INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATION & MANAGEMENT

IJRCM

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-Gage, India [link of the same is duly available at Inflibnet 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 2980 Cities in 165 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

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We invite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the areas of Computer Science & Applications;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 mentionthe 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

DATA HIDING TECHNIQUE FOR E-TENDERING USING STEGANOGRAPHY

MAHAVEER PRASAD TAWANIA
STUDENT
SHEKHAWATI ENGINEERING COLLEGE
DUNDLOD

ABHISHEK DIDEL
ASST. PROFESSOR
SHEKHAWATI ENGINEERING COLLEGE
DUNDLOD

SAURABH MAHESHWARI
ASST. PROFESSOR
GOVERNMENT WOMEN ENGINEERING COLLEGE
AJMER

ABSTRACT

Tenders are filed for any contractual work to choose the vendor who satisfies all the terms and conditions. The criteria for selection also include the minimum proposed bid to deliver the desired services. Tendering is the best method to get all the services with minimum cost. Unfortunately, in India many tenders are forged or forcefully changed. Leaking the tender amount by some person in tender management, forcefully asking the persons to withdraw tenders are the major problems in making this process secure and genuine. We propose a secure tender filing system which may be connected to an online system where the vendor needs not to present himself before the tender authority. The tender can only be opened by the vendor. Even the higher authorities cannot break this digital seal. The secure information like amount, etc. about the tender is embedded into a vendor selectedvideo. Vendor is not going to enter the amount physically anywhere. This info will be digitally secured in this video. Every time to see the tender amount the vendor has to enter a secret key. He also has to selectsome personalized images through PII method. The digital seal also has information of the time of tender filing. No updates are allowed after a fixed time. The seed for embedding of the secret information has dependence on both the vendor and the tendering organization. None of them can forge on their side.

KEYWORDS
Digital seal, online tendering, Personal image identification, video steganography, watermarking.

1. INTRODUCTION

The information to be hidden is called the secret message, which can be copyright information or confidential data, and public information can be named as carriers of message such as audio or video clips and more. Key controls the information hiding process [10]. Secret information is hidden into carriers and the carriers having secret information are then passed through the communication channel. A detector is then used to recover secret information from the carrier with the help of key. So, information hiding technique may be divided into two parts:

1. **Information embedding algorithm–**It uses the key to achieve the secret information hidden.
2. **Hidden information detection /extraction method** – It uses the host key from the hidden to detect/ recover the secret information. In the key premise of the unknown, third party host is difficult to get hidden or deleted, and even find secret information.

Steganography deals with studying the collection of techniques aimed to embed sensitive information into another file. This file is known as "container file" or "cover file" (graphs, documents, executable programs, etc.). By doing this, information is passed to third parties without being noticed and can only be retrieved by a legitimateuser who knows a specific algorithm to extract it. This science has aroused great interest in recent years since it has been used by crime and terrorist organizations. However, this is not a new invention, but has been employed since ancient times. This topic is intended to introduce the concept of steganography, and differentiating it from cryptography. Steganography has its roots in our civilization from an immemorial time and has been traditionally used by military and intelligence agencies, criminals and police, as well as by civilians who want to disobey government restrictions. However traditional steganography was only based on ignoring the covert channel used, digital channels *(image, video, audio, communication protocols, etc.) are* nowadays used to achieve that target. In many cases, the container object is known, what is ignored is the algorithm to insert information into that object. Steganography provides a solution to the prisoner's problem: two prisoner of a high-security prison, A and B, who are in separate cells, want to communicate with each other to prepare a plan to escape. However, all information exchanged between them is examined by a security guard who, in view of any suspicion of covert communication, isolates them from one another. By means of steganography the guard analyses seemingly innocuous messages which contain a subliminal channel really useful to the prisoners.

As we know in the transmission and sharing of digital data internet plays an important role. Due to worldwide or publicized medium some confidential data may be stolen, copied, edited or deleted by an unauthorized user. So security must be providing to transmission data. Encryption is the well-known technique to provide security for data transmission using various methods. Encryption technique makes data to unreadable and meaningless or unnatural. Sometime meaningless message may be attracted by unauthorized user, so new technique must be used for secure data transmission known as "steganography".

In steganography technique data, which sender want to keep confidential is known as secret message can be text, audio, video, image and other types of data which can be represented by a stream of bits. Cover is the medium in which secret message is embedded and show as the original with hiding the presence of secret message. Message embedding technique is mainly dependent on the structure of cover and using digital images provides more security for hide the secret message. Cover image embedding with secret message is known as "stego image". Stego image look similar to cover image, no one can differentiate between stego image and cover image. To provide higher security before embedding the secret message into cover image message should be encrypted. For this process, sender use stego key for ensuring that only receiver who knows the respective decoding key to extract the message from stego image. For this method cover image is separated from stego image and that separated area works as a key at decoding side for improved security.

There are mainly following two points that must be considered during designing of the steganographic system:

i) Invisibility: It cannot be seen by human eyes the difference between original cover image and stego image.

ii) Capacity: For more security the cover image can carry more data.

There has been a rapid growth of interest in steganography for two main reasons [8]:

- The publishing and broadcasting industries have become interested in techniques for hiding encrypted copyright marks and serial numbers in digital films, audio recordings, books and multimedia products.

- Restrictions on the availability of encryption services have motivated people to study methods by which private messages can be embedded in seemingly innocuous cover messages.

The basic model of steganography comprises of the following factors:

- Cover object (container object): It is the object used to carry the hidden message.
- Stego-object: It is the cover object together with the hidden message
- Adversary: These are all those entities from whom the covert information is being hidden. The adversary can be passive or active. A passive adversary suspects that covert communication may be taken place and tries to discover the algorithm extracted from the stego-object, but does not attempt to alter that object. An active adversary, apart from trying to find out the covert communication algorithm, modifies the stego-object with the aim to corrupt any attempt of subliminal messaging.
- Steganalysis: Science that studies the detection (passive attacks) and/or cancellation (active attacks) of information hidden behind different covers, as well as the possibility of finding the useful information inside them (existence size).

There are several suitable carriers below to be the cover-object [9]:

(a) Network Protocols such as TCP, IP and UDP.
(b) Audio that using digital audio formats such as wav, midi, avi, mpeg, mpi and voc.
(c) File and Disk that can hides and append files by using the slack space.
(d) Images file such as bmp, gif and jpg, where they can be both color and gray-scale.

There are many limitations are available in usual tender processing system, such as delay in processing, human being interfacing during processing, insufficient transparencyand unavailability of security etc. Due to this tenders are copied or changed forcefully. Causes this tender is going in to the wrong hand and work done by them is not good and other tender cannot take this tender. So it is a big challenge for government or organization to provide security, reduce time of processing and make a fair competition for this type of tender. For this government or organization provide web based online E-Tendering process.

Internet is using for communication of different vendors and organization. Due to this internet communication third person not only access the confidential data, but also modify the data. So it must be necessary for vendors to provide high security for online tendering process.

The fair and successfully implementation of online tendering system must satisfy following criteria:-

1. Reducing cost of tender
2. Reducing time for tender processing
3. Data can be accessed anytime and anywhere only by authorized vendor.
4. Fairness and liability in the process.
5. improved efficiency and productivity
6. High level security

The tendering process in Government organizations lacks the transparency due to non-involvement of the bidder in the bid opening process. Some of the bidders are illegally benefitted to change their amount even after last date of tender submission. These changes are done to beat the lowest bid by illegally opening the tender envelopeswithout all the bidders being present. So a system is obviously needed to submit tenders online inan authenticated envelope such that the biddinginformation cannot be leaked without the customized information given by the bidder. Also the time of tender filing should be there inside the envelope so that no one can change this information after the last date of filing tender. The available steganography techniques are very costly in terms of space and time. Complexity of the process can be decreased by adding some user dependent random secret keys. The original message should not be hidden to the video; instead user dependent keys should be used. The localization of the secret message in the video should not depend on single secret key. Third party involvement should be there to authorize the process**.**

2. LITERATURE SURVEY

This paper describes the main proposal of information hiding technology, analyses the information hiding principle and Information hiding system model and information hiding system characteristics [10, 25], discusses the current main branch of information hiding technology and applications and information hiding problems and prospects for the future development direction.

In now days Information hiding technology is going into new research directions such as multimedia communication and multimedia signal processing, because it provides a new idea of information security [25], our research for information security provides a new direction, from the different application purposes can be studied, with the knowledge economy and information age, informationhiding technology will be more perfect on the theoretical system, it will obtain great commercial value.

2.1 DATA HIDING WAVELETS

A new image data hiding technique is proposed in this paper, which is based on Discrete Wavelet Transform (DWT).This new technique is useful for obtain Stego image by hiding a secret message into cover image using two secret keys. This technique has many high stronger image processing operations such as image compression, cropping, blurring, sharping, median filter and addition of noise to the Stego image [1, 8]. With extraction of Stego image the embedded secret data can be identified with high visual quality. Stego image is look like as an original cover image. Here does not require the original cover image to extract embedded secret data in this technique. The comparison with the other existing techniques, the proposed technique is superior to others.

Discrete wavelets transform (DWT) based image data hiding technique has been proposed in this paper. The Stego image has high peak signal to noise ratio (PSNR) value. So, existence of the secret-image is not noticed by the unauthorized person. The extracted secret image and original secret image look like as same [1]. If applied the some image processing operations such as JPEG compression, blurring, cropping, median filter, sharpen, and addition of noise to the Stego-image. It is noticed that in theproposed technique, to extract the embedded secret image, it does not require the original cover image. With comparison to other existing techniques proposed technique is superior.

2.2 VIDEO STEGANOGRAPHY

Protect the video copyright with an effective method known as “digital watermarking for video”. This paper summarizes the theories, features, model and classic algorithms of video watermarking techniques [25], and then discusses thealgorithms' advantages and disadvantages. The key techniques and the development tendency of the video watermarking are discussed finally.

Video watermarking technology develops the second generation from the first generation with the development of video compression standards. In the first generation of video watermarking technology algorithms nothing to do with video content, but in second generation algorithm is based on video content [10, 25]. Watermark energy is extending to all the pixels in the frame, focuses on the discussion of computation and watermark strength, regardless of content by mostly first-generation watermarking scheme. Take more concentration to the combination of the watermark and the synchronization of the watermark by the second generation of video watermarking scheme. From all above, major development direction of video watermarking is watermarking scheme based on video content or video object attributes.

2.3 DATA TRANSMISSION ENVELOPE

It must be necessary to secure transmission of important information like banking and military. The process of hiding secret data inside a video is known as Video Steganography. Changes in the pixel colors is negligible, so human eyes cannot recognize the addition of information to the video [9]. To provide an efficient and a secure method for video Steganography is the main aim of this paper.

An index is created for the secret information using the proposed method andthis index is located in the frame of the video itself. This frame containing the location of secret information with the help of placed index. So due to thismethod at the receiving end, with the help of index only secret data, which arecontaining by the frames, are analyzed rather than analyzing the entire video during the extraction process [9, 12]. With compared to the normal method of

hiding information frame-by-frame in a sequential manner, in this method less chances of finding the hidden information by an attacker. Computational time taken during the extraction process is also reduced by this method.

So, a feasible solution for video steganography is provided by this paper. Video is considered as a set of frames or images and changes in the output images after addition of hidden information is not recognizable by human eyes in this method [9]. Computational time taken is very less due to using simple mathematical calculation in this method. This method is simple and very effective for video steganography. Beside the simplicity in the implementation, security is also provided in this method to hidden information during transmission.

2.4 IMPORTANCE OF VIDEO ENVELOPES

Digital watermarking is a technique, which embedding the secret information into multimedia data. So in now days, it gained large attention to all over world. For resolving copyright ownership and verifying the integrity of content the watermark of digital images, audio, video, and other media products in general has been proposed. The definition and basic framework of watermark techniques is introduced first in this paper [14], after that the basic theoretical and evaluation criteria are explained. Finally, described theapplication area and possible research direction of digital watermark technology.

Recently, with the large development of new technologies and communication network, it's easier to enter into the world of digital multimedia and also easier to unauthorized copying and illegal spread of multimedia information as like audio, video and image. There is a difficulty in the provide protection against the various types of attacks in the present watermark technology [21]. Copyright protection, access and copy control, digital fingerprints, and other aspects of the application are limited in digital watermark technology. So trying to solve these issues many researchers are working.

In addition, the lack from the general framework of watermarking algorithm design is informative, put forward the reasonable has guiding significance for the strength of the watermarking model framework if can, will give watermarking algorithm design big convenience [14]. It can forecast that protect the multimedia information by using a digital watermark will become a more and more popular in the world.

2.5 LIFE CYCLE OF SECRET INFORMATION

Process of embedding information into a digital signal such that it is difficult to eliminate is known as "Digital watermarking". This digital signal may be audio, images or video etc. information is also carried with the signal if it is copied. Different watermarks are carried by a signal at the same time [12]. Use of watermarking in copyright protection systems is described in this paper, which are usable to prevent unauthorized copying of digital media. In this by using a copy device watermark is retrieving from the signal before making a copy; it's depending on the contents of thewatermark to make a decision by the device to copy or not.

It is of course impossible to provide a complete list for application of digitalwatermarking. However, it is interesting to note the risinginterest in easilybroken watermarking technologies. Applications related to copy protection of printed media are the main promise [24]. Protection of bills with digital watermarks is an Example of it. Many companies have working for projects in this direction and expected to completely functioning solutions will be available soon.

2.6 SELECTION OF ENVELOPES

With the increase of media sharing by using the advancement of internet services and various storage technologies video piracy has become an increasing problem [21, 24]. So, copyright protection mechanisms includes digital watermarking become an interesting area of research for scientists, mainly in designing a seamless algorithm for effective implementation. Mainly within video data, digital watermarking involves embedding secret symbols used for copyright detection purposes. The state of the art in video watermarking techniques is describing in this paper.

An important review on various available techniques is provides by it and also provides the main key performance indicators include the strength, speed, capacity, reliability, imperceptibility and computational complexity.

It is shown from the Comparisons between the above mentioned different schemes that spatial domain approaches are performs out by frequency domain schemes [24]. Comparison with the lossy compression, noise addition and geometrical attacks such as rotating and cropping frequency domain schemes are stronger. As the embedding is done in the middle frequencies, among the frequency domain, DCT based scheme is the strongest against lossy compression, whereas DWT based schemes is strongest against the noise addition.

Against pixel removal, shearing and the rotating, the DFT-based watermarking schemes have better resistance. Artificial Intelligence (AI) algorithms is likely to be use by researchers in various operations while for authentication feature based watermarks are used, such as in making decision for appropriate embedding location, the feasible payload and recognition of the extracted watermark. In the area of video watermark, some of still open areas of research are [24, 26]:

- Against some of especially attacks which are designed for videos such as frame dropping, averaging and statistical analysis; many of existing watermarking schemes are not strong.
- The capacity of watermarking payload.
- Focused by the existing algorithm is very rarely on watermarking in audio signal of a video, yet videos consist of sequence of images and audio often.
- No algorithm is designed for protection against all types of attacks; each of them is designed for protection against some specific attacks.
- It shown that focuses of most researchers for their proposed algorithms are on strength and imperceptibility, but in real-time applications, there is not a good attention for computational complexities and time of extracting algorithms.

With the study on the existing techniques for video watermarking, in the future this research area may guide to use of more feature-based techniques and for decision making in different parts of watermarking process, also applying more Artificial Intelligence (AI) algorithms.

2.7 MOTION ENVELOPES FOR VIDEO STEGANOGRAPHY

In this paper, a new video steganography algorithm is proposed and realized which is based on the H.264/AVC Video coding standard. To control embedding and the secret transporter, a motion vector component feature is designed by this algorithm [26]. Visual invisibility and statistical invisibility of video sequence will not be affected by the information embedded. It is shown by the experiments that the algorithm with a large capacity of embedding and high transportation use can be implemented fast and effectively.

A motion vector components based video steganography algorithm is proposed in this paper. P, B macro block (or sub-block) motion vector are selected as steganography carriers. For control embedded operation characteristics of motion vector components is designed. The qualities of higher transporter use, Efficiency of embedding and capacity of large embedding with good visual invisibility and statistical invisibility are obtained by this algorithm. Finally, due to its fast and effective implementation, it can be described that the operation of algorithm is simple and practically it can be meet with the requirements of secret communication.

3. PROPOSED METHOD

3.1 INFORMATION INPUT

3.1.1 User id (uid)

This is a unique id assigned to each bidder. All the bidders need to register once and set a secret password. This ID is merged with the bidding amount in the digitally sealed envelope. The name of the envelope stored is also kept as this ID, so a bid corresponding to a bidder is searched using this ID as primary key.

3.1.2 Secret Password (PWD)

This password is known to the bidder only. This password will be added to the other information to generate the seed localization key.

3.1.3 Bidding Amount (BAMT)

This is the amount of tender. This is a lump sum amount which is to be paid to the bidder if the work proposed in the tender is done successfully. A minimum and maximum limit on this amount is generally mentioned by the tenderer. The bidder keeps this amount as minimum as possible to get the tender. This bid is submitted in a sealed envelope and this is the primary criterion to issue the tender to a particular bidder on minimum bidding amount. Our whole algorithm is to make this amount secure using a digital envelope. Since this amount can be leaked to some other bidder who can change his bid to minimum after comparison to other bidders.

3.1.4 Bidding Time (TIME)

The seal for the bidding amount should be created in such a manner that it can be opened only in presence of the bidder on the bid opening day. No tampering with this amount can be done. A time is given by which the tender filing and quotation submission is to be done. After this time no updates are allowed. So it is quite necessary to enter bidding time information also inside the tender envelope. This information will indicate when the envelope was sealed. The bidding amount can only be extracted if this time is matched during the extraction. No change in the tenders could be done after last date of tendering. If some changes are done in the tender then after the last date then it would record the time also. So the illegal tampering will be detected.

3.2 ENTERPRISE DEPENDENT KEY

This is an innovative key that will be chosen by the enterprise which is issuing tender. This information is required to authenticate each envelope that it is certified from the tenderer. It can be compared to a tender process where bidder has to send a bid in the prescribed format and in the envelope provided by the tenderer. The bid amount can only be extracted properly if this value is same as given by the tenderer. The main benefit of this key is that no bidder can claim a false bid since all the bids are certified from this key. If the bid has been filed in time then the amount can only be extracted successfully if EDK has been used during embedding, this authenticated embedding procedure from tenderer side.

3.3 SEED LOCALIZATION KEY

The indexes in the PII images from where the intensities will be selected are determined using this key. This is known as seed localization key. SLK is generated as string concatenation of EDK, PWD and TIME.

SLK=strcat (EDK, PWD, TIME);

Conversion of this SLK to the indexes for localization of indexes in the PII images is done through summation of all the digits in this key. That summation is the row index of PII image and column index is calculated by subtraction of a predefined value from row index.

```
% Conversion of PWD, EDK and Time combination to index number of the PII images
sum1=0;
n = 0;
While (SLK/10^n) >= 1
n = n+1;
end
for i = 1: n
k = SLK - floor (SLK/10^i)*10^i;
SLK = SLK - k;
m (i) = floor (k/10^(i-1));
end
Index=sum (m);
Indey=index-30;
```

3.4 PERSONAL IMAGE IDENTIFICATION(PII)

This is an innovative process to add one more tier for security. The bidder will be identified when he enters correct login password. In addition to this classical method for security some images are also presented in front of him and he has to select three images on after other in same order from those images. During bid opening the same images in same order are to be selected by the bidder to open the bid. Any person knowing the password will not be able to get the bid since he will never know which images were selected by the bidder. The passwords have to be stored somewhere in database but there is common set of images for all the bidders and only choice is to be made. No indication regarding the choice is stored anywhere.

3.5 PSEUDORANDOM SEED

Pseudorandom number generator is used to generate the random sequences. These sequences are not completely random. The same PN sequences can be regenerate dif the seed given to the PN generator function is same. This seed is created using the selected intensities value from the PII images. The random number generator is reset using this seed. The random values generated in an order are always same whenever the generator is reset with the same seed. This brings a dependence of the random values on the bidder selection during Personal image identification.

3.6 USER DEPENDENT KEY

These are the values that are decided from the user information. The user selects images through PII method. The seed for the PN generator is created by selection of specific intensities. This is one of the random values generated from random number generator using PII intensity selection as seed.

```
% Generation of user dependent keys to embed the binary of the bidding amount this are the values to be substituted in place of the current intensity value
UDK0=randi (128, 1);
UDK1=randi (128, 1) +127;
```

3.7 INSERTION GUIDANCE SEQUENCE

This is a pseudorandom sequence which guides the embedding of the secret information inside the video frame. It is used to locate the pixel for embedding of the UDK0 and UDK1 in the video frame selected by the incremental sequence. Any pixel in the range of maximum row and column number can be selected.

```
% Insertion Guidance sequence generation which will be used for insertion at different frames
for i=1: nframes
IGS (i, 1) =randi (row,1);
end
for i=1: nframes
IGS (i, 2) =randi (col, 1);
End
```

3.8 INCREMENTAL FRAME SEQUENCE

This is the sequence which is created using the seed and used to select the proper frame for the insertion of the secret information. It will have values 1, 2 or 3 which will be used as increment for the frame number. If the current frame of insertion is 11 and IFS value is 2 at that index, then next insertion frame will be 11+2=13.

```
incr = randi (3, 1, secretinflen);
```

3.9 VIDEO STEGANOGRAPHY

Steganography deals with studying the collection of techniques aimed to embed sensitive information into another file. By doing this, information is passed in ordinance of third parties without being noticed and can only be retrieved by a legitimate user who knows a specific algorithm to extract it. We are using an adaptive yet user dependent novel algorithm for video steganography that will embed the secret bidding information inside the video frames. The algorithm replaces the intensity values at the locations determined by the insertion guidance sequence (IGS). The IGS gives the row and column values for inserting the user dependent keys (UDK). The secret key is scanned bit by bit and the frame to insert that bit is selected through incremental frame sequence (IFS). In the selected frame the embedding locations are decided by IGS. At those locations UDK1 or UDK0 are replaced according to the bit value of the secret information. Mathematical details of this algorithm are given in algorithm section.

3.10 TAMPER PROTECTION SEAL

The tendering process cannot be completed without proper sealing of the quotation envelope. Digital method for tendering should also have a digital seal procedure. This is done through cyclic redundancy check of the video frames. If any tampering of the video file is done it must be rejected and its backup copy from the central sever should be used then. The CRC process is very time consuming and mathematically complex. So CRC of whole frame is not done to save time. The new information added in the frame is dependent on IGS and IFS. So CRC of only those pixels is done which have been updated due to embedding.

This saves much time with the needed security. If any tampering with the pixels that were having info is done the CRC fails and the video rejected. If any other part of the video is modified then there is no problem. So the CRC method proposed is accurate and efficient.

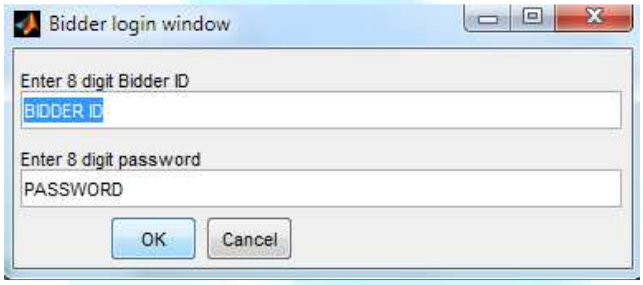
```
for mm=1: secretinflen
if embed (mm) =='1'
crcseq1(mm)=mov(jj).cdata(IGS(mm,1),IGS(mm,2),1);
else
crcseq1(mm)=mov(jj).cdata(IGS(mm,1),IGS(mm,2),1);
end
jj=jj+incr (mm);
if jj>nframes
jj=1;
end
end
% Generating Cyclic redundancy check sequence
bincrc1=de2bi (crcseq1, 8,'left-msb')';
ID=str2double (answer1 (1, :));
hexid=dec2hex (ID, 8);
hexid = strcat ('0x', hexid);
% Create a CRC-16 CRC generator, then use it to generate a checksum for the binary vector represented by the ASCII sequence '123456789'.
gen = crc.generator ('Polynomial', hexid,'ReflectInput', true, 'ReflectRemainder', true);
```

4. SIMULATION RESULTS

4.1 BIDDER ID AND PASSWORD INPUT

Following figure gives an input dialog where two values bidder id and password can be entered both during fling and opening of tender.

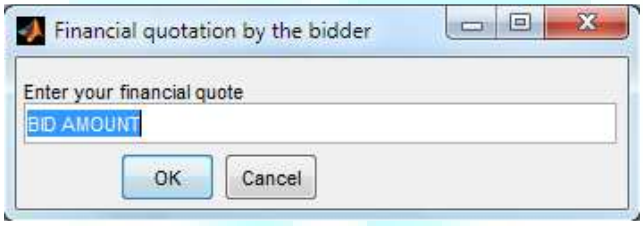
FIGURE 1: BIDDER ID AND PASSWORD INPUT FOR AUTHENTICATION



4.2 BIDDING AMOUNT INPUT

This input window will appear during tender filing process only. There is no requirement during tender opening process. The bidding amount can be entered here.

FIGURE 2: BIDDING AMOUNT INPUT



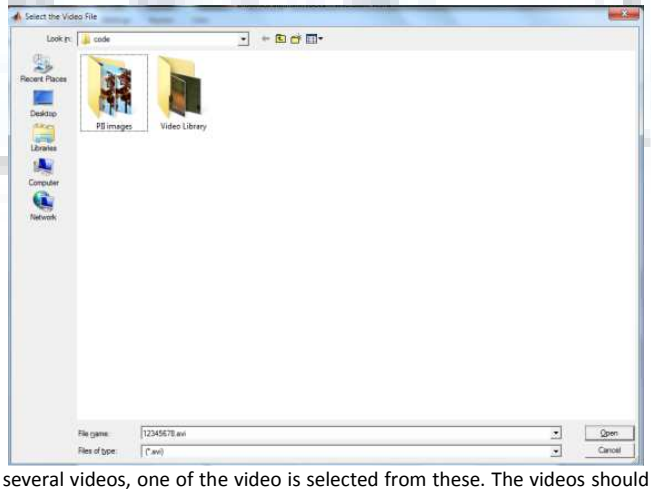
There is no minimum or maximum limit over this amount, but this limit can be decided by the tenderer.

4.3 TENDERING PROCESS

4.3.1 Digital envelope selection

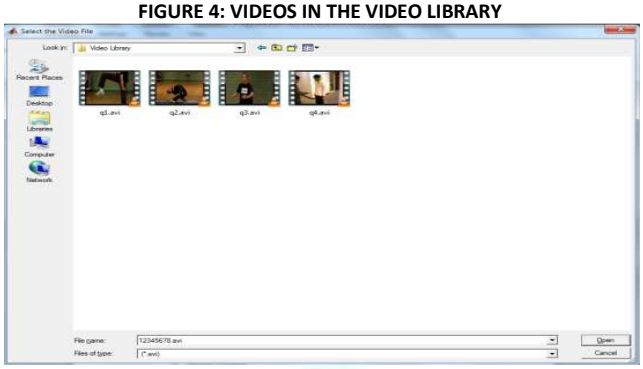
Video selection is done using this window that will be an envelope for the secret data. There is a rich library of the videos and can be changed regularly for new tenders. A bidder will select one of the video from these and the entered amount will be embedded into this video using the proposed algorithm.

FIGURE 3: VIDEO LIBRARY AND PII IMAGE LIBRARY



When the main folder is opened there are several videos, one of the video is selected from these. The videos should not have any significance from the tender point of view. They should not have any relevance to the field of tendering. They can be shared through a public sharing medium like YOUTUBE etc.

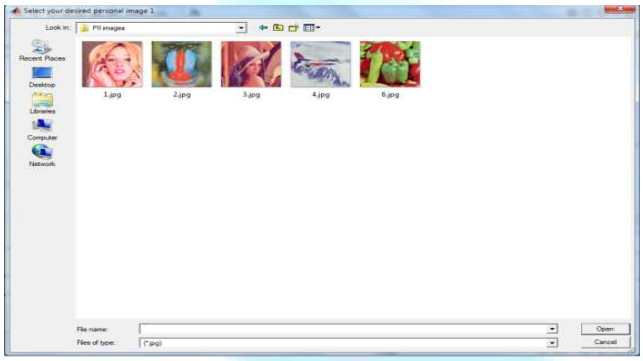
FIGURE 4: VIDEOS IN THE VIDEO LIBRARY



4.3.2 PII Image Selection

In this step the bidder has to select some images from the available PII images. The images are selected one by one. The same image can be selected any number of times. But the order of the images is to be remembered during registration since the same order is to be followed during tender opening process. So the bidder has to remember which images were selected and also the order in which the images were selected to extract the bid amount from the video envelope.

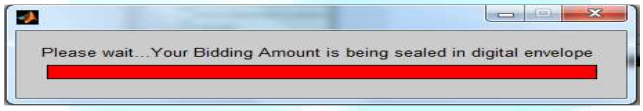
FIGURE 5: PERSONAL IMAGE SELECTION



4.4 DIGITAL SEAL GENERATION

The following figure shows the progress of the embedding process of the bidding amount in the digital envelope.

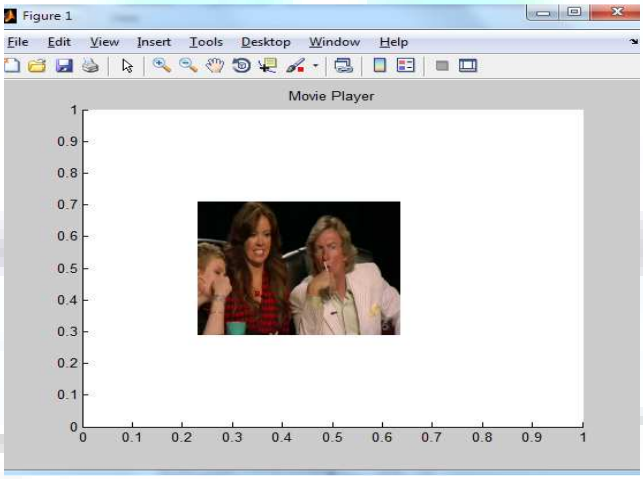
FIGURE 6: PROGRESS OF THE BIDDING AMOUNT INSERTION



4.5 VIDEO PLAYBACK

Once the secret information has been embedded in the video, the video can be displayed. The video can be seen to have no changes due to embedding.

FIGURE 7: VIDEO PLAYBACK



4.6 QUALITY CONTROL

The quality of the video embedded should not have enough visible noise. The noise level can be measured by PSNR and histogram comparison between the original and embedded frame.

4.6.1 PSNR

Since very small number of pixels has been disturbed it does not lead to any visible difference in the video. This disturbance can be quantified using the PSNR metric which measuresthe embedded noise in one signal with respect to the original signal. Here embedded signal is our stego video and original signal is the video in which the embedding has been done.

We calculate the average PSNR of all the embedded frames with their respective original frames. This average values for different videos have been checked and infinite value suggests that there is no visual noise in these two frames.

Peak Signal-to-Noise Ratio (PSNR) measures the quality of two images, the watermarked image and the original host image. The value of PSNR usually ranges from 20 dB (low quality) to 40 dB (high quality). PSNR is used to evaluate the difference between the watermarked image and the original image. The NC is applied to determine the degree of similarity between the original watermark and the extracted watermark. The PSNR and the NC are calculated as follows:

$$\text{PSNR} = 10\log_{10}\left(\frac{255^2}{\text{MSE}}\right)\text{dB}$$

$$\text{where MSE} = \frac{1}{A_p \times B_p}\sum_{I=0}^{A_p-1}\sum_{j=0}^{B_p-1}(X(i,j) - X_w(i,j))^2$$

Where, X and X_W are the original and watermarked images respectively of size A_p x B_p represent the height and width of the images. X'_W represents the extracted watermark.

The value of the PSNR between the original and the embedded video frames has been calculated and its value is coming Infinite. This means there is no visible difference in the video before and after embedding.

4.6.2 Histogram Comparison

Following histograms represents the frequencies of the various intensities in a randomly chosen frame before and after the embedding. There is no difference in the histograms. The peaks are same in both so a histogram comparison cannot predict that the data is contained in the video and our secret message is safe.

FIGURE 8: HISTOGRAM OF ONE ORIGINAL VIDEO FRAME

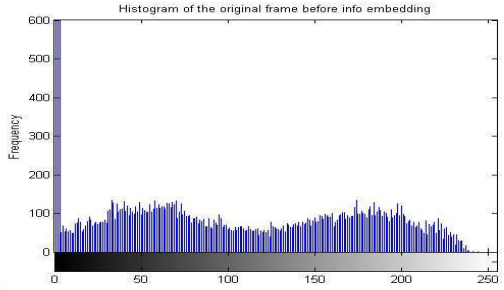
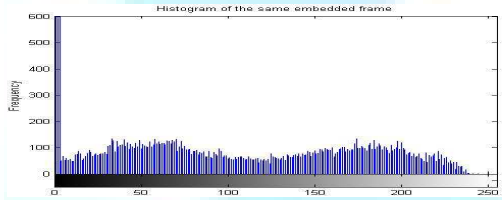


FIGURE 9: HISTOGRAM OF THE SAME EMBEDDED VIDEO FRAME



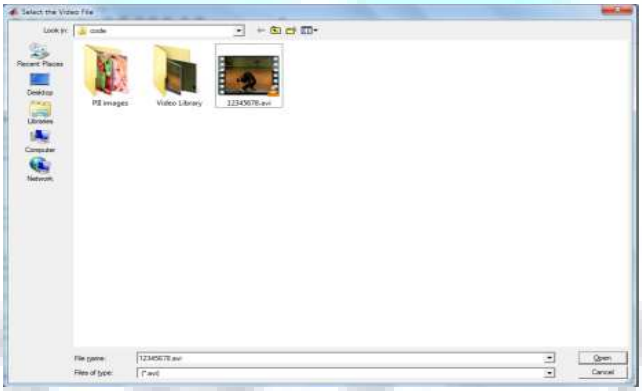
4.7 TENDER OPENING

Tender opening is reverse procedure of the tender filing process. In this process the bid amount is disclosed in presence of the bidder.

4.7.1 Envelope Input

The Bidding envelope is selected by the bidder which is identified by bidder ID.

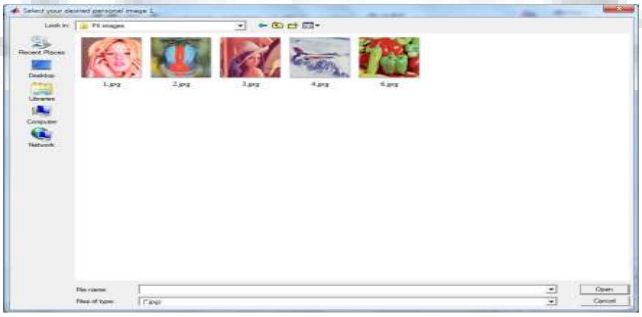
FIGURE 10: ENVELOPE INPUT



4.7.2 Personal image verification

The images from the selection pane are selected for personal image verification. The same images in same order are to be selected to extract the bidding information successfully.

FIGURE 11: PII IMAGES SELECTION FOR VERIFICATION



4.8 DIGITALLY SEALED ENVELOPE VERIFICATION

4.8.1 Successful Bidding Amount Display

If the PII images, password and EDK are same then the amount is successfully extracted from the sealed envelope. If the tampering protection is intact then only the bid amount is extracted from the video.

FIGURE 12: SUCCESSFUL EXTRACTION OF BID AMOUNT FROM THE ENVELOPE

```
Envelope is found digitally sealed and it is authentic bid

bidamt =

    36925814
```

4.8.2 Tampered

If tampering of the video files has been done then the tampering protection seal will be broken and CRC verification will fail. In this case the tender opening process will not progress and reject the video file, giving the error presented in following figure.

FIGURE 13: ERROR GENERATED DUE TO TAMPER PROTECTION SEAL FAILURE

```
Error using tenderopening (line 201)

CRC Check Failed cannot proceed futher, envelope tempering has been done
```

5 CONCLUSION

This scheme is novel in this area and has no algorithmic comparisons. The concept of digital video envelope, EDK, UDK and other secret keys is completely novel. We are also using framed video data hiding method so we have compared our results reported by some papers in this area. The results are very good as there is no visual change in the Stego video and the PSNR values are also coming infinite. The main idea to check the hidden bidding information i.e. histogram checking is also not able to detect the presence of the data. Extra involvement of tampering protection seal avoids any tampering of this video. This approach is successful landmark for data hiding in the videos for online tendering. We are planning in future to include some frequency domain transforms to make it comparable with other techniques in the frequency domain.

REFERENCES

1. Abdelwahab, A.A.; Hassaan, L.A., "A discrete wavelet transform based technique for image data hiding," *Radio Science Conference, 2008. NRSC 2008. National*, vol., no., pp.1,9, 18-20 March 2008
2. Ahmed A. Abdelwahab and Lobna A. Hassaan, "A Discrete Wavelet Transform Based Technique for Image Data hiding" IEEE 25th National Radio Science Conference,p.1-9, March 2008.
3. Anjali A.Shejul, U.L Kulkarni, "A DWT based approach for Steganography using Biometrics", IEEE International Conference on Data Storage and Data Engineering, pp.39-43, Feb.2010.
4. A. Joseph Raphael, V.Sundaram, "Cryptography and Steganography- A Survey", International Journal of Computer Applications in Technology, vol.2 (3), pp.626-630, May 2011.
5. A. Kumar, Km. Pooja, "Steganography- A Data Hiding Technique", International Journal of Computer Applications, vol. 9-No.-7, pp.19-23, November 2010.
6. A. Mishra , A. Gupta, D.K. Vishwakarma , "Proposal of a New Steganographic Approach", IEEE International Conference on Advances in Computing, Control, and Telecommunication Technologies, pp.175-178, December 2009.
7. A. Nag, S. Ghosh, S. Biswas, D. Sarkar, P. Pratim Sarkar, "An Image Steganography Technique using X-Box Mapping", IEEE-International Conference on Advances in Engineering, Science and Management, pp.709-713, March 2012.
8. Babu, K.S.; Raja, K.B.; Kiran, K.K.; Manjula Devi, T.H.; Venugopal, K.R.; Patnaik, L.M., "Authentication of secret information in image Steganography," *TENCON 2008 - 2008 IEEE Region 10 Conference* , vol., no., pp.1,6, 19-21 Nov. 2008
9. Balaji, R.; Naveen, G., "Secure data transmission using video Steganography," *Electro/Information Technology (EIT), 2011 IEEE International Conference on*, vol., no., pp.1, 5, 15-17 May 2011.
10. ChunyingGu; Xiaoli Cao, "Research on information hiding technology," *Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on*, vol., no., pp.2035, 2037, 21-23 April 2012.
11. D. Neeta, K. Snehal, "Implementation of LSB Steganography and Its Evaluation for Various Bits", IEEE 1st International Conference on Digital Information Management, pp.173-178, December 2006.
12. Dukhi, R.G., "Watermarking: A copyright protection tool," *Electronics Computer Technology (ICECT), 2011 3rd International Conference on*, vol.5, no., pp.36, 41, 8-10 April 2011.
13. Fabien A.P. Petitcolas, Ross J. Anderson and Markus G. Kuhn, "Information hiding- A Survey", Proceeding of IEEE, special issue on protection of Multimedia content , 87(7) pp.1062-1078, July 1999.
14. Min Liu, "Study of Digital Video Watermarking," *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on*, vol.2, no., pp.77, 80, 23-25 March 2012.
15. Mishra, A.; Gupta, A.; Vishwakarma, D. K., "Proposal of a new steganographic Approach," *Advances in Computing, Control, & Telecommunication Technologies, 2009. ACT '09. International Conference on* , vol., no., pp.175,178, 28-29 Dec. 2009.
16. M. Ram alingam, Stego Machine- "Stego Machine- Video Steganography using Modified LSB Algorithm", World Academy of Science, Engineering and Technology, pp.502-505, 2011.
17. Nag, A.; Ghosh, S.; Biswas, S.; Sarkar, D.; Sarkar, P.P., "An image steganography technique using X-box mapping," Advances in Engineering, Science and Management (ICAESM), 2012 International Conference on , vol., no., pp.709,713, 30-31 March 2012.
18. Neeta, D.; Snehal, K.; Jacobs, D., "Implementation of LSB Steganography and Its Evaluation for Various Bits," Digital Information Management, 2006 1st International Conference on, vol., no., pp.173, 178, 6-6 Dec. 2006.
19. Prabakaran. G, Bhavani. R, "A Modified Secure Digital Image Steganography Based on Discrete Wavelet Transform", IEEE International Conference on Computing, Electronics and Electrical Technologies , pp.1096-1100, March 2012.
20. R.Balaji ,G. Naveen , "Secure data Transmission using Video Steganography", IEEE International conference on Electro/Information Technology(EIT), pp.1-5, May 2011.
21. R. M. Goudar, S. J. Wagh, and M. D. Goudar. 2011. Secure data transmission using steganography based data hiding in TCP/IP. In Proceedings of the International Conference & Workshop on Emerging Trends in Technology (ICWET '11). ACM, New York, NY, USA, 974-979.
22. S. Tanako, K. Tanaka and T. Sugimura, "Data Hiding via Steganographic Image Transformation", IEICE Trans. Fundamentals, vol. E83-A, pp. 311-319, February, 2000.

23. Sirsendusarbavidya, Sunil Karforma, "UML implementation of E-Tendering using Secret Key Digital Watermarking", International Journal of Computer and Distributed System Volume: 1, Issue: 2, 72-75, 2012.
24. Shojanazeri, H.; Wan Adnan, W.A.; Ahmad, S.M.S.; Saripan, M.I., "Analysis of watermarking techniques in video," *Hybrid Intelligent Systems (HIS), 2011 11th International Conference on* , vol., no., pp.486,492, 5-8 Dec. 2011.
25. Xing Chang; Weilin Wang; Jianyu Zhao; Li Zhang, "A survey of digital video watermarking," *Natural Computation (ICNC), 2011 Seventh International Conference on* , vol.1, no., pp.61,65, 26-28 July 2011.
26. Wang Jue; Zhang Min-qing; Sun Juan-li, "Video steganography using motion vector components," *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on*, vol., no., pp.500, 503, 27-29 May 2011.

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 tosupply 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 youhave 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