

INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATION & MANAGEMENT

IJR
CM



A Monthly Double-Blind Peer Reviewed (Refereed/Juried) Open Access International e-Journal - Included in the International Serial Directories

Indexed & Listed at:

Ulrich's Periodicals Directory ©, ProQuest, U.S.A., EBSCO Publishing, U.S.A., Cabell's Directories of Publishing Opportunities, U.S.A.

Open J-Gate, India [link of the same is duly available at Inlibnet of University Grants Commission (U.G.C.)]

Index Copernicus Publishers Panel, Poland with IC Value of 5.09 & number of libraries all around the world.

Circulated all over the world & Google has verified that scholars of more than 3770 Cities in 175 countries/territories are visiting our journal on regular basis.

Ground Floor, Building No. 1041-C-1, Devi Bhawan Bazar, JAGADHRI – 135 003, Yamunanagar, Haryana, INDIA

<http://ijrcm.org.in/>

CONTENTS

Sr. No.	TITLE & NAME OF THE AUTHOR (S)	Page No.
1.	USING CYBER PEDAGOGY (WIBEKI/01/2014) MODEL TO INITIATE MULTILITERACIES AND PROMOTE A VIRTUAL CLASSROOM: A PILOT STUDY <i>WILLIAM NKOMO, BERTHA KARIMBIKA & KITSO MOLEFE</i>	1
2.	THE RIGHT TO HEALTH – A CONSTITUTIONAL VIEW <i>HIRANMAYA NANDA & DR. JAYADEV PATI</i>	11
3.	FINANCIAL PERFORMANCE OF SELECT PRIVATE SECTOR BANKS USING CAMEL APPROACH <i>DR. H N SHIVAPRASAD</i>	14
4.	A COMPARATIVE STUDY OF SELECTED EQUITY DIVERSIFIED SCHEMES IN MUTUAL FUND <i>DR. VIJAY H. VYAS</i>	24
5.	THE INFLUENCE OF INTELLIGENT TRANSPORTATION SPACES IN INTELLIGENT TRANSPORTATION SYSTEM <i>KALAISELVI S, SANGEETHALAKSHMI G & SIVASANKARI A</i>	33
6.	A STUDY ON THE SOCIO-ECONOMIC CHARACTERISTICS OF INTERNET BANKING ADOPTERS IN CHENNAI METROPOLITAN CITY WITH REFERENCE TO INDIAN BANK <i>P.SARAVANAN & P.SRIDHARAN</i>	37
7.	COMPARATIVE STUDY OF NEW RAPID BUSINESS PROCESS MODEL WITH EXISTING MODEL BPMN AND UML-AD <i>AMIT LAXMIDAS VADERA & DR. YOGESH R. GHODASARA</i>	42
8.	A DETAILED STUDY ON QUALITY OF SERVICE IN COMPUTER NETWORKS <i>HARIPRIYA N, SANGEETHALAKSHMI G & SIVASANKARI A</i>	48
9.	TATA GROUP AND CSR: AN EXEMPLARY CASE REVIEW <i>KOMAL CHAUDHARY</i>	52
10.	THREE DIMENSIONAL HEALING: BENEFITS FROM THE WELLNESS <i>DR. VANDANA DESWAL</i>	55
11.	EMOTIONAL INTELLIGENCE AND JOB PERFORMANCE IN SERVICE INDUSTRY <i>PREETI BHASKAR</i>	60
12.	AN OVERVIEW OF THE BANKING INDUSTRY IN INDIA <i>DR. SHILPAN D. VYAS & PARINA S. VYAS</i>	66
13.	COUNTERFEITING GOODS IN GULF BUSINESS: ANY ECONOMIC IMPACT? <i>DR. THRESIAMMA VARGHESE & KARIMA AL. QARTOOPI</i>	74
14.	GREEN MARKETING: AN INDIAN EXPERIENCE <i>KANCHAN SEHRAWAT, AMOGH TALAN, DR. A. K. TYAGI & GAURAV TALAN</i>	77
15.	ROLE OF RBI AND GOVERNMENT OF INDIA TOWARDS FINANCIAL INCLUSION OF THE RURAL POOR: ISSUES AND SUGGESTIONS <i>MANOHAR LAMANI & SANGANAGOUDA PATIL</i>	81
16.	CORPORATE SOCIAL RESPONSIBILITY: REGULATION AND ITS SURVEILLANCE <i>RACHANA VISHWAKARMA</i>	85
17.	PAGE RANK ALGORITHMS BASED ON WEB CONTENT MINING AND WEB STRUCTURE MINING <i>N.KANCHANA</i>	90
18.	WEB CONTENT MANAGEMENT SYSTEM: COMPONENTS AND SECURITY <i>OMOSEBI, PAUL ADEOYE & OLORUNLEKE, FEHINTOLUWA E.</i>	93
19.	DETERMINANTS AND PROSPECTS OF ECONOMIC GROWTH IN ETHIOPIA <i>HABTAMU NIGATU ELALA</i>	96
20.	HIGHLY SECURED LOSSLESS IMAGE CRYPTOGRAPHY ALGORITHM BASED ON HAAR WAVELET TRANSFORM <i>MAHIMA GUPTA</i>	105
	REQUEST FOR FEEDBACK & DISCLAIMER	108

CHIEF PATRON**PROF. K. K. AGGARWAL**

Chairman, Malaviya National Institute of Technology, Jaipur

(An institute of National Importance & fully funded by Ministry of Human Resource Development, Government of India)

Chancellor, K. R. Mangalam University, Gurgaon

Chancellor, Lingaya's University, Faridabad

Founder Vice-Chancellor (1998-2008), Guru Gobind Singh Indraprastha University, Delhi

Ex. Pro Vice-Chancellor, Guru Jambheshwar University, Hisar

FOUNDER PATRON**LATE SH. RAM BHAJAN AGGARWAL**

Former State Minister for Home & Tourism, Government of Haryana

Former Vice-President, Dadri Education Society, Charkhi Dadri

Former President, Chinar Syntex Ltd. (Textile Mills), Bhiwani

CO-ORDINATOR**DR. SAMBHAV GARG**

Faculty, Shree Ram Institute of Business & Management, Urjani

ADVISORS**DR. PRIYA RANJAN TRIVEDI**

Chancellor, The Global Open University, Nagaland

PROF. M. S. SENAM RAJU

Director A. C. D., School of Management Studies, I.G.N.O.U., New Delhi

PROF. S. L. MAHANDRU

Principal (Retd.), Maharaja Agrasen College, Jagadhri

EDITOR**PROF. R. K. SHARMA**

Professor, Bharti Vidyapeeth University Institute of Management & Research, New Delhi

EDITORIAL ADVISORY BOARD**DR. RAJESH MODI**

Faculty, Yanbu Industrial College, Kingdom of Saudi Arabia

PROF. PARVEEN KUMAR

Director, M.C.A., Meerut Institute of Engineering & Technology, Meerut, U. P.

PROF. H. R. SHARMA

Director, Chhatrapati Shivaji Institute of Technology, Durg, C.G.

PROF. MANOHAR LAL

Director & Chairman, School of Information & Computer Sciences, I.G.N.O.U., New Delhi

PROF. ANIL K. SAINI

Chairperson (CRC), Guru Gobind Singh I. P. University, Delhi

PROF. R. K. CHOUDHARY

Director, Asia Pacific Institute of Information Technology, Panipat

DR. ASHWANI KUSH

Head, Computer Science, University College, Kurukshetra University, Kurukshetra

DR. BHARAT BHUSHAN

Head, Department of Computer Science & Applications, Guru Nanak Khalsa College, Yamunanagar

DR. VIJAYPAL SINGH DHAKA

Dean (Academics), Rajasthan Institute of Engineering & Technology, Jaipur

DR. SAMBHAVNA

Faculty, I.I.T.M., Delhi

DR. MOHINDER CHAND

Associate Professor, Kurukshetra University, Kurukshetra

DR. MOHENDER KUMAR GUPTA

Associate Professor, P.J.L.N. Government College, Faridabad

DR. SAMBHAV GARG

Faculty, Shree Ram Institute of Business & Management, Urjani

DR. SHIVAKUMAR DEENE

Asst. Professor, Dept. of Commerce, School of Business Studies, Central University of Karnataka, Gulbarga

DR. BHAVET

Faculty, Shree Ram Institute of Business & Management, Urjani

ASSOCIATE EDITORS**PROF. ABHAY BANSAL**

Head, Department of Information Technology, Amity School of Engineering & Technology, Amity University, Noida

PROF. NAWAB ALI KHAN

Department of Commerce, Aligarh Muslim University, Aligarh, U.P.

ASHISH CHOPRA

Sr. Lecturer, Doon Valley Institute of Engineering & Technology, Karnal

TECHNICAL ADVISOR**AMITA**

Faculty, Government M. S., Mohali

FINANCIAL ADVISORS**DICKIN GOYAL**

Advocate & Tax Adviser, Panchkula

NEENA

Investment Consultant, Chambaghat, Solan, Himachal Pradesh

LEGAL ADVISORS**JITENDER S. CHAHAL**

Advocate, Punjab & Haryana High Court, Chandigarh U.T.

CHANDER BHUSHAN SHARMA

Advocate & Consultant, District Courts, Yamunanagar at Jagadhri

SUPERINTENDENT**SURENDER KUMAR POONIA**

CALL FOR MANUSCRIPTS

We invite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the areas of Computer Science & Applications; Commerce; Business; Finance; Marketing; Human Resource Management; General Management; Banking; Economics; Tourism Administration & Management; Education; Law; Library & Information Science; Defence & Strategic Studies; Electronic Science; Corporate Governance; Industrial Relations; and emerging paradigms in allied subjects like Accounting; Accounting Information Systems; Accounting Theory & Practice; Auditing; Behavioral Accounting; Behavioral Economics; Corporate Finance; Cost Accounting; Econometrics; Economic Development; Economic History; Financial Institutions & Markets; Financial Services; Fiscal Policy; Government & Non Profit Accounting; Industrial Organization; International Economics & Trade; International Finance; Macro Economics; Micro Economics; Rural Economics; Co-operation; Demography; Development Planning; Development Studies; Applied Economics; Development Economics; Business Economics; Monetary Policy; Public Policy Economics; Real Estate; Regional Economics; Political Science; Continuing Education; Labour Welfare; Philosophy; Psychology; Sociology; Tax Accounting; Advertising & Promotion Management; Management Information Systems (MIS); Business Law; Public Responsibility & Ethics; Communication; Direct Marketing; E-Commerce; Global Business; Health Care Administration; Labour Relations & Human Resource Management; Marketing Research; Marketing Theory & Applications; Non-Profit Organizations; Office Administration/Management; Operations Research/Statistics; Organizational Behavior & Theory; Organizational Development; Production/Operations; International Relations; Human Rights & Duties; Public Administration; Population Studies; Purchasing/Materials Management; Retailing; Sales/Selling; Services; Small Business Entrepreneurship; Strategic Management Policy; Technology/Innovation; Tourism & Hospitality; Transportation Distribution; Algorithms; Artificial Intelligence; Compilers & Translation; Computer Aided Design (CAD); Computer Aided Manufacturing; Computer Graphics; Computer Organization & Architecture; Database Structures & Systems; Discrete Structures; Internet; Management Information Systems; Modeling & Simulation; Neural Systems/Neural Networks; Numerical Analysis/Scientific Computing; Object Oriented Programming; Operating Systems; Programming Languages; Robotics; Symbolic & Formal Logic; Web Design and emerging paradigms in allied subjects.

Anybody can submit the **soft copy** of unpublished novel; original; empirical and high quality **research work/manuscript anytime** in **M.S. Word format** after preparing the same as per our **GUIDELINES FOR SUBMISSION**; at our email address i.e. infoijrcm@gmail.com or online by clicking the link **online submission** as given on our website ([FOR ONLINE SUBMISSION, CLICK HERE](#)).

GUIDELINES FOR SUBMISSION OF MANUSCRIPT

1. **COVERING LETTER FOR SUBMISSION:**

DATED: _____

THE EDITOR
IJRCM

Subject: SUBMISSION OF MANUSCRIPT IN THE AREA OF

(e.g. Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/Engineering/Mathematics/other, please specify)

DEAR SIR/MADAM

Please find my submission of manuscript entitled '_____ ' for possible publication in your journals.

I hereby affirm that the contents of this manuscript are original. Furthermore, it has neither been published elsewhere in any language fully or partly, nor is it under review for publication elsewhere.

I affirm that all the author (s) have seen and agreed to the submitted version of the manuscript and their inclusion of name (s) as co-author (s).

Also, if my/our manuscript is accepted, I/We agree to comply with the formalities as given on the website of the journal & you are free to publish our contribution in any of your journals.

NAME OF CORRESPONDING AUTHOR:

Designation:

Affiliation with full address, contact numbers & Pin Code:

Residential address with Pin Code:

Mobile Number (s):

Landline Number (s):

E-mail Address:

Alternate E-mail Address:

NOTES:

- a) The whole manuscript is required to be in **ONE MS WORD FILE** only (pdf. version is liable to be rejected without any consideration), which will start from the covering letter, inside the manuscript.
- b) The sender is required to mention the following in the **SUBJECT COLUMN** of the mail:
New Manuscript for Review in the area of (Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/Engineering/Mathematics/other, please specify)
- c) There is no need to give any text in the body of mail, except the cases where the author wishes to give any specific message w.r.t. to the manuscript.
- d) The total size of the file containing the manuscript is required to be below **500 KB**.
- e) Abstract alone will not be considered for review, and the author is required to submit the complete manuscript in the first instance.
- f) The journal gives acknowledgement w.r.t. the receipt of every email and in case of non-receipt of acknowledgment from the journal, w.r.t. the submission of manuscript, within two days of submission, the corresponding author is required to demand for the same by sending separate mail to the journal.

2. **MANUSCRIPT TITLE:** The title of the paper should be in a 12 point Calibri Font. It should be bold typed, centered and fully capitalised.

3. **AUTHOR NAME (S) & AFFILIATIONS:** The author (s) **full name, designation, affiliation (s), address, mobile/landline numbers**, and **email/alternate email address** should be in italic & 11-point Calibri Font. It must be centered underneath the title.

4. **ABSTRACT:** Abstract should be in fully italicized text, not exceeding 250 words. The abstract must be informative and explain the background, aims, methods, results & conclusion in a single para. Abbreviations must be mentioned in full.

5. **KEYWORDS:** Abstract must be followed by a list of keywords, subject to the maximum of five. These should be arranged in alphabetic order separated by commas and full stops at the end.
6. **MANUSCRIPT:** Manuscript must be in **BRITISH ENGLISH** prepared on a standard A4 size **PORTRAIT SETTING PAPER**. It must be prepared on a single space and single column with 1" margin set for top, bottom, left and right. It should be typed in 8 point Calibri Font with page numbers at the bottom and centre of every page. It should be free from grammatical, spelling and punctuation errors and must be thoroughly edited.
7. **HEADINGS:** All the headings should be in a 10 point Calibri Font. These must be bold-faced, aligned left and fully capitalised. Leave a blank line before each heading.
8. **SUB-HEADINGS:** All the sub-headings should be in a 8 point Calibri Font. These must be bold-faced, aligned left and fully capitalised.
9. **MAIN TEXT:** The main text should follow the following sequence:

INTRODUCTION

REVIEW OF LITERATURE

NEED/IMPORTANCE OF THE STUDY

STATEMENT OF THE PROBLEM

OBJECTIVES

HYPOTHESES

RESEARCH METHODOLOGY

RESULTS & DISCUSSION

FINDINGS

RECOMMENDATIONS/SUGGESTIONS

CONCLUSIONS

SCOPE FOR FURTHER RESEARCH

ACKNOWLEDGMENTS

REFERENCES

APPENDIX/ANNEXURE

It should be in a 8 point Calibri Font, single spaced and justified. The manuscript should preferably not exceed **5000 WORDS**.

10. **FIGURES & TABLES:** These should be simple, crystal clear, centered, separately numbered & self explained, and **titles must be above the table/figure. Sources of data should be mentioned below the table/figure.** It should be ensured that the tables/figures are referred to from the main text.
11. **EQUATIONS:** These should be consecutively numbered in parentheses, horizontally centered with equation number placed at the right.
12. **REFERENCES:** The list of all references should be alphabetically arranged. The author (s) should mention only the actually utilised references in the preparation of manuscript and they are supposed to follow **Harvard Style of Referencing**. The author (s) are supposed to follow the references as per the following:
 - All works cited in the text (including sources for tables and figures) should be listed alphabetically.
 - Use (ed.) for one editor, and (ed.s) for multiple editors.
 - When listing two or more works by one author, use --- (20xx), such as after Kohl (1997), use --- (2001), etc, in chronologically ascending order.
 - Indicate (opening and closing) page numbers for articles in journals and for chapters in books.
 - The title of books and journals should be in italics. Double quotation marks are used for titles of journal articles, book chapters, dissertations, reports, working papers, unpublished material, etc.
 - For titles in a language other than English, provide an English translation in parentheses.
 - The location of endnotes within the text should be indicated by superscript numbers.

PLEASE USE THE FOLLOWING FOR STYLE AND PUNCTUATION IN REFERENCES:

BOOKS

- Bowersox, Donald J., Closs, David J., (1996), "Logistical Management." Tata McGraw, Hill, New Delhi.
- Hunker, H.L. and A.J. Wright (1963), "Factors of Industrial Location in Ohio" Ohio State University, Nigeria.

CONTRIBUTIONS TO BOOKS

- Sharma T., Kwatra, G. (2008) Effectiveness of Social Advertising: A Study of Selected Campaigns, Corporate Social Responsibility, Edited by David Crowther & Nicholas Capaldi, Ashgate Research Companion to Corporate Social Responsibility, Chapter 15, pp 287-303.

JOURNAL AND OTHER ARTICLES

- Schemenner, R.W., Huber, J.C. and Cook, R.L. (1987), "Geographic Differences and the Location of New Manufacturing Facilities," Journal of Urban Economics, Vol. 21, No. 1, pp. 83-104.

CONFERENCE PAPERS

- Garg, Sambhav (2011): "Business Ethics" Paper presented at the Annual International Conference for the All India Management Association, New Delhi, India, 19–22 June.

UNPUBLISHED DISSERTATIONS AND THESES

- Kumar S. (2011): "Customer Value: A Comparative Study of Rural and Urban Customers," Thesis, Kurukshetra University, Kurukshetra.

ONLINE RESOURCES

- Always indicate the date that the source was accessed, as online resources are frequently updated or removed.

WEBSITES

- Garg, Bhavet (2011): Towards a New Natural Gas Policy, Political Weekly, Viewed on January 01, 2012 <http://epw.in/user/viewabstract.jsp>

HIGHLY SECURED LOSSLESS IMAGE CRYPTOGRAPHY ALGORITHM BASED ON HAAR WAVELET TRANSFORM

MAHIMA GUPTA
STUDENT
SHOBHIT UNIVERSITY
MEERUT

ABSTRACT

Along with the rapid increasing growth of computer and network technologies, images are being transmitted more and more frequently. Security of image is a big issue. Image information is lively and visual, and has been an important means of expressing information of person. There are many encryption algorithm had been available each one having some strength and weakness. Image cryptography can use text cryptosystems to encrypt images directly, since image size is greater than text. Image encryption can be classified into lossy and lossless encryption methods. Lossless encryption methods are more applicable than lossy encryption methods when marginal distortion is not tolerable. In the proposed system, find the hash value of image using by image hashing toolbox. Image hashing is very easy to the tamper with digital data without leaving any clues. Under these circumstances, integrity verification has become an important issue in the digital world. After finding the hash value, the image is transformed into the frequency domain using the wavelet transform, Image processing and analysis based on the continuous or discrete image transforms are classic techniques. The image transforms are widely used in image filtering, data description, etc. Nowadays the wavelet theorems make up very popular methods of image processing, denoising and compression. The image transform theory is a well-known area characterized by a precise mathematical background. Considering that the Haar functions are the simplest wavelets, these forms are used in many methods of discrete image transforms and processing then the image sub-bands are encrypted in a such way that guarantees a secure, reliable, and an unbreakable form. The encryption involves scattering the distinguishable frequency data in the image using a reversible weighting factor amongst the rest of the frequencies. The algorithm is designed to shuffle and reverse the sign of each frequency in the transformed image before the image frequencies are transformed back to the pixel domain. The decryption algorithm reverses the encryption process and restores the image to its original form.

KEYWORDS

Wavelets, Haar Transform, Lossless image encryption/decryption, Symmetric key encryption, Image hashing, Block based matrix transformation.

INTRODUCTION

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. It is an effective way of protecting sensitive data stored on media or transmitted over unsecured network communication paths. With the rapid development of communication and internet technology, there is always a growing concern about the security of multi-media information such as image. A major challenge is to protect the confidentiality and integrity of such images so that the visual data cannot be misused. Applications like information storage, information management, patient information security, satellite image security, telemedicine, military information security etc. which require information security. Different cryptographic methods are used by different organization for protecting their confidential data. But cryptography hackers are always trying to break the cryptographic method. For this reason cryptographers are trying to develop new cryptographic method to keep the data safe as far as possible. For this reason, cryptographers are always trying to propose new methods and techniques to keep data/information secure. Until now, several data encryption algorithms had been presented such as DES, AES, IDEA, RSA, etc. most of which are used for encrypting text data. It is not suitable to use them for multimedia data because multimedia data is different from text message, has larger scale of data, higher redundancy and stronger correlation between pixels. Image encryption methods can be classified into either lossy or lossless. In lossy encryption methods, where the image details are somewhat distorted, the resulting decrypted image is different from the original image. Due to the characteristics of human perception, and depending on the application, a decrypted image with little distortion is usually acceptable. However, lossless encryption methods are more applicable in applications where the distorted-free original image is required. If attacker tampers or modifies the image's sub band then target user cannot analyzed that receiving image is original or not. So by hashing we can provide the integrity as well as authenticity to the image over the unsecure network. In the proposed algorithm, the image is transformed into the frequency domain using the Discrete Wavelet Haar Transform (DWT) with two levels of decomposition, where the image sub-bands are processed in such a way that ensures that the original image can never be recovered without using the proposed decryption algorithm. The image decryption is also applicable in the frequency domain where the image sub-bands are converted back to their original form by reversing the encryption process.

SPATIAL FREQUENCY TRANSFORMATION

We have deal with images in many domains. Now we are processing signals (images) in frequency domain. In spatial domain, we deal with images as it is. The value of the pixels of the image change with respect to scene. Whereas in frequency domain, we deal with the rate at which the pixel values are changing in spatial domain.

SPATIAL DOMAIN

In simple spatial domain, we directly deal with the image matrix.

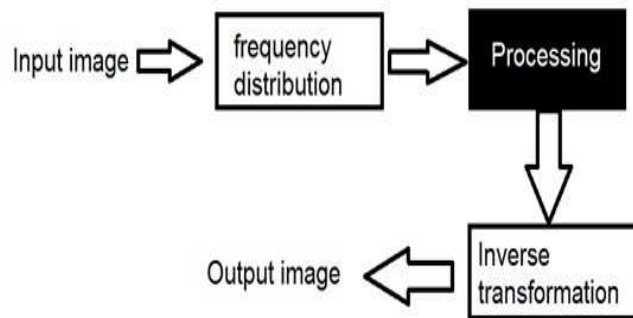
FIG. 1



FREQUENCY DOMAIN

We first transform the image to its frequency distribution. Then our black box system performs whatever processing it has to perform, and the output of the black box in this case is not an image, but a transformation. After performing inverse transformation, it is converted into an image which is then viewed in spatial domain.

FIG. 2: IMAGE PROCESSING IN FREQUENCY DOMAIN



In this research, the DWT Haar transform is used. Proposed algorithm is simple, effective, and secure. Compared to the rest of the algorithms in this domain, the proposed algorithm introduces lossless image cryptography that surpasses the lossy algorithms by preserving every single detail in the image; hence it is the category under which this research falls. The purpose of image transformation is to represent the image's highly correlated data in another de-correlated form, by switching from the spatial to the frequency domain. Any transformation technique should be reversible and computationally tractable with low memory requirement and a low number of arithmetic operations. Image based transform methods yield better results at the cost of extra complexity, so in this research, DWT is chosen as the transformation method.

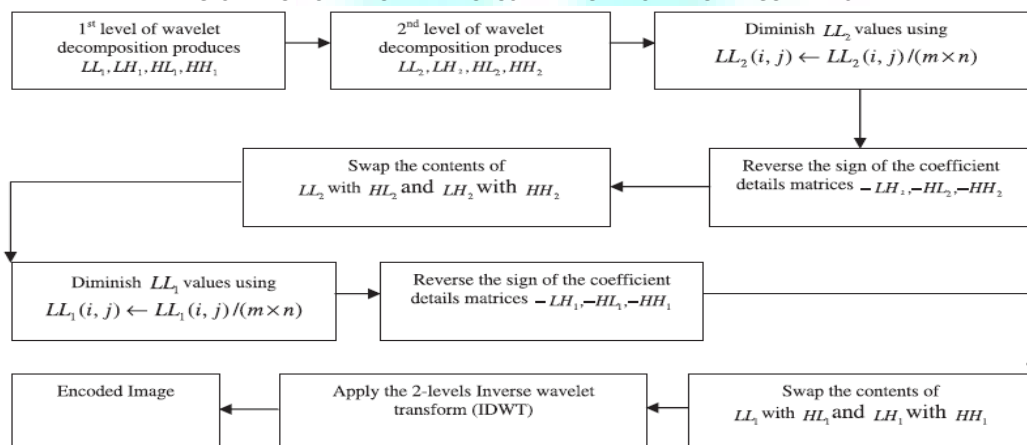
IMAGE HASHING

Hash functions are frequently called message digest functions. Their purpose is to extract a fixed-length bit string from a message (image, documents, etc.). Hash functions have found varied applications in various cryptographic, compiler and database search applications. In cryptography, hash functions are typically used for digital signatures to authenticate the message being sent so that the recipient can verify its source. Recently, there has been a lot of interest in using hash functions in multimedia applications both for security and indexing. A key feature of conventional cryptographic hashing algorithms such as message digest 5 (MD5) and secure hash algorithm 1 (SHA-1) is that they are extremely sensitive to the message, i.e. changing even one bit of the input will change the output dramatically. However, multimedia data such as digital images go through various manipulations such as compression, enhancement, cropping, and scaling. An image hash function should instead take into account the changes in the visual domain and produce hash values based on the image's visual appearance. Such a hash function would be useful in identifying images in databases, in which the image possibly undergoes incidental changes (such as compression and format changes, common signal processing operations, scanning or watermarking). A second significant application of a perceptual image hash could be for robust image authentication. In such cases, the hash must be invariant under perceptually insignificant modifications to the image but detect malicious tampering of image data. Several other applications can be identified in the areas of watermarking and information embedding in images.

ENCRYPTION ALGORITHM

The encryption algorithm uses the DWT to encrypt the image and compute (wavelet decomposition) the approximation coefficients matrix and details coefficients matrices of the target (original) image using the Haar transform in the first wavelet decomposition. The approximation coefficients matrix is then used to produce the second wavelet decomposition, i.e. encryption process repeated again on the 1st level of wavelet decomposition. The use of two-levels of wavelet decompositions keeps the algorithms' complexity low, i.e., lower number of computations compared to N-levels of wavelet decompositions. Weighting factor can be used as the encryption key in this algorithm. In proposed system 2-levels Inverse Discrete Wavelet Transform (IDWT) of the image is performed. The image frequencies are transformed back to the pixel domain, with the pixel values changed and the image details concealed.

FIG. 3: A FLOWCHART OF THE PROPOSED IMAGE ENCRYPTION ALGORITHMS



There are following steps of encryption algorithm

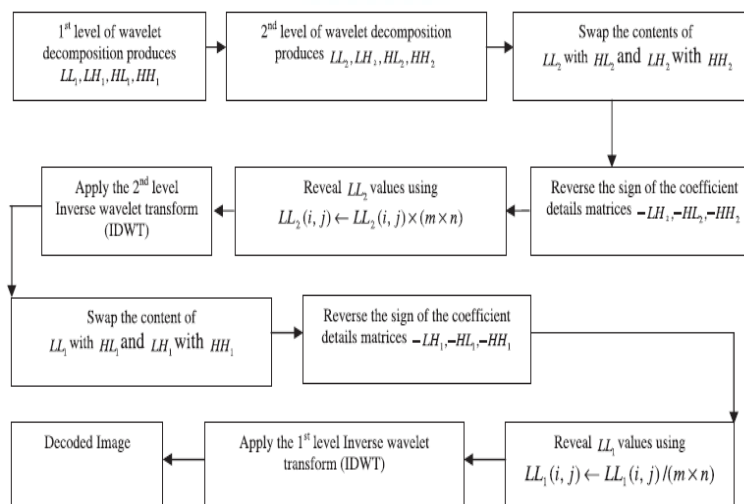
- Weighting factor can be used as the encryption key in this algorithm.
- 1st level of wavelet decomposition produces LL1, LH1, HL1, and HH1, where LL1 is the approximation matrix and LH1, HL1, HH1 are detail coefficients.
- 2nd level of wavelet decomposition (matrix LL1 is used) produces LL2, LH2, HL2, HH2.
- Diminish LL2 values using $LL2(i,j) \leftarrow LL2(i,j)/(m \times n)$, where m and n are matrix dimension.
- Reverse the sign of the coefficient details matrices $LH2 \leftarrow -LH2 \times -1$, $HL2 \leftarrow -HL2 \times -1$, $HH2 \leftarrow -HH2 \times -1$, the reason behind performing the sign reverse operation is that the magnitude of the sinusoid corresponds to its contrast (the difference between the darkest and brightest peaks of the image).
- A negative magnitude represents contrast-reversal, i.e. the bright become dark, and vice-versa.
- Swap the contents of LL2 with HL2 and LH2 with HH2.
- Diminish LL1 values using $LL1(i,j) \leftarrow LL1(i,j)/(m \times n)$.
- Reverse the sign of the coefficient details matrices $-LH1, -HL1, -HH1$.

- Swap the contents of LL1 with HL1 and LH1 with HH1.
- Apply the 2-levels Inverse wavelet transform.
- Encoded Image.

DECRYPTION ALGORITHM

The decryption algorithm reveals the image's original details. This process is inverse of encryption process. The decoding process of the 1st wavelet decomposition is similar to that of the 2nd level. Thus, decoding the 1st level of the wavelet decomposition is achieved. In the last stage, the inverse discrete wavelet transform of the image is performed. The image frequencies are transformed back to the pixel domain, with the pixel values unaffected and the image details revealed. Using the proposed encryption/decryption algorithm, the decrypted image pixels will have the same values as the original image.

FIG. 4: A FLOWCHART OF THE PROPOSED IMAGE DECRYPTION ALGORITHM



There are following steps of encryption algorithm:

- 1st level of wavelet decomposition produces LL1, LH1, HL1, and HH1, where LL1 is the approximation matrix and LH1, HL1, HH1 are detail coefficients.
- 2nd level of wavelet decomposition (matrix LL1 is used) produces LL2, LH2, HL2, HH2.
- Swap the contents of LL2 with HL2 and LH2 with HH2.
- Reverse the sign of the coefficient details matrices $LH2 <- LH2 \times -1$, $HL2 <- HL2 \times -1$, $HH2 <- HH2 \times -1$.
- Reveal LL2 values using $LL2(i, j) <- LL2(i, j) \times (m \times n)$, where m and n are matrix dimension.
- Apply the 2-levels Inverse wavelet transform.
- Swap the contents of LL1 with HL1 and LH1 with HH1.
- Reverse the sign of the coefficient details matrices $-LH1$, $-HL1$, $-HH1$.
- Reveal LL1 values using $LL1(i, j) <- LL1(i, j) \times (m \times n)$.
- Apply the 1st level Inverse wavelet transform.
- Decoded Image.

CONCLUSION

Now a day's images play an important role in our lives, it is used in many applications. Therefore it is essential to protect the integrity and confidentiality of images. In this paper we presented survey of various image encryption techniques. Each technique having some advantages and disadvantages, so there is a need to design algorithm that reduce the correlation between the image pixels and increase the entropy so it is very difficult to decrypt by hacker. The proposed technique shuffles the image pixel position perfectly and changes the value of each pixel.

REFERENCES

1. N. Sethi, D. Sharma, Novel method of image encryption using logistic mapping, *Int. J. Comput. Sci. Eng.* 1 (2) (2012) 115–119
2. S. Maniccam, N. Bourbakis, Lossless image compression and encryption using SCAN, *Elsevier J. Pattern Recognit.* 34 (6) (2001) 1229–1245
3. S. Tedmori, N. Al-Najdawi, Lossless image cryptography algorithm based on discrete cosine transform, *Int. Arab J. Inform. Technol.* 9 (5) (2012) 471–478;
4. S. Tedmori, N. Al-Najdawi, Lossless image cryptography algorithm based on discrete cosine transform, *Image Proc.* 24 (3) (1983) 363–381.
5. Sinha, K. Singh, A technique for image encryption using digital signature, *Elsevier J. Opt. Commun.* 218 (4–6) (2004) 229–234.
6. X. Zhang, Scalable coding of encrypted images, *IEEE Trans. Image Process.* 21 (6) (2012) 3108–3114.

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, International Journal of Research in Computer Application & Management (IJRCM) acknowledges & appreciates your efforts in showing interest in our present issue under your kind perusal.

I would like to request you to supply your critical comments and suggestions about the material published in this issue as well as on the journal as a whole, on our E-mail infoijrcm@gmail.com for further improvements in the interest of research.

If you have any queries please feel free to contact us on our E-mail infoijrcm@gmail.com.

I am sure that your feedback and deliberations would make future issues better – a result of our joint effort.

Looking forward an appropriate consideration.

With sincere regards

Thanking you profoundly

Academically yours

Sd/-

Co-ordinator

DISCLAIMER

The information and opinions presented in the Journal reflect the views of the authors and not of the Journal or its Editorial Board or the Publishers/Editors. Publication does not constitute endorsement by the journal. Neither the Journal nor its publishers/Editors/Editorial Board nor anyone else involved in creating, producing or delivering the journal or the materials contained therein, assumes any liability or responsibility for the accuracy, completeness, or usefulness of any information provided in the journal, nor shall they be liable for any direct, indirect, incidental, special, consequential or punitive damages arising out of the use of information/material contained in the journal. The journal, nor its publishers/Editors/Editorial Board, nor any other party involved in the preparation of material contained in the journal represents or warrants that the information contained herein is in every respect accurate or complete, and they are not responsible for any errors or omissions or for the results obtained from the use of such material. Readers are encouraged to confirm the information contained herein with other sources. The responsibility of the contents and the opinions expressed in this journal is exclusively of the author (s) concerned.

ABOUT THE JOURNAL

In this age of Commerce, Economics, Computer, I.T. & Management and cut throat competition, a group of intellectuals felt the need to have some platform, where young and budding managers and academicians could express their views and discuss the problems among their peers. This journal was conceived with this noble intention in view. This journal has been introduced to give an opportunity for expressing refined and innovative ideas in this field. It is our humble endeavour to provide a springboard to the upcoming specialists and give a chance to know about the latest in the sphere of research and knowledge. We have taken a small step and we hope that with the active co-operation of like-minded scholars, we shall be able to serve the society with our humble efforts.

Our Other Journals

