enough. The score we found for an unbound ligand was almost the half the value that we derived. The high 'Area' of interaction also reveals tight binding. The ligand was bound well inside the active site cleft and no nonspecific interaction was found. Therefore, the binding of isoflavone to the estrogen receptor definitely indicates potential of a predictive drug. PocketFinder results scoring confirmed that isoflavone and estrogen share the same binding cleft (**FIGURE 6** and **FIGURE 7**). Isoflavone, as it seems to accelerate estrogen activity, works as an agonist of estrogen for the receptor.

Modern rational drug designing belongs to a twofold process. At first, potential hit are generated using approaches as carried out here. However, irrespective of values hits have to be analyzed furthermore in the molecular level physically. Despite our significant scoring values we believe the drug protein interaction will have to be further investigated physically.

Many drugs that we consume today sprang from ancient herbal science. However, use of many traditional herbal plants has been questioned by skeptics. Few hardliner, calling into question of herbal practices, have even gone into the degree of calling some of the ancient 'herbal science' a 'voodoo science'. Others, more measured critics have termed most uses to have a mere mollifying effect rather than any active drug response. In this context, predicting mode of action of herbal plants certainly is a happening field that concerns issues starting from religious to purely scientific. Our study on this particular plant was based on local observation that it works well to cure menstrual complexities. We believe our results underpin the scientific background behind the use with verifiable proof.

Our study here should give us better insight about how the traditional use of *O. squarrosa* is riveted well inside science rather than folklore. We hope, this study would help in designing a more efficient rational drug in the future and also would help us collect more natural products from the plant concerned. Hence, we hope the study will assist us to understand the beauty underneath natural products, to unlock the mystery of nature itself.

## 5. REFERENCES

- [1] Li X, Huang J, Yi P, Bambara RA, Hilf R, Muyan M (2004). Single-chain estrogen receptors (ERs) reveal that the ERalpha/beta heterodimer emulates functions of the ERalpha dimer in genomic estrogen signaling pathways. *Mol. Cell. Biol.* 24 (17): 7681–94. doi:10.1128/MCB.24.17.7681-7694.2004. PMC 506997. PMID 15314175.
- [2] Ascenzi P, Bocedi A, Marino M (August 2006). Structure-function relationship of estrogen receptor alpha and beta: impact on human health. *Mol Aspects Med* 27 (4): 299–402. doi:10.1016/j.mam.2006.07.001. PMID 16914190.
- [3] Bourguet W, Germain P, Gronemeyer H (October 2000). Nuclear receptor ligand-binding domains: three-dimensional structures, molecular interactions and pharmacological implications. *Trends Pharmacol Sci* 21 (10): 381–8. doi:10.1016/S0165-6147(00)01548-0. PMID 11050318.
- [4] Kaufman PB, Duke JA, Brielmann H, Boik J, Hoyt JE (1997). A comparative survey of leguminous plants as sources of the isoflavones, genistein and daidzein: implications for human nutrition and health. *J Altern Complement Med* 3 (1): 7–12. doi:10.1089/acm.1997.3.7. PMID 9395689.
- [5] Heber, D (2008). Plant Foods and Phytochemicals in human health. In Berdanier, C.D, Dwyer, J.T., Feldman, E.B.. CRC Press. pp. 176–181
- [6] Mashiach E, Schneidman-Duhovny D, Peri A, Shavit Y, Nussinov R, Wolfson HJ. An integrated suite of fast docking algorithms. *Proteins*. 2010 Nov 15;78(15):3197-204.
- [7] Schneidman-Duhovny D, Inbar Y, Polak V, Shatsky M, Halperin I, Benyamini H, Barzilai A, Dror O, Haspel N, Nussinov R, Wolfson HJ. Taking geometry to its edge: fast unbound rigid (and hinge-bent) docking. *Proteins*. 2003 Jul 1; 52(1): 107-12.
- [8] Holger Gohlke, Manfred Hendlich, Gerhard Klebe (1999) Knowledge-based scoring function to predict protein-ligand interactions *Journal of Molecular Biology* 295 (2): 337-356

- [9] Kennelly EJ, Baggett S, Nuntanakorn P, Ososki AL, Mori SA, Duke J, Coleton M, Kronenberg F. (2002) Analysis of thirteen populations of black cohosh for formononetin. *Phytomedicine*; 2002, 9:461–467.
- [10] S. F. Dyke, W. D. Ollis, M. Sainsbury (1961) Synthesis of Isoflavones. Part III.1 Caviunin, *Journal of Organic Chemistry* 26, 2453
- [11] J.B. Harborne (1967) Comparative biochemistry of the flavonoids-VI: Flavonoid patterns in the bignoniaceae and the gesneriaceae, *Phytochemistry* 6 (12)
- [12] J.B. Harborne (1965) Plant polyphenols—XIV: Characterization of flavonoid glycosides by acidic and enzymic hydrolyses *Phytochemistry* 4 (1):107-120
- [13] Paul S. Cooke, David L. Buchanan, Dennis B. Lubahn and Gerald R. Cunha (1998). Mechanism of Estrogen Action: Lessons from the Estrogen Receptor- $\alpha$  Knockout Mouse; *Biology of Reproduction* September 1, 1998 vol. 59 no. 3 470-475
- [14] Duhovny D NR, Wolfson HJ (2002): Efficient Unbound Docking of Rigid Molecules. In Gusfield et al., Ed. *Proceedings of the 2'nd Workshop on Algorithms in Bioinformatics(WABI)* Rome, Italy, *Lecture Notes in Computer Science*.
- [15] Schneidman-Duhovny D, Inbar Y, Nussinov R, Wolfson HJ. PatchDock and SymmDock: servers for rigid and symmetric docking. *Nucl. Acids. Res.* 33: W363-367, 2005.
- [16] Zhang C, Vasmatzis G, Cornette JL, DeLisi C. (1997) Determination of atomic desolvation energies from the structures of crystallized proteins. *J Mol Biol.* 267(3):707-26
- [17] Renmin Liu AL, Ailing Sun, Jichun Cui, Lingyi Konga, (2004): Preparative isolation and purification of three flavonoids from the Chinesemedicinal plant *Epimedium koreamum* Nakai by high-speed counter-current chromatography. *Journal of Chromatography A*
- [18] Vissandjee B, Barlow R, Fraser DW. Utilization of health services among rural women in Gujarat India. *Public Health* 1997; 111(3):135–148.
- [19] I. L. Finar. *Organic Chemistry, Volume 2: Stereochemistry and The Chemistry Natural Products*, 5<sup>th</sup> edition; Longmans Green & Co.

# An Integrated Algorithm Supporting Confidentiality and Integrity for Secured Access and Storage of DICOM Images

**Suresh Jaganathan**

*Assistant Professor*

*Department of Computer Science and Engineering*

*Sri Sivasubramania Nadar College of Engineering,*

*Chennai, Tamilnadu, India*

*whosuresh@gmail.com*

**Arun Fera M**

*PG Scholar*

*Department of Computer Science and Engineering*

*Sri Sivasubramania Nadar College of Engineering,*

*Chennai, Tamilnadu, India*

*fera26@gmail.com*

---

## Abstract

In healthcare industry, the patient's medical data plays a vital role because diagnosis of any ailments is done by using those data. The high volume of medical data leads to scalability and maintenance issues when using health-care provider's on-site picture archiving and communication system (PACS) and network oriented storage system. Therefore a standard is needed for maintaining the medical data and for better diagnosis. Since the medical data reflects in a similar way to individuals' personal information, secrecy should be maintained. Maintaining secrecy can be done by encrypting the data, but as medical data involves images and videos, traditional text based encryption/decryption schemes are not adequate for providing confidentiality. In this paper, we propose an algorithm for securing the DICOM format medical archives by providing better confidentiality and maintaining their integrity. Our contribution in this algorithm is of twofold: (1) Development of Improved Chaotic based Arnold Cat Map for encryption/decryption of DICOM files and (2) Applying a new hash algorithm based on chaotic theory for those encrypted files for maintaining integrity. By applying this algorithm, the secrecy of medical data is maintained. The proposed algorithm is tested with various DICOM format image archives by studying the following parameters i) PSNR - for quality of images and ii) Key - for security.

**Keywords:** Medical Images, DICOM, Encryption, Healthcare, Confusion, Diffusion, Message Digest

---

## 1. INTRODUCTION

Patient's data plays a major role in the healthcare industry where the data is used for diagnosis of any ailments. Nowadays digital form of storing them replaced the traditional film based medical images. Storing them on-site (within the hospital network) is not an efficient solution for current and future trend because of issues such as scalability, and interoperability. Therefore there must be an off-site management of the patient's data. These medical data are in image and video formats such as i) CR (Computed Radiography) images, ii) CT (Computed Tomography) images, iii) MR (Magnetic Resonance) images and iv) PET (Positron Emission Tomography) images etc. Since they need to be communicated to experts across the world to diagnose and to take decisions for treatment, some standard format must be followed for maintaining and transferring which led to the development of DICOM (Digital Imaging and Communications in Medicine) standard. This standard includes the format for maintaining the medical data in (.dcm) format [1, 2].

The main concern regarding the medical data is the confidentiality. Since the medical data involves patients data it must be kept secretly like an ATM pin number. Health Insurance

Portability and Accountability Act (HIPAA) [1] is an act in US that tells about how secure the patient's medical data should be. In future it is sure that all the countries will bring out the same kind of act and is mandatory to protect the data. Many such security issues come in picture such as, confidentiality, authentication, authorization and integrity [3]. All these issues must be considered while providing security to the medical data. The confidentiality is provided by encrypting the medical data before they are stored in off-site. Unlike text messages, image data has special features such as high redundancy, bulk capacity which generally make encrypted image data vulnerable to attacks via cryptanalysis. Because of high correlation among pixels, directly treating image data as ordinary data for encryption will make file format conversion impossible. Usually these images are huge in size, which together makes traditional encryption methods difficult to apply and slow in process. Hence in this case, content encryption, where only the image data are encrypted, leaving file header and control information unencrypted is preferable. In addition to confidentiality, integrity also must be maintained for the medical data since they are stored off-site.

Two general principles that guide the design of cryptographic ciphers are diffusion and confusion [4]. Diffusion means spreading out the influence of a single plain-text digit over many cipher text digits, so that the statistical structure of the plain-text becomes unclear. Confusion means using transformations that complicate the dependence of the statistics of the cipher text on the statistics of the plain-text. They are closely related to the mixing and ergodicity properties of chaotic maps [5].

Rest of the paper is organized as, Section 2 explains some of the related work done. Section 3 provides details about the chaotic cat map employed for providing confusion. Section 4 provides details of improved chaotic cat maps which provide diffusion along with confusion. Section 5 gives a brief explanation of proposed hash algorithm for providing integrity. Section 6 explains the architecture of the proposed algorithm for securing the medical images. Experimental results for the proposed algorithm are presented in Section 7, and at last, Section 8 concludes the work with references.

## **2. RELATED WORK**

In [3], a hash algorithm is discussed based on logistic chaotic map whose first round input value acts as a key. It is compared with the MD5 algorithm and proved that it is better for image data.

In [6], the encryption method for image data is based on confusion and diffusion where the confusion is carried out by any kind of chaotic map like Arnold, Baker map etc and diffusion is carried out by a XOR based function. In [15], a parametric hashing algorithm that is invariant to encryption by allowing a small part of the statistical signature of the original image to emerge despite the encryption process is developed. In [17], the diffusion function is carried out with modulo operation since the inverse is very difficult to find. An attack to image encryption using chaotic cat map is possible once if the key values are known to the adversary and known-image attack is the one which commonly occurs in case of key theft [19].

## **3. CHAOTIC CAT MAP**

### **3.1 Usage of Confusion**

Confusion is one of the important aspects of cryptography. Confusion is meant for confusing the statistical attackers to derive the original data from the statistics of the cipher data. The high initial-value sensitivity and ergodicity properties of chaotic map are very essential in providing confusion for medical image data. Advantages of using confusion are i) Sensitivity to initial conditions and control parameters and ii) pseudo-randomness and ergodicity. Also it has some disadvantages they are i) after the period of the cat map is reached, the original image appears and ii) once the key parameters are leaked, the adversary can easily decrypt the cipher data. In the confusion process, many different 2D chaotic maps are used, such as the Baker map, the Cat map and the Standard, which must be used to realize the confusion of all pixels [5]. Some of the 3D maps currently in practice are just extensions of 2D chaotic maps [7]. Even chaotic maps can

provide integrity. Chaotic maps properties are in close relation with the cryptosystem security. First, its parameter is used as confusion key. The higher the parameter sensitivity is, then higher the key sensitivity and the stronger the cryptosystem. Secondly, the initial-value sensitivity and state ergodicity of the chaotic map determine the confusion strength. In chaotic confusion process, initial value refers to the initial position of a pixel. Thus, the higher the initial-value sensitivity is, then smaller the correlation between adjacent pixels and the more random, the confused image. Similarly, state ergodicity means that a pixel in certain position can be permuted to any position with the same probability. Thus, the higher the state ergodicity is, then more random the confusion process and the more difficult the statistic attack [8]. Therefore, the chaotic map with high initial-value sensitivity and state ergodicity is preferred [9]. Other than this chaotic theory other encryption schemes for images are T-matrix and watermarking [10]. In [11], it is proved that chaotic based image encryption works efficiently than traditional AES based encryption. In [12], chaos based encryption is done with the help of traditional wavelet transform.

### 3.2 Mathematical Details [Confusion]

Let  $(X, d)$  be a metric space. Then a map  $f$  is said to be (Devaney) chaotic on  $X$  if it satisfies the following conditions:

- $f$  exhibits sensitive dependence upon its initial conditions
- $f$  is topologically transitive

The dependence on initial conditions is very important in chaos as it makes hard to determine long term behavior of dynamical systems which show signs of chaos. If a chaotic output is generated by one set of initial conditions and then if it is changed with a little number of bits, then the output will change drastically. As mentioned previously, chaos is sometimes seen as meaning of random or unstable, but it is important to make sure that the randomness also exhibits the conditions from the definition of chaos [13].

The Arnold Cat Map is a discrete system [14] that stretches and folds its trajectories in phase space [15] as shown in the equation 1.

$$\begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} = \begin{pmatrix} 1 & p \\ q & pq + 1 \end{pmatrix} \begin{pmatrix} x_i \\ y_i \end{pmatrix} \text{ mod } N \quad (1)$$

where  $x_{i+1}$  and  $y_{i+1}$  are the pixel positions of the cipher image,  $x_i$  and  $y_i$  are the pixel positions of original image,  $N$  is the number of columns considered while applying the cat map.

The values  $p$  and  $q$  indicate the parameters which must be kept secret and act like the key values. One more important condition of cat map is that it must be area preserving. To achieve this, the determinant value should be 1 so that the reverse operation can be applied [16].

## 4. IMPROVED CHAOTIC CAT MAP

### 4.1 Diffusion

Due to some of the demerits of confusion, we go for diffusion. Diffusion [17] is another important aspect of cryptography which aims at providing additional security. In our proposed system, diffusion is done for the data that is got from the process of confusion. For diffusion function, a change of a pixel can spread to other pixels, which keeps the cryptosystem of high plain-text sensitivity.  $(0, 0)$  is the first pixel position in normal scan mode, which cannot be permuted by chaotic maps. So by applying diffusion process, the first pixel is always changed by addition operation with diffusion key  $Q_{i-1}$ . If a change happens in a pixels gray-level, then the change can cause great ones in other pixels through diffusion process [18]. Thus, the greater the changes caused by diffusion process are, then higher the cryptosystem plaintext sensitivity and the more difficult the systems security against differential attack [19].

#### 4.2 Mathematical Details [Diffusion]

The relationship between the first pixels plaintext  $P_0$ , diffusion key  $Q_1$  and cipher text  $Q_0$  is

$$Q_0^n = [D(P_0, Q_{-1})]^n \quad (2)$$

where  $D()$  is the diffusion function. A powerful diffusion function is given in equation 3,

$$Q_i = P_i \oplus (4 * Q_{i-1} * (1 - Q_{i-1})) \quad (3)$$

where  $P_i$  is the current plain text pixel,  $Q_i$  is the current cipher text pixel and  $Q_{i-1}$  is the initial value of diffusion process which is used as a key for diffusion process. Here the second term in the formula is a kind of logistic cat map which also provides pseudo randomness. Since we use a XOR operation which considers each and every bit of the input pixel value, it brings a stronger security by making the statistical relation among the plain images and the cipher images. Advantages of using Diffusion are i) since we use a kind of logistic map for diffusion, it provides a random behavior so that a tiny change in the plain image is reflected in more than one pixel in the cipher image [20] and ii) Pseudo-randomness and ergodicity. Disadvantages are i) usually the diffusion function takes some time to complete its operation because the real valued arithmetic operation consume much computation time and ii) once the key parameters are leaked, the adversary can easily decrypt the cipher data.

### 5. PROPOSED HASH ALGORITHM

The hash algorithm is mainly used for providing integrity. Generally a hash function takes a variable length data as input and produces a fixed length output hash value [15]. One main aspect of hash algorithm is that it must be injective i.e. any two inputs should not result in same hash values. Since patients' medical data are of our primary concern, distortion of them may lead to wrong diagnosis and even threaten patients' life. Traditional methods like MD5, SHA etc can be used to generate hash values. But since images don't fit themselves as good candidates for traditional hash algorithms [3], a new direction has emerged in calculating hash for images. It led to calculating hash based chaotic theory which deals with dynamic systems. Some chaotic maps like logistic maps are a kind of irreversible map [3] which does not produce original data after getting reversed. This algorithm makes full use of every bit in an image file to generate initial vector and to control the digesting process. The proposed hash algorithm involves both traditional methods and chaotic map and is discussed in Section 5.

### 6. ARCHITECTURE OF PROPOSED ALGORITHM

Figure 1 shows the architecture of our proposed algorithm. The proposed algorithm uses both confusion and diffusion properties of cryptography. DICOM standard is used for both storing and exchanging the medical files such as scan images. By applying confusion and diffusion to the DICOM format medical images, their confidentiality is maintained. The keys used for confusion and diffusion must be known only to authorized persons. Some methods are proposed based on confusion for providing confidentiality but they are vulnerable to known plain image attack since confusion only rearranges the pixels. This algorithm is against the known plain image attacks when diffusion is applied. The proposed approach takes two parts 1) encrypting/decrypting the medical files 2) calculating hash values. Both the parts are done with some mathematical equations which represent the chaotic based theory.

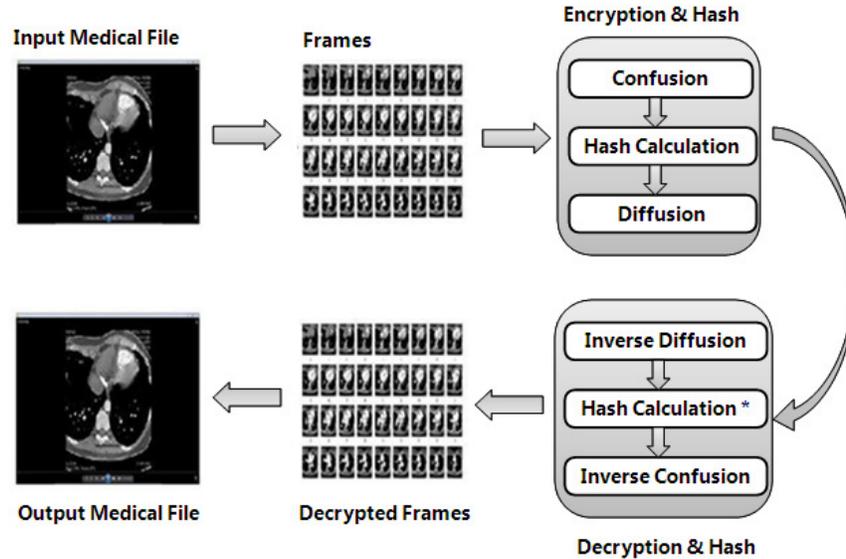


FIGURE 1: Architecture of the proposed algorithm

### Part 1: Encryption

- Convert the DICOM file into a video sequence using third party software. e.g.: Rubo DICOM viewer
- The video file is converted to individual frames
- Extract the pixel coordinates starting from the left top for all the frames
- Apply the formula to perform confusion

$$\begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} = \begin{pmatrix} 1 & p \\ q & pq + 1 \end{pmatrix} \begin{pmatrix} x_i \\ y_i \end{pmatrix} \text{ mod } N$$

where  $x_{i+1}$  and  $y_{i+1}$  are the pixel positions of the cipher image,  $x_i$  and  $y_i$  are the pixel positions of original image,  $N$  is the number of columns considered while applying the cat map

- Apply the below formula to perform diffusion

$$Q_i = P_i \oplus (4 * Q_{i-1} * (1 - Q_{i-1}))$$

where  $P_i$ , is the current plain text pixel,  $Q_i$  is the current cipher text pixel and  $Q_{i-1}$  is the initial value of diffusion process which is used as a key for diffusion process

### Decryption

- Apply the formula to perform inverse diffusion

$$P_i = Q_i \oplus (4 * Q_{i-1} * (1 - Q_{i-1}))$$

where  $P_i$ , is the current plain text pixel,  $Q_i$  is the current cipher text pixel and  $Q_{i-1}$  is the initial value of diffusion process which is used as a key for diffusion process

- Apply the formula to perform inverse confusion

$$\begin{pmatrix} x_i \\ y_i \end{pmatrix} = \begin{pmatrix} pq + 1 & -p \\ -q & 1 \end{pmatrix} \begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} \text{ mod } N$$

where  $x_{i+1}$  and  $y_{i+1}$  are the pixel positions of the cipher image,  $x_i$  and  $y_i$  are the

- pixelpositions of original image, N is the number of columns considered while applying the cat map
- From the pixel values, construct the frames
- Convert the individual frames to a video file

## Part 2: Hash algorithm

- The output of confusion process is applied to hash algorithm because calculating hash after diffusion will lead to collision due to the property of diffusion function.
- For each individual images of the DICOM file:
  - i) Calculate SHA-512 for the image which produces a128 byte message digest
  - ii) Divide 128 bytes into eight 16 bytes
  - iii) Calculate XOR for the nearest pairs so that four outputs are obtained
  - iv) For each of those four outputs, apply the logistic map as in equation 4, four times with the key parameter as the values obtained from the previous step

$$x_{n+1} = y_{n+1} (1 - x_n) \quad (4)$$

where  $y_{n+1}$  is the current plain text pixel,  $x_n$  is the previous hash value and  $x_{n+1}$  is the current hash value. After iterating through all pixels the lastly obtained hash value is provided to next step

- v) Concatenate the results from the previous step
- vi) Apply MD5 for the obtained value which is the final hash value of the image containing 32 digit hexadecimal numbers.

## 7. EXPERIMENTAL RESULTS

The proposed improved chaotic cat map algorithm is applied to various DICOM format image archives and tests are conducted. The results are verified with PSNR values for QoS and with key for security.

Peak Signal to Noise Ratio (PSNR) is used as a quality parameter for reconstruction of compression images or videos. Here signal is in the original data and the noise is in the compressed data. Calculating PSNR values by using equations 5 and 6 is used as estimation to human awareness for reconstructing quality of compressed data or encrypted data. Two steps are involved in calculating PSNR values.

### PSNR Calculation:

Step 1: Calculate Mean Square Error [MSE]

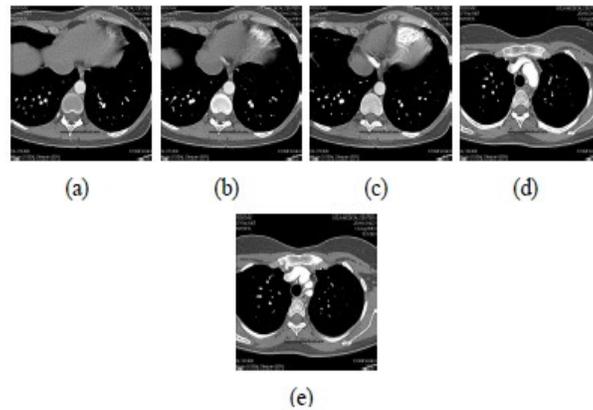
$$\begin{aligned} d(f(x,y),f'(x,y)) &= ||(f(x,y) - f'(x,y))||^2 \\ &= \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} ((f(i,j) - f'(i,j))^2), \end{aligned} \quad (5)$$

where  $f(x,y)$  and  $f'(x,y)$  original and reconstructed images respectively,  $m$  and  $n$  are image size.

Step 2:

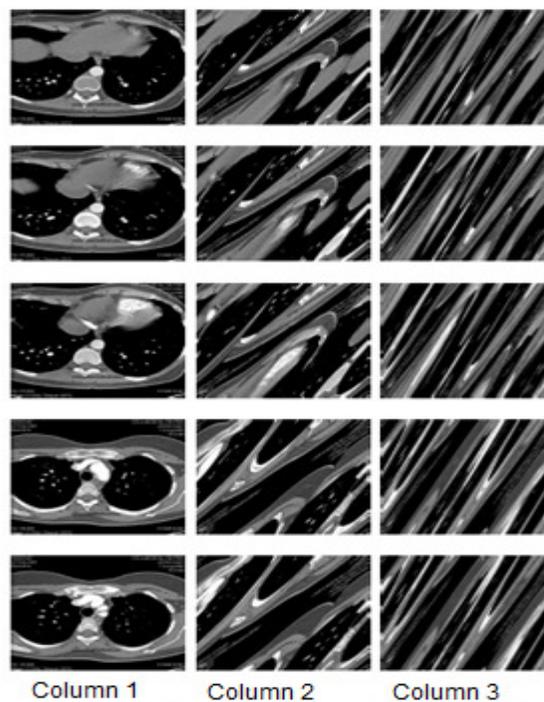
$$PSNR = 10 \log_{10} \frac{1}{MSE} \quad (6)$$

Figure 2 shows the test DICOM file (FEROVIX) used in this paper for evaluating the proposed algorithm.



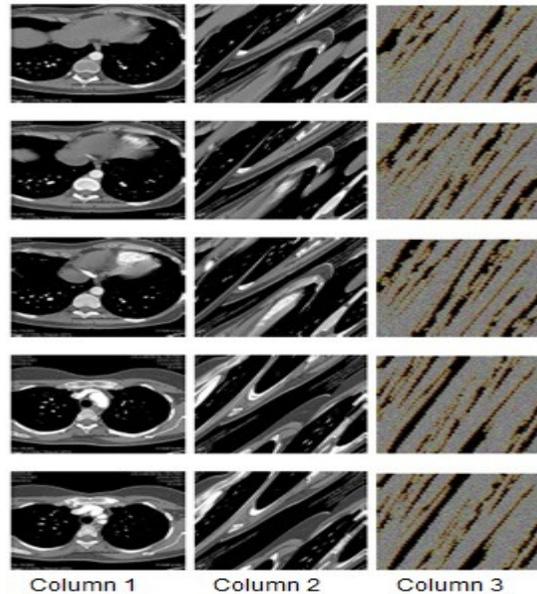
**FIGURE 2:** Sample Test Sequence

Sample test images are taken from a DICOM file which contain details of *Ferovix* CT scan images e.g. Lungs. These test images (shown in Column 1 of Figure 3) are encrypted using Arnold Chaotic Cat Map and its results are shown in Figure 3. When the images are encrypted using Arnold Chaotic Cat Map, the pixels are rearranged. Hence a shuffled image is obtained as input (shown in Column 2 of Figure 3). Images are encrypted using the key (1,1). If the key value is changed, the original is not obtained which is shown in Column 3 of Figure 3.



**FIGURE 3:** Applying Chaotic Cat Map

As stated earlier, applying Chaotic Cat Map only is not enough for security and is vulnerable to crypt-analysis. Hence the diffusion is applied with confusion, which makes the crypt-analysis harder, hence improved security. Figure 4 shows the image sequences after applying confusion (Column 2 of Figure 4) and diffusion (Column 3 of Figure 4).



**FIGURE 4:** After applying proposed algorithm [Confusion and Diffusion]

Tested DICOM image sequences are encrypted with the available chaotic cat map algorithm and also with the proposed algorithm i.e. applying both confusion and diffusion. Table 1 shows the PSNR values obtained to check the viewable quality of DICOM images after decryption for confusion and after applying the proposed algorithm i.e. both confusion and diffusion. When confusion is applied to the image, the pixels values are rearranged when applying inverse operation, some pixels are not rearranged properly hence, there is a decrease in PSNR value (shown in blue color (bottom) in Figure 5), when applying only diffusion the pixels value are changed and there is no rearrange of pixels and when doing inverse operation the original image is obtained, hence increase in PSNR value (shown in red (top) in Figure 5).

When applying the proposed algorithm i.e. combination of confusion and diffusion, the viewable quality of image after decryption comes in between two extremes (shown in green color (middle) in Figure 5), having quality viewable image reproduction.

Bit rate [kb]	Confusion	Diffusion	Proposed Algorithm
	[dB]	[dB]	[dB]
350	33.83	42.99	38.41
360	33.26	42.6	37.93
380	33.35	42.6	37.97
390	33.14	42.35	37.74
400	32.94	39.06	36

**TABLE 1:** PSNR Comparison for various algorithms

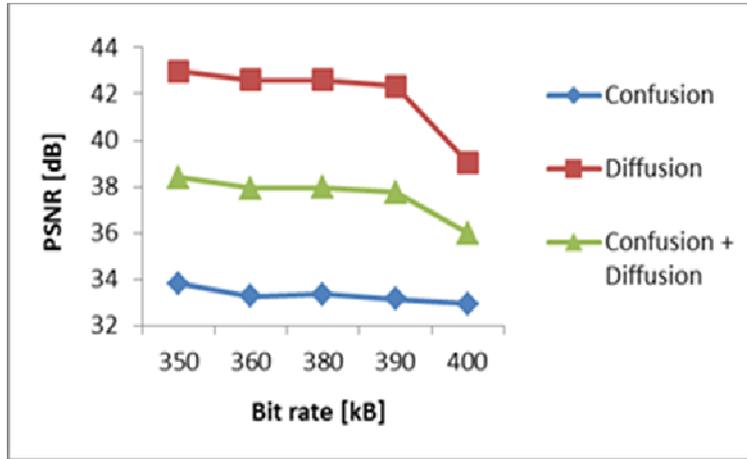


FIGURE.5: Graph showing PSNR values for various algorithms

The proposed hash algorithm is applied to various DICOM format image archives and tests are conducted. The results are verified by changing the bits in the image so that even a single bit change in the image leads to a different hash value. The results show that collision does not occur among different images and also the results have proved that. Research result shows that, because of the inherent characteristics of Chaos Maps and Hash function lead to the simplicity, high sensitivity to initial conditions and good performance of our algorithm.

Table 2 shows the message digests generated by the DICOM images taken under study and also after applying confusion.

Hash Value DICOM images	Hash Value After confusion
dbfba83ff1532c94d90d85dfe2de828b	91bb4fefe246308a17d16e36efd9e587
e665305217c723a3cf3802310eacf2ee	0b81f3066191ead6b18337baec6f9741
3ad46f25268952bdfa17e6a1d1786df7	5802f25d5bece1e741cd12c363cecc50
1697cb8ba4c40858fd152414fc3daebd	7d280caca60b370f0b182b268e62a377
e2a64ec5b8a1db0401c026ef938e5e65	5b25d654e9beb5589a09f503b770c128

TABLE 2: Message digests for various images

Table 3 shows the message digest generated by the DICOM images taken under study along with the message digest generated if any random bit is changed in the image got after applying confusion.

Hash value for DICOM images	Hash value After one bit change
dbfba83ff1532c94d90d85dfe2de828b	2781b4fb71b0ebb7bcea1ef776c425c7
e665305217c723a3cf3802310eacf2ee	b37e49729158afdd8d0e1539adc387a1
3ad46f25268952bdfa17e6a1d1786df7	da52e005b51377ca7f3fae35f7dad744
1697cb8ba4c40858fd152414fc3daebd	c20931bf34df388fa71211b4149faa47
e2a64ec5b8a1db0401c026ef938e5e65	159513702c1b5452ddcdc98fb8bd777b

TABLE 3: Message digests for various images

The average rate of bits changed (P) is given by equation 7,

$$P = (B/128)*100 \tag{7}$$

where B is the average number of bits changed while a random bit gets changed due to some attack or modification by unauthorized person. Table 4 shows the individual values of P for the images that are taken in study. The average rate of bits changed (P) is 52.80 for all those images. Since the hash algorithm relies on each and every bit of the image, the resulting message digest is very hard to find and also to infer the plain text from the message digest.

Input Image in column 2 of FIGURE 3	Number of bits changed in resultant image out of 128 when random bits are changed in input image	Rate of change of bits
Image 1	68	53.12
Image 2	69	53.9
Image 3	65	50.78
Image 4	70	54.68
Image 5	66	51.56

**TABLE 4:** Average rate of changed bits

## 8. CONCLUSION

In this paper we proposed a new algorithm for providing two fold securities for maintaining the confidentiality and integrity of patient's medical data. Confusion is provided by means of Arnold Cat Map and diffusion is provided by means of a strong diffusion function. By employing this algorithm, we found that this algorithm suits well for medical images and is tested for QoS with PNSR and security level with keys. Integrity is provided by means of combining traditional hash algorithms with logistic cat map. Future work entails in storing the DICOM medical archives in cloud environment due to their large size and maintaining the authenticity by means of providing certificates to authorized users.

## 9. REFERENCES

- [1] Chia-Chi Teng, Jonathan Mitchell, Christopher Walker, Alex Swan, Cesar Davila, David Howard, Travis Needham (2010), "A Medical Image Archive Solution in the Cloud". IEEE, 10.1109/ICSESS.2010.555234 3, pp 431-434
- [2] Suresh Jaganathan, M B Geetha Manjusha, 2011, "dFuse: An Optimized Compression Algorithm for DICOM-format image archive", International Journal of Biometrics and Bioinformatics (IJBB), Volume (5) ,Issue (2) , 42-52, ISSN: 1985-2347
- [3] Zhiliang Zhu, KeZhai, Beilei Wang, Hongjuan Liu, Huiyan Jiang (2009) "Research on Chaos-based Message Digest Method for Medical Images". IEEE, 1109/CISP.2009.5301139, pp 1-510
- [4] LjupEoKocarev, GoceJakimoski, Toni Stojanovski, Ulrich Parlit (1998), "From chaotic maps to encryption schemes", Circuits and Sys tems, 1998. ISCAS 98. Proceedings of the 1998 IEEE International Symposium. 10.1109/ISCAS.1998.698968, vol.4, pp 514 – 517.
- [5] YUAN-BIAO ZHANG, "Chaos based cryptography. An alternative to algebraic cryptography".2008.
- [6] Yaobin Mao and Guanrong Chen (2005), "Chaos-Based image encryption". [www.open-image.org/725publication/journal/CBIE.pdf](http://www.open-image.org/725publication/journal/CBIE.pdf)
- [7] Guanrong Chen, Yaobin Mao b, Charles K. Chui (2003) "A symmetric image encryption scheme based on 3D chaotic cat maps". Science Direct, doi:10.1016 / j.chaos.2003.12.022.

- [8] Kwok-Wo Wong, Bernie Sin-Hung Kwok, and Wing-Shing Law (2006), "A Fast Image Encryption Scheme based on Chaotic Standard Map". Cryptography and Security conference cited as arXiv:cs/0609158v1 , Volume 372, Issue 15, pp 2645-2652.
- [9] Ling Bin, Liu Lichen, Zhang Jan (2010) "Image encryption algorithm based on chaotic map and S-DES". IEEE ,10.1109/ICACC.2010. 5486998, pp 41-44.
- [10] Monisha Sharma (2010), "Image encryption techniques using chaotic schemes: A review". International Journal of Engineering Science and Technology Vol. 2(6),2359-2363, ISSN: 0975-5462, pp 1-10.
- [11] Muhammad Asim and VarunJeoti,(2007) "Image Encryption: Comparison between AES and a Novel Chaotic Encryption Scheme" IEEE. 10.1109/ICSCN.2007.350697, pp 65-69.
- [12] Zhu Yu, Zhou Zhe, Yang Haibing, Pan Wenjie, Zhang Yunpeng (2010), "A Chaos-Based Image Encryption Algorithm Using Wavelet Transform" IEEE , 10.1109/IEMBS.2010.5628061, pp 1037-1040.
- [13] De wang, Yuan-biaozhang (2009) "Image encryption algorithm based on s-boxes substitution and chaos random sequence". International Conference on Computer Modeling and Simulation, DOI 10.1109/ICCMS.2009.26.
- [14] Gabriel Peterson (1997), Arnolds Cat Map, Math 45 Linear Algebra, Fall 1997.
- [15] Kashyap, S.; Karthik, K. (2010) "Authenticating encrypted data". IEEE, 10.1109/NCC.2011.5734696, pp 1-5.
- [16] Katherine Struss (2009) "A Chaotic Image Encryption". Spring, Mathematics Senior Seminar, 4901.
- [17] Shiguolian, Jinsheng Sun, Zhiquan Wang (2005) "Security analysis of a chaos-based image encryption algorithm". Science direct, Physica A: Statistical Mechanics and its Applications 351 (2-4) , pp 645-661.
- [18] Kwok-Wo Wong, Bernie Sin-Hung Kwok, and Wing-Shing Law (2006) "A Fast Image Encryption Scheme based on Chaotic Standard Map". Cryptography and Security conference cited as arXiv:cs/0609158v1 , Volume 372, Issue 15, pp 2645-2652.
- [19] ShuaiRen, ChengshiGao, Qing Dai, XiaoFeiFei (2010) "Attack to an Image Encryption Algorithm based on Improved Chaotic Cat Maps".3rd International Congress on Image and Signal Processing (CISP2010), 10.1109/CISP.2010.5647659, pp 533-536.
- [20] Kwok-Wo Wong, Bernie Sin-Hung Kwok,(2007) "An Efficient Diffusion Approach for Chaos-based Image Encryption". 3rd International conference Physics and Control (Physcon 2007)

## Estimation of Age Through Fingerprints Using Wavelet Transform and Singular Value Decomposition

**P. Gnanasivam**  
Department of ECE  
Agni College of Technology  
Chennai, 603103, India

*pgnanasivam@yahoo.com*

**Dr. S. Muttan**  
address.com  
Centre for Medical Electronics, Department of ECE,  
College of Engineering  
Anna University  
Chennai, 600025, India

*muthan\_s@annauniv.edu*

---

### Abstract

The forensic investigators always search for fingerprint evidence which is seen as one of the best types of physical evidence linking a suspect to the crime. In this paper discrete wavelet transform (DWT) and the singular value decomposition (SVD) has been used to estimate a person's age using his/her fingerprint. The most robust K nearest neighbor (KNN) used as a classifier. The evaluation of the system is carried on using internal database of 3570 fingerprints in which 1980 were male fingerprints and 1590 were female fingerprints. Tested fingerprint is grouped into any one of the following five groups: up to 12, 13-19, 20-25, 26-35 and 36 and above. By the proposed method, fingerprints were classified accurately by 96.67%, 71.75%, 86.26%, 76.39% and 53.14% in five groups respectively for male and by 66.67%, 63.64%, 76.77%, 72.41% and 16.79% for female. Finger-wise and Hand-wise results of age estimation also achieved.

**Keywords:** Age Estimation, Discrete Wavelet Transform, Singular Value Decomposition, K-Nearest Neighbor.

---

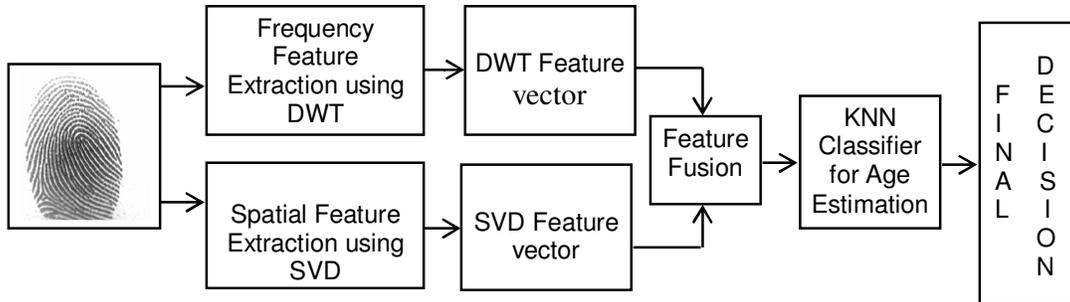
### 1. INTRODUCTION

Age information is important to provide investigative leads for finding unknown persons. Existing methods for age estimation have limited use for crime scene investigation because they depend on the availability of teeth, bones, or other identifiable body parts having physical features that allow age estimation by conventional methods. In this paper, age of a person is estimated from the fingerprints using DWT and SVD. The science of fingerprint has been used generally for the identification or verification of person and for official documentation. Fingerprint analysis plays a role in convicting the person responsible for an audacious crime. Fingerprint has been used as a biometric for the gender and age identification because of its unique nature and do not change throughout the life of an individual [1].

In fingerprint, the primary dermal ridges (ridge counts) are formed during the gestational weeks 12-19 and the resulting fingerprint ridge configuration (fingerprint) is fixed permanently [2-3]. Ridges and their patterns exhibit number of properties that reflect the biology of individuals. Fingerprints are static and its size and shape changes may vary with age but basic pattern of the fingerprint remains unchanged. Also, the variability of epidermal ridge breadth in humans is substantial [4]. Dermatoglyphic features statistically differ between the sexes, ethnic groups and age categories [5]. Gender and age determination of unknown can guide investigators to the correct identity among the large number of possible matches.

According to 'Police-reported crime statistics in Canada, 2010 [6], Crimes tend to be disproportionately committed by youth and young adults and the rate of those accused of a *Criminal Code* offence peaked at 18 years of age and generally decreased with increasing age. As per the publication of 'crime in India statistics-2010, published by National Crime

Records Bureau [7], the crime rate is higher for the age range of 18 to 44 and decreases after 44. Thus the age estimated is categorized in to any one of the five groups: up to 12, 13-19, 20-25, 26-35 and 36 and above. The features of the fingerprints grouped are trained and classified using the KNN classifier. Figure 1 illustrates the process of DWT and SVD based age estimation method.



**FIGURE 1:** DWT and SVD based age estimation method

Only few works were concentrated in the age estimation using the fingerprint. In the view of protecting children from accessing online sites that are harmful to minors, John D Woodward, testified before a hearing of ‘commission on online child protection’ [8]. According to him, there are no age verification biometrics, no age determination biometrics and no age estimation biometrics. Based on the fingerprint ridge width the age and sex were determined [4]. Many Earlier works were related the fingerprint image quality and the age of a person [9-11]. Other works in the way of age estimation used the speech recognition [12], face [13-15] etc. In this work, authors proposed a method of identifying range of the age using the discrete wavelet transform and the singular value decomposition

Wavelet transform is a popular tool in image processing and computer vision because of its complete theoretical framework, the great flexibility for choosing bases and the low computational complexity [16]. As wavelet features has been popularized by the research community for wide range of applications including fingerprint recognition, face recognition and gender identification using face, authors have confirmed the efficiency of the DWT approach for the gender identification using fingerprint.

The SVD approach is selected for the gender discrimination because of its good information packing characteristics and potential strengths in demonstrating results. The SVD method is considered as an information-oriented technique since it uses principal components analysis procedures (PCA), a form of factor analysis, to concentrate information before examining the primary analytic issues of interest [17]. K-nearest neighbours (KNN), gives very strong consistent results. It uses the database which was generated in the learning stage of the proposed system and it classifies genders of the fingerprints.

The outline of this paper is as follows: the fingerprint feature extraction using DWT and SVD is described in Section 2; we then proposed the age classification using fingerprint features in Section 3; the experimental results are presented in Section 4; Section 5 comes to the conclusion and future work.

## 2. FINGERPRINT FEATURE EXTRACTION

Feature extraction is a fundamental pre-processing step for pattern recognition and machine learning problems. In the proposed method, the energy of all DWT sub-bands and non-zero singular values obtained from the SVD of fingerprint image are used as features for the estimation of age. In this section, DWT and SVD based fingerprint feature extractions are described.

### 2.1 DWT Based Fingerprint Feature Extraction

Wavelets have been used frequently in image processing and used for feature extraction, de-noising, compression, face recognition, and image super-resolution. Two dimensional DWT

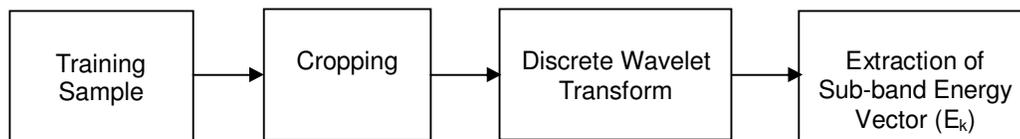
decomposes an image into sub-bands that are localized in frequency and orientation. The decomposition of images into different frequency ranges permits the isolation of the frequency components introduced by “intrinsic deformations” or “extrinsic factors” into certain sub-bands. This process results in isolating small changes in an image mainly in high frequency sub-band images. Hence, discrete wavelet transform (DWT) is a suitable tool to be used for designing a classification system.

The 2-D wavelet decomposition of an image is results in four decomposed sub-band images referred to as low–low (LL), low–high (LH), high–low (HL), and high–high (HH). Each of these sub-bands represents different image properties. Typically, most of the energy in images is in the low frequencies and hence decomposition is generally repeated on the LL sub band only (dyadic decomposition). For k level DWT, there are  $(3^k) + 1$  sub-bands available. The energy of all the sub-band coefficients is used as feature vectors individually which is called as sub-band energy vector (E). The energy of each sub-band is calculated by using the equation (1).

$$E_k = \frac{1}{RC} \sum_{i=1}^R \sum_{j=1}^C |x_k(i, j)| \tag{1}$$

Where  $x_k(i, j)$  is the pixel value of k<sup>th</sup> sub-band and R, C is width and height of the sub-band respectively.

Figure 2 shows the block diagram of the frequency feature extraction by using DWT. The input fingerprint image is first cropped and then decomposed by using the DWT. For level 1, number of subbands are 4 and 3 subbands are added for each next levels Thus the increase in levels of DWT increases the features.



**FIGURE 2:** DWT based fingerprint feature extraction

## 2.2 SVD Based Fingerprint Feature Extraction

The Singular Value Decomposition (SVD) is an algebraic technique for factoring any rectangular matrix into the product of three other matrices. Mathematically and historically, it is closely related to Principal Components Analysis (PCA). In addition it provides insight into the geometric interpretation of PCA. As noted previously, the SVD has long been considered fundamental to the understanding of PCA.

The SVD is the factorization of any  $(k \times p)$  matrix into three matrices, each of which has important properties. That is, any rectangular matrix A of k rows by p columns can be factored into U, S and V by using the equation (2).

$$A = USV^T \tag{2}$$

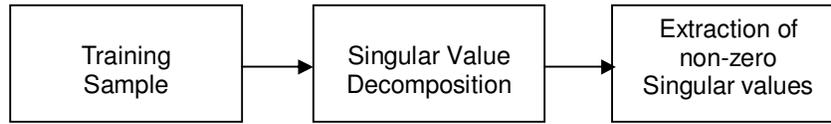
Where

$$U = AA^T \tag{3}$$

$$V = A^T A \tag{4}$$

And S is a  $(k \times p)$  diagonal matrix with r non-zero singular values on the diagonal, where r is the rank of A. Each singular value is the square root of one of the Eigen values of both  $AA^T$  and  $A^T A$ . The singular values are ordered so that the largest singular values are at the top left and the smallest singular values are at the bottom right, i.e.,  $s_{1,1} \geq s_{2,2} \geq s_{3,3}$  etc. Among the three rectangular matrices, S is a diagonal matrix which contains the square root Eigen values from U or V in descending order. These values are stored in a vector called Eigen vector (V). As the internal database contains images of size 260x300 pixels, the feature

vector of SVD is of the size  $1 \times 260$ . The spatial feature extraction by using SVD is shown in Fig 3.



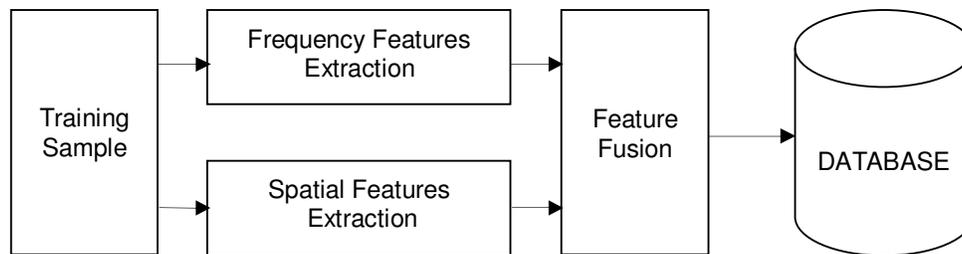
**FIGURE 3:** SVD based fingerprint feature extraction

### 3. FINGERPRINT AGE ESTIMATION

The proposed system for age estimation is built based on the concatenation of fingerprint features obtained by using DWT and SVD. This section describes two different stages named as learning stage and classification stage and the KNN classifier used for the age classification.

#### 4.1. Learning Stage

The feature vector  $V$  of size  $1 \times 260$  obtained by SVD and the sub band energy vector  $E$  of size  $1 \times 19$  obtained by DWT are fused to form the feature vector and used in the learning stage. The fusion of feature vector  $V$  and  $E$  is done by concatenation of features that are widely used for feature level fusion. The resulting feature vector is of the size  $1 \times 279$  ( $1 \times 260 + 1 \times 19$ ). The learning stage is shown in Fig 4.



**FIGURE 4:** Learning stage of the proposed gender classification system

The learning algorithm is as follows:

#### Learning Algorithm:

[Input] all samples of fingerprint with known class (Gender)

[Output] the feature vector of all samples as database

- 1) Decompose the fingerprint with 6 level decomposition of DWT.
- 2) Calculate the sub-band energy vector ( $E$ ) using (1).
- 3) Calculate the Eigen vector ( $V$ ) using (2).
- 4) Fuse the vectors  $E$  and  $V$  to form the feature vector for the particular fingerprint.
- 5) Insert this feature vector and the known class into the database.
- 6) Repeat the above steps for all the samples.

#### 4.2. KNN Classifier

In pattern recognition, the  $k$ -nearest neighbour algorithm (K-NN) is the generally used method for classifying objects based on closest training examples in the feature space. K-NN is a type of instance-based learning where the function is only approximated locally and all computation is deferred until classification. In K-NN, an object is classified by a majority vote of its neighbours, with the object being assigned to the class most common amongst its  $k$  nearest neighbours ( $k$  is a positive integer, typically small). If  $k = 1$ , then the object is simply assigned to the class of its nearest neighbour. The neighbours are taken from a set of objects for which the correct classification is known. This can be thought of as the training set for the algorithm, though no explicit training step is required.

### 4.3. Classification Stage

In the classification phase, the fused feature vector of the input fingerprint is compared with the feature vectors in the database by using the K-Nearest Neighbour classifier. The distance measure used in the classifier is 'Euclidean Distance'. The detailed classification algorithm is detailed below.

#### Classification Algorithm

[Input] unknown fingerprint and the feature database

[Output] the class of the fingerprint to which this unknown fingerprint is assigned

- 1) Decompose the given unknown fingerprint with 6 level decomposition of DWT.
- 2) Calculate the sub-band energy vector (E) using (2).
- 3) Calculate the Eigen vector (V) using (1).
- 4) Fuse the vectors E and V to form the feature vector for the given unknown fingerprint.
- 5) Apply KNN classifier and find the class of the unknown fingerprint by using the database generated in the learning phase.

## 4. EXPERIMENTAL RESULTS

In this section, the performance of the proposed Age estimation algorithm is verified by using the internal database. The success rate (in percentage) of age classification using the combination of both DWT and SVD are summarized and discussed. DWT level 5, 6 and 7 were tried and from the results, DWT level 6 is identified as the optimum for the age estimation.

### 4.1. Data Set

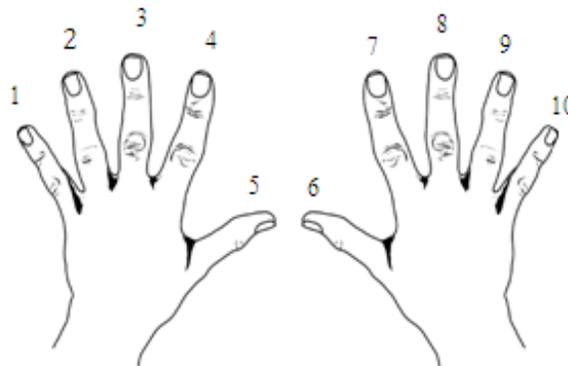
The fingerprint images of internal database were collected by using Fingkey Hamster II scanner manufactured by Nitgen biometric solution [18], Korea. Every original image is of size 260x300 pixels with 256 grey levels and resolution of 500 dpi. The internal database includes all ten fingers of the subject scanned. The images are collected from males and females of different ages. From the internal database, irrespective of quality and age, all ten fingers of 3570 fingerprints in which 1980 were male fingerprints and 1590 were female fingerprints are used for testing and training. These 3570 fingerprint images are separated into two sets. For the learning stage 2/3 of total images are used. The remaining images are used in the classification stage. Table 1 shows the age and gender wise samples of the internal database. The crime rate recorded is high between the ages of 12 to 35. Below the age of 12 and above 36 the crime rate is few and thus large samples from 283 persons (156 male and 127 female) were used for testing the method. These samples are classified under the three groups as 13-19, 20-25 and 26-35. Each person's all fingers are scanned and frequency features were identified through DWT and spatial features were identified through SVD. Initially, KNN was applied for the feature set of DWT alone. Similarly, KNN was applied for the feature set of SVD alone and the fused feature set of DWT and SVD.

Age Group	Male	Female	Total
Up to 12	70	60	130
13-19	190	320	510
20-25	1050	680	1730
26-35	320	270	590
36 and above	350	260	610
Total Samples	1980	1590	3570

TABLE 1: Age and gender wise samples details

All the fingers of a person are scanned to test the proposed algorithm. The proposed method is tested with all five fingers of the left and right hand. Thus to have the reference of the fingers, the scanned fingers were numbered as follows. Little finger to thumb fingers of left

hand is numbered as 1 to 5. Thumb to little fingers of right hand is numbered as 6 to 10 as shown in figure 5.



**FIGURE 5:** Finger numbering

**4.1 Age Estimation**

In table 2 the success rates (in percentage) of age estimation for the male fingerprints are tabulated. For the fingerprints of the male persons whose age lies below 12 years, the success rate is achieved with 96.67%. In this category, other than the left hand thumb, the age is estimated exactly for all fingers. The success rate in the age group of 20-25 is reasonably good (86.26%) and thus useful for crime investigation, as this group crime rate is higher than other groups. In addition, if there is availability of right thumb and right index finger, the success is nearly 90%. Similarly the success rate for the remaining group is achieved as 71.75%, 76.39% and 53.14% for the age groups of 13-19, 26-35 and 36 and above respectively. Maximum success rate is achieved in the age group of 'up to 12' for all fingers except the left thumb. Low success rate is recognized for the age group of '36 and above'.

Fingers	Age groups				
	up to 12	13-19	20-25	26-35	36 and above
1	100.00	72.22	80.81	75.00	51.43
2	100.00	84.21	83.84	72.22	51.43
3	100.00	72.22	86.87	69.44	54.29
4	100.00	66.67	83.84	83.33	51.43
5	66.67	66.67	88.89	72.22	51.43
6	100.00	77.78	89.90	80.56	54.29
7	100.00	72.22	83.84	80.56	51.43
8	100.00	66.67	87.88	69.44	57.14
9	100.00	72.22	89.90	80.56	54.29
10	100.00	66.67	86.87	80.56	54.29
Average	96.67	71.75	86.26	76.39	53.14

**TABLE 2:** Success rate (in percentage) of age estimation for the male fingerprints

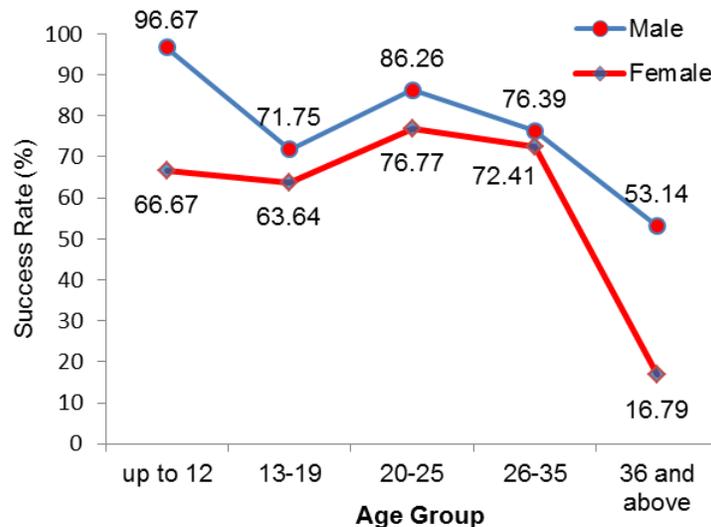
Similar to the male age estimation, the success rates (in percentage) of age estimation for the female fingerprints are calculated. For the fingerprints of the female persons whose age lies below 12 years, the success rate is achieved with 66.67%. The success rate in the age group of 20-25 is reasonably good (76.77%) and thus useful for crime investigation, as this group crime rate is higher than other groups. In addition, if there is availability of right and left small fingers of female, the success is nearly 81%. Similarly the success rate for the remaining group is achieves as 63.64%, 72.41% and 16.79% for the age groups of 13-19 26-35 and above 36 respectively. Maximum success rate is recognized for the right little finger of the age

group '20-25' and the lowest success rate are notices in the right ringer finger of the age group '36 and above. Finger-wise age estimation success rate is tabulated in table 3.

Fingers	Age groups				
	up to 12	13-19	20-25	26-35	36 and above
1	66.67	63.64	80.00	68.97	17.86
2	66.67	63.64	76.92	75.86	14.29
3	66.67	63.64	78.46	68.97	17.86
4	66.67	63.64	72.31	72.41	14.29
5	66.67	63.64	78.46	75.86	17.86
6	66.67	63.64	73.85	72.41	14.29
7	66.67	63.64	72.31	72.41	21.43
8	66.67	63.64	76.92	68.97	21.43
9	66.67	63.64	76.92	72.41	10.71
10	66.67	63.64	81.54	75.86	17.86
Average	66.67	63.64	76.77	72.41	16.79

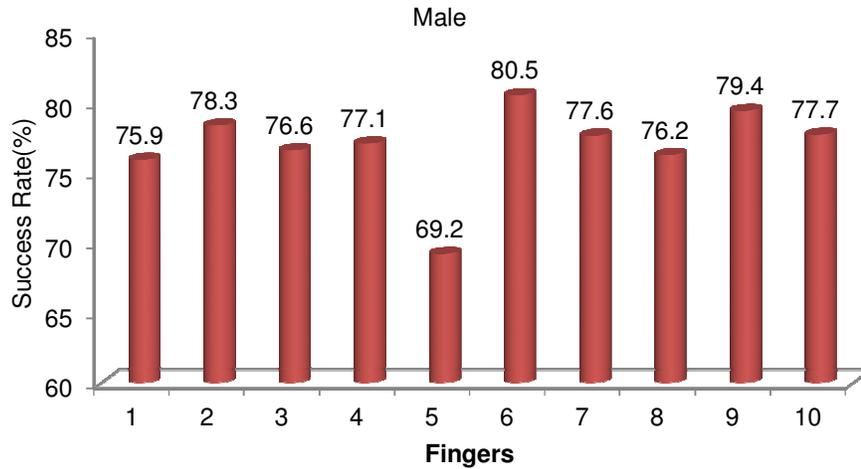
**TABLE 3:** Success rate (in percentage) of age estimation for the female fingerprints

Age group-wise average success rate for male and female is shown in the line diagram of figure 6. Maximum success rate of 96.67% is achieved for the age group of 'up to 12' years of male fingers and 76.77% is achieved for '20-25' age group for female fingers. For the age group of '36 and above', the success rate is low and 53.14% and 16.79% for male and female fingers respectively.

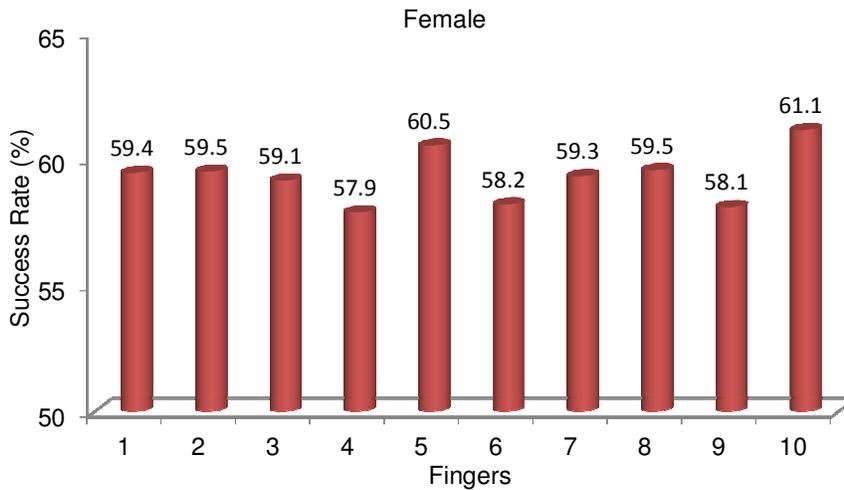


**FIGURE 6:** Age group-wise Average success rate

By average for any given fingers, 76.84% success rate is achieved for the male and 59.26% is achieved for the female fingers in all the five groups. Also, age estimation for the right and left hand are calculated. As discussed, left hand small finger to thumb fingers are named 1 to 5 and the right hand thumb finger to small finger are named 6 to 10. Average age estimation, for the left hand fingers among all the fingers are calculated as 75.41% for male and 59.28%. Similarly, 78.28% and 59.23% are the success rates for right hand fingers of male and female respectively among all groups. Finger-wise success rate for the male and female fingers are shown in figure 7(a) and 7(b) respectively.



(a)



(b)

FIGURE 7: Finger-wise success rate (a) Male (b) Female

## 5. CONCLUSIONS

In this work, we have proposed a new method of age estimation from fingerprint images based on level 6 DWT and SVD. The level 6 DWT is selected as optimum level by analysing the results obtained for other levels. DWT and SVD also applied to classify the fingerprints in to the five age groups. According to the crime reports of Canada and Indian police record, ages has been grouped as up to 12, 13-19, 20-25, 26-35 and above 35. Exact estimation of age group is achieved for the age group below 12 years. For the age group of 36 and above the success rate is not reasonably good.

Higher crime rate has been recorded in Canada and Indian police records in the ages, ranges 20 to 35 of both male and female. The proposed method gives age estimation rate of 81.33% and 74.59 for male and female respectively. If the right thumb and right ring fingers of male is given, the success rate is attained as 85.23% and 78.7% for female little fingers. The overall success rate is 76.84% for male and 59.26% for female. While testing the right hand male fingers alone, 78.28% of accurate estimation is attained. Similarly for the male, irrespective of right or left hand the success rate is 59.3%. More accuracy rate of age estimation can be achieved if more number of samples in each category is trained.

For better results of age estimation, authors are working in collecting huge samples in the each category is initiated. In addition, the research work has been extended using the spatial parameters of fingerprint. Moreover, it is aimed to use various other classifiers for the better results. In the proposed work five age groups has been made for the age estimation. In the future work, more groups will be made to find the age of the suspect or the person.

## 6. REFERENCES

- [1] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, "Handbook of Fingerprint Recognition", first ed., Springer, New York, 2003.
- [2] J. John, Mulvihill, and David W. Smith, "The genesis of dermatoglyphics,"the journal of Pediatrics, vol. 75, no. 4, pp. 579-589, 1969.
- [3] W. Babler, "Embryologic development of epidermal ridges and their configurations," In: Plato CC, Garruto RM, Schaumann BA, editors. Dermatoglyphics: Science in Transition.
- [4] Miroslav Kralik, Vladimir Novotny, "Epidermal Ridge Breadth: An Indicator of Age and Sex in Paleodermatoglyphics", Variability and Evolution, Vol. 11, pp. 5-30, 2003.
- [5] Harold Cummins, Walter J. Walts, and James T McQuitty, "The breadths of epidermal Ridges on the finger tips and palms - A study of variation." American Journal of Anatomy, vol. 68, no.1, pp. 127-150, 1941.
- [6] Shannon Brennan and Mia Dauvergne, Police-reported crime statistics in Canada, 2010, <http://www.statcan.gc.ca/pub/85-002-x/2011001/article/11523-eng.htm>
- [7] Crime in India 2010-Statistics, National Crime Records Bureau, Ministry of Home Affairs, Government of India, <http://ncrb.nic.in>.
- [8] John D. Woodward, Jr., "Is Biometrics an age verification technology", Testimony, RAND's publications, June 2000.
- [9] Shimon K. Modi, Prof. Stephen J. Elliott, Jeff Whetsone and Prof. Hakil Kim," Impact of Age Groups on Fingerprint Recognition Performance" In IEEE Workshop on Automatic Identification Advanced Technologies, 2007pp. 19-23.
- [10] S. K. Modi, and S. J. Elliott, "Impact of image quality on performance: Comparison of young and elderly fingerprints," in International Conference on Recent Advances in Soft Computing (RASC), 2006 pp.10-12.
- [11] S. J. Elliott, and N. C. Sickler, "An evaluation of fingerprint image quality across an elderly population vis-a-vis an 18-25-year-old population," In International Conference security Technology, 2005 pp. 68-73.
- [12] Tobias Bocklet, Andreas Maier, Elmar Noth, "Age Determination of Children in Preschool and Primary School Age with GMM-based Super vectors and Support Vector Machines/Regression", international conference on Text, Speech and Dialogue, 2008, pp. 1-9,.
- [13] Mohammad EL Deeb and Motaz El-Saban, "Human age estimation using enhanced bio-Inspired features (EBIF)", In International Conference on Image Processing (ICIP), 2010, pp. 1589-1592.
- [14] Khoa Luu, Karl Ricanek, Tien D Bui, and Ching Y Suen, "Age estimation using Active Appearance Models and Support Vector Machine regression", in International \ Conference on Biometrics Theory Applications and Systems, 2009, pp. 1-5.
- [15] Andreas Lanitis, Chrisina Draganova, and Chris Christodoulou, "Comparing Different Classifiers for Automatic Age Estimation", IEEE Transactions on Systems, Man, and Cybernetics-Part B: Cybernetics, Vol. 34, no.1, pp. 621-628, 2004.

- [16] Bai-Ling Zhang, Haihong Zhang, and Shuzhi Sam Ge, "Face Recognition by Applying Wavelet Subband Representation and Kernel Associative Memory", IEEE Transactions on neural networks, vol. 15, no. 1, pp. 166-177, 2004.
- [17] G. Golub, and W. Kahane, "Calculating the singular values and pseudo-inverse of a matrix", Journal of Society for industrial and application mathematics series B: numerical analysis, vol. 2, no. 2, pp. 205-224, 1965.
- [18] Nitgen Company, Fingkey Hamster II fingerprint sensor <http://www.nitgen.com/eng/>

## INSTRUCTIONS TO CONTRIBUTORS

The *International Journal of Biometric and Bioinformatics (IJBB)* brings together both of these aspects of biology and creates a platform for exploration and progress of these, relatively new disciplines by facilitating the exchange of information in the fields of computational molecular biology and post-genome bioinformatics and the role of statistics and mathematics in the biological sciences. Bioinformatics and Biometrics are expected to have a substantial impact on the scientific, engineering and economic development of the world. Together they are a comprehensive application of mathematics, statistics, science and computer science with an aim to understand living systems.

We invite specialists, researchers and scientists from the fields of biology, computer science, mathematics, statistics, physics and such related sciences to share their understanding and contributions towards scientific applications that set scientific or policy objectives, motivate method development and demonstrate the operation of new methods in the fields of Biometrics and Bioinformatics.

To build its International reputation, we are disseminating the publication information through Google Books, Google Scholar, Directory of Open Access Journals (DOAJ), Open J Gate, ScientificCommons, Docstoc and many more. Our International Editors are working on establishing ISI listing and a good impact factor for IJBB.

The initial efforts helped to shape the editorial policy and to sharpen the focus of the journal. Starting with volume 6, 2012, IJBB appears in more focused issues. Besides normal publications, IJBB intend to organized special issues on more focused topics. Each special issue will have a designated editor (editors) – either member of the editorial board or another recognized specialist in the respective field.

We are open to contributions, proposals for any topic as well as for editors and reviewers. We understand that it is through the effort of volunteers that CSC Journals continues to grow and flourish.

### LIST OF TOPICS

The realm of International Journal of Biometrics and Bioinformatics (IJBB) extends, but not limited, to the following:

- Bio-grid
- Bioinformatic databases
- Biomedical image processing (registration)
- Biomedical modelling and computer simulation
- Computational intelligence
- Computational structural biology
- DNA assembly, clustering, and mapping
- Fuzzy logic
- Gene identification and annotation
- Hidden Markov models
- Molecular evolution and phylogeny
- Molecular sequence analysis
- Bio-ontology and data mining
- Biomedical image processing (fusion)
- Biomedical image processing (segmentation)
- Computational genomics
- Computational proteomics
- Data visualisation
- E-health
- Gene expression and microarrays
- Genetic algorithms
- High performance computing
- Molecular modelling and simulation
- Neural networks

**CALL FOR PAPERS**

---

**Volume: 6 - Issue: 4 - August 2012**

**i. Paper Submission: May 31, 2012    ii. Author Notification: July 15, 2012**

**iii. Issue Publication: August 2012**

## **CONTACT INFORMATION**

### **Computer Science Journals Sdn Bhd**

B-5-8 Plaza Mont Kiara, Mont Kiara  
50480, Kuala Lumpur, MALAYSIA

Phone: 006 03 6207 1607  
006 03 2782 6991

Fax: 006 03 6207 1697

Email: [cscpress@cscjournals.org](mailto:cscpress@cscjournals.org)

CSC PUBLISHERS © 2011  
COMPUTER SCIENCE JOURNALS SDN BHD  
M-3-19, PLAZA DAMAS  
SRI HARTAMAS  
50480, KUALA LUMPUR  
MALAYSIA

PHONE: 006 03 6207 1607  
006 03 2782 6991

FAX: 006 03 6207 1697  
EMAIL: [cscpress@cscjournals.org](mailto:cscpress@cscjournals.org)