BLUE EYES TECHNOLOGY

Swati

Assistant Professor, Dept of CS, C.R.M. JAT PG College

Hissar, Haryana (India)

ABSTRACT

The world of science cannot be measured in terms of development and progress. It has now reached to the technology known as "Blue eyes technology" that can sense and control human emotions and feelings through gadgets. The eyes, fingers, speech are the elements which help to sense the emotion level of human body. The basic idea behind this technology is to give the computer the human power. We all have some perceptual abilities. That is we can understand each other's feelings. For example we can understand ones emotional state by analyzing his facial expression. If we add these perceptual abilities of human to computers would enable computers to work together with human beings as intimate partners. The "BLUE EYES" technology aims at creating computational machines that have perceptual and sensory ability like those of human beings. This paper implements a new technique known as Emotion Sensory World of Blue eyes technology which identifies human emotions (sad.happy.exclted or surprised) using image processing techniques by extracting eye portion from the captured image which is then compared with stored images of data base.

Keywords : CSU (Central System Unit), DAU (Data Acquisition Unit) , Emotion Mouse, MAGIC (Manual And Gaze Input C), Simple User Interest Tracker (SUITOR).

I. INTRODUCTION

Imagine yourself in a world where humans interact with computers. It has the ability to gather information about you and interact with you through special techniques like facial recognition, speech recognition, etc. It can even understand your emotions at the touch of the mouse. It verifies your identity, feels your presents, and starts interacting with you .Human cognition depends primarily on the ability to perceive, interpret, and integrate audio-visuals and sensoring information. Adding extraordinary perceptual abilities to computers would enable computers to work together with human beings as intimate partners. Researchers are attempting to add more capabilities to computers that will allow them to interact like humans, recognize human presents, talk, listen, or even guess their feelings. The BLUE EYES technology aims at creating computational machines that have perceptual and sensory ability like those of human beings. It uses non-obtrusive sensing method, employing most modern video cameras and microphones to identify the user's actions through the use of imparted sensory abilities. The machine can understand what a user wants, where he is looking at, and even realize his physical or emotional states. The BLUE EYES technology aims at creating computational machines that have perceptual and sensory ability like those of human beings. It uses non-obtrusige sensing method, employing most modern video cameras and microphones to identifies the users actions through the use of imparted sensory abilities. The machine can understand what a user wants, where he is looking at, and even realize his physical or emotional states. In the name of BLUE EYES Blue in this term stands for Blue tooth (which enables wireless communication) and eyes because eye movement enables us to obtain a lot of interesting and information. Blue

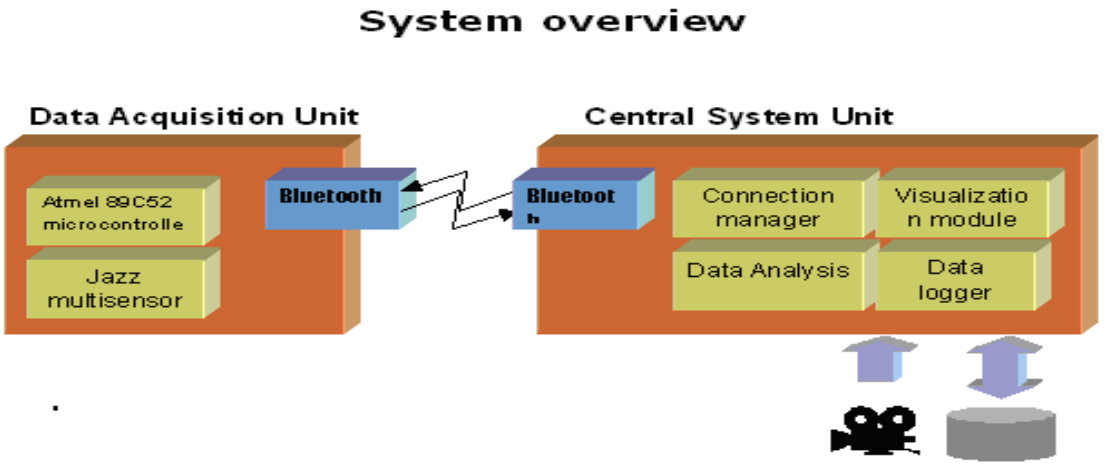
Eyes system consists of a mobile measuring device and a central and a central analytical system. The mobile device is integrated with Bluetooth module providing wireless interface between sensors worn by the operator and the central unit. ID cards assigned to each of the operators and adequate user profiles on the central unit side provide necessary data personalization so the system consists of

1.1 Data Acquisition Unit

Data Acquisition Unit is a mobile part of the Blue eyes system. Its main task is to fetch the physiological data from the sensor and send it to the central system to be processed. Data Acquisition Unit are to maintain Bluetooth connections to get information from sensor and sending it

1.2 Centarl System Unit

CSU maintains other side of the Blue tooth connection, buffers incoming sensor data, performs online data analysis records conclusion for further exploration and provides visualization interface.



II. EMOTION COMPUTING

Rosalind Picard (1997) describes why emotions are important to the computing community. There are two aspects of affective computing: giving the computer the ability to detect emotions and giving the computer the ability to express emotions. Not only are emotions crucial for rational decision making, but emotion detection is an important step to an adaptive computer system. An important element of incorporating emotion into computing is for productivity for a computer user. A study (Dryer & Horowitz, 1997) has shown that people with personalities that are similar or complement each other collaborate well. For these reasons, it is important to develop computers which can work well with its user.

2.1 Theory

Based on Paul Ekman's facial expression work, we see a correlation between a person's emotional state and a person's physiological measurements. Selected works from Ekman and others on measuring facial behaviours describe Ekman's Facial Action Coding System . One of his experiments involved participants attached to devices to record certain measurements including pulse, galvanic skin response (GSR),temperature ,somatic movement and blood pressure. He then recorded the measurements as the participants were instructed to mimic facial expressions which corresponded to the six basic emotions. He defined the six basic emotions as anger, fear, sadness, disgust, joy and surprise.

2.2 Result

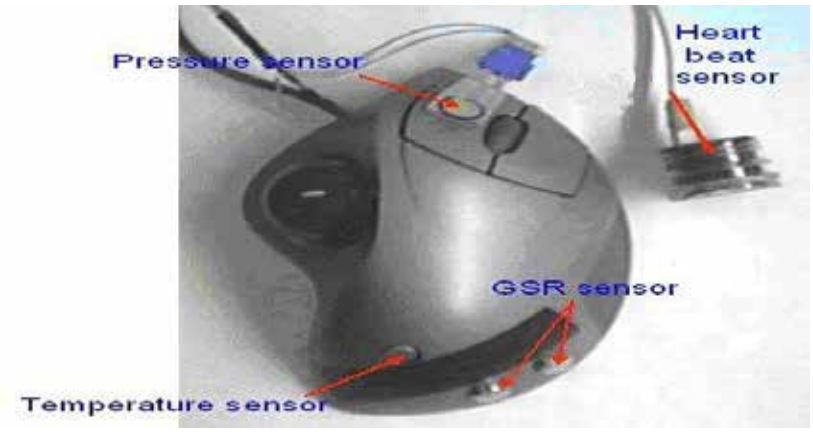
The data for each subject consisted of scores for four physiological assessments [GSA, GSR, pulse, and skin temperature, for each of the six emotions (anger, disgust, fear, happiness, sadness, and surprise)] across the five minute baseline and test sessions. GSA data was sampled 80 times per second, GSR and temperature were reported approximately 3-4 times per second and pulse was recorded as a beat was detected, approximately 1time per second. To account for individual variance in physiology, we calculated the difference between the baseline and test scores. Scores that differed by more than one and a half standard deviations from the mean were treated as missing. By this criterion, twelve score were removed from the analysis. The results show the theory behind the Emotion mouse work is fundamentally sound.

III. TYPES OF EMOTION SENSORS

3.1 For Hand

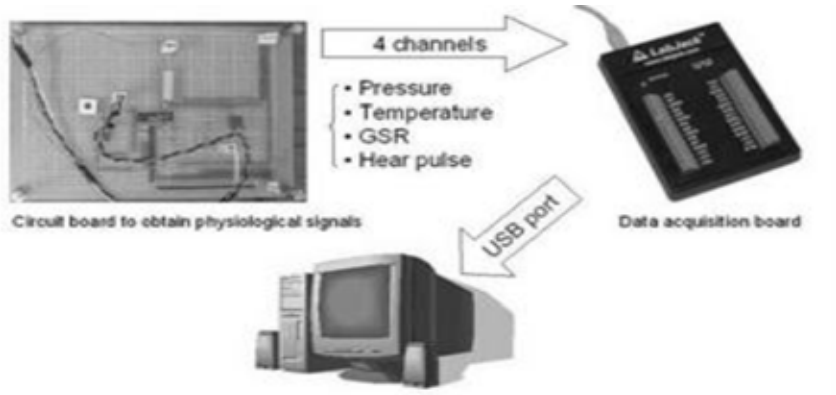
3.1.1 Emotion Mouse

One goal of human computer interaction (HCI) is to make an adaptive, smart computer system. This type of project could possibly include gesture recognition, facial recognition, eye tracking, speech recognition, etc.



Emotional Mouse

Another non-invasive way to obtain information about a person is through touch. People use their computers to obtain, store and manipulate data using their computer. In order to start creating smart computers, the computer must start gaining information about the user. Our proposed method for gaining user information through touch is via a computer input device, the mouse.



System Configuration for Emotional Mouse

From the physiological data obtained from the user, an emotional state may be determined which would then be related to the task the user is currently doing on the computer. Over a period of time, a user model will be built in order to gain a sense of the user's personality. The scope of the project is to have the computer adapt to the user in order to create a better working environment where the user is more productive.

3.1.2 Sentic Mouse

The Sentic Mouse is an experiment inspired by the work of Peter J. Lang, Ward Winton, Lois Putnam, Robert Kraus and Dr. Manfred Clynes, that provides a first step toward designing a tool to measure a subject's emotional valence response. The goal of the experiment is to begin to apply quantifying values to emotions and ultimately to build a predictive model for emotion theory. Peter J. Lang and others showed subjects a series of pictures and asked them to self-rate their emotional response. Dr. Manfred Clynes conducted a series of sentic experiments, gathering data from the vertical and horizontal components of

Sentic Mouse

finger pressure. Under the auspices of the Affective Computing research group, these three models were applied to the interaction between humans and computers. Using a computer to provide the affective stimulus to the human subject, an experiment was conducted which combined all three emotion studies. An ordinary computer mouse was augmented with a pressure sensor to collect sentic data as in Dr. Clynes experiments.The three measured results: sentic data, heart rate, and self-assessment, were then readily compared against each other as well as against the theoretically predicted results to assess the subject's emotional valence for each slide.

3.2. For Eyes

3.2.1 Expression Glasses

Expression Glasses provide a wearable "appliance-based" alternative to general-purpose machine vision face recognition systems. The glasses sense facial muscle movements, and use pattern recognition to identify meaningful expressions such as confusion or interest.

Expression Glasses

A prototype of the glasses has been built and evaluated. The prototype uses piezoelectric sensors hidden in a visor extension to a pair of glasses, providing for compactness, user control, and anonymity.

3.2.2 Manual and Gaze Input Cascaded (Magic) Pointing

We propose an alternative approach, dubbed MAGIC (Manual And Gaze Input C) as caded pointing. With such an approach, pointing appears to the user to be a manual task, used for fine manipulation and selection. However, a large portion of the cursor movement is eliminated by warping the cursor to the eye gaze area, which encompasses the target. Two specific MAGIC pointing techniques, one conservative and one liberal, were designed, analyzed, and implemented with an eye tracker we developed. They were then tested in a pilot study.

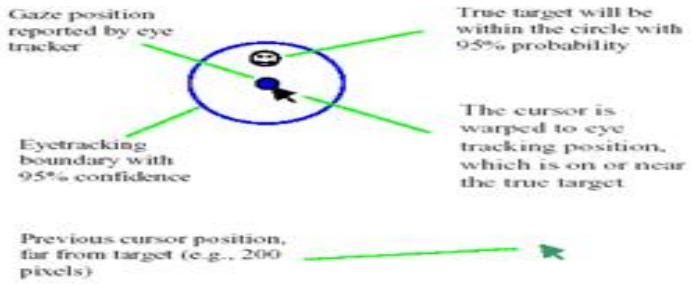


Figure 1. The liberal MAGIC pointing technique: cursor is placed in the vicinity of a target that the user fixates on.

The user can then take control of the cursor by hand near (or on) the target, or ignore it and search for the next target. Operationally, a new object is defined by sufficient distance (e.g., 120 pixels) from the current cursor position, unless the cursor is in a controlled motion by hand. Since there is a 120-pixel threshold, the cursor will not be warped when the user does continuous manipulation such as drawing. Note that this MAGIC pointing technique is different from traditional eye gaze control, where the user uses his eye to point at targets either without a cursor or with a cursor that constantly follows the jittery eye gaze motion. Once the manual input device has been actuated, the cursor is warped to the gaze area reported by the eye tracker. This area should be on or in the vicinity of the target.

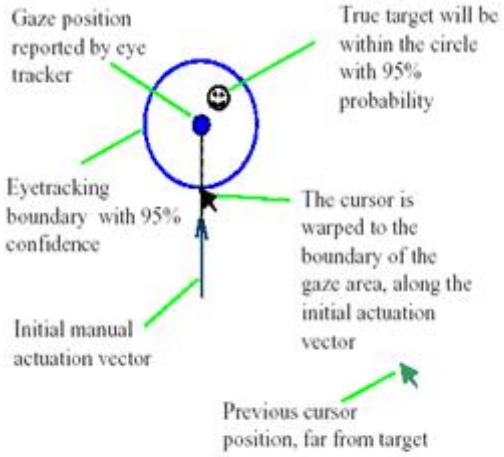


Figure 2. The conservative MAGIC pointing technique with "intelligent offset"

Both the liberal and the conservative MAGIC pointing techniques offer the following potential advantages

1. Reduction of manual stress and fatigue, since the cross screen long-distance cursor movement is eliminated from manual control.

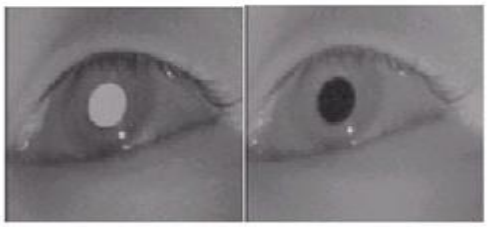
2. Practical accuracy level. In comparison to traditional pure gaze pointing whose accuracy is fundamentally limited by the nature of eye movement, the MAGIC pointing techniques let the hand complete the pointing task, so they can be as accurate as any other manual input techniques.

3. A more natural mental model for the user. The user does not have to be aware of the role of the eye gaze.

4. Speed. Since the need for large magnitude pointing operations is less than with pure manual cursor control, it is possible that MAGIC pointing will be faster than pure manual pointing.

3.2.3 The Ibm Almaden Eye Tracker

Since the goal of this work is to explore MAGIC pointing as a user interface technique,



Bright (left) and dark (right) pupil images resulting from on- and off-axis illumination. The glints, or corneal reflections, from the on- and off-axis light sources can be easily identified as the bright points in the iris.

When the light source is placed on-axis with the camera optical axis, the camera is able to detect the light reflected from the interior of the eye, and the image of the pupil appears bright . This effect is often seen as the red-eye in flash photographs when the flash is close to the camera lens. Bright (left) and dark (right) pupil images resulting from on- and off-axis illumination. The glints, or corneal reflections, from the on- and off-axis light sources can be easily identified as the bright points in the iris. The Almaden system uses two near infrared (IR) time multiplexed light sources, composed of two sets of IR LED's, which were synchronized with the camera frame rate. One light source is placed very close to the camera's optical axis and is synchronized with the even frames. Odd frames are synchronized with the second light source, positioned off axis. The two light sources are calibrated to provide approximately equivalent whole-scene illumination.

3.3. For Voice

3.3.1 Artificial Intelligent Speech Recognition

It is important to consider the environment in which the speech recognition system has to work. The grammar used by the speaker and accepted by the system, noise level, noise type, position of the microphone, and speed and manner of the user's speech are some factors that may affect the quality of speech recognition. The user speaks to the computer through a microphone, which, in used; a simple system may contain a minimum of three filters. The more the number of filters used, the higher the probability of accurate recognition. Presently, switched capacitor digital filters are used because these can be custom-built in integrated circuit form. These are smaller and cheaper than active filters using operational amplifiers. The filter output is then fed to the ADC to

translate the analogue signal into digital word. The ADC samples the filter outputs many times a second. Each sample represents different amplitude of the signal . Each value is then converted to a binary number proportional to the amplitude of the sample. A central processor unit (CPU) controls the input circuits that are fed by the ADCS. A large RAM (random access memory) stores all the digital values in a buffer area. This digital information, representing the spoken word, is now accessed by the CPU to process it further. The normal speech has a frequency range of 200 Hz to 7 kHz. Recognizing a telephone call is more difficult as it has bandwidth limitation of 300 Hz to3.3 kHz.

IV. THE SIMPLE USER INTEREST TRACKER (SUITOR)

Computers would have been much more powerful, had they gained perceptual and sensory abilities of the living beings on the earth. What needs to be developed is an intimate relationship between the computer and the humans. And the Simple User Interest Tracker (SUITOR) is a revolutionary approach in this direction. By observing the Webpage at netizen is browsing, the SUITOR can help by fetching more information at his desktop. By simply noticing where the user's eyes focus on the computer screen, the SUITOR can be more precise in determining his topic of interest. It can even deliver relevant information to a handheld device. IBM's Blue Eyes research project began with a simple question, according to Myron Flickner, a manager in Almaden's USER group: Can we exploit nonverbal cues to create more effective user interfaces? One such cue is gaze the direction in which a person is looking. Flickner and his colleagues have created some new techniques for tracking a person's eyes and have incorporated this gaze-tracking technology into two prototypes. One, called SUITOR (Simple User Interest Tracker), fills a scrolling ticker on a computer screen with information related to the user's current task. SUITOR knows where you are looking, what applications you are running, and what Web pages you may be browsing. "If I'm reading a Web page about IBM, for instance," says Paul Maglio, the Almaden cognitive scientist who invented SUITOR, "the system presents the latest stock price or business news stories that could affect IBM.

V. APPLICATIONS

The following are the applications of the Blue Eyes System.

1. At power point control rooms.
2. At Captain Bridges
3. At Flight Control Centers
4. Professional Drivers

VI. CONCLUSION

The Blue Eyes system is developed because of the need for a real-time monitoring system for a human operator. The approach is innovative since it helps supervise the operator not the process, as it is in presently available solutions. We hope the system in its commercial release will help avoid potential threats resulting from human errors, such as weariness, oversight, tiredness or temporal indisposition. The use of a miniature CMOS camera integrated into the eye movement sensor will enable the system to calculate the point of gaze and observe what the operator is actually looking at. Introducing voice recognition algorithm will facilitate the communication between the operator and the central system and simplify authorization process. Despite considering in the

report only the operators working in control rooms, our solution may well be applied to everyday life situations. These new possibilities can cover areas such as industry, transportation, military command centres or operation theatres. Researchers are attempting to add more capabilities to computers that will allow them to interact like humans, recognize human presents, talk, listen, or even guess their feelings. Blue Eyes emphasizes the foundations of the project – Bluetooth technology and the movements of the eyes. Bluetooth provides reliable wireless communication whereas the eye movements enable us to obtain a lot of interesting and important information.

REFERENCES

[1] Kenneth Holmqvist, Marcus Nyström, and Fiona Mulvey. Eye tracker data quality: what it is and how to measure it. In Proceedings of the Symposium on Eye Tracking Research and Applications, pages 45–52. ACM, 2012.

[2] Joseph j.carr & john m.brown, “introduction to blue eyes technology”,published in ieee spectrum magazine.II. A.jajszczyk, “automatically switched blue eyes networks :Benefits and Requirement,” IEEE blue toooth.feb 2005,vol 3,no1,pp.

[3] A .Banerje,, “Generalized multi protocol label switching: an over view of computer enhancements and recovery techniques “IEEE”commun. Magvol39.IV.J.jones,L.ong, and m.lazer,”creating and intelligent technology network/worldwide interoperability demonstration.”IEEE commun .mag.,vol 42.

[4] D. Watts, et al., "Implementing IBM Director 5.20. SG24- 6188", IBM Corp., April 2007.

[5] Microsoft Corp., "Microsoft System Management Server Planning Guide", 2008.

[6] C. Cook, et. al., "An Introduction to Tivoli Enterprise. SG24- 5494", IBM Corp”.

[7] HP, "HP Systems Insight Manager Technical Reference Guide", November 2005.

[8] F. Sacerdoti, et. al., "Wide Area Cluster Monitoring with Ganglia", IEEE Cluster 2003 Conference, Hong Kong, December 2003.

GALLIUM AND IRON-DOPED ZINC OXIDE THIN FILMS DEPOSITED BY PULSED LASER DEPOSITION TECHNIQUE: STRUCTURAL, OPTICAL AND MORPHOLOGICAL PROPERTIES

Karmvir Singh[1], Rakesh Dhar[2], Devendra Mohan[3]

[1,2,3] *Department of Applied Physics*

Guru Jambheshwar University of Science and Technology, Hisar, Haryana (India)

ABSTRACT

A 100 nm thick, undoped, 2 wt% gallium (Ga) and 2 wt% iron (Fe) doped zinc oxide (ZnO) thin films were deposited on glass substrates at substrate temperature of 450 ^{o}C by pulsed laser depositions technique. The structural and optical properties of the deposited films were studied by X-ray diffraction and UV-visible spectroscopic analysis. The Surface morphology of the deposited films were also investigated by atomic force microscopy (AFM). All the deposited thin films based on undoped ZnO, Ga-doped (GZO) and Fe-doped (FZO) show hexagonal wurtzite structure. The deposited films are maintaining more than 90% transmittance in entire visible range. The average grain size calculated from AFM analysis were found to be 106 nm, 52 nm and 359 nm for undoped ZnO, GZO, FZO films, respectively. The band gap values of the prepared thin films were found to be of 3.25 eV, 3.29 eV and 3.48 eV for undoped ZnO, GZO, FZO films, respectively.

Keywords: Optical Properties, Structural Properties, Transparent Conductive Oxide, Undoped and Doped Zno.

I. INTRODUCTION

Transparent conducting oxide (TCO) thin films such as (ZnO, SnO_2) are widely used in optoelectronic applications devices, such as panel displays, solar cells & sensors etc. Among the various TCOs, Indium-tin-oxide (ITO) films are used extensively on account of their high transmittance in the visible range and high electrical conductivity. Recently, ZnO films have attracted considerable attention as an alternative to ITO because of their excellent properties due to various doping, low cost and non-toxicity [1]. Zinc oxide (ZnO), which is one of the most important binary II-VI semiconductor compounds, has a hexagonal wurtzite structure, direct energy wide band gap of 3.37 eV at room temperature and a large exciton binding energy (approximately 60 meV) [2].ZnO thin films have been prepared by several methods such as molecular beam epitaxy [3], pulsed laser deposition [PLD] [4], sintering [5], chemical spray [6,7], r.f. magnetron sputtering [8], ion plating [9]and solid state reaction [10].Among them, PLD is very useful to grow high quality thin films. PLD is one of the better techniques to grow oxide films as well as to maintain the stoichiometry of the target into the film structure [11].In this paper we have studied, the structural, optical and morphological properties of gallium and iron doped zinc oxide thin films deposited on glass substrate by pulsed laser deposition technique[PLD].

II. EXPERIMENTAL DETAILS

The undoped ZnO (purity-99.5%), gallium doped ZnO (GZO) (purity99.9%), Iron (Fe) doped ZnO (FZO) (99.9%) thin films were deposited on1 cm×1cm glass substrates. All the targets were prepared by solid state reaction route. The targets were subjected to 6 M Pa pressure. These targets were sintered at 1150 ºC for 12 h.The target distance was to be fixed at 5 cm during deposition. The glass substrate was ultrasonically cleaned with acetone and methanol each for 5 minutes before loading in to the chamber. The vacuum was achieved $1\times10^{-6.}$ Torr with the help of rotary and turbomolecular pump. The undoped ZnO, GZO, FZO thin films were deposited at a fixed temperature at 450^{0}C.The KrF excimer (λ=248 nm, pulse duration of 30 ns, Laser repetition rate= 10 Hz) laser was to be set during the experiment. The oxygen partial pressure was mainted at 1×10^{-3} mTorr. The deposition time was fixed for 20 minutes for all the samples.The average thickness of the prepared samples was to be 100 nm. The Prepared thin films were characterized by X-ray diffraction (XRD), (Bruker D8 Advance) using a CuKα and a mono-chronmator having value 50 KV and 300 mA. Ambious Technology was used to measure the thickness of the thin films. The surface morphology where as of the thin films was studied by Atomic force microscopy (AFM). The optical transmission spectra of the thin films were recorded by using the instrument (Perkin Elmer Lambda 950) Spectrophotometer.

III. RESULTS AND DISCUSSION

3.1 Structural Properties

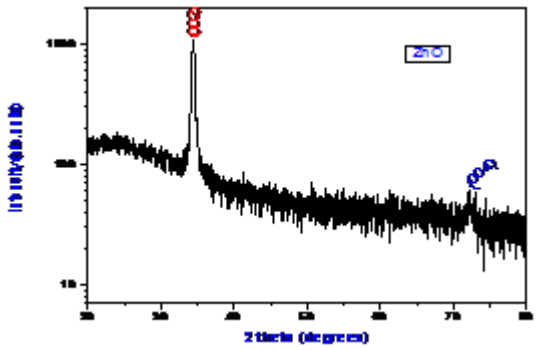


Fig.1. (A) Undoped Zno Thin Films.

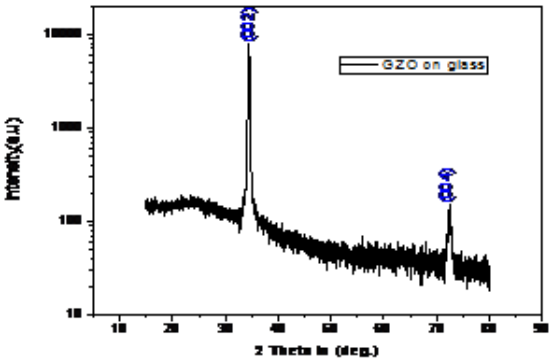


Fig.1 (B). Ga Doped Zno Thin Films.

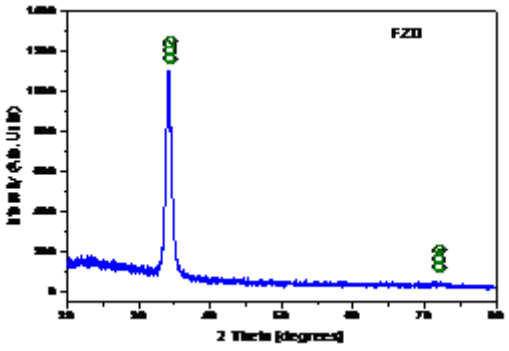


Fig.1(C). Fe Doped Zno Thin Film on Glass

Fig. 1. Xrd Patterns of (A) Undoped Zno (B) 2 Wt % GZO (C) 2wt % FZO Thin Films.

Fig.1 shows the crystal structural behavior of undoped ZnO,GZO,FZO thin films respectively. The XRD patterns of undoped and GZO thin films exhibited a strong reflection peaks having (002) plane or c-axis

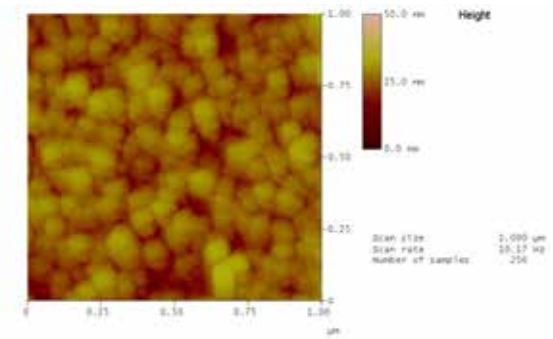
orientation, whereas there was no extra peak is observed in FZO thin film. The doping concentration was negligibly small, so the diffraction peaks corresponding to ga, fe ions were not observed. The positions of the diffraction peaks showed that all the films have a c-axis oriented behavior composed of hexagonal wurtzite stricture.

3.2 Surface Morphology

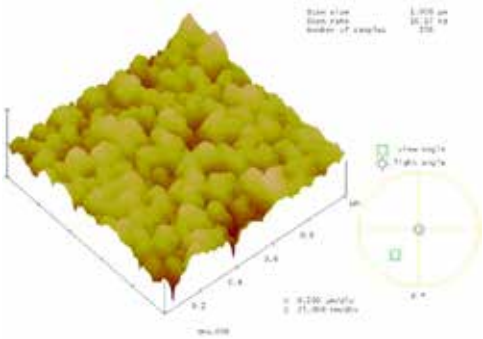
Fig.2 (a, b, c,) represents the AFM images undoped ZnO, Gallium doped ZnO (GZO), and Fe doped ZnO (FZO) thin films. Surface analysis of the samples were characterized by Atomic Force Microscopy in contact mode .The scan area was 2×2 μm during the AFM measurement. The average grain size was measured of undoped ZnO, GZO and FZO thin films was 106 nm for (ZnO), 52 nm for (GZO) 359 nm for (FZO) with the help AFM technology respectively. The surfaces of the undoped ZnO films shows the agglomeration of grains in 2(D),but in case of 3(D) some impurities are appearing in 3(D) when we doped the gallium atom in to the ZnO thin films the surface will be very smooth uniform surface which is very well matched with xrd data. The Fe doped ZnO (FZO) thin films also shows a very smooth and plane surface.

Table I. Shows The Surface Properties Of Undoped Zno, GZO, And FZO Respectively

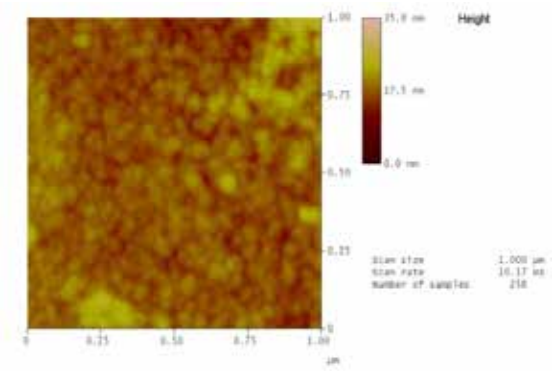
Sample Code	Grain size in nm	Sample Roughness
1.Undoped ZnO	106 nm	3.718 nm
2.GZO	52 nm	2.048 nm
3. FZO	359 nm	14.334 nm



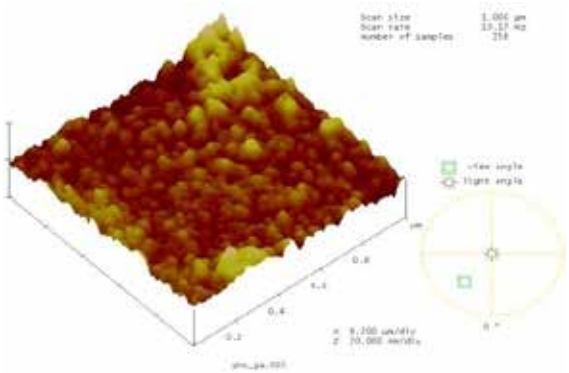
ZnO in 2(D).



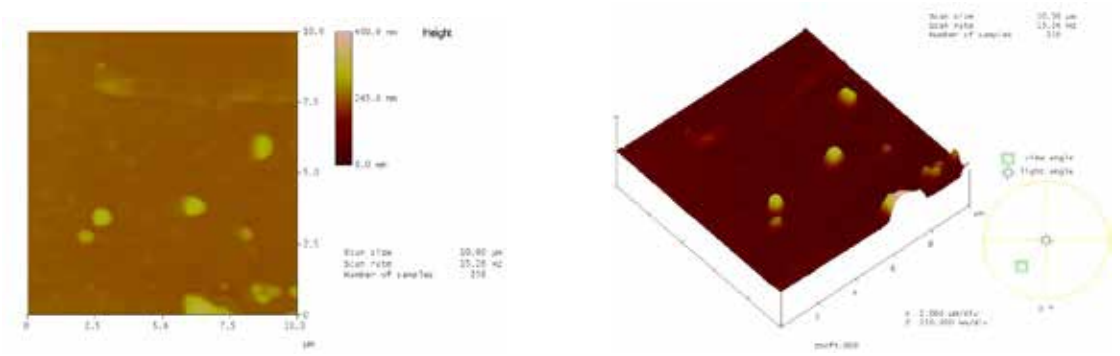
ZnO in 3(D)



ZnO ga in (2D)



ZnO ga in 3(D)



FZO in 2(D). **FZO in 3(D).**

Fig. 2.Shows AFM Images of Undoped Zno (A) 2 Wt % Ga Doped Zno (B), 2 Wt % Fe (C) Thin Films.

3.3 Optical Properties

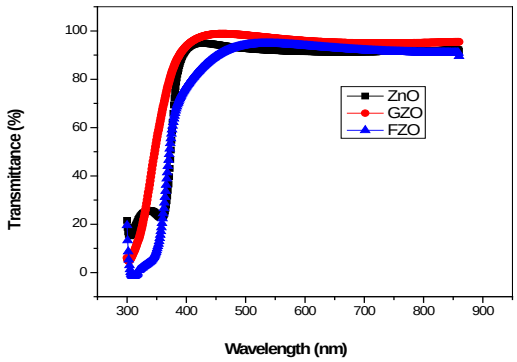
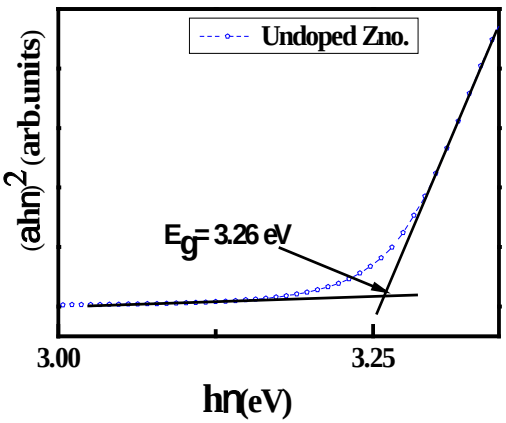


Fig.3 Shows the Optical Transmittance Spectra of Undoped Zno, 2wt% GZO And (C) 2 Wt% FZO Thin Films.

Fig.3 shows the optical transmittance spectra of the undoped ZnO, Ga doped ZnO, Fe doped ZnO thin films. All the samples have a transmittance over 70% which lies in the visible range. All the measurements were done at room temperature. The high transmission in the visible region is a very important factor in many applications (12). The Optical transmittance spectra were taken with the help of (Perkin Elmer USA Model Lambda: 950) by UV-Vis spectroscopy at room temperature. The wavelength was set between 300 nm to 1100 nm during measurement. The results show that the transmittance are varied for each samples having range 80% to 95 % in all thin films the optical transmittance of GZO 2 wt %, of Gallium in Zn0 is higher than that of two other samples. Theoretically the relationship between the absorption coefficient (α) and photon energy (*hν*) for direct transition as $(\alpha h\nu)^2 = (h\nu - Eg)$ where *Eg* is the optical energy band gap. This band gap can be estimated by extrapolation of the linear portion of an $(\alpha h\nu)^2$ vs *(hν)tau* plot as given in Figure 3(a,b,c) [13].

3.4 Optical Energy Band Gap

The optical energy band gap calculated for the undoped ZnO, gallium doped ZnO (GZO), Fe doped ZnO (FZO) thin films was 3.25 eV,3.29 eV,3.48 eV respectively.



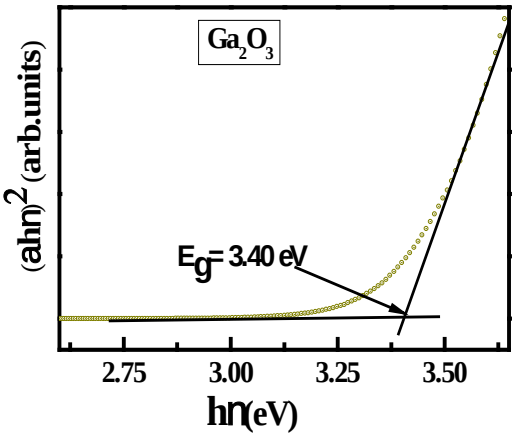


Fig. 4 (a) Measurement of Optical Energy Band Gap of ZnO Thin Films is (3.25 eV).

Fig.4(b). Measurement of 2 wt % Optical Band Gap of Gallium Doped ZnO Thin Films (3.48 eV).

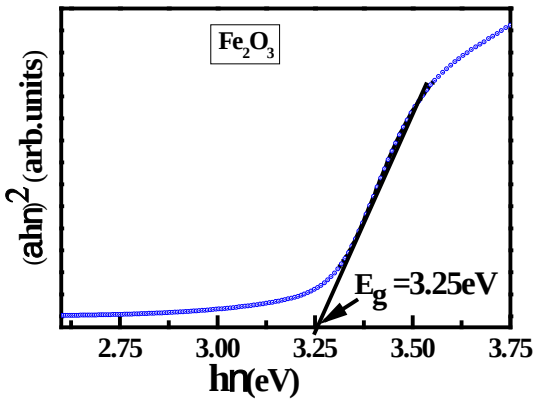


Fig. 4(C). Measurement of Optical Band Gap Of 2 Wt% Fe Doped Zno Thin Films (3.29 Ev).

Table 2: The Optical Band Gap was to be Calculated Using Tauc's Plot are Given Below.

Sample Code	Optical transmittance	Optical energy Band gap.
ZnO	98 %	3.25 eV
GZO	94 %	3.48 eV
FZO	94.94 %	3.25eV

IV. CONCLUSIONS

We have successfully prepared the undoped, Ga doped ZnO, and Fe doped ZnO thin films prepared by pulsed laser deposition technique. All the samples have approximately the same thickness of 100 nm and the same substrates temperature (450^0C).The c-axis orientation was developed in the case of GZO thin films, but the c-axis orientation was inhibited when doping ZnO with Fe. The Ga and Fe ions acted as inhibitors for suppressing

the grain growth of ZnO. The average grain size of ZnO from AFM image analysis indicate decreased from 101 nm to 50 and 25 nm when ZnO was doped with 2wt% Ga and 2 wt% Fe respectively. All thin films gave a transmittance over 80 % in the visible region and band gap values of undoped ZnO, GZO and FZO thin films come out to be 2.75eV, 2.5eV and 2.61 eV, respectively.

V. ACKNOWLEDGEMENTS

The authors are very thankful to UGC-DAE Indore for various characterization and synthesis support. In particular acknowledge the help rendered by Dr. R.J. Chaudhary (scientist D) at UGC-DAE consortium of scientific research Indore. I am also thankful to Dr. Rajesh punia and Dr. Amit yadav for helpful guidance. One of the author karmvir singh is thankful to UGC for financial help in the form of UGC-BSR fellowship.

REFERENCES

[1.] Sang Eun Park, Jung Chul Lee, Pung Keun Song, Journal of the Korean Physical Society, Vol. 54, No. 3, March 2009, pp. 1283~1287.

[2.] Said Benramache, Boubaker Benhaoua and Hamza Bentrah, Journal Of Nanostructure in Chemistry 2013, 3:54

[3] Mandalapu L J, Xiu F X, Yang Z and Liu J L 2007 Solid State Electron.51 1014–7

[4] Yamada T, Nebiki T, Kishimoto S, Makino H, Awai K, Narusawa T and Yamamoto T 2007 Superlatt.Microstruct.42 68–73

[5] Ma Q B, Ye Z Z, He H P, Zhu L P, Wang J R and Zhao B H 2007 Mater ,Lett.61 2460-3.

[6] Kishimoto S, Hayashi K, Hamaguchi H, Makino H, Yamada T, AQ4 Miyake A and Yamamoto T 2007 Phys. Status Solidi b 244 1483–9

[7] Gomez H and Olvera M de la L 2006 Mater. Sci.Eng.B134 20–6 AQ5

[8] Park S M, Ikegami T, Ebihara K and Shin P K 2006 Appl. Surf.Sci. 253 1522–7

[9] Osada M, Sakemi T and Yamamoto T 2006Thin Solid Films 494 38–41

[10] Yamamoto T, Sakemi T, Awai K and Shirakata S2004 Thin Solid Films 451-452 439-44.

[11]. S. Karamata, R.S. Rawata, T.L. Tana, P. Leea, S.V. Springhama, E. Ghareshabania,b, R. Chenc, H.D. Sunc Applied Surface Science 257 (2011) 1979–1985.

[12]. Sumetha Suwanboon, Tanattha Ratana and Thanakorn Ratana, walailak J Sci& Tech 2007; 4(1); 111-121.

[13]. R N Gayen, K Sarkar, S Hussain, R Bhar & A K Pal Indian Journal of Pure & Applied Physics Vol. 49, July 2011, pp. 470-477.

TECHNOLOGY AFFLUENCE IN MANUFACTURING INFORMATION SYSTEM

Reepu

Department of Management, Punjab Institute of Technology, Nandgarh, Punjab (India)

ABSTRACT

Technology has tremendous influence in almost every field of work. Its hoofmarks also exists across the trails of manufacturing as they have made entire processes more subtle by reducing costs, incorporating more flexibility into the operation, thereby causing products to be consistently qualitative and hence an improved one. Information Systems of manufacturing rely on the process types used in an organization. A varied range of sources are also important as they will only supplement the organization with informative inputs. Technological implications have reformed the entire manufacturing operation by the introduction of Material Requirement planning, Manufacturing Resource Planning, Enterprise Resource Planning and Enterprise Asset Management for a complete solution.

Keywords: Enterprise Asset Management, Enterprise Resource Planning, Manufacturing Resource Planning, Material Requirement Planning, Technology etc

I. INTRODUCTION

Manufacturing operations now-a-days is engrossed with multi-faceted techniques like Just in Time, Manufacturing Resource Planning etc. Development of such innumerable techniques demands the manifestation of more technological components which can lead to quicker, accurate, customer - desired results. So, a Manufacturing Information System has been engraved which support information about all from scratch to the final dealing.

Sources: Information about manufacturing is collected from various viable sources like:

Both Macro and Micro environment have a significant influence over the operations of an organization. Adequate referrals to newspapers, magazines, government reports, journals etc must be made for knowledge acquisition. Workstations on the production floor enable one to gather data about the utilised production processes. Inventory related information is also important for billing as well as for continuation of production processes. Information about vendor would facilitate information regarding the quality, quantity, price, available quantity etc. Statistical data about personnel would equip about workable force on the shop. Entire set of operation managed completely under unionised members must be kept under a close vigilance. Engineering handbooks also provide detailed specifications of the various tools and equipments utilised.

II. REVIEW OF LITERATURE

Song L, et al (1997) formulated a framework using Object Oriented Methodology as they believed that agile manufacturing exists due to the development of virtual enterprise structures, enabling companies to transact well. Entire work is co-ordinated by Workflow Managers using Client Server model. Irani Z, et al (2001)

researched about the implementation issues in context to a case study company. They have well analyzed the positioning of the firm and the usage of technological as well as human resource component towards Manufacturing Information System. Mclaren T.S., et al (2004) proposed that organizational capabilities when coaxed with Supply Chain Manufacturing Information System yielded high operational capability as well as flexibility. Overall efficiency was also improved. Sharma M.K., et al (2005) analysed the usage of Information System among 210 SMEs operational in Western part of India by conducting an exploratory study and found several issues like real time data transfer, integration, information sharing, connectivity etc. Chituc C-M, et al, (2009) highlighted about the architecture, performance and implementation of a manufacturing engineering system with the concurrent usage of wise information and communication technology.

III. BUILDING BLOCKS

Production undergoes a series of phases beginning from production scheduling to actual production and hence preparing reports about inventory levels. Hence, the process types in the organization forms the building block of Manufacturing Information System.

There may be project processes apposite with projects of desired characteristics but normally manufactured in low volume. There may not be a complete description of the array of activities, but the time involved is normally huge. Examples of such a process include oil drilling processes etc. Jobbing processes, on the other hand, utilises shared resources to manufacture entire product line. Such processes are oriented to develop those products which would satisfy the needs of few, as products are normally produced in low volume. Batch processes alike to jobbing, however do not offer assorted products as the production is run in a batch. Products undergo a similar process. Mass processes tend to produce less variety of goods but the production is done in masses. For example a water bottling plant etc. Continuous processes ahead of plot of mass production, produces low variety products in a continuous stream flow but manufactures in huge amount. Characterised with rigid processes, a plant utilizing such process manufactures continuously and hence requires huge capital.

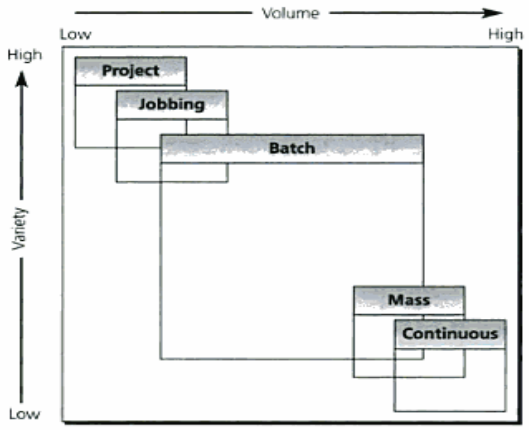


Fig.1 Product Process Paradigm [Source: Mike Pycraft]

In context to service organizations, professional services are offered. Such services render customers with customizable offerings. With great zeal attempt is made to maintain services at both front line and backend. It is a people oriented mechanism, with greater emphasis on mainstream process in order to deliver a qualitative service. Service shops lie amid of the continuum of professional and mass services. It presents assortment of product and service outlook so consequential support to both front end and back end for the entire system set up

is crucial. While mass services presume modest customer interactions as back end support is considered to be more important. Hence, more effort is made towards the development of decisive elements which may drive away the entire process. Examples include railway network etc.

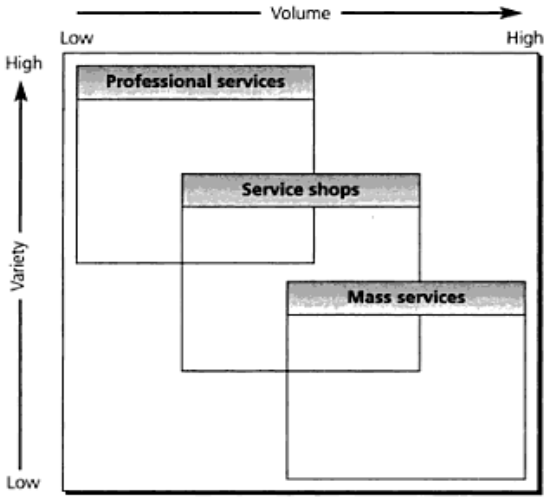


Fig.2 Service Process Paradigm [Source: Mike Pycraft]

IV. TECHNOLOGICAL AFFLUENCE IN MANUFACTURING

Technological impact can be clearly embossed over the entire manufacturing process.

§ Material Requirement Planning

The underlying principle of MRP is to ascertain the requirements of desired product characteristics and hence planning over it. A clear elucidation of the type, quantity, quality of material is made and hence the emphasis is laid upon procuring of the material. MRP certainly reduce the inbound manual calculations recognised as complex due to continuous environmental impact. MRP requires access to the various inventory records, set of bill receipts and even master production schedule. These three enable a firm to form a concrete plan about required quantities, their acquisition time period and even utilisation dates for the production and due dates (if any). With the passage of time MRP has evolved into Manufacturing Resource Planning II.

Oliver Weight propounded that a careful consideration of not only the material oriented planning is crucial, entire resources need to be carefully planned. Hence MRP2 formed modules for procurement, data collection related to production and alike, capacity planning, sales and deliberate attempt towards cost reduction is also made.

§ Enterprise Resource Planning

To drive customer with better results a supple system named as ERP has been introduced. ERP integrated the different modules of customer, supplier and manufacturing so as to yield customer better deliverables. Databases are coalesced and common terms with same meanings are also introduced. Interfaces for similar functioning are even identical. Business processes are analysed using client system architecture. Maintenance of such alike structures was also economical.

Usage of ERP has introduced businesses with several benefits.

§ The cycle time with the usage of ERP has reduced drastically.

§ With the usage of common data elements across multiple platforms having similar functionalities the time and cost has also diminished.

- The increased costs of inventory management have further lessened.
- Web enabled interfaces enables management of resources, customers and financial over-dues with an ease.
- Information can be easily accessed over different mediums.
- Communication channels become wide open over horizontal and vertical forums.
- Customer can be serviced better due to rapid response time.
- Due to frequent availability of data, inventory replenishment becomes a matter of few seconds. Hence, even order can be placed with suppliers swiftly.
- Interactions across the network hence became easier and that too with less of operating costs.
- Products are even delivered on time.

A company may orderly manage Customer, Supplier and Inventory modules through ERP, but for an absolute management across the organization, maintenance is also crucial which can be achieved with the help of Enterprise Asset Management (EAP).

EAP originates as a consequence of the maintenance operations of ERP. Majority of activities in case of an ERP can be well planned but maintenance can never be planned well before. The various sub activities in case of EAM involves the scheduling of the various maintenance operations and even the after math management of various financial and human activities.

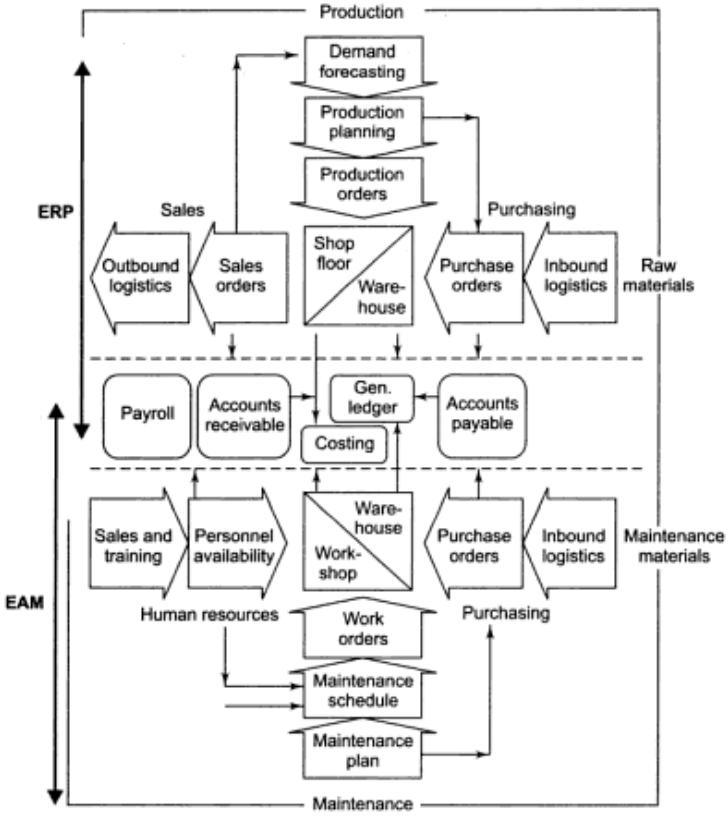


Fig. 3 ERP and EAM Constituents [Source: Mahadeo]

V. CONCLUSION

Several organizations rely on MIS like MRP, MRP II, ERP and EAM. Such systems enable tracking the progress of manufacturing processes with an ease. Their underlying mechanism have proved to be more constructive as the cycle time, process time, operational costs etc all have narrowed down to a greater extent, but

organization must keep a close vigilance on the sources upon which the entire Manufacturing Information System is dependent upon because correct feed in of the data will generate better outcomes for the organization, enabling them to achieve their objectives.

REFERENCES

[1] Song L., et al, Design and Implementation of Virtual Information System for Agile Manufacturing, IIE Transactions on Design and Manufacturing, special issue on Agile Manufacturing, Vol.29 (10), pp. 839-857, 1997.

[2] Irani Z., et al, Transforming Failure into Success through Organizational Learning: An Analysis of Manufacturing Information System, European Journal of Information Systems, 10, 55-56, 2001.

[3] Mc Laren T.S., et al, Supply Chain Management Information Systems Capabilities: An exploratory study of electronics manufacturers, Information Systems and eBusiness Management, Vol. 2, Issue 2, pp 207-222, July 2004.

[4] Sharma M.K., et al, Practice of Information Systems, Evidence from select Indian SMEs, Journal of Manufacturing Technology Management, Vol. 17, No.2, pp 199-223, 2005.

Proceeding Papers

[5] Chituc C.M., et al, Challenges and Trends in Distributed Manufacturing Systems: Are wise engineering systems the ultimate answer?, Second International Symposium on Engineering Systems MIT, 2009.

 ISBN: 978-81-931039-3-7

MARKETING DECISION SUPPORT SYSTEM

Reepu

Department of Management, Punjab Institute of Technology, Nandgarh, Punjab (India)

ABSTRACT

Every organization resides in turbulent economy. Pressures of tax, cost, competition, human and financial challenges besieges around it. Now-a-days the emerging trends of Liberalisation Privatization Globalization have fuelled even more competition in the sector. Therefore, they need to carefully plan and execute its different components to gain a competitive edge. Marketing Management Support System is an advocate of organizational performance consistency and has numerous constituents. Marketing Decision Support System (MDSS), an element of it, if properly executed becomes a source of exemplary performance. The present paper is an attempt to completely acquaint about Marketing Decision Support System, its elements, characteristics, implementation, usage and even the associated risks of it. This paper enables to acclimatize about the different facets of MDSS.

Keywords: Characteristics, Elements, Implementation, MDSS, Risks, Usage etc

I. INTRODUCTION

In earlier time period, Marketing Managers in Western companies often require factual information, which means data availability as well as accuracy has been an utmost concern for them. This led to the creation of Marketing Decision Support System. This system comprises of marketing oriented information, its analysis and associated marketing reports for effectual decision making. Marketing Decision Support Systems are decentralized in nature i.e. managers can easily access the data anywhere so as to furnish organization in achieving their objectives.

Marketing Management Support System, a system supporting the infrastructure of IT, with detailed analysis of the marketing related data, is a reservoir of marketing based knowledge. A Marketing decision support system also forms one of the subset of Marketing Management Support System as delineated:

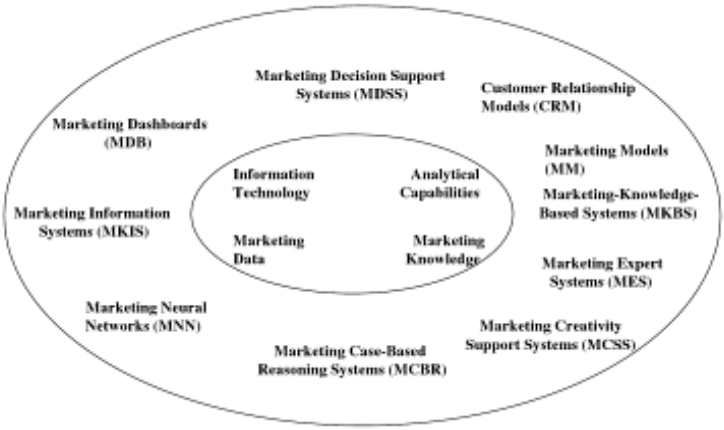


Fig.1 Types of Marketing Management Support System [Source: Bruggen G.H.V.]

II. REVIEW OF LITERATURE

Wierenga B. et al (1997) identified that external environmental factors, organizational factors, task environment factors, user factors and implementation factors have profound impact. Adoption and Usage rate have been found to be more in case of Consumer goods companies rather than companies dealing in business-to-business sector. Stern D. (2003) researched that Marketing Decision Support System have been extensively utilized by several organizations, but still there underlies a resilience towards its full implementation. Research showed lack of understanding for which the researcher has instituted several educational programmes which may enable a Manager to forecast well. Baggio R. Et al (2005) highlighted the impact of Decision Support System over the tourism industry. Key developmental framework which presented a combined purview of distributed knowledge, data and model bases have been outlined. Grubor A. (2009) believed that global marketing environment has also become crucial for an organization. According to him any company can be well managed if the assessment made for the organization is just not only analysed for domestic operation , but also viewed in light of global domain. Bhatia A (2011) focussed on the determination of several parameters for the development of a DSS framework in case of banking sector by relying upon the data collected from the respondents of branches, regional, zonal and head office of State Bank of Patiala.

III. ELEMENTS OF MDSS

The viable immediate external and internal environment has always huge impact on the decision making of the organization. MDSS too has been vulnerable to it. An organization should develop a database for both internal as well as external environment. Data retrieval from different sources, level of information to be upheld and scope of coverage are decisive factors for the creation database. A standardised set of organisational formats would make database management easier. A MDSS must support statistical package so as to ascertain the data sets against the statistical methods which will enable to generate concrete results. Mathematical models will further enable to check the feasibility of the operations.

3.1 Characteristics

A MDSS always:

- Interacts without any requirement of a computer programmer i.e. a Marketing Manager may always interact with the system to find the solution of any query without waiting for a more formalised scheduled reports.
- Support flexibility i.e. A MDSS displays content as per the query stream inserted For e.g. A member from top level management may be previewed with more aggregate related outcomes instead of any Manager who have to follow a detailed analysis of the subject matter.
- Shores up discovery i.e. a manager may always form a problem definition, may locate solutions and can even generate a trend line (if possible) delineating even the past information.
- Comprehends the solution of a problem even for a new one, incompatible with computer language i.e. it may even outcast the basic formalities and present information supporting just the important features of it.

3.2 Implementation and Usage of MDSS

Any organization which tends to use such a system requires certain modification in organizational structure.

- Top management support is vital for it. A system can never be turn out to be successful if Top management does not make any deliberate attempt to fully equip its organizational elements with its utility, power and efficiency. Even the organizational members must be conversant with its usage, role, benefit etc. of it, so that the system can be implemented to the roots of an organization.
- Organization must train all the non users so that their decision in the upcoming future does not prove to be futile, because a MDSS adds power to a user statement by linking it with practical and alike edifice in contrast to a MIS which is more centralized in its approach and provides mere information which several researchers have found to be less informative for constituting any decision.
- Further, involvement of functional level managers while crafting any decision may cause it to be more acceptable and will generate more positive outcomes. Moreover such an attempt will add more information to a statement. Even the information acquired from such sources tends to be even more reliant in comparison to others. It can easily acquaint the user with 'what if' questions.
- Such decisions affect firm's prosperity for a longer period of time. Firm has to undergo the consequences of such decisions. Therefore, every intended design, formulations in it must be crafted carefully.
- The decisive factors in Marketing Decision Support System must be aforementioned for which the perspectives like maximisation of profit or wealth of shareholders or satisfaction of firm i.e. their objectives are achievable in real or certain incremental steps can be undertaken.
- A MDSS require large commitment of firm's resources for a longer time frame. Their actions have enduring impacts on the organization. Hence, firm need to be cautious in implementing its proposals or else deteriorating fallacies may eat up the organizational revenue.
- External environment is always dynamic. Environmental scanning considering the facets which can prove to be crucial for an organization as well as those which are futile must be listed and evaluated against the passage of time so that the outcomes can be manoeuvred.
- Manager's knowledge, risk taking ability, personality etc is vital for such a system as their forecasts enable the firm to optimally choose among the several decisions. Hence, MDSS is positioned along the future directives.
- Rationality is also essential i.e. A MDSS must honour the best one from the various alternatives or even the live wire must be able to acknowledge the optimum from the given set of alternatives, so that interest of several stakeholders can be taken along.
- Organization has to dwell in an ever changing turbulent times due to which they reliance just only on MDSS would not be sufficient, a group effort is mandatory. Group cohesiveness will cause an organization to understand the special characteristics associated with the decision and its prolonging influence, thereby causing the organization to survive in such fierce competition.

3.3 Risks

MDSS can drive better outcomes for an organization with the elimination of the following taints:

- MDSS has time constraints associated with it, i.e. the marketing functionaries may spend majority of its time for developing such MDSS which may affects its operational duties.
- While designing MDSS the targeted performance must be accustomed with the certainty of the involved functional level managers, and then only the desired will prove to be real.

§ To realize utmost outcomes, those who could not derive out true decisions from it, must be trained over it so there unachievable targets can be worked upon.

IV. CONCLUSION

Marketing Decision Support System may circumvent the operation of several deteriorating operations with its utilities. Facilitating interaction without even the requirement of a computer programmer, decentralized in approach, a marketing manager may develop optimum, recent outcomes generating a rapid stride towards attainment of organizational success. However, for adequate implementation and usage of MDSS, a consistent top management support, their knowledge, managerial style, values, ethics, accompanied with entailment of operational and functional managers, careful analysis of external environment, commitment of firm's resources over a longer period of time etc is adamant. But certain risks like allocation of majority of time of managers over its development may cause managers to lose their laser like required focus over operational duties may also happen.

REFERENCES

Journal Papers

[1] Wierenga B. et al, Marketing Decision Support System: Adoption, Use and Satisfaction, International Journal of Research in Marketing, 14, pp. 275-290, 1997.

[2] Grubor A., Global Marketing Decision Support System, Management Information Systems, Vol.4, No.1, pp.021-027, 2009.

[3] Bhatia A., A Framework for Decision Support System for the banking sector- An Empirical study of State Bank of Patiala, IJCTA, Vol.2, pp. 1368-1378,2011.

Proceeding Papers

[4] Stern D, Increasing Acceptance of Managers for the use of Marketing Decision Support System, Proceedings of Australian and New Zealand Marketing Academy Conference, Australia, pp2373-2379, 2003.

[5] Baggio R. Et al, Decision Support Systems in a Tourism Destination: Literature Survey and Model Building, Proceeding of 2nd Conference of the Italian Chapter of Association for Information Systems, Italy 1-2, 2005.

FINANCIAL MANAGEMENT SYSTEMS

Reepu

Department of Management, Punjab Institute of Technology, Nandgarh, Punjab (India)

ABSTRACT

Finance has been regarded as the life line of any organization. Every organizational activity may preclude if not supported in monetary terms. The sustenance may sink if the finances are not handled promptly. Therefore, many organizations have traversed from manual systems to financial management systems. Packed with various data models this system creates a master file thereby coupling the data models of varied business units with which the unanimous data flows as such, thereby facilitating the managerial decision making. This paper manoeuvres the underlying aspects of such extant core modules of Financial Management Systems (FMS).

Keyword|: Advantages, Features, Financial Management Systems, Master File, Modules etc

I. INTRODUCTION

Organizational success does not presume any cut and dried rules, however their strategic decision must strive for profit as well as wealth maximization of its shareholders. Each and every routinized tasks of an organization are impossible without financial management. Finance can be described as organization's root. Organization tends to grow rapidly if rooted firmly. So, decisions relating from working capital management to capital budgeting to the choice of capital structure require careful consideration of risk-return profile. Finance exists there in all, like from making payments to outside creditors to even employees of an organization. So, managing this finance using a finance management system has become a fad.

Finance Management System allows an organization to manage different segments of finance using software via the intranet platform. Its elements have become a viable cause of performance improvement as well as circumvention of various types of risks, thereby generating adequate returns. Its functional facets enable superior classification of different types of budget, coalesces even accounting systems with it, enhances management of cash, receivables and inventory management and even the evaluation as well as control becomes easier. Such a system facilitates even the reporting system thereby reducing time and saving costs.

II. REVIEW OF LITERATURE

Heidenhof G., et al (2001) researched about the need of reformations made in the financial systems in several African nations comprising of Ghana, Tanzania, Burkina Faso, Malawi and Uganda. They further outlined the implementation approaches normally utilised viz. Centralised approach, Decentralised Approach and Combination Approach. Even the designing of roll out strategy have also been discussed. Parikh T., et al (2003) presented a design artefact formulated after conducting field visits, with users as semi-literate village women, which posses certain characteristics like Colour, Tabular data presentation, Discrete task spaces, Iconic legend, Numeric data formats and Representational Icons. They believed that such digital platform would unify the user related content and is less expensive. Diamond J., et al (2005) found that there has been huge emphasis in the developing countries over computerising entire government accounting systems. However, they believed that

implementation should be done in phases, with adequate number of personnel deployed over it, having true passion as well as commitment. Peterson S., (2006) presented two frameworks one among which distinguishes between reengineering and process change, while the second framework acknowledged factors like scope, schedule and budget. Ibrahim S., et al (2014) highlighted the role of globalisation for the adoption of GIFMIS in Nigeria. The system has espoused the financial tasks delivering greater accuracy but according to the paper, corruption prevails there to a much larger extent which may generate refutation from GIFMIS.

III. CORE MODULES

Existent core modules and its sub-modules in a FMS are:

3.1 Inventory

Using a Financial Management System for the management of inventory enables an organization to deal with several queries like when to purchase, how to purchase, who can be a potential source etc. With the help of such a system, the issues of over stocking and even under stocking can be given a proper check. Both can become perilous, as over stocking may cause unnecessary blockage of funds, overemphasizing over redundant stocks, which may become a costly affair. Under stocking, on the other hand, might even cease the operations of an organization. Thus creating alerts at danger levels or low levels is mandatory. With the help of a FMS, organization may manage different storing operations single headedly, management of it through the software becomes more dexterous. Moreover, keeping a check on the pilferage, deterioration, replenishment levels etc of each and every item of inventory of an organization becomes effortless.

Pricing Concerns:

Now-a-days, such systems even support the pricing of closing stock of inventory, undertaking the government norms. Normally, following methods are employed:

- First In First Out
- Last In First Out
- Base Stock method of valuation
- Average Price Method: (a) Simple average price method (b) Weighted average price method
- Market Price Method
- Standard Price Method

Government has instituted certain rules and regulations for inventory pricing, so as keep a check over malpractices.

To manage the inventory, organization may even utilise certain tools and techniques. Normally, methods employed for such purpose include ABC Analysis, V.E.D Analysis, Just In Time, Perpetual Inventory Set up, Aging schedule, inventory reports, lead time, Economic Order Quantity, Inventory Turnover ratios etc.

3.2 Payment System

FMS facilitates the management of account receivables as well as payables. Sub-systems enable linkage of organization with suppliers, so that payments can be made and even received electronically. Normally, Electronic Data Interchange model is employed for it, which contains several standardized formats like bill of lading, order requisition form etc. The adoption rate for EDI have subsequently grown as it is an inexpensive method, deploying more qualitative product with quicker processing speed but yielding accurate results, thereby leading to faster decision making. It even supplements the firm over its workable areas, leading to more

effective outcomes. To implement it, organization may choose from a set of approaches, for instance, they may select that payment and remittance moving independently or both payment and remittance flowing concurrently either through their own proprietary set up or through bank as a medium or the payments may drift through the channel of banking software and data related to remittance may flow over directly through a data communication link established with the supplier or through a VAN. VANs may hold the data till it has been accepted over the counter line. It may even convert the data into an acceptable format. Organization may select a transmission medium depending upon its transmission costs and may opt for electronic payment method as offered by its bank (if not having a proprietary set up).

3.3 Accounting

Financial Management System endows with account related information. It supplements information from data recording to the preparation of entire accounting cycle.

With the help of FMS, data can be easily posted into a journal. With journalising being completed, the recorded transactions may be transferred to its respective accounts of a ledger. If the difference exists between the records of two, those have to be balanced, using a balancing figure, after which it should be assured that the credit side balances should be equivalent to debit side balances. With the correct ascertainment of the two, the organization then may easily prepare the Profit & Loss Statement and even the Balance Sheet. Due to FMS, the accounting cycle will undoubtedly produce more effectual outcomes.

Accounts Receivables are also easily handled in a jiffy, but with precision. The Customer details, his orders are stored in the database, the relevant particulars hence can be easily accessed. Credit checks are also employed, alerts are also embedded whenever the credit limit is exceeded or the balance amount does not prevail. Prior to the shipment, the particulars can be checked thoroughly. Accounts payable is another important module of FMS. Due to its continuous tracking feature, it causes organization to save more by setting reminders for making payments within the discount period or before the due date. It even maintains the standardized formats like vouchers etc.

Management Accounting:

Management Accounting enables decision making by taking into account the information of both financial and cost accounting. Due to FMS, the decision making become quite uncomplicated, as the data sets across the different platforms can be easily coalesced into the master file, due to which it becomes easier to generate reports on account of which management can easily equip the corporate with optimal decision making.

IV. ADVANTAGE OF FMS

FMS allows the integration of several data model's insertions into the master file, consequent of which preparation of financial statements becomes the task of minutes. Process models, further, unifies and initiates the processing of data of different Business Units therefore, enriching corporate accounting experience. Customer driven information is also delivered with a single touch using a delivery model.

V. CONCLUSION

Financial Management System may set the trail of organizational success. With the usage of different modules, overemphasis on unnecessary repetitive superfluous information can be easily dwindled. With the employment of inventory module, management of danger stock, minimum and maximum levels, even pricing of the closing

stocks etc can be handled appropriately. Payment Systems through EDI over the organization's proprietary set up or bank's software definitely adds more convenience. Management of Accounts Receivables and Accounts Payables through this system dispose expediency to the next higher level. Entire accounting cycle from journalizing to preparation of financial statements can be deduced by unifying the operations into the master file, leading management to form adequate decisions.

REFERENCES

[1] Heidenhof G., et al, Design and Implementation of Financial Management Systems: An African Perspective, Africa Regional Working Paper Series No.25, December 2001.

[2] Parikh T., et al, Design Studies for a Financial Management System for Micro-Credit Groups in Rural India, CUU, 2003.

[3] Diamond J., et al, Introducing Financial Management Information Systems in Developing Countries, IMF Working Paper, 2005.

[4] Peterson S., Automated Public Financial Management in Developing Countries, Faculty Research Working Paper Series, Harvard University, October 2006.

[5] Ibrahim S., et al, Globalisation and The Emergence of Government Integrated Financial Management Information System (GIFMIS): The Nigeria's Experience, Journal of Economics and International Business Research, Vol.2 (3), pp. 37-47, 2014.

MICROSTRIP ANTENNA WITH SLOTS FOR UWB COMUNICATIONS

Poonam Ghanghas[1], Prem Bhushan Mital[2]

[1]Research Scholar, [2]Professor, ECE ,

FET Manav Rachna International University, Faridabad,

ABSTRACT

Microstrip patch antennas with slots are a promising candidate for ultra-wideband (UWB) radio communication that has created interest in the subject of UWB antennas. Many designs for UWB antennas have been proposed. In the present work, a microstrip patch antenna with tapered slots at the patch center has been used to provide a return loss of about -9 dB for a frequency range from 4 to 7 GHz.

Key Words: Multi-Band Antenna, Patch Antenna , Paper Thin Antenna , Slot Antennas, Ultra-Wide Band Antenna

I. INTRODUCTION

The use of printed circuit technology has brought about a rapid growth in the development of antennas, having patches of conducting materials etched on one side of a dielectric substrate the other side being a metal ground plane . As the resulting printed circuit board is very thin (about 1mm thick).The microstrip patch antennas are also known as paper-thin antennas [1,2,3]. The simplest configuration of a microstrip antenna is shown in Fig.1.

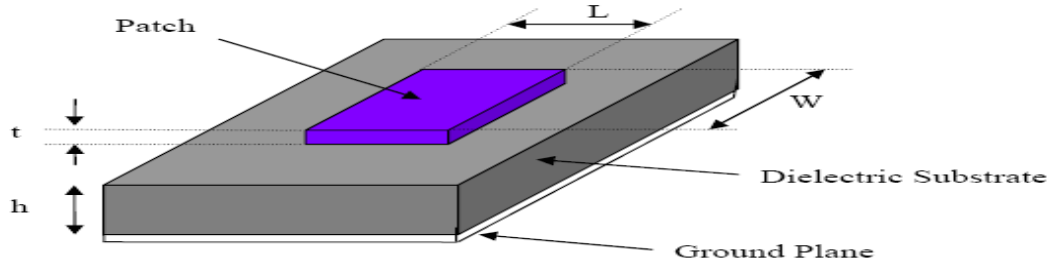


Figure 1 : Microstrip Antenna Configuration

The popularity of such antennas arises from the fact that the structure is plannar in configuration and enjoys all the advantages of the printed circuit technology. The feed lines and matching networks are fabricated simultaneously with the antenna structure. The solid state components can also be added directly on the microstrip antenna board. Hence such antennas are compatible with modular designs.These antennas meet the prime requirements, i.e. small size, low weight etc. and hence are easy to manufacture on a mass scale.These antennas do not disturb aerodynamic flow or disrupt the mechanical structure [4,5] linear and circular polarisations are possible. Dual –frequency antennas

can be constructed. These antennas are replacing old and bulky ones on aerospace vehicles e.g. on satellites , missiles, rockets, aircrafts etc [6,7].

The main limitations are :

- Narrow bandwidth (a few percent)
- Practical limitation on maximum gain (-20dB)
- Radiate in to a half plane
- Poor end fire radiation
- Low power handling capability
- Possibility of excitation of surface waves.

Various shapes of patches used in practice are shown in Fig.2. The choice depends on the required type of polarisation of the radiated field viz., linear, circular or elliptical polarisation.

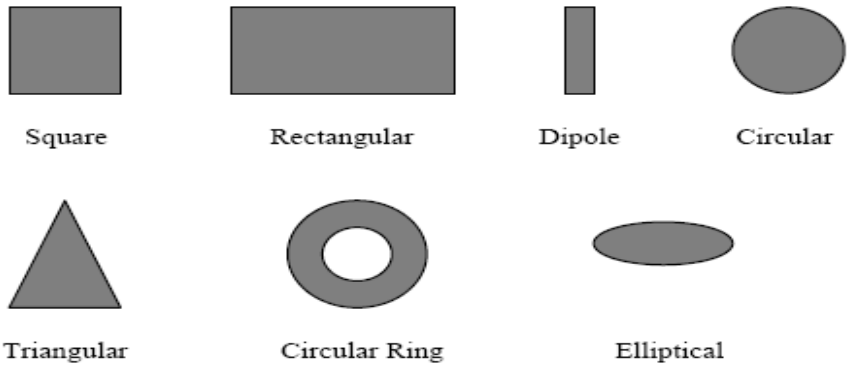


Figure 2. Various Microstrip Antenna Patches used

II. ANTENNA DESIGN

Here in this configuration,we propose a microstrip patch antenna with tapered slots at the patch center. Smooth transition in the slot shape is an important factor in minimizing resonance and hence increasing bandwidth [8,9.10]. The tapered slots are etched on a patch of size 40mm x20 mm. The substrate has a dielectric constant of 4.4 and thickness h= 0.0254 cm . The combined length and maximum width of the slot are 34 mm and 3mm respectively and the fed point is placed at the patch center.

III. SIMULATION RESULTS

The antenna maintains a a return loss of about -9 dB for a frequency range from 4 to 7 GHz as shown in fig. 3. The antenna exhibits near linear phase characteristics. The shape of skots , thickness, lengthand width of patch determine the bandwidth of antenna.

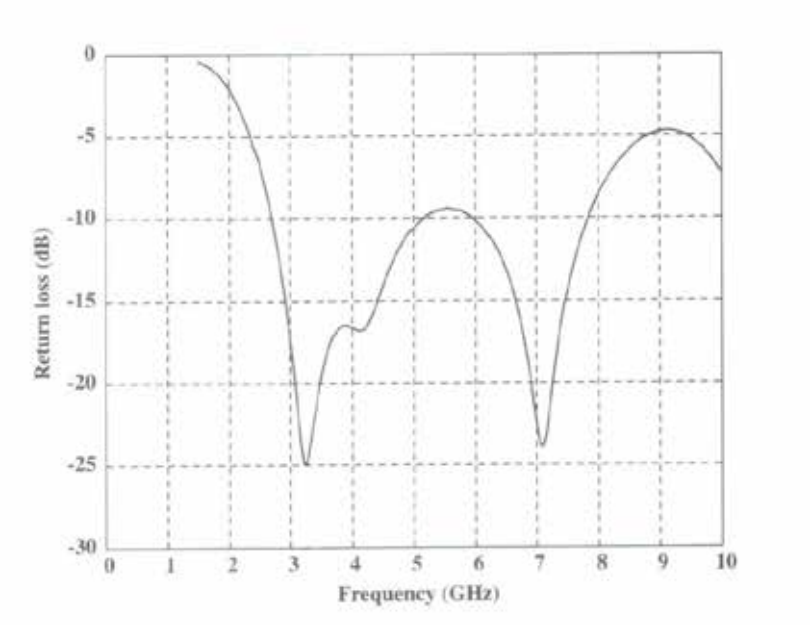


Figure 3: Measured Return Loss of Antenna

IV. CONCLUSION

A new UWB microstrip patch antenna with tapered slots at the patch center is presented in this paper. The simulation results show that the antenna maintains a a return loss of about -9 dB for a frequency range from 4 to 7 GHz with a sharp roll off at the notch band to reduce interference from existing indoor radio frequency.

REFERENCES

[1]. Robert A. Sainati, " CAD OF Micrstrip Antennas for wireless Application".

[2]. A.Balanis, " Antenna Theory, Analysis and Design" John Wiley and Sons. INC , New York 1997.

[3]. R.Garg, P Bhartia, I. Bahal, A.Ittipiboon, " Microstrip Antenna Design Handbook", Airtech House.Boston 2001.

[4]. S.Silver, Microwave Antenna Theory and Design" McGraw Hill Book Company,INC, New York ,1947.

[5]. M.Pozar and D.H.Schaubert, Microstrip Antennas: The Analysis and design of Microstrip Antennas and arrays, IEEE, Press,1995.

[6]. K.F.Lee,Ed, Advances in Microstrip and Printed Antennas, John Wiley, 1997.

[7]. E. Gardiol, " Broadband patch Antennas " Artech House.

[8]. M.Pozar," Input impedance and mutual coupling of rectangular microstrip antennas" IEEE, Trans. Antennas and propagation .vol AP-30.PP 1191-1196.Nov.1982

[9]. S.B.Cohn , " Slot line on a dielectric substrate " , IEEE Transactions on Microwave theory and techniques, vol. MTT-17,pp768-778, oct 1969.

[10]. Y.Yoshimura, " A microstrip line slot antenna ",IEEE Transactions on Microwave theory and techniques, vol. MTT-20 ,pp760-762, Nov. 1972.

 ISBN: 978-81-931039-3-7

DATA HIDING USING RC4 ALGORITHM IN IMAGE FORM

Geetanjali N. Narhare[1], Savita R. Bhosale[2]

[1]PG Scholar, Computer Engineering, MGMCET Kamothe, Navi Mumbai (India)

[2]AssistantProfessor, Electronics and Telecommunication, MGMCET Kamothe, Navi Mumbai (India)

ABSTRACT

As we know that the improved technologies in communication, Security is very important in several fields. So we should make an arrangement of security of our valuable data. Data contain different types of data that include text, audio, video, graphics images. This paper enlighten the problem of transmitting redundant data over an insecure, bandwidth-constrained communications channel. In this proposed system, secret messages are encrypted before embedding it into the cover image which gets high security to secret data RC4 algorithm is used to encrypt secret messages and Least Significant Bits (LSB) based data embedding technique is used to high encrypted messages. To hide encrypted messages into BMP image file, pseudorandom sequences are used. A content owner encrypts the original uncompressed image using an encryption key. After that, a data-hider may compress the least significant bits (LSB) of the encrypted image using a data-hiding key to create a sparse space to accommodate some additional data. If the receiver has both the data-hiding key and the encryption key, the receiver can extract the additional data and the original image without any loss.

Keywords: Digital Image Processing, Image encryption, Image Recovery, RC4, Reversible Data Hiding, Security

I. INTRODUCTION

It is important that the dada transmitting in high security which was not affected by visible loss of data. To hide secret data in such manner that data can be reversed, Reversible Data Hiding (RDH) technique is used. Data can be restored to its original manner without any loss and also without using any other information. This can be termed as safe embedding. At the end of the receiver, hidden data is extracted and image is also restored in its original form. This technique is more useful in applications in which original image should remain intact even after data embedded is retrieved [1, 2]. Reversible data embedding can be viewed as an information carrier. It is impossible for human eyes to distinguish between embedded image and original image. Because of this, reversible data embedding can be thought as secret communication model. As an effective and standard means for privacy protection, encryption converts the ordinary signal into unintelligible data, so that the traditional signal processing usually takes place before encryption or after decryption [3, 4]. The traditional way of transmitting redundant data is to first compress the data to reduce the redundancy, and then to encrypt the compressed data to mask its meaning. The sender should encrypt the original data and the network provider tend to compress the encrypted data without any knowledge of the cryptographic key and the original data. At the

side of receiver, a decoder integrating decompression and decryption functions for reconstructing the original data [5,6].

II. PROCEDURE OF ENCRYPTION AND DECRYPTION WITH FLOW DIAGRAM

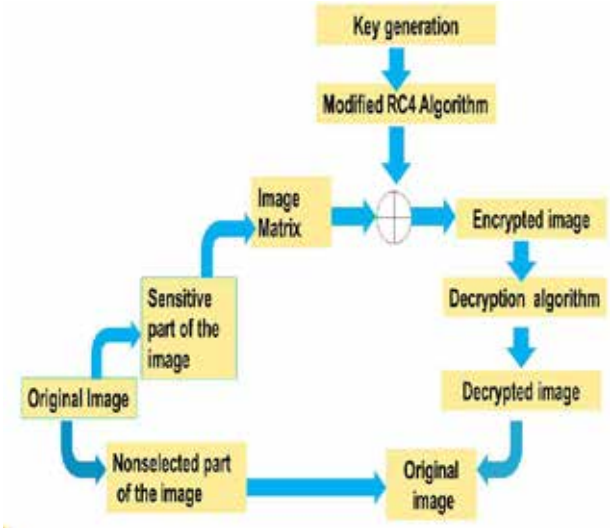


Fig. 1: Procedure of Encryption And Decryption

Normally cryptography starts with taking an image as an input after that applying the required algorithm encrypting the image that is called encrypted image. But for selected image encryption first of all we have to specify the regions we are going to encrypt. Then the encryption algorithm works. By using algorithm the selected parts of the image is being encrypted and the other parts remains as it is. We got the encrypted image after the end of this step. With the help of same algorithm we can decrypt the selected regions. We again got the original image back, after the end of this process. The overall procedure is shown in Figure 1.

III. PROPOSED SYSTEM DESIGN

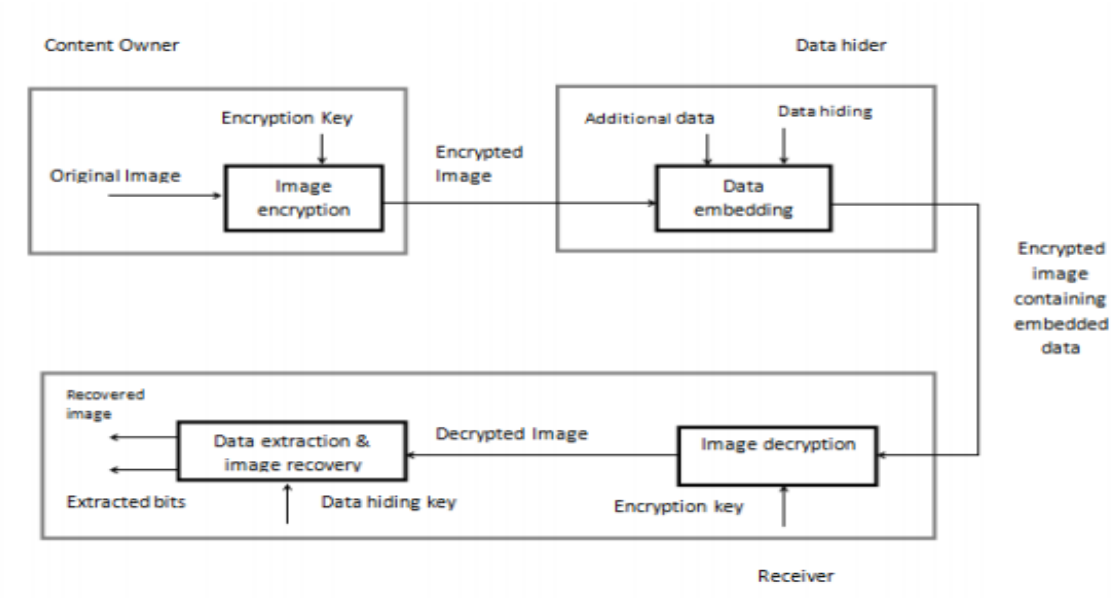


Fig 2.Proposed System Data Hiding İn Encrypted İmage

A owner of content encrypts the original image using an encryption key, then a data-hider can embed additional data into the encrypted image with the help of a data-hiding key though the receiver does not know the original data. With an encrypted image containing additional data, a receiver may first decrypt it according to the encryption key, and then recover the original image and extract the embedded data according to the data-hiding key.

3.1 Image Encryption Types

Image encryption involves two types, generation of encryption key and generation of pseudo-random sequence.

3.1.1 Generation of Encryption Key

Encryption key is 128 bit value. By using the random function, encryption key generated randomly. The random function generates the random key in an uniformly distributed function.

3.1.2 Generation of Pseudo-Random Sequence

It consists of random bits generated using the encryption key. In this paper, RC-4 algorithm is used to create the pseudo-random sequence using the 128-bit encryption key. It is represented as sequence of bytes or an array of bytes. The number of bytes generated should be equal to the number of pixels in the input image provided the pixels are represented as 8-bit values. If the pixels are represented as 16-bit values then the number bytes in pseudo-random sequence should be double the number of pixels.

IV. DATA EMBEDDING

In embedding, encrypted pixels are formed with the use of some parameters and LSB's of other encrypted pixels are compressed to create more space so that more data can be added. Data hider pseudo-randomly chooses Np encrypted pixels that will be used to carry the parameters for data hiding according to a data-hiding key,. Here, Np is a positive integer, for example, Np=20.The other (N-Np) encrypted pixels are pseudo-randomly permuted and divided into a small number of groups. Each group contain L pixels. The permutation way is also determined by the data-hiding key. For each pixel-group, collect the M least significant bits (LSB) of the L pixels, and indicate them as B(k,1),B(k,2)…B(k, M. L)where k is a group index within[1,(N-Np)/L] and M is a positive integer less than 5. The data-hider also produces a matrix G sized (M.L-S) × M.L, which is composed of two parts.

$$G= [I_{M.L-S} Q] \quad (1)$$

Data hiding key is used to derive pseudo binary matrix i.e. Q sized (M.L-S) × S which is right part, and left part is (M.L-S) × (M.L-S) identity matrix. Where S is small positive integer. Then next procedure is embed all the values of parameters M, L and S into LSB of NP. So, the rate is:

$$R = ((N-NP). (S/L) – NP) / N = S / L \quad (2)$$

where, R is encrypted data embedded rate, N is Number of pixels present in the encrypted image, NP is Number of pixels which carries the parameters, S is Small positive integer and L is Number of pixels in each pixels group.

V. DATA-EXTRACTION AND IMAGE-RECOVERY

Our proposed scheme contains image encryption, data embedding and data extraction phase. At encryption side, encryption is done using an encryption key. Then, the data-hider compresses the LSB of the encrypted image

using a data-hiding key to create a sparse space to accommodate the additional data. At the second side, embedded data can be easily retrieved from the encrypted image containing additional data according by using data-hiding key. It affects only LSB, a decryption with the encryption key, the result is similar to the original image. By using both encryption algorithms and data hiding keys we can effectively extract original image by using spatial correlation in natural image. Fig. 3 shows the three cases at the receiver side.

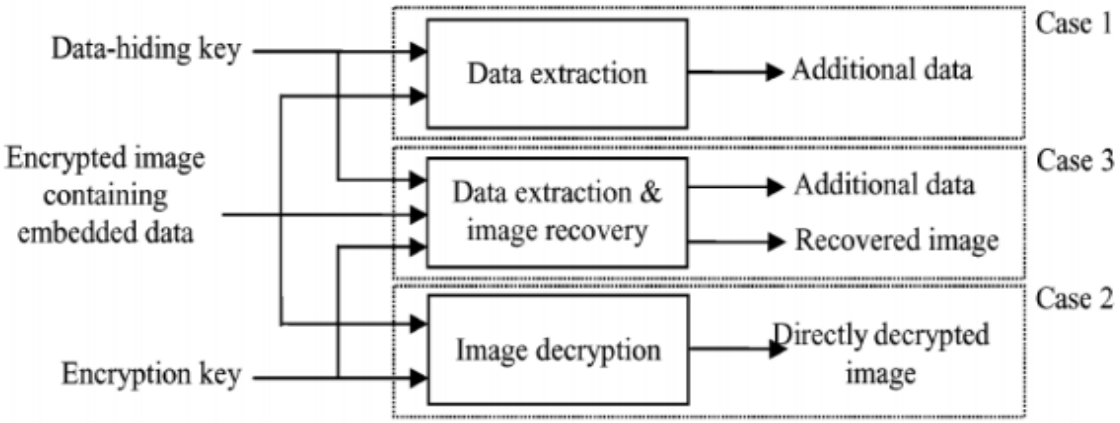


Fig.3. Three Cases At Receiver Side of The Proposed Separable

In this phase, there are three cases that, in first case a receiver has only the data-hiding key, in second case only the encryption key, and in third case both the data-hiding and encryption keys, respectively. If the receiver has only the data-hiding key by using an encrypted image containing embedded data, , he may first acquire the values of the parameters M, L and S from the LSB of the Np particular encrypted pixels. And then, the receiver permutes and divides the other. (N-NP) pixels into (N-NP)/L groups and extracts the S embedded bits from the M LSB-planes of each group. When consuming the total (N-NP).S/L extracted bits, then receiver can divide into NP new LSB of certain encrypted pixels and (N-NP).S/L-NP additional bits.

Important thing is that because of selection and permutation of the pseudo-random pixel, any attacker without helping the data-hiding key cannot obtain the parameter values and the pixel-groups, therefore the embedded data cannot extract. Moreover, the receiver can successfully extract the embedded data by using data-hiding key. Representing the bits of pixels in the encrypted image containing embedded data, the receiver can decrypt the received data from the encrypted data in the M LSB-planes. Assuming that the original distribution of the data in the M LSB planes is uniform, the alteration energy per each decrypted pixel is because the probability of this case.

$De = (2)^{n-2M} = \sum_{\beta=0}^{2M-L}(\alpha - \beta)\ ^2$ (3)

Here, the alteration in the NP selected pixels is also ignored since their number is significantly less than the image size N. So, the value of PSNR in the directly decrypted image

$PSNR = 10.\log_{10}(AE)$ (4)

Where AE is Average Energy. If the receiver has both the data-hiding and the encryption keys, receiver may goal to the embedded data extract and original image recovery. According to the data-hiding key, the values of M, L and S are the original LSB of the NP selected encrypted pixels, and the (N-NP).S/L-NP are additional bits can be extracted from the encrypted image enclosing embedded data. By placing the NP LSB into their original locations, the encrypted data of the NP selected pixels are recovered, and their original gray values can be properly decrypted using the encryption keys.

VI. RIVEST CIPHER 4 (RC4) ALGORITHM

This algorithm is developed by Ronald Rivest and thus, the name of the algorithm was put after Ronald's Rivest name. RC1, RC2, RC3, RC4, RC5 and RC6 is the series of RC algorithm.RC4 is symmetric key algorithm. It is one of the algorithm which is used for both encryption and decryption as the data stream is simply XORed with the generated key sequence. The key stream is completely independent of the plaintext used. It uses a flexible length key from 1 to 256 bit to modify a 256-bit state table. The state table is used for consequent generation of pseudo-random bits after that to generate a XORed pseudo-random stream with the plaintext to give the cipher text. The algorithm can be divided into two stages: First stage is initialization, and other operation. In the first stage the 256-bit state table, S is populated, using the key, K as a seed. Once the state table is setup, it continues to be modified in a regular pattern as data is encrypted. The initialization process can be summarized by the pseudo-code.

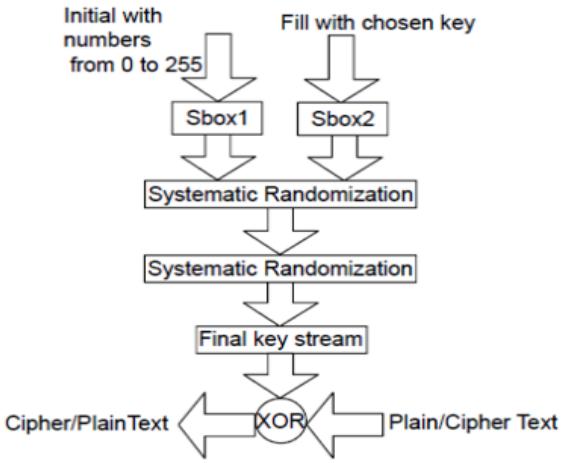


Fig 4. Rc4 Encryption Algorithm

This algorithm generates a pseudo-random stream values. XORed is the input value with these values, bit by bit. The process of encryption and decryption is the same as the data stream is just XORed with the generated key sequence. If it is fed in an encrypted message, it will produce the output of decrypted message, and if it is fed in plain text message, the encrypted version will produce. The RC4encryption algorithm is shown in Fig.4.

VII. RESULTS AND DISCUSSIONS

The test image Lena sized 512 ×512 is used as the original image in the experiment. After image encryption, the eight encrypted bits of each pixel are converted into a gray value to generate an encrypted image.

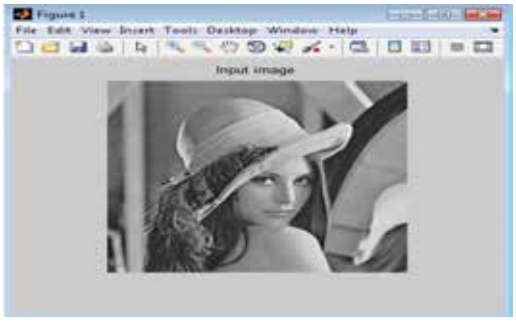


Fig 5. Original Image

Fig 6. Encrypted Image

Let M=2, L=76 and S=1 to additional bits into the encrypted image. The encrypted image containing the embedded data embedding rate R is 0.013158 bit per pixel (bpp). With an encrypted image containing embedded data, we could extract the additional data using the data-hiding key. Then, embed the values of the parameters M, L and S into the LSB of NP selected encrypted pixels.

Np = 20, N = 262144, M = 2, L = 76 and S = 1

Enter a maximum of 214 characters: Geetanjali

Data Embedded Rate = 0.013158 bpp

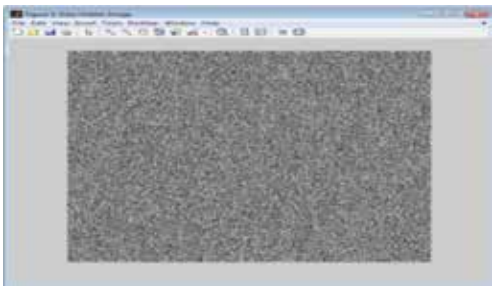


Fig.7. Data Hiding Image

Fig 8. Decrypted Image

When putting the value Np, N, M, L and S with the maximum characteristics value the correspond encrypted image, data hiding image and decrypted images fallen one by one. If we directly decrypted the encrypted image containing embedded data using the encryption key, the value of PSNR in the decrypted image was 40.0 dB, which verifies the theoretical value 40.0 dB is calculated. PSNR of the decrypted image = 40.930937 dB

The recovered image and directly decrypted image are shown in Fig.9 and Fig.10 respectively. The image recovered using RC4 algorithm is same as the original image.

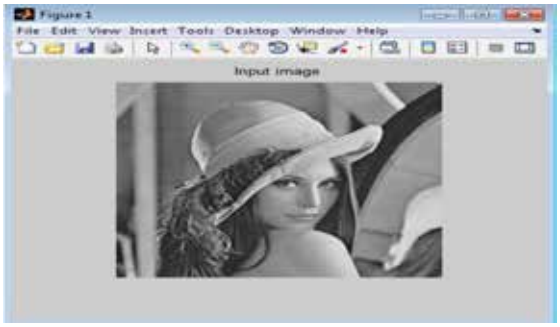


Fig 9. Image Recovery

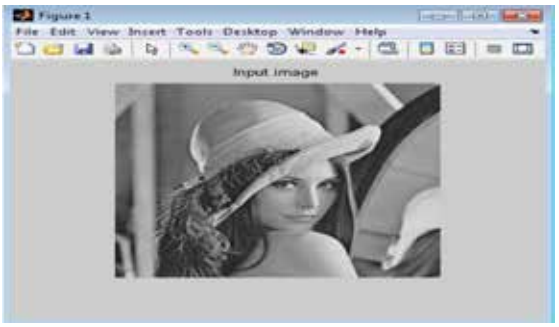


Fig 10.Directlydecrypted Image

VIII. CONCLUSION

With the encryption key Pseudo random structure consists of random bits generated. In this paper to create sequence of pseudo-random in the 128-bit encryption key by using RC-4 algorithm. With the parameters we can additional data inserted in to an encrypted image. Additional data which is encrypted in image. With an encrypted image containing additional data, with data-hiding key receiver can extract the additional data, or using only the encryption key can obtain an image similar to the original one. When using both of the encryption and data-hiding keys, the embedded additional data can be successfully extracted and the original image can be perfectly recovered by exploiting the spatial correlation in natural image. Compared with the other

algorithms, the proposed system demonstrated successful accuracy in recovering the original images. In the future, a comprehensive combination of image encryption and data hiding compatible with lossy compression deserves further investigation.

IX. ACKNOWLEDGEMENT

I am Geetanjali Narhare, would like to thank Prof. S.R.Bhosale of Electronics and Telecommunication Department, MGMCET Kamothe, Navi Mumbai, India, for her contribution to this work.

REFERENCES

[1]. X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," IEEE Trans. Inform. Forensics Security, vol. 6, no. 1, pp. 53–58, Feb. 2011.

[2]. W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," IEEE Trans. Image Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

[3]. T. Bianchi, A. Piva, and M. Barni, "Composite signal representation for fast and storage-efficient processing of encrypted signals," IEEE Trans. Inform. Forensics Security, vol. 5, no. 1, pp. 180–187,Feb.2010.

[4]. S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative encryption and watermarking in video compression," IEEE Trans. Circuits Syst. VideoTechnol., vol. 17, no. 6, pp. 774–778, Jun. 2007.

[5]. Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354– 362, Mar.2006.

[6]. M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992–3006, Oct. 2004.

[7]. Glover, P. and M. Grant, Digital Communications, 2nd edition, Person Education, 2004.

[8]. M Joset Pieprzyk, et. al., Fundamentals of Computer Security, Springer, 2003.

[9]. M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. B. Natale, and A Neri, "A commutative digital image watermarking and encryption method in the tree structured Haar transform domain," Signal Processing:

[10]. Image Commun., vol. 26, no. 1, pp. 1–12, 2011.Z. Wang and A. C. Bovik, "A universal image quality index," IEEE Signal Process. Lett., vol. 9, no. 1, pp. 81–84, Jan. 2002.

ONE-STEPSECANT" A GEOMETRICAL SHAPE RECOGNITION ALGORITH

Anjali Gangwar[1], Amrita Kaur[2], Deep Kumar Sharma[3]

[1,2,3]PG Scholar, SRMSCET, Bareilly (India)

ABSTRACT

The purpose of this paper is to recognise the geometrical shapes likesquare and ellipse by using the "one-step-secant" algorithm of neural network. Firstly, a neural network with two layers and two input vectors is built. The first layer has twenty neurons, while the second one includes only two neurons. Then a training base and a test base through generating "rand" function is created . Each of the base consists of one hundred shapes: fifty squares and fifty ellipses. Lastly, testing of the network with the help of a performance function (MSE=Mean Squared Error) and "one-step-secant" algorithm takes place.

Keywords: Neural Network, Epoch, MSE

I. INTRODUCTION

There is no commonly accepted definition of a neural network. But, most people in the field would agree that a neural network is a network of many simple mainframes ("units"), each possibly able with a small extent of local memory. The units are linked by communication networks ("connections"), which typicallytransmit numeric (as opposed to symbolic) data, determined by several means. The units function only on their local data and on theinputs they receive via the networks. The control to local actions is often comfortable during training [1], [2].

Neural network can be divided into three architectures, namely single layer, multilayer network and competitive layer. In a net, the layers number can be defined on the basis of a number of interconnected weights in a neuron. A single layer network consists in only one layer of connection weights, whereas, a multilayer network consists in more than one layer of connection weights. The network also contains an additional layer called hidden layer. Multilayer networks can be used to solve more complicated problems compared to single layer network. Both of the network are also called feed-forward network where the signal flows from the input units to the output units in a forward direction [2].

The inverse error propagation algorithm has been created through simplification of a learning rule of Widrow-Hoff of multitask networks and differential and nonlinear transferring functions. In this paper we used a variant of the opposite error propagation algorithm.

Input vectors and equivalent "target" vectors are used to train the network until this can estimated a function, connecting input vectors with specific output vectors, or categorize the input vectors in a user mode specification.

Standard algorithm of opposite error propagation is related to the gradient decrease. The notion of inverse propagation of error is similar to the manner in which the gradient is computed for nonlinear multitask

networks. There are numerousoperations for the standard algorithm that are based on other standard optimization techniques, like the conjugate gradient method or the Newton method.

Networks with opposite training error propagation tend to offer practicalanswers. This is happening in a suitable way, when input values which were not seen before, are introduced. Generally, new sets of input values are leading to similar outputs such as correct output (target output) for input vectors used in training. Those are similar to the new sets. Thissimplification property allows entertaining a network on a characteristic set of input/output pairs. It is also conducting to satisfactory results without network training on all the other possible input/output pairs.

II. BACKGROUND

In most cases, Training a neural network is an exercise in numerical optimization of a usually nonlinear objective function ("objective function" means whatever function you are trying to optimize and is a slightly more general term than "error function" in that it may include other quantities such as penalties for weight decay.

Methods of nonlinear optimization have been studied for hundreds of years, and there is aenormousworks on the subject in fields such as mathematical analysis, operational research, and statistical computing (e.g. [3], [4]). Masters in [5] has a good basicconversation of conjugate gradient and Levenberg- Marquardt algorithms in the environment of neural networks.

There is no single best method for nonlinear optimization. You need to choose a method based on the features of the problem to be solved. For independent functions with continuous second derivatives (which would include feed-forward nets with the most popular differentiable activation functions and error functions), three universal algorithms have been found to be operative for most practical purposes:

- For a small number of weights, stabilized Newton and Gauss-Newton algorithms, including various Levenberg-Marquardt and trust-region algorithms, are efficient. The memory required by these algorithms is proportional to the square of the number of weights.
- For a moderate number of weights, various quasi-Newton algorithms are efficient. The memory required by these algorithms is proportional to the square of the number of weights.
- For a large number of weights, various conjugate-gradient algorithms are efficient. The memory required by these algorithms is proportional to the number of weights.

In most applications, it is suitable to train several networks with different numbers of hidden units. Rather than train each network, start with completely random weights, it is usually more effective to use constructive learning. Constructive learning can be done with any of the predictable optimization methods or with the various "prop" methods, and can be very effective at finding good local optima at less expense than full-blown global optimization methods.

III. METHOD

This paper presents the first part of ancomprehensive project, which we need to achieve. Thus, we mean to discover the geometrical shapes described by a person’s movement through the air. However, to achieve this, first we have to create a transferable device which could offer the necessary plots on the path. In this paper we

used geometrical shapes in the xOy (bidimensional) plane, i.e. we used the bidimensional case. The next step would be to spread these to the xyz plane, for the tridimensional plane.

In this paper we recommend the operation of geometrical shape recognition: Square and geom. ellipse, for a given number of points. This paper starts from the concept of recognition of the geometrical shapes traced by one person through the air.

Quasi-newton method involves generating a sequence of matrices $G^{(k)}$that represents gradually accurate estimates to the inverse hessian $H^{(-1)}$.Using only the first derivative information of E, the updated expression is asfollows:

$$G^{(k+1)}=G^{(k)}+\frac{pp^T}{p^T v}-\frac{\left(G^{(k)}v\right)v^T G^{(k)}}{v^T G^{(k)} v}+\left(v^T G^{(k)}v\right)uu^T \qquad (1)$$

where

$$p=w^{(k+1)}-w^{(k)},$$

$$v=g^{(k+1)}-g^{(k)},$$

$$u=\frac{p}{p^T v}-\frac{G^{(k)}v}{v^T G^{(k)}v} \qquad (2)$$

and T represents transpose of a matrix. The problem with this approach is the necessity of calculation and storage of the estimated Hessian matrix for every iteration. The One-Step-Secant (OSS) is an approach to bridge the gap between the conjugate gradient algorithm and the quasi-Newton (secant) approach. The OSS approach doesn't store the complete Hessian matrix; it assumes that at each iteration the previous Hessian was the identity matrix. This has the advantage that the new search direction can be calculated without calculating a matrix inverse [2].

Newton's method is ansubstitute to the conjugate gradient methods for fast optimization. The basic step of Newton's method is

$$x_{k+1}=x_k-A_k^{-1}g_k \qquad (3)$$

where*k* *A* is the Hessian matrix (second derivatives) of the performance index at the current values of the weights and biases. Newton's method frequently converges quicker than conjugate gradient methods. Inappropriately, it is complex and costly to calculate the Hessian matrix for feed forward neural networks. There is a class of algorithms that is based on Newton's method, but which doesn't need calculation of second derivatives. These are called quasi-Newton (or

secant) methods. They update an approximate Hessian matrix at each iteration of the algorithm. The update is calculated as a function of the gradient.

The quasi-Newton method has been most effective is the Broyden, Fletcher, Goldfarb, and Shanno (BFGS) update. This algorithm has been implemented in the „trainbfg" routine. The BFGS algorithm is described in [6].

Since the BFGS algorithm needs more storage and calculationin each iteration than the conjugate gradient algorithms, there is need for a secant approximation with smaller storage and calculationnecessities. The one step secant (OSS) method is an effort to link the gap between the conjugate gradient algorithms and the quasi-Newton (secant) algorithms. This algorithm does not store the complete Hessian matrix; it assumes that at each

iteration, the previous Hessian was the identity matrix. This has the additional advantage that the new search direction can be calculated without computing a matrix inverse [1].

This algorithm needs more calculation in each iteration and more storage than the conjugate gradient methods, although it usually converges in less iteration. The approximate Hessian must be stored, and its dimension is n*n, where n is equal to the number of weights and biases in the network.

For very large networks it may be better to use strong back-propagation (Rprop) (in the „trainrp" routine) or one of the conjugate gradient algorithms. For smaller networks, however, „trainbfg" (BFGS quasi-Newton back-propagation) can be an efficient training function.

However, for complex networks, where number of connection is great (large), this algorithm is not very fast because it needscontrol and the notice Hessian approximate matrix. Full view handled problem in which we have twenty neurons on first layer and two input vectors, is necessitating a secant approximation with small requirements of control and notice. Therefore, in this case we used One-Step-Secant algorithm.

General description of method:

To pretend the giving out of the coordinate To pretend the processing of the coordinate points taken from the above-mentioneddevice,square and geom. ellipses have been generated in a random manner. Meaningful this and the fact that a person will not define, usually, perfect geometrical shapes, some expectations were measured for obtaining a real case:

- The shapes are traced anywhere in a requirement area, angle in down left (for

geom. ellipse, angle in down left of square what framing) full of random coordinates with a uniform distribution (abscissa respective angle there is between 0 and 100; likewise and ordinate), thus permitting a wide-ranging position of the traced form, like in the real case, when outlining is made inside a room with magnitudes from conditions.

- The shapes are drawn anywhere inside a specified area, the left lower corner (for geom. ellipse, the left lower corner of thesquare which surrounds it) having random coordinates with a constantdelivery (abscissa of the respective corner is between 0 and 100; likewise the ordinate). Thus a variedplacing of the drawn shapes is possible, like in the real case, when the outlining is done inside a room with quantifiedmagnitudes.

- The magnitudes of the shapes are createdcasually (again with an uniform distribution, so as not to create preferential dimensions).s

- Each coordinate of each point is affected by a constant noise, thus, allowing a tracing with limitations, exactly like in the real case.

The project was realized in Matlab version 7.0 and it is based on the idea of neural networks. The operation of the algorithms specific to neural networks was made with the use of the Neural Network Toolbox in Matlab. Neural networks are composed of simple elements which function in equivalent. These elements are encouraged from the biological nervous systems. As in nature, the function of network is determined in large by the connections between elements. A neural network may be skilled to realize certain function by set the values of the connections (synapses or weights) between elements. Generally, the neural networks are set or skilled, so that a certain set of input values would lead to a value of expected output (a target). Such a situation is presented in Fig. 1. The network is set through the association between the output value and the target (the expectedvalue), until the output of network approaches the target, with a given equalizer. In universal, many such input/target pairs are used for

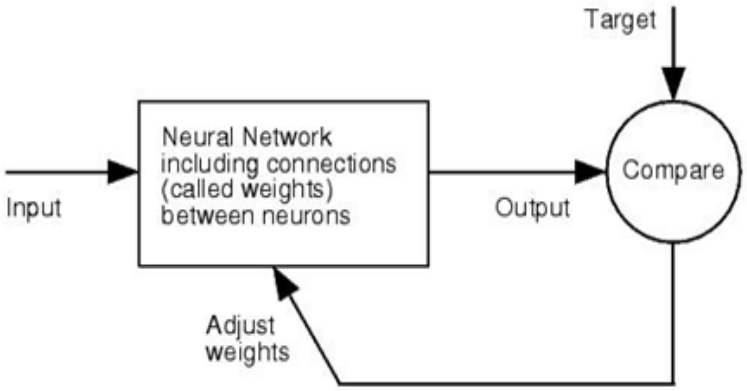


Fig. 1 - The comparison between the output value and the target

exercisenetwork.Neural networks have been trained to understand complex functions in wide-rangingapplications such as: shapes recognition (as in this case), classification, speech and voice signal recognition, control systems, medical imagistic and many others.

The area of neural networks has a history of about five eras, but has found solid application only in the last 20 years and continues to develop in fastermeasure. Thus, the idea of neural network is completely dissimilar from the traditional ideasindirect in areas such as control systems or the optimization of the systems where the terminology (mathematical statistics) and the designing actions were established and applied for many years.

Implementation procedure:

The first step is to build up a neural network with two layers and two input vectors. The first input vector contains abscissa points, and the second one contains ordinate points. Regarding the layers; the first one has twenty neurons, while the second one includes only two neurons.

The second step is to create a training base and a test base using the “rand” function. Each base contains one hundred shapes: fifty squares and fifty geom. ellipses.

The third step is testing the network by using a performance function (MSE=Mean Squared Error, where the error value is the amount by which the value output by the network differs from the training value. For example, if we required the network to output 0 and it output a 1, then Err = -1) and “one-stepsecant” algorithm. To assure the convergence towards the expected value while on any training set we realize a “while” loop that iterates the network initialization.

The result of the testing made one the exercise base must be under the value 1e-5; while for the test base is under the value 1e-4. These results are the errors that are reasonable enough for a correct classification. Further to these errors, the function also displays a value in which the development parameters are stored during the training. This is called epoch (An epoch is the presentation of the entire training set to the neural network. For example, in the case of the AND function an epoch consists of four sets of inputs being presented to the network (i.e. [0,0],

[0,1], [1,0], [1,1])).

The gradient of a function of two variables $F(x, y)$ is defined as:

$$\nabla F = \frac{\partial F}{\partial x}\hat{i} + \frac{\partial F}{\partial y}\hat{j}$$

and can be supposed of as a collection of vectors pointing in the direction of growing values of *F*. In Matlab, numerical gradients (differences) can be calculated for functions with any number of variables.

Algorithm "trainoss" [1] can train any network as long as its weight, net input, and transfer functions have derived functions. Back-propagation is used to calculate derivatives of performance perf with respect to the weight and biasvariables X. Each variable is adjusted according to the following [9]:

$$X = X + a * dX (5)$$

where*dX*is the search direction. The parameter is selected to minimize the performance along the search direction. The line search function searchFcn is used to locate the minimum point. The first search direction is the negative of the gradient of performance. In successive iterations the search direction is calculated from the new gradient and the previous steps and gradients according to the following formula:

$$dX = -gX + Ac * X_{step} + Bc * dgX (6)$$

where*gX*is the gradient, *step X* is the change in the weights on the previous iteration, and *dgX*is the change in the gradient from the last iteration. (For a more detailed discussion of the one step secant algorithm see [7]).

Training stops when any of these conditions occur:

1. The maximum number of epochs (repetitions) is reached.
2. The maximum amount of time has been exceeded.
3. Performance has been minimized to the goal.
4. The performance gradient falls below min-grad.
5. Validation performance has increased more than max_fail times since the last time it decreased (when using validation).

The program can be called through the function "rec_form". This has a facultative parameter which represents the number of points upon which the latter training and recognition are made. The understood value of this parameter is 48. To be used for recognition, the trained network is used as a parameter for the „sim" function which verifies the behavior of the network on a shape inserted from the keyboard. If the function returns the value 0 1, the network has recognized the introduced shape with a square but if the returned value is 0 0, the network has recognized the introduced shape as being an ellipse.

Training the network is time consuming. It generallyacquires after several epochs, depending on how large the network is. Thus, large network essential more training time compared to the smaller one. Basically, the network is trained for several epochs and stopped after reaching the maximum epoch. For the same reason minimum error tolerance is used provided that the differences between network output and known outcome are less than the specified value. We could also stop the training after the network encounters certain stopping criteria. During training the network powerstudy too much.

For this project during training, authentication set is used in its place of training data set. After a few epochs the network is tested with the authentication data. The training is stopped as soon as the error on authentication set increases quickly higher than the last time it was checked [8].

IV. EXPERIMENTAL RESULTS

In this paper we analyzed three cases. In first case, the performance has met at epoch number 52 of 500 (500 is number maxim of epochs in our case), in the second case the performance has attained at epoch number 146 of

500 and the third case the performance has met at epoch number 148 of 500. Results obtained in those there cases analyzed in this article are:

In Table 1, 2 and 3 we have MSE and gradient at some epochs of those analyzed, until met the performance. Fig. 2 (a), (b) and (c) shows network when met the performance that is at

maximum epoch.

(a) Represent the first case;

(b) Represent the second case;

(c) Represent the third case.

Fig. 3 (a), (b) and (c) shows network after training. Fig. 4 (a), (b) and (c) shows results obtained with this method.

(a) For the first case we have the following results:

Table 1

The performance system after epoch number 52

Epoch	MSE /1e-005	Gradient
0 of 500	0. 377322	0. 505532
25 of 500	0. 0381433	0. 648829
50 of 500	7.70679e-005	0.0338334
52 of 500	5.45577e-006	0.000132798

In first case the performance has met after epoch number 52.

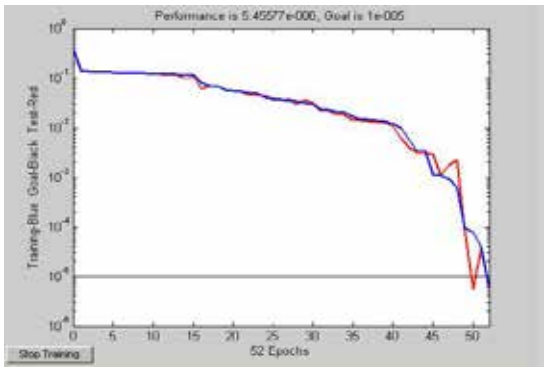


Fig. 2 (a) Maximum Epoch (in First Case is 52)

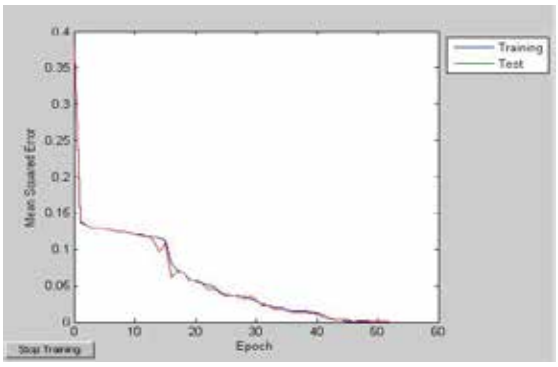


Fig. 2 (b) MSE After Training Networks in First Case

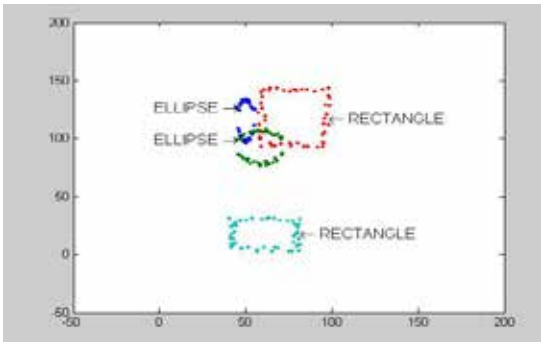


Fig. 2 (C) Results Obtained After Training Network in the First Case

(b) For the second case we have:

Table 2

The performance system met after epoch number 146

Epoch	MSE /1e-005	Gradient
0 of 500	0.511977	0.568587
25 of 500	0.0560792	0.16273
50 of 500	0.00763521	0.132888
75 of 500	0.000238334	0.000582092
100 of 500	0.000123981	0.000801856
100 of 500	2.34438e-005	5.7238e-005
146 of 500	9.38845e-006	5.50573e-005

In second case the performance has met after epoch number 146.

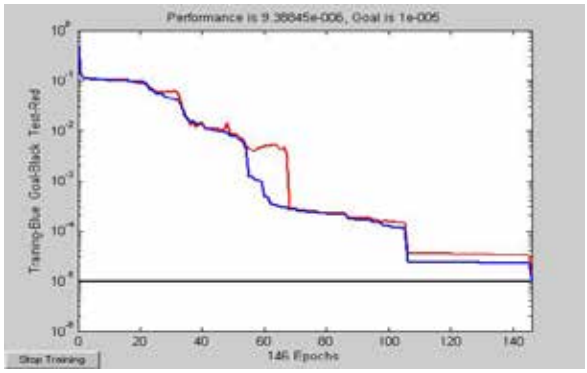


Fig. 3 (A) Maximum Epoch (In Second Case Is 146)

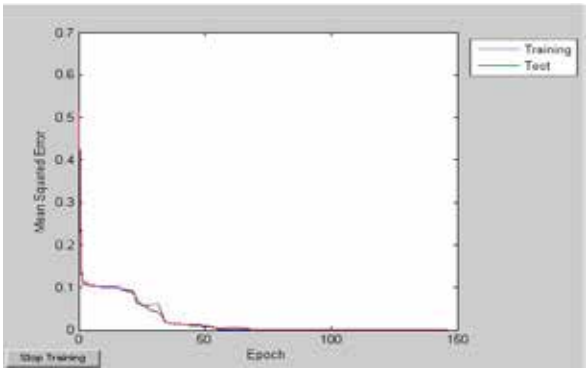


Fig. 3 (B) MSE After Training Networks In Second Case

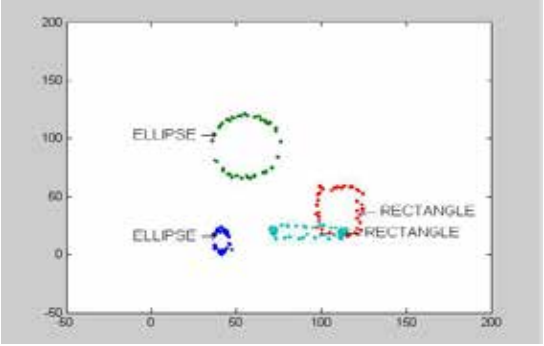


Fig. 3 (C) Results Obtained After Training Network in Second Case

(c) For the third case we have:

Table 3

The performance system met after epoch number 148

Epoch	MSE /1e-005	Gradient
0 of 500	0.292855	0.511591
25 of 500	0.029315	0.275339
50 of 500	0.00040364	0.00105794
75 of 500	1.58091e-005	3.21924e-005
100 of 500	1.53045e-005	4.51943e-005

125 of 500	1.50264e-005	3.37123e-005
141 of 500	2.71875e-006	1.39385e-005

In third case the performance has met after epoch number 148.

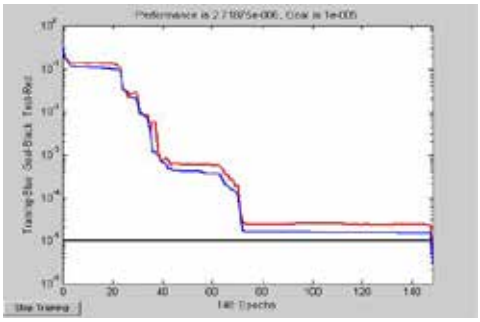


Fig. 4 (A) Maximum Epoch (In Third Case Is 148)

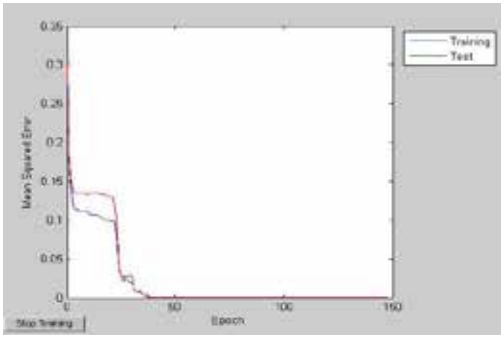


Fig. 4 (B) MSE After Training Networks In Third Case

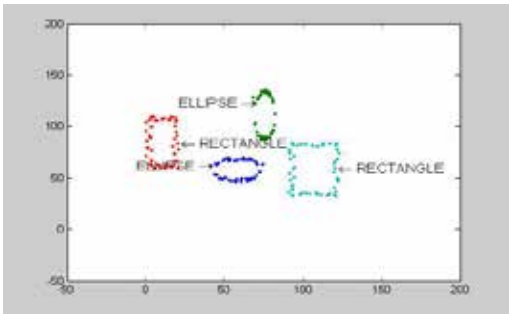


Fig. 4 (C) Results Obtained After Training Network in Third Case

V. CONCLUSIONS

For this project, the conjugate gradient algorithm influences a similar performance in a shorter time similar with "one-step-secant" method, with the variance that in some of the training cases the program blocks during the training time. Also, sometimes during the training the error "Divide by zero" arises. Therefore, one-step-secant algorithm is a sufficient algorithm that may achieve training without blockage during the running time of the program.

One-Step-Secant method representing a cooperation solution between conjugate gradient algorithms (methods with requirements low calculation) and quasi-Newton algorithms and this method no stocking complete Hessian matrix, but suppose that at each iteration previous Hessian matrix is identity matrix. This thing have additional advantage that new pursuit direction can be computing without computing inverse matrix, so in the case of Quasi-Newton algorithms.

This method may deal a helpful support for designing different geometrical shapes in many applications of current interest.

On the other hand, there are some points that should be better in additional work, such as improving the network algorithm, improving the simplification ability, etc. If the values of the performance function on training set is over 1e-5 value and on test set is over 1e-4, our program would be blocked. Helped by this program, we'll obtain the best results using the values of text frontstated.

In the future we propose to develop this application for more values of the performance function. In the near days to come, we will get new and more complete results for the performance function. Also we will spread the functionality of our algorithms so as to be able to make online plot of geometrical shapes with the use of satisfactorytransferable devices.

REFERENCES

[1] ***Matlab Help – Neural Network Toolbox

[2] Bishop C. M., Neural Networks for Pattern Recognition, Oxford Press, 1995.

[3] Bertsekas, D. P. (1995), Nonlinear Programming, Belmont, MA: Athena Scientific, ISBN 1- 886529-14-0.

[4] Bertsekas, D. P. and Tsitsiklis, J. N. (1996), Neuro-Dynamic Programming, Belmont, MA: Athena Scientific, ISBN 1-886529-10-8.

[5] Masters, T. (1995) Advanced Algorithms for Neural Networks: A C++ Sourcebook, NY: John Wiley and Sons, ISBN 0-471-10588-0

[6] Dennis, J.E., and R.B. Schnabel, Numerical Methods for Unconstrained Optimization and Nonlinear Equations, Englewood Cliffs, NJ: Prentice-Hall, 1983.

[7] Battiti, R., First and second order methods for learning: Between steepest descent and Newton's method, Neural Computation, **Vol. 4**, No. 2, 1992, pp. 141-166.

[8] Prechelt, L. (1998). Early Stopping-but when? Neural Networks: Tricks of the trade, (pp. 55- 69). Retrieved March 28, http://www.ipd.ira.uka.de/~prechelt, 2002.

[9] C. Aykanat, K. Oflazer, R. Tahboub. “Parallel Implementation of the Back-propagation Algorithm on Hypercube Systems, in Proceedings of the NATO Advanced Study Institute on Parallel and Distributed Computing, (Springer Verlag), Ankara, Turkey, July 1991.

 ISBN: 978-81-931039-3-7

A SURVEY ON DATA ENCRYPTION USING DNA TECHNIQUE

Prema T.Akkasaligar[1], Farhat Mulla[2]

[1]*Professor, Department of CSE, BLDEA's Dr.P.G.Halakatti College of Engineering and Technology, Bijapur, Karnataka, (India)*

[2]*M.Tech (CSE), Student of BLDEA's Dr.P.G.Halakatti College of Engineering and Technology, Bijapur, Karnataka, (India)*

ABSTRACT

The present paper focuses mainly on the review of literature of encryption techniques using DNA technology. The sensitive information such as financial transactions, medical records of patients and personal records are transmitted over the network is more vulnerable to attacks. The new concept is introduced called DNA computing, brings a new hope for unbreakable algorithms. The paper aims at extensive experimental study of implementation of various available DNA encryption techniques.

Keywords: Encryption, Decryption, DNA Computing, DNA Cryptography

I. INTRODUCTION

Now a day's, providing security is one of the great challenge because of the advancement in digital communication technology, growth of computer power and storage. The different encryption techniques such as symmetric encryption and asymmetric encryption enables security of sensitive information, but the code breakers have come up with various methods to crack these algorithms. A new concept of DNA computing is introduced. Deoxyribonucleic acid (DNA) represents the genetic blueprint of living creatures. DNA is unique for each individual. DNA contains instructions for assembling cells. Every cell in the human body has a complete set of DNA. DNA is a polymer made of monomers called deoxyribonucleotides. Each nucleotide consists of three basic items: deoxyribose sugar, a phosphate group and a nitrogenous base. There are two types of nitrogenous bases: purines (Adenine (A) and Guanine (G)) and pyrimidines (Cytosine(C) and Thymine (T)). Since nucleotide differs only in terms of their bases, we use the base abbreviations to identify them. Single-stranded DNA molecules are simply chains of nucleotides where two consecutive nucleotides are bounded together by a strong covalent bond along a sugar-phosphate "backbone". The most important feature of DNA is the Watson–Crick complementarity of bases. Bonding between single strands occurs by the pairwise attraction of bases; A bonds with T and G bonds with C. The pairs (A; T) and (G; C) are therefore known as complementary base pairs. The two pairs of bases form hydrogen bonds between each other, two bonds between A and T, and three bonds between G and C. In [1] authors have introduced the first trial of DNA based cryptography in which a substitution method using libraries of distinctly, one time pads, each of which defines a specific, randomly generated, pairwise mapping and an XOR scheme utilizing molecular computation and indexed, random key strings are used for encryption.

II. LITERATURE SURVEY

To study and analyze more about the encryption techniques, the following literature survey has been done.

In [2-3], authors have presented an encryption technique using DNA technology. Algorithm works on plaintext and provides more security using the technology of DNA synthesis, polymerase chain reaction (PCR) and DNA digital coding along with traditional cryptography. By applying the special function of primers to PCR amplification, the primers and coding mode are used as the key of the scheme. The traditional encryption method and DNA digital coding both together are used to pre-process the plaintext, which can effectively prevent attack from a possible word as PCR primers. The issues and difficulties of cryptography computing and biological difficulties, provide a double security safeguards for the scheme. The security analysis shows that the encryption scheme has high confidential strength [4]. Moreover, the cost of this encryption scheme will be cut greatly with the progress of biological technologies in the future.

In [5], authors have jointly developed a method called text encryption using DNA stenography where hiding of data is done by applying five different steps. The receiver applies the process of identifying and extracting the original message which is hidden in DNA reference sequence. The main goal is exploring characteristics of DNA molecules, searching for simple methods of realizing DNA cryptography, and laying the basis for future development.

At encryption end, shift each letter in the message to a new letter where the shifted value is k. The shifted message is converted into a binary string B using ASCII value conversion and then convert binary string B into segments, where each bit is of size k = 2, hence convert B into a fake DNA string. After converting into fake DNA, matrix A is constructed. Matrix can be constructed by converting each alphabet in the text into a fake DNA strand. Each DNA strand for the alphabets is taken as a column to construct a 4 x k matrix, where k is the length of the original message. Now obtain a new string by concatenation of the rows of A and send the new string obtained to the receiver. At the decryption end, obtain the matrix A using the new string which is obtained previously. Obtain the binary string B from the conversion table and get the shifted message from the ASCII table. Finally obtain original message using the shift key.

In [6], authors have worked on RGB image encryption algorithm based on DNA encoding combined with chaotic map. RGB image has a high pixel correlation in spatial domain, but traditional encryption algorithm is mostly used to process it on the R, G and B layers, respectively. It is difficult to eliminate the pixel correlation in spatial domain. Aiming to the characteristics of RGB image, authors have used binary DNA encoding to make the mathematical problems into biological problems and introduce the biological knowledge of DNA computing into the proposed algorithm. The algorithm security is decided by chaotic system and DNA operation, to obtain dual security. The algorithm firstly carries out DNA encoding for R, G and B components of RGB image. The addition of R, G, and B are realized by DNA addition. After that complementation operation is carried out using the DNA sequence matrix controlled by logistic. Three gray images are obtained after decoding, finally the encrypted RGB image is reconstructed which uses image pixels disturbed by logistic chaotic sequence.

This encryption algorithm is effective, simple to implement and has a large secret key space, strong secret key sensitivity. Meanwhile, it can resist exhaustive attack, statistical attack, and thus it is suitable for RGB image encryption. In addition, the algorithm also has certain reference value for encryption of video, audio and other multimedia data. The speed performance of the proposed algorithm is not ideal, but authors have used

mathematical model to simulate the proposed algorithm in electronic computer and with the development of the DNA chip technology, it is not difficult to use ultra-large-scale parallel computing, power of DNA computing to implement the algorithm.

In [7], authors have worked on DNA based cryptographic Techniques. DNA encryption comes from DNA computing, initiated with the idea of "computing using DNA not on DNA". A lot of work has been done in the area and many researchers have done encryption based on different techniques like DNA digital encoding, PCR amplification, DNA synthesis, electrophoresis etc. Here an attempt is made for the message encryption along with the idea of adding authentication and message integrity. Encryption can be applied before or after authentication to maintain data confidentiality and data integrity so that only intended receiver can read or modify the data.

In [8], author has presented the method for cloud security. The cloud can be provided more security using DNA cryptography. The major concerns in cloud are the lack of confidentiality, integrity and authentication among the cloud users and service providers. The author in this paper proposed a new techniques for security schemes, to ensure data confidentiality, integrity, authentication and also DNA cryptographic algorithms are adopted for the optimization of data security in cloud computing. Although in its primitive stage, DNA cryptography is shown to be very effective. Theoretical analysis should be performed before its real applications, because it requires a high tech lab and computational limitations, as well as the labor-intensive extrapolation means so far. This makes the efficient use of DNA cryptography, difficult in the security world. The concept of DNA cryptography is used for very powerful and unbreakable encryption technology.

In [9], authors have worked on the technique called DNA based cryptography using random key generation scheme. They have presented a new DNA encryption technique based on mathematical matrix manipulation where they have used a secure generation algorithm for encryption process. The benefit of key generation scheme is, always get a new cipher text for same plaintext and same key. So it provides a good security layer which does not give any hint about plaintext. DNA binary strands support feasibility and applicability of DNA based cryptography. The security and the performance of the DNA based cryptographic algorithms are satisfactory for multilevel security applications of today's network. Certain DNA algorithms can resist exhaustive attack, statistical attack and differential attack. DNA computing is viable and DNA authentication methods have shown great promise in the marketplace of today and it is hoped that its applications will continue to expand. DNA cipher is the beneficial supplement to the existing mathematical cipher. If the molecular word is controlled then it may be possible to achieve vastly better performance for information storage and security .

In [10], authors have presented a paper, DNA based cryptography using permutation and random key generation. Initially plaintext is converted into ASCII code, ASCII code is again converted into binary form to get the data in 0's and 1's. These binary values are encoded in DNA sequences to nucleotide conversion where each of the four bases is represented by combinations of 0's and 1's. A DNA sequence is selected as a key and grouped into the blocks in which each block is of 4 characters. Then a table is created based on the positions of each character in the key sequence. Based on table and the randomly selected DNA sequence, text gets converted into encrypted form. Finally the encrypted sequence with the key is sent to the receiver. The DNA sequence in decryption process gets decoded into binary then that binary is converted into ASCII and finally ASCII to the plaintext. The method explains how traditional cryptography differs from the emerging DNA cryptography.

In [11], authors have presented a paper on enhanced information security using DNA cryptographic. The DNA cryptography is a new and promising area to achieve higher information security, using the characteristics of human DNA. Lots of DNA based encryption methods are proposed by several researchers. In [12], authors have given an idea using some special properties of DNA sequences to encrypt data. The method secretly selects a reference DNA sequence for encryption. In [13], authors have presented a method of data hiding where the data is encrypted using amino acid; DNA based playfair cipher and also use complementary rules to hide the resultant cipher text in a DNA sequence. In [14], authors have used a sort of indexing method over the complementary DNA sequence.

The present algorithm is more secure and uses a couple of 28 bit DNA sequence to generate the secret encryption key after a number of computations. Moreover a better level of message encryption technique is proposed where two rounds of encryption has been carried out among the plain text to generate two secret keys and produce a cipher DNA sequence with appending some extra information within it. As approximately 55 million publicly available DNA sequences are available, it is almost impossible for an intruder to predict the sequence. The message encryption approach is also better than the available cryptographic algorithms based on the DNA due to using some special operations performed on the data. Thus it is very much difficult for the intruders to apply different cryptanalysis on the cipher text.

In [15], authors have presented a paper on secure transmission of plaintext using DNA based message encoding. In the recent year few works on qualitative and quantitative analysis on DNA based cryptography as well as many new cryptographic techniques are proposed by the researchers. Bibhash Roy et al. [16-18] have proposed a DNA sequence based encryption and decryption process. The authors have proposed a unique cipher text generation procedure as well as a new key generation procedure. But the experimental result shows that the encryption process requires high time complexity. In [19], authors have designed a DNA encryption technique based on 4*4 matrix manipulations and using a key generation scheme which makes data much secure. In [20], authors have presented a theoretical and empirical based analysis on application of DNA cryptography.

In [21], author has designed a new method by integrating DNA computing in IDEA. Such conceptual works can be useful in the development of this new born technology of cryptography to fulfil the future security requirements. In this paper; a proposal is given where the concept of DNA is being used in encryption and decryption process. The theoretical analysis shows this method to be efficient in computation, storage and transmission; and it is very powerful in certain attacks. This paper also presents a secured symmetric key generation scheme which generates primary cipher and this primary cipher is then converted into final cipher using DNA sequences, so as to make it again more complicated in reading. Finally, the implementation methodology and experimental results are presented.

In actual scenario, DNA cryptography is far away from realization because in current time it can be performed only in labs using chemical operations. In order to provide better security and reliable data transmission an effective method of DNA based cryptography is presented. In this method the mixture of mathematical and biological concepts are used to get the encrypted data in the form of DNA sequences. The benefit of the scheme is that it makes difficult to read and guess about plaintext. The proposed algorithm has two phases in consequence: these are primary cipher text generation using substitution method followed by final cipher text generation using DNA digital coding.

In [22], authors have presented a symmetric key cryptosystem based on the DNA symmetric cryptosystem using index. As a result of applying the block cipher, the cryptosystem can be standardized and synchronized. Besides,

by applying the method that ciphers plaintext strings have a proper computing with the result come from pseudo random number generator to create cipher text, it presents a proper random key sequence to improve security.

The DNA based encryption provides security but some additional level of security is added using index. The algorithm encodes each character into ASCII codes. According to the nucleotide sequence, the author should convert it to the DNA coding. Besides, the author selected the special DNA sequence as the encryption index, and likewise, the pre-treated plaintext will be divided into different groups. Next, the key created by the chaos key generator based on the logistic mapping and initialized by the number x_0 and μ will take XOR operation with the block-plaintext. The algorithm stores the position as the cipher text. The validity of the algorithm can be proved through simulation and the theoretical analysis, including bio-security and math security. The algorithm has a huge key space, high sensitivity to plaintext, and an extremely great effect on encryption. The algorithm provides an excellent performance of its encryption and an anti-attack ability.

In [23], authors have presented an asymmetric DNA mechanism, a more reliable and more powerful encryption than the OTP DNA symmetric algorithm. The purpose of this paper is to compare the time required to complete the encryption/decryption in the case of the DNA cipher with the time required by other classical encryption algorithms. The DNA cipher requires a longer time for encryption and decryption, comparatively to the other ciphers. Authors would expect these results because of the platform used for developing this algorithm. Java cryptography architecture contains the classes of the security package Java 2 SDK, including engine classes. The methods in the classes that implement cryptographic services are divided into two groups. The first group is represented by the APIs (Application Programming Interface) and the second group is represented by the SPIs (Service Provider Interface). Each SPI class is abstract. In order to implement a specific service, for a specific algorithm, a provider must inherit the corresponding SPI class and implement all the abstract methods. All these methods process array of bytes while the DNA cipher is about strings. The additional conversions from string to array of bytes and back, makes this cipher to require more time for encryption and decryption then other classic algorithms. To emphasize the difference between DNA and classical algorithms a dedicated application (smart cipher) is developed.

The dedicated application shows the encryption and decryption time. Based on this criterion and the strength of the cipher, the user can estimate the efficiency of the used algorithm. The authors have compared the execution time of the DNA symmetric cipher with the time required by other classical encryption algorithms. The algorithm is tested on a random text of 360 characters, which is in string format. To be able to compute the time required for encryption and decryption, authors have used the public static nanoTime() method from the system class which gives the current time in nanoseconds. It is important to understand that the execution time varies depending on the OS used, the memory load and on the execution thread management. Authors have therefore measured the execution time on 3 different machines one machine is Intel Core 2 Duo 2140, 1.6 GHz, 1 GB RAM, Vista OS and second one is Intel Core 2 Duo T6500, and finally third machine is 2.1 GHz, 4 GB RAM, Windows 7 OS. The first machine and second machine (with Windows OS) have larger time variations for the encryption and decryption processes. The third machine, based on the linux platform, offers a better stability, since the variation of the execution time is smaller.

In [24], authors have presented a paper on enhanced level of security using DNA computing technique with hyper elliptic curve cryptography. DNA based elliptic curve cryptographic technique require larger key size to encrypt and decrypt the message resulting in increased processing time, more computational and memory overhead. To overcome the above limitations, DNA strands are used to encode the data to provide first level of

security and HECC encryption algorithm is used for providing second level of security. HECC is better than the existing public key cryptography technique such as RSA, DSA, AES and ECC in terms of smaller key size. DNA cryptography is a next generation security mechanism, storing almost a million gigabytes of data inside DNA strands. Hence this proposed integration of DNA computing based HECC provides higher level of security with less key size of HECC-80 bits than ECC-160 bits and with less computational and memory overhead.

In this present method first level of security is provided by converting original text message into DNA nucleotide which can able to store millions of data in a single DNA strands. Further encoded nucleotide is converted into numbers. Second level of security is provided by converting numbers into points using Koblitz method. These points act as plaintext for encryption using hyperelliptic curve cryptography. MATLAB simulation tool is used to simulate the proposed cryptographic scheme for different key size and processing time. Recent research shows that HECC are well suited for various software and hardware platforms and their performance is compatible to that of ECC.

In [25], authors have presented a DNA based implementation of YAEA encryption algorithm, used to enhance the security of cryptography. The investigation conducted in this paper is based on a conventional symmetric encryption algorithm called “Yet another Encryption Algorithm” (YAEA) developed by Saeb and Baith. It was Adleman, with his pioneering work [Adleman, 1994], who set the foundation for the new field of bio-computing research. His main notion is to use actual chemistry to solve problems that are either unsolvable by conventional computers, or require a massive amount of computation.

The present method is effortlessly scalable for large digital information products. The algorithm is effective at encrypting and decrypting digital information from biological DNA strand. The algorithm utilizes a sequential search algorithm in order to locate and randomly return one of the many positions of quadruple DNA nucleotides sequence representing the binary octets of plain-text characters. The decryption process is achieved by using the pointer file and the same random binary file that is available to both sender and receiver in advance. The algorithm is a symmetric cipher consisting of recording pointers to the randomly selected locations of the file in the searchable DNA strand for each plaintext character. Authors have conducted a test by recording the time needed to encrypt the “Uncle Tom’s Cabin” novel using six different DNA strands of different lengths. Utilizing a dedicated 3.2 GHz CPU employing 3G RAM.

III. PERFORMANCE PARAMETERS

In [26], authors have presented a paper on hybrid encryption using DNA technology. They defined a set of parameters, based on which the performance can be evaluated and compared with the existing encryption technique using DNA technology such parameters are as follows.

3.1 Statistical Analysis

The encrypted image should not have any statistical similarity with the original image to prevent the leakage of information

3.2 Histogram Analysis

To get the good performance, histogram of original image and encrypted image should not be similar.

3.3 Correlation Coefficient Analysis

In most of the plaintext-images, there exists a high correlation among adjacent pixels, while there is a little correlation between neighbouring pixels in the encrypted image. It is the main task of an efficient image encryption algorithm to eliminate the correlation of pixels. Two highly uncorrelated sequences have approximately zero correlation coefficient [27].

3. 4 Differential Attacks

Attackers often make a slight change for the original image, use the proposed algorithm to encrypt the original image before and after changing, and compare two encrypted images to find out the relationship between the original image and encrypted image.

3.5 Known-Plaintext and Chosen Plaintext Attacks

For encryption with a higher level of security, the security against both known-plaintext and chosen-plaintext attacks are necessary. Chosen/Known-plain text attacks are such attacks in which one can access/choose a set of plain texts and observe the corresponding encrypted texts.

3.6 Brute Force Attack

Brute force attack or exhaustive key search is a strategy that can be used against any encrypted data by an attacker who is unable to take advantage of any weakness in an encryption system that would otherwise make his task easier. It involves systematically checking all possible keys until the correct key is found [26].

IV. CONCLUSION

Now a days, the security for the data has become highly important since sensitive information such as financial transactions, medical and personal records are transmitted through public communication facilities and also transmission of digital products over the open network occur very frequently. In this paper, the survey is done on existing works on the encryption techniques using DNA. The different DNA encryption techniques are studied and analyzed well to promote the performance of the encryption methods also to ensure the security proceedings. To sum up, all the techniques are useful for real-time encryption. Each technique is unique in its own way, which might be suitable for different applications. Everyday new DNA encryption technique is evolving hence fast and secure conventional DNA encryption techniques will always work out with high rate of security.

REFERENCES

[1] Gehani, Ashish La Bean, Thomas H. Reif, H.John, “DNA based cryptography”, Dimacs Series in Discrete Mathematics and Theoretical ComputerScience, 2000, pp.162-167.

[2] J. Kawai and Y. Hayashizaki, DNA book. Genome Res, Vol. 13, 2003, pp.1488–1495.

[3] T. Kamei, “DNA-containing inks and personal identification systemusing them without forgery”, Jpn. Kokai Tokkyo Koho, 2002, p.8.

[4] Guangzhao Cui , Limin Qin , Yanfeng Wang , Xuncai Zhang, “An encryption scheme using DNA technology”, Computer Engineering and Applications,2008, pp.37-42.

[5] M. Yamuna, Nikhil Bagmar, Vishal, "Text encryption using DNA stenography", International Journal of Emerging Trends & Technology in Computer Science, 2013, Volume 2, Issue 2, ISSN 2278-6856,pp.231-233.

[6] Lili Liu, Qiang Zhang, Xiaopeng Wei, "A RGB image encryption algorithm based on DNA encoding and chaos map", Computers and Electrical Engineering, 2012, www.elsevier.com/locate/compeleceng, pp.1-9.

[7] Kritika Gupta, Shailendra Singh, "DNA based cryptographic techniques: a review", international Journal of Advanced Research in Computer Science and Software Engineering, 2013, Volume 3, Issue 3, ISSN: 2277 128X , pp.607-610.

[8] Anup R. Nimje, "Cryptography in cloud-security using DNA (Genetic) techniques", 2012, Vol. 2, Issue5, ISSN: 2248-9622, pp.1358-1359.

[9] P.Surendra Varma, K.Govinda Raju, "Cryptography based on DNA using random key generation scheme", International Journal of Science Engineering and Advance Technology, IJSEAT ,2014, Vol 2, Issue 7, ISSN 2321-6905, pp.168-175.

[10] Bonny BRaj, Panchami, "DNA based cryptography using permutationand random key generation method, International Conference On Innovations & Advances In Science, Engineering And Technology",2014, Volume 3, Special Issue 5, ISSN (Online) : 2319 – 8753, ISSN (Print) : 2347 – 6710, pp.263-267.

[11] AbhishekMajumdar, Meenakshi Sharma, "enhanced information security using DNA cryptographic Approach", International Journal of Innovative Technology and Exploring Engineering, 2014, Volume-4 Issue-2, ISSN: 2278-3075, pp.72-76.

[12] H.Z. Hsu and R.C.T.Lee, "DNA based encryption methods", The 23rd Workshop on Combinatorial Mathematics and Computation Theory, National Chi Nan University Puli, NantouHsies, Taiwan 545, April 2006, pp.145-150.

[13] AmalKhalifa and Ahmed Atito. "High-capacity DNA-based stegano graphy", The 8th International Conference and informatics and Systems (INFOS2012), IEEE, May.2012, pp.76-80.

[14] Mohammad Reza Abbasy, PouryaNikfard, Ali Ordi, Mohammad RezaNajaf Torkaman, "DNA base data hiding algorithm", in international Journal on New Computer Architectures and TheirApplications.2012, ISSN: 2220-9085, pp.183-192.

[15] SnehalJavheri, Rahul Kulkarni, "Secure data communication and cryptography based on DNA based message encoding", International Journal of Computer Applications, 2014,Volume 98– No.16, pp.35-40.

[16] Bibhash Roy, GautamRakshit, PratimSingha, Atanu Majumder, Debabrata Datta, "An improved symmetric key cryptography with DNA based strong cipher", ICDeCom, 2011, Feb' 24-25'2011, pp.1-5.

[17] Bibhash Roy et al, "A DNA based symmetric key cryptography", ICSSA, 2011, 24-25 Jan'11.

[18] Bibhash Roy, GautamRakshit, PratimSingha, Atanu Majumder, Debabrata Datta, "An enhanced key generation scheme based cryptography with DNA logic", IJICT, 2010-11, Volume 1 No. 8, Dec' 2011.

[19] Miki Hirabayashi, Akio Nishikawa, "Analysis on secure and effective applications of a DNA based cryptosystem", IEEE computer Society, 978-0-7695-4514-1/11, 2011, pp.205-210.

[20] Nucleotide base pairing of strands, http://dedunn.edblogs.org, 2012.

[21] TusharMandge, Vijay Choudhary, "A DNA encryption technique based on matrix manipulation and secure key generation scheme", ICICES Journal, 2013,Print ISBN:978-1-4673-5786-9, pp.47-52.

[22] Zhang Yunpeng, Zhu Yu, Wang Zhong, Richard O.Sinnott, "Index based symmetric DNA encryption algorithm", Proceedings of the 4th International Congress on Image and Signal Processing, 2011, http://hdl.handle.net/11343/32713 , pp.2290–2294.

[23] Er.RanuSoni, Er.VishakhaSoniand Er.Sandeep Kumar Mathariya, "Innovative field of cryptography: DNA cryptography", CS & IT-CSCP, 2012, pp. 161–179.

[24] P.Vijayakumar, V.Vijayalakshmi, G.Zayaraz, "Enhanced level of security using DNA computing technique with hyperelliptic curve cryptography", ACEEE Int. J. on Network Security, 2013, Vol. 4, No. 1,pp.1-5.

[25] T. Amin, MagdySaeb, Salah El-Gindi, "A DNA-based implementation of YAEA encryption algorithm", IASTED International Conference on Computational, 2006.

[26] Grasha Jacob1, A. Murugan, "A hybrid encryption scheme using DNAtechnology", The International Journal of Computer Science and Communications Security, 2013, Volume 3, pp.61-65.

[27] Hiremath P.S., Prema T.Akkasaligar and Sharan Badiger, "Speckle noise reduction in medical ultra sound image, advancement and breakthrough in ultra sound images", in Tech Publisher, Crortia, 5th june 2013, pp.201-241, (DOI:10.5772156519).

THE NOVEL IMAGE BASED CAPTCHA FOR SECURITY IN WEB APPLICATIONS

Miss Rachana P G [1], Dr. Shrinivasa Naika C L [2]

[1]Student, [2]Assistant Professor, Computer Science and Engineering, UBDTCE, VTU (India)

ABSTRACT

Internet is being used for various activities by great range of users even through smart phones, tablets and other mobile devices. It is crucial for websites to differentiate human users and computer programs because malicious computer programs are threat for availability and security of websites. The challenge is to stop automated scripts from enforcing DOS attack, while ensuring proper service to genuine users. This paper proposes a novel image based CAPTCHA which overcome the disadvantage of language dependency in text CAPTCHA and it combines touch based input methods favored by mobile devices to solve CAPTCHA which is generated through unique steps. To solve CAPTCHA, user must correctly identify visually distorted human faces embedded in complex background without selecting any non human faces.

Keywords: CAPTCHA, Face detection, Mobile Security, Web Security

I. INTRODUCTION

Security is a major concern on web exposed systems holding valuable data or something that can be compromised.

There are many types of attacks that can be carried out on these systems. A variety of bots, spiders, DOS attacks, domain hijacking, worms and spam pose a serious threat to online systems and can cause major losses. So there is a great need for secondary authentication to reduce automated attacks while posing a minimal hindrance to legitimate users. CAPTCHA is one of the possible ways to classify human users and automated scripts. Completely Automated Public Turing Test to Tell Computers and Humans Apart or CAPTCHA is the standard security technology designed to distinguish between genuine users and automated scripts. The objective of CAPTCHA is to ensure proper service to genuine users while minimizing the attacks by bots. CAPTCHAs are being used for several services including web and financial services, and to provide security against malicious attacks. CAPTCHA focuses on developing tests that are easy for humans to solve and difficult for automated approaches. The challenge is to stop automated scripts from enforcing DoS attack. Existing CAPTCHA algorithms can be broadly grouped into three classes [1]: (1) text based, (2) image-based, and (3) video- and audio-based CAPTCHAs. Text-based CAPTCHAs are the most common and widely used form. These CAPTCHAs require the users to decipher text that has been visually distorted and rendered as an image. A major shortcoming of these early approaches was vulnerability to segmentation, where each character could be identified in isolation. This greatly simplifies attacks using optical character recognition techniques. One solution was proposed to design the CAPTCHA such that one-to-one mapping between characters and outlines

was distorted. As an alternative to text, several CAPTCHA applications utilize image classification or recognition tasks as part of their test and overcome disadvantage of language dependency. Other than text and image CAPTCHAs, video and audio CAPTCHAs have also been proposed. Video-based CAPTCHAs function by posing the tagged videos with descriptive text. To provide access for visually-impaired users, audio CAPTCHAs are used as an alternative to standard visual CAPTCHAs. These work by playing a recording of words or letters which users are then asked to enter.

Due to recent developments in technology, users are rapidly adopting smart phones, tablets, and other non-traditional smart computing devices in lieu of desktop and laptop computers. Traditional input devices such as keyboards and mice are being replaced by more interactive touch screen technology. With advanced mobile devices, users can easily access Internet services such as online shopping and e-banking. These large-scale applications require improved interfaces (including security systems) designed to easily serve the growing mobile market [2]. Presently, a number of techniques provide device-level security to protect users in case of loss or theft of their mobile device. Solutions based on typing such as passwords and PIN codes dominate, but newer mobile-friendly techniques such as picture puzzles [3], tracing patterns [4], and biometrics features including touch pattern analysis [5], fingerprints, and facial images are gaining popularity and acceptance. While many online service providers have completely redesigned their website portals or maintain special mobile versions of their websites, relatively little progress has been made with similar redesigns of application-layer security tool to protect the online resources which mobile users access. CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart) is one major example of a security tool.

Key contributions of this research include:

1) Design of an interactive non-keyboard-based (touch screen-compatible) image CAPTCHA to facilitate easy use on mobile devices.

2) Generation of computationally-challenging face detection CAPTCHA tests to provide enhanced security.

In this paper, we propose a Novel Image based CAPTCHA method. In section 2, we analyze the main design idea of this new implementation of CAPTCHA mechanism. In section 3 we give an example of our implementation, and illustrate the flow chart step by step. Section 4 concludes with a research summary.

II. DESIGN

In this paper, we present Novel Image Based CAPTCHA — in which four to six distorted face/non-face images are embedded in a complex background and a user has to correctly mark the center of all the face images within a defined tolerance.

2.1 Algorithm of Design

CAPTCHA generation:

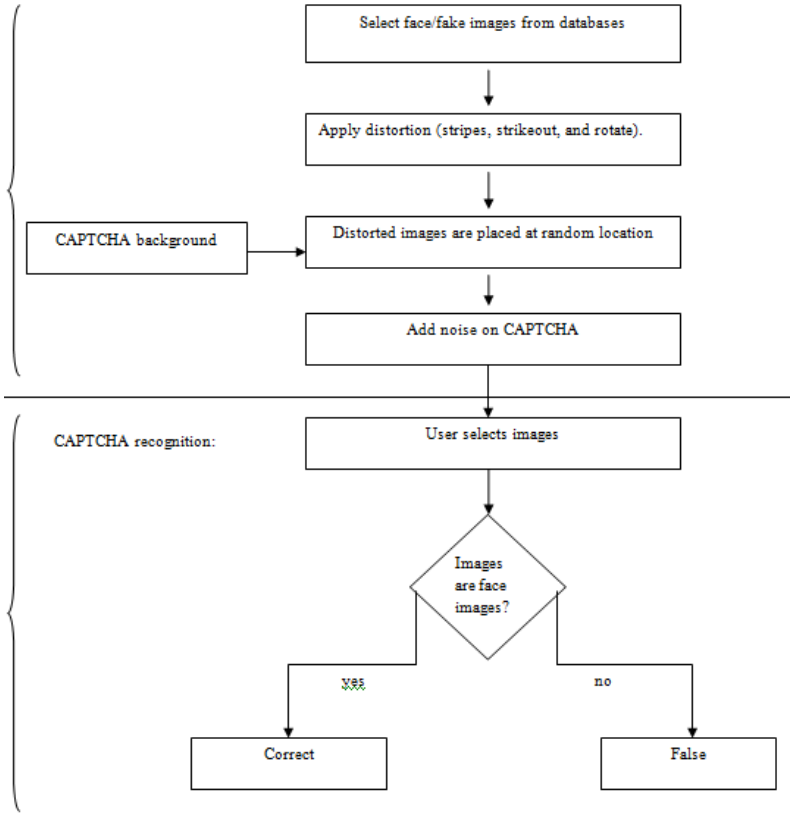


Fig.1 Algorithm of Design

III. THE PROPOSED NOVEL IMAGE BASED CAPTCHA ALGORITHM

The proposed Novel Image Based CAPTCHA algorithm utilizes the limitations of automatic algorithms to create image CAPTCHAs. In other words, the proposed algorithm is based on optimizing sets of parameters on which standard face detection algorithms fail but humans can succeed. The process of using Novel Image Based CAPTCHA is as follows:

- The face CAPTCHA image containing distorted and occluded genuine face images and fake images on a random background is shown to a user.
- The user must select all genuine face images present in the CAPTCHA.
- If all the responses are correct (i.e. approximate center of all genuine faces are marked correctly) then the test is solved otherwise not.

3.1 Generating Novel Image Based CAPTCHA

In the Novel Image Based CAPTCHA design, we choose the following parameters (and related operations):

- The first parameter is the total number of images, both genuine and fake faces, and is represented as n_{total}. Genuine faces are images of real humans collected from different publicly available face databases. Fake faces are images of cartoons and other objects known to generate false positives by automatic face detectors.
- The number of genuine face images in a CAPTCHA, represented as n_{face}, is the second parameter. In a given CAPTCHA, $n_{total} = n_{face} + n_{fake}$. Where n_{face} is the number of fake images. For a given CAPTCHA,

we only need to define n_{fake} and n_{face}. Also, randomly changing these parameters in each (new) CAPTCHA can change the content such that only a genuine human user can respond correctly.

- The third parameter, CAPTCHA background B, is important to make sure that background has randomness to confuse automatic face detection algorithms. B contains parameters such as the number of background shapes to be generated (n_s), the number of dilation operations to be adopted (n_d), and the number of random portions to be placed (n_p).
- Location (x, y) of each constituent image is an important factor. With random location, the segmentation is more difficult than if a static location scheme is used.
- Next, five distortion operations are applied as follows:

Ø Stripes of three to six pixels width are applied on some constituent images (faces and fake faces) in the CAPTCHA. It is not necessary that this operation is applied uniformly on all face or fake face images in a CAPTCHA. An example of this operation is shown in Fig. 2(a).

Ø Rotate operation is used to rotate the constituent face and fake images with θ^0 angle (Fig. 2(b)).

Ø Strikeout operation, as shown in Fig. 2(c), is used to cover key facial features such as eyes and mouth with some transparency.

Ø Blending operation is used to smoothly blend the constituent face and fake images with the background, as shown in Fig. 2(d).

Ø Noise addition. Using the above mentioned parameters and operations, the CAPTCHA image is prepared and then noise is added on the complete CAPTCHA image. The type parameter is used to select the type of noise to be applied (additive, multiplicative or salt & pepper). Collectively, these parameters are referred to as n_s.

(a) and (b) **(c)** **(d)**

Fig.2 Illustrating the Effect of (A) Stripes,(B) Rotation, (C) Strikeout And (D) Blending with The Background and Noise Adding.

3.1.1 Background Generation

Here, we have followed the random color approach, in this approach; the background image is created using random shapes such as circles, squares, and crosses with randomly chosen sizes and colors. These shapes are then pasted on the canvas at random co-ordinates to generate the final background image. This background image is then dilated before being used for CAPTCHA generation.

a. b.

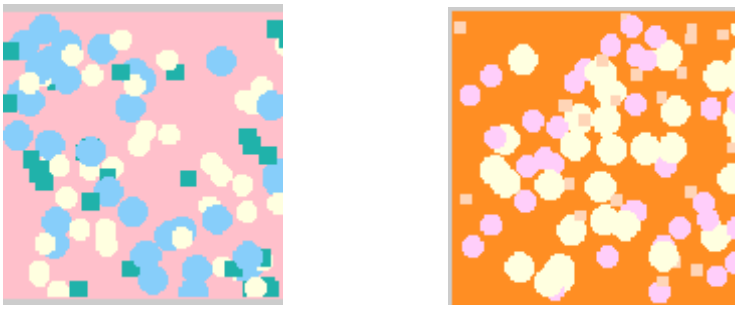


Fig.3. a and b: Background Generation Using Random Color Approach.

To make the background more complex for automated bots to attack or break the CAPTCHA, we are using different types of noises such as Gaussian noise and salt pepper noise. In order to make image selection complex for automated systems we are using different structural elements such as disks, ball and square shapes and we are dilating the shapes to make CAPTCHA solving easier for human and difficult for automated systems.

3.1.2 Novel Image Based CAPTCHA generation

Below are the steps in generating Novel Image Based CAPTCHA:

Step 1: From a set of genuine and false face images, randomly select $n_{face} \geq 2$ (i.e., the number of face images) and

$n_{fake} \geq 1$ (i.e., the number of fake images).

Step 2: Each constituent image (both genuine and fake) is processed using the distortion operations (stripes, strikeouts, and rotate).

Step 3: Each constituent face image is placed at a randomly selected location (x, y) on the CAPTCHA background B.

Step 4: At the end, one of the three noise operations {additive, multiplicative, or salt & pepper}, is applied on the complete CAPTCHA image to generate the final CAPTCHA.

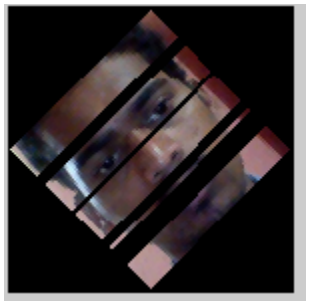


Fig.4 Image Underwent Distortion Operation.

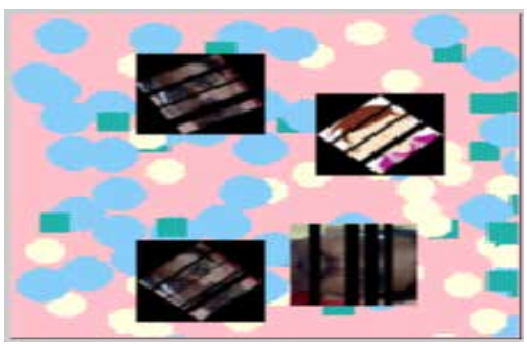


Fig.5 Placing Images in Random Location

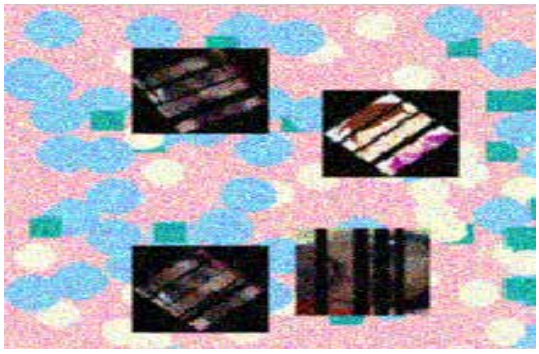


Fig.6 Addition of noise

IV. CONCLUSION

This paper presents the Novel Image Based CAPTCHA algorithm that utilizes the difference between face detection capabilities of humans and automated algorithms. By combining face detection with visual distortions, it is possible to create a test that is simple for human users to solve while effectively eliminating automated attacks. The proposed methodology offers major benefits over traditional text-based CAPTCHAs, most notably language independence. By incorporating the proposed Novel Image Based CAPTCHA into existing online authentication schemes, developers can substantially reduce the likelihood of credentials-based attacks. In requiring users to solve the CAPTCHA in addition to providing a username and password, an additional dimension of complexity can be added that requires human effort. The Novel Image Based CAPTCHA point-and-click-based implementation adds this additional stage with minimum difficulty for users. It can be readily used on mobile devices since it has no language requirements and does not require a keyboard for data entry.

REFERENCES

[1] Gaurav Goswami et al., FaceDCAPTCHA: Face detection based color image CAPTCHA , Future Generation Computer Systems (2012),doi:10.1016/j.future.2012.08.013.

[2] R. A. Botha, S. M. Furnell, and N. L. Clarke, ``From desktop to mobile: Examining the security experience," Comput. Security, vol. 28, nos. 3_4, pp. 130_137, 2009.

[3] J.-C. Birget, D. Hong, and N. Memon, ``Graphical passwords based on robust discretization," IEEE Trans. Inf. Forensics Security, vol. 1, no. 3, pp. 395_399, Sep. 2006.

[4] N. Ben-Asher, N. Kirschnick, H. Sieger, J. Meyer, A. Ben-Oved, and S. Möller, ``On the need for different security methods on mobile phones," in Proc. 13th Int. Conf. Human Comput. Interaction with Mobile Devices and Services, 2011, pp. 465_473.

[5] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, ``Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication," IEEE Trans. Inf. Forensics Security, vol. 8, no. 1, pp. 136_148, Jan. 2013.

[6] H. Lee, S.-H. Lee, T. Kim, and H. Bahn, ``Secure user identi_cation for consumer electronics devices," IEEE Trans. Consum. Electron., vol. 54, no. 4, pp. 1798_1802, Nov. 2008.