TWO-CHANNEL NON-INTERACTIVE MULTI-LEVEL KEY ESTABLISHMENT FOR BUNDLE SECURITY PROTOCOL OF DELAY/DISRUPTION TOLERANT NETWORKS (DTNS)

M. Srimathi[1] , M.Karthigha[2]

[1] PG scholar, [2]Assistant Professor, Department of CSE,
Sri Ramakrishna Engineering College, Coimbatore (India)

ABSTRACT

Protected, low-overhead key establishment is vital to maintain the high level of confidence and security that are necessary in several categories of Delay Tolerant Networks (DTNs). A small number of works presenting solutions to DTN key establishment have concentrated principally on targeted networking atmospheres. In this work, to deal with the key establishment concern for Bundle Protocol (BP), a time-evolving topology model and two-channel cryptography is formulated to design well-organized and non-interactive multilevel key exchange protocol. A time-evolving model is employed to properly model the periodic and fixed behaviour patterns of space DTNs, and consequently, a node can plan when and to whom it should transmit its public key. In the meantime, the application of two-channel cryptography allows DTN nodes to exchange their public keys or revocation position information, with authentication assurance and in a non-interactive approach. This approach facilitates to set up a secure context to maintain BSP, tolerating huge delays, and unanticipated loss of connectivity of space DTNs. The experimental investigation reveals the security and provides enhancement in peculiarities, problems and opportunities a DTN network maintenance.

Keywords*: *Bundle Authentication, Cryptographic Controls, Key Establishment, Space-Based Delay Tolerant Networks

I. INTRODUCTION

Delay – Disruption Tolerant Architecture, DTN is meant to provide connectivity in Heterogeneous networks which lack incessant connectivity due to disruptions or considerable delays like that of networks operating in mobile or extreme terrestrial environments or planned network in space. The DTN effectively improves network communications where the network connectivity is Periodic/Intermittent and or Prone to disruptions [1]. The Store and Forward technique via the Bundle Protocol (BP) of the Delay Tolerant Network facilitates the flow of data/information across any complex or intermittent network traffic. Initially developed for Deep Space Communication (Inter Planetary Internet), the Delay-Disruption Tolerant Network communication model can also be used in Wireless (Terrestrial) environments, both in Military and Civilian Applications. The design of DTN and the protocol did not evolve without consideration for security which led to the development of relevant security documentations [2] [3] to address DTN-related security issues. The security documentations highlight security requirements, define design considerations, identify possible threats as well as open issues.

From the DTN security documentations and the security analysis in [4,5], the identified threats this work is designed to address are masquerading, modification and replay.

The use of PKI is associated with constraints like authorization server unavailability and limited capabilities of certain nodes for cryptographic operations. The focus of this paper is to investigate how PKI concept can be used to provide an authentication solution that does not depend on server availability during post trust establishment network communication while taking the capabilities of the entities into consideration. The existing PKI based schemes in DTN are [5] and [6,7]. These schemes either use certificates and encourage large storage of security credentials or depend on server availability. Here utilized a time-evolving topology model and twochannel cryptography to design efficient and noninteractive key exchange protocol.

The contributions of this paper are summarized as follows: 1) Implementing traditional PKI to provide trust initiation/establishment; 2) introducing the proposed two-channel cryptography and out-of-band channels for PKI based certificate; 3) proposing a time-evolving model to formally model the periodic and predetermined links of space DTNs; and 4) evaluating the performance of the proposed and reference schemes through simulation.

II. TWO-CHANNEL CRYPTOGRAPHY AND OUT-OF-BAND CHANNELS

As above-mentioned, the BSP needs a way of distributing public keys to support for this specification. Generally, anon-interactive message authentication protocol uses two separate channels. One is a broadband insecure channel and the other is a narrow-band authenticated channel. Some practical narrow-band channels include Voice-over-Internet-Protocol (VoIP), data imprinting by a user, Near Field Communication (NFC), infrared, laser, or visible light between two devices [8]. The narrow-band channels are generally called as Out-Of-Band (OOB) channels [9]. What follows are the common assumptions on twochannel cryptography. A broadband channel is insecure and an adversary has full control over this channel. The adversary can eavesdrop any messages sent over the broadband channel, modify the messages sent via this channel, and insert a forged message into this channel at any time that it likes. On the other hand, an adversary has limited control over the narrow-band authenticated channel. In detail, the adversary cannot modify the information transmitted over the narrowband authenticated channel. Balfanz et al. introduced the idea of hashing the data to be authenticated and delivering the hash value over the narrow-band authenticated channel to the verifier [10].In Figure 1, a broadband insecure channel is denoted by a single arrow line and a narrow-band authenticated channel is denoted by a double arrow line. In practice, the narrow-band channels are generally derived from OOB channels, which can be used in space DTNs context for bootstrapping security contexts and exchanging public keys. There are several issues that need to be addressed, such as, the balance between usability and security, the adaptation to diverse scenarios and contexts. A laser channel is used for implementing an OOB channel in space DTNs. In addition, the major merits of OOB channels are message integrity and authentication, instead of confidentiality.

2.1 Design of Network Model and Adversary Model

In this section, the network model and the adversary model is described, followed by design goals.

2.1.1 Network Model

In this work, space DTNs which can bridge between heterogeneous subnetworks using the Bundle Protocol suits are considered. Such a space network is recognized as evolving over time, i.e., its topology changes when some nodes appear, disappear because of being sheltered by celestial bodies, or move around. For space DTNs, this time-evolving property is periodic and predetermined. Given the prior knowledge pertaining to the relevant movement of celestial bodies and the positions of ground-based network nodes, space DTNs can be modelled by utilizing the time-evolving topology model. At least, ground stations and relay satellites with predetermined orbits can offer a deterministic framework which serves as the backbone for space networks.

In case of scheduled and periodic contacts, the public key exchange, update and the issuing of revocation status can be implemented based on time evolving network models combined with two-channel message authentication mechanisms, since OOB channels are easy to be achieved owning to the periodic and predetermined security aware contacts. In a time-evolving network model [11], a sequence of static graphs is needed to model this type of networks. As shown in Fig.1, each static graph is a snapshot representing nodes and the contacts between them at a certain moment. In this diagram there is no end-to-end path between some node pairs at one time-step, and the network is not connected at some time-steps as well. Then, the dynamic network with a sequence of snapshots is able to describe the evolution of the topology and the node mobility over a period of time.

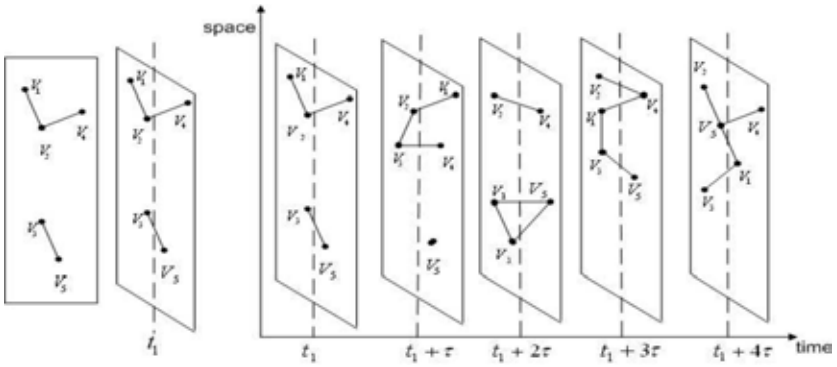


Fig.1. Time-Evolving Model of Dtns

2.1.2 Adversary Model

Consider that the adversary's objective is to make the receiver (Bob) accept a public key PK along with the identity of the sender (Alice), when the public key PK was never sent by Alice to Bob. Two main types of attacks are considered: impersonation attacks and substitution attacks. An impersonation attacker attempts to convince the receiver (Bob) that a public key PK is sent from the sender (Alice), but Alice never sent PK and this session is factually initiated by the adversary. Here, note that, according to the model, the adversary cannot modify the data delivered over the narrowband authenticated channel, but he/she can replay this data.

2.1.3 Design Goals

Design goal is to address the key management issue of BSP for space DTNs, and to design a public key exchange protocol that will replace the application of any conventional online key distributing protocol or PKI. Specifically, aimed at making a public key generally-available, updating a public key, and repealing a public key, without resorting to the conventional mechanisms such as online key distributing, shared secrets, PKI, or trusted third parties. Here, a public key exchange protocol is a protocol that is used to exchange authentic copies of public keys between nodes.

2.2 The Proposed Scheme

The current BSP is built on the assumption that the DTN nodes already have access to authenticated copies of each other's public keys. That is, the DTN nodes know who they are supposed to be talking to. This assumption can be achieved by combining pre-authentication with periodic key exchange via OOB channels. In this section, proposed public key establishment scheme which will provide a fundamental key management support for BSP of space DTNs. The scheme consists of two stages: a bootstrap stage and an exchange stage.

2.1.2 Initiating and Bootstrapping Security Contexts

In this paper, pre-authentication mechanism is preferred to use to bootstrap the secure contexts for BSP secure communications. At bootstrapping stage, by exploiting two-channel cryptography techniques, the authentication information comes directly and demonstratively from their owners via authenticated OOB channels, and then the legality of this information can be confirmed easily. With respect to pre-authentication for space DTNs, an appropriate OOB channel is considered to be a manner with human attention. What this means is that the parties exchange key information via physical contacts (a type of authenticated OOB channels), such as injecting authenticated public keys by space mission authority, which is able to support demonstrative and authoritative identification. Another candidate OOB channel is audio band or vision band between two nodes. The demonstrative properties of such OOB channels with human attention enable a target device to be identified in communication. The key information that is established via such physical contacts during pre-authentication will then is used for subsequent secure communication using BSP.

2.3 Non-Interactive Multi-Level Key Establishment

NMKE is based on multi-variate symmetric polynomials, which was first proposed in [12] for group key agreement. In particular, at the initialization stage of NMKE, the root node of the hierarchy generates a ran- dom six-variate polynomial $\mathcal{F}(x_1; x_2; x_3; y_1; y_2; y_3)$ (referred to as the *master polynomial*) in the finite field $F_q, s.t., \mathcal{F}(, x_i, \ldots, y_i;) = \mathcal{F}(; y_i; ; ; x_i;), i = 1; 2; 3$. For each node *A* at the second level, the root node assigns a public identifier *IDA* to *A* and gives *A* a five-variate polynomial share $\mathcal{G}_A(x_2; x_3; y_1; y_2; y_3) = \mathcal{F}(ID_A; x_2; x_3; y_1; y_2; y_3)$. Then *A* further distributes four-variate polynomial shares to its chil- dren nodes (say *B*), $\mathcal{H}_B(x_3; y_1; y_2; y_3) = \mathcal{G}_A(IDB; x_3; y_1; y_2; y_3)$. Finally, a leaf node *C* that is a child of *B* obtains a three- variate polynomial share $U_C(y_1; y_2; y_3) = \mathcal{H}_B(ID_C; y_1; y_2; y_3)$.

In NMKE, each node has an unique identification vector (IV), which consists of three elements and is used for key establishment. The root node's IV is (null; null; null), where the value of null is equal to 1. The IV of a second-level node A is $(ID_A; null; null)$, and a third-level node B whose parent is A has the IV $(ID_A; ID_B; null). (ID_A; ID_B; ID_C)$ is the IV of C, which is a child of B. To compute a secret key, each node evaluates its polynomial share by fixing all x's (if any) to be null and setting all y's as the elements of the other node's IV. For example, when C attempts to establish a shared key with a second-level node D, C computes $K_{C,D} = U_C(ID_D; null; null) = \mathcal{F}(ID_A; ID_B; ID_C; ID_D; null; null)$, while D computes $K_{D,C} = \mathcal{G}_D(null; null; ID_A; ID_B; ID_C) = \mathcal{F}(ID_D; null; null; ID_A; ID_B; ID_C)$.

Due to the symmetry property of $\mathcal{F}(x_1; x_2; x_3; y_1; y_2; y_3), K_{C,D} = K_{D,C}$.

The above construction can only achieve partial resistance to collusion attacks at each level. To address this problem, Random Perturbation Polynomials (RPPs) is added to the polynomial shares that are distributed to

third-level nodes and leaf nodes. The purpose of this is to prevent the attacker from getting the original polynomial shares, which are the essences of breaking the master polynomial. In particular, A generates (for its child B) a four- variate perturbed polynomial share

$\mathcal{H}'_B(x_3; y_1; y_2; y_3) = \mathcal{H}_B(x_3; y_1; y_2; y_3) + h_B(x_3; y_1; y_2; y_3)$ where $h_B(x_3; y_1; y_2; y_3)$is a RPP with r-bit outputs, $r < l = \lceil \log_2 q \rceil$ and $\mathcal{H}_B(x_3; y_1; y_2; y_3) = \mathcal{G}_A(ID_B; x_3; y_1; y_2; y_3)$. Similarly, C obtains $U'_C(y_1; y_2; y_3) = U_C(y_1; y_2; y_3) + u_C(y_1; y_2; y_3)$. Due to the existence of RPPs, the least significant r bits of the outputs of polynomial evaluations are perturbed. Hence, the most significant $l - r$ bits of the outputs are used as the key. If the $(l - r)$ bit key segment is not long enough to resist brute-force-based attacks, multiple master polynomials can be used simultaneously and concatenating these key segments can form a strong cryptographic key.

The design of RPPs is combining Lagrange interpolation and the construction algorithm for univariate perturbation polynomials. Let $I_1; I_2; I_3$ denote the domains of $x_1; x_2; x_3$ $(or\ y_1; y_2; y_3)$, respectively. In other words, I_i is the set of identifiers of the nodes at the $(i + 1)$-th level. Let JX denote the set of identifiers of X's children. In NMKE, the RPP for a four-variate polynomial share (of node B) is constructed as $h_B(x_3; y_1; y_2; y_3) = \sum_{i=1}^{\lambda} \alpha_{B,i}(x_3) \cdot \beta_{B,i}(y_1) \cdot \psi_i(y_2; y_3)$

where,

- $\alpha_{B,i}(x_3), i \in [1, \lambda]$ is a $r_1$bit RPP constructed on the fly using Lagrange interpolation with randomly picked data points $\{(c_j, d_j): c_j \in J_B, d_j \in_R [0, 2^{r_1} - 1]\}$
- $\beta_{B,i}(y_1), i \in [1, \lambda]$ is a r_2-bit RPP constructed on the fly using Lagrange interpolation with randomly picked data points$\{(e_j, f_j): e_j \in I_1, f_j \in_R [0, 2^{r_2} - 1]\}$
- $\psi_i(y_2; y_3), i \in [1, \lambda]$is a r3-bit RPP pre-computed using the algorithm

Note that the degrees of $\alpha_{B,i}(x_3)\ and\ \beta_{B,i}(y_1)$ are $|J_B|$ and $|I_1|$, respectively, which are fairly small since there are limited number of nodes (resp. children) at the first level (resp. of B). Furthermore, the construction algorithm ensures that $\psi_i(y_2; y_3)$can have a small degree and scale to potentially large domains $(i.e., I_2 \times I_3)$. The perturbation length of $h_B(x_3; y_1; y_2; y_3)\ is\ r = r_1 + r_2 + r_3$. Similarly, the construction of three-variate RPP for leaf node C is $u_C(y_1; y_2; y_3) = \sum_{i=1}^{\lambda} \beta_{C,i}(y_1) \cdot \psi_i(y_2; y_3)$

III. NON-INTERACTIVE MULTILEVEL PUBLIC KEY EXCHANGE FOR SPACE DTNS

In addition to initiating and bootstrapping as above described, the DTN nodes need to exchange and update their public keys periodically in the future life of the network. In the proposed scheme, the network nodes implement this process not blindly, but according to schedule. The schedule model is derived from space-time graph that illustrates security-aware contacts between space DTN nodes at certain time steps. When a period for exchanging or updating comes, each DTN node sends its public key and the authentication information for this key to the security-aware neighbors, according to a predetermined space-time graph. In the following subsections, first presented the non-interactive *multilevel*public key exchange protocol using two-channel cryptographic technologies, and then introduce the space-time graph for space DTNs. Thereafter, the public key exchange mechanism based on space-time graphs is given.

3.1 Public Key Exchange Protocol

Due to high delays and unexpected loss of connectivity, an interactive protocol does not work well in space DTNs. This motivates a design of non-interactive *multilevel*key exchange protocols in an authenticated manner. As discussed above, two-channel cryptography and OOB channels have advantages on designing a non-interactive *multilevel*message authentication protocol, which utilized to enable two DTN nodes to securely exchange their public keys (or revocation status information). The main idea is to exchange a public key, that may be long term or ephemeral, on the normal channel, and independently calculate a cryptographic hash value from this public key. This hash value is then transmitted from one device to the other over the OOB channel, in order to verify that the public key exchanged on the normal channel has not been altered. Because of only processing at security-aware nodes, i.e., a "single hop" from a security-aware forwarder to the next security-aware intermediate receiver [13], an authenticated OOB is easily achieved. Accordingly, by utilizing two-channel cryptography, public keys can be authenticated between a forwarder and the next intermediate receiver, if it is needed. Here considered a space node V_i that possesses the public key PK_i and performs the following protocol. This protocol enables V_i to securely send its public key PK_i to another node V_j which is reachable in one hop for V_i. In more detail, the protocol is performed as follows:

1) The sender, V_i, appends its identity ID_i as well as the current time t to its public key PK_i, and thereafter sends the result $PK_i \| ID_i \| t$ to the receiver V_j over a broadband insecure channel (a traditional channel);

2) The sender, V_i, computes $h = H(PK_i \| ID_i \| t)$

3) The sender, V_i, sends the authentication information for its public key, i.e., h, to the receiver $V_j$over the narrowband authenticated channel (often OOB channels);

4) When receiving the public key $PK_i' \| ID_i' \| t'$ and the authentication information h' for this public key from $V_i$over the traditional channel and the OOB channel respectively, the receiver V_j accepts PK_i as the public key of $V_i$if t' is the correct timestamp and $h' = H(PK_i' \| ID_i' \| t')$; otherwise, reject it.

Further illustrated this process in the following Fig.2. Here, *H* is a collision resistant hash function. In order to resist birthday attacks, the size of *h* needs at least 160 bits. Mashatan and Stinson gave a formal security proof for the non-interactive *multilevel*message authentication protocol on which the above key exchange protocol is built [14].In addition, in this protocol introduced timestamps to protect it from replay attacks since it is a one-pass protocol and inherently open to replay attacks. This means that nodes would need to have a common notion of time, just as precisely determining windows of communication opportunities and correct antenna-pointing, for example. The time synchronization issue is one of the current areas of space DTN research. Most works aim at using suitable modifications to the Network Time Protocol (NTP) and the CCSDS Proximity-1 Space Link Protocol. NTP is widely used to synchronize computers in the Earth Internet and has been deployed in low-orbit Earth orbiters. In this paper, assumed that space DTNs have time synchronization.

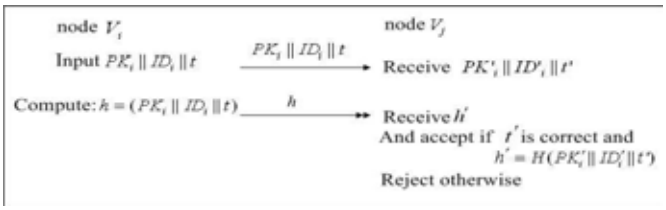


Fig.2. Non-interactive multilevel public key exchange protocol

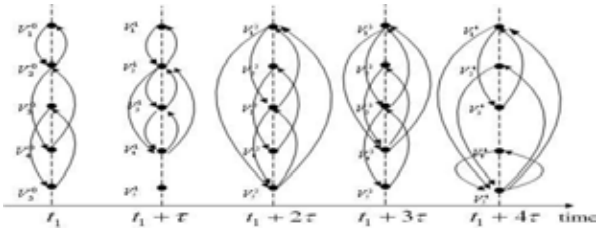


Fig.3. Space-time graphs for space DTNs

IV. SPACE-TIME GRAPHS BASED PUBLIC KEY EXCHANGE FOR SPACE DTN

Now the public key exchange protocol is described based on the above-generated space-time graph specifying when and to whom a node should send its public key. When a period comes, say t_1, the process for public key exchange is started. According to the space-time graph, each node sends its public key to all the predictable nodes reachable in one hop, via the non-interactive protocol given by Fig.2. Each node V_i, i = 1,..., n performs as follows (used "→" to denote the protocol given in Figure 3):

1) At time t_1, $V_i \rightarrow V_{j1}$, when the node V_{j1} is one-hop reachable for $V_i$at this moment;

2) At time $t_1 + \tau$, $V_i \rightarrow V_{j2}$, when the node V_{j2} is onehop reachable at this moment and not one-hop reachable at the preceding moment t_1;

3) At time $t_1 + 2\tau$, $V_i \rightarrow V_{j3}$, when the node V_{j3} is onehop reachable at this moment and not one-hop reachable at the preceding moments t_1 as well as $t_1 + \tau$ (i.e., not one-hop reachable at all the preceding time points in the time dimension of the space-time graph); and so on.

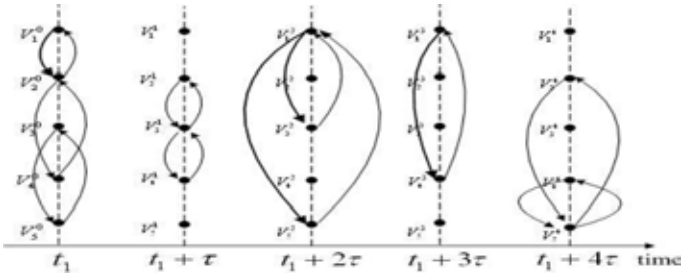


Fig.4. Public key exchange based on space-time graph

As shown in Fig.4, a directed arc line $v_{i,j}^{t}$ denotes that node $V_i$sends its public key and the corresponding authentication information to one of its one-hop reachable nodes $V_j$at time t, by utilizing a two-channel cryptography technologies. For node V_1, at time t_1, it sends its public key to node V_2 in a non-interactive and authenticated manner, since V_2 is its one-hop reachable node at that moment. At time $t_1 + 2\tau$, V_1 sends its public key to V_3 and V_5 respectively.

Then, at time $t_1 + 3\tau$, V_1 sends its public key to V_4. Thus, all the other nodes in this network have gotten the public key of node V_1. Illustrated this process with bold arc lines.

From another perspective, at time t_1, key exchange takes place between three pairs (V_1, V_2), (V_2, V_4) and (V_3, V_5). At time $t_1 + \tau$, key exchange takes place between $V_2$and V_3, as well as V_3 and V4. Then, at time $t_1 + 2\tau$, two pairs, (V_1, V_3) and (V_1, V_5), perform this key exchange protocol. Only one pair (V_1, V_3) exchanges keys at time $t_1 + 3\tau$. At time $t_1 + 4\tau$, there are two pairs, (V_2, V_5) and (V_4, V_5), performing public key exchange process. Finally, it is seen that all nodes in the network given in Fig.1 complete public key exchange in four slots from

t_1.It is important to note that the similar method can also be applied to exchange public key revocation messages between space DTN nodes. In this way, the authentication and integrity of public key revocation message can also be guaranteed. This is another essential issue of secure space DTNs [15].

With the scheduled and periodic contacts, the public key exchange, public key update and the revocation status issuing can be implemented based on time-evolving network models combined with two-channel message authentication mechanisms. Unlike the traditional PKI, here it does not need a Certification Authority (CA) and no certificate is involved. Via the above mechanism, the backbone network, including DTN gateways that connect various DTN domains, achieves the support of generally-available public keys. Nevertheless, there are still some nodes that might never be in contact with some others. Considering this case, let the DTN security gateways to bridge between the nodes in the backbone network and the nodes in the sub-networks. This means a hierarchical strategy. Specifically, the backbone network and the access sub-network respectively run the above protocol interiorly. A DTN security gateway forwards the public keys from the nodes in the domain or sub-network that the gateway controls to the nodes in the backbone network, along with its own public key. Meanwhile, the gateway also forwards the public keys of the nodes outside of the sub-network to the nodes in the sub-network that it controls.

4.1 Security Consideration

In the public key exchange protocol (Figure 3) based on two-channel cryptography, $PK_i \| I\ D_i \| t$ and its corresponding hash value $h = H(PK_i \| I\ D_i \| t)$ respectively correspond to the message M and its hash value in the protocol given in Figure 1. A formalssecurity proof for this protocol, on which the key exchange protocol is built, is given by Mashatan and Stinson [10]. Here just briefly sketched the key points specifying the security of the scheme. Two types of attackers are defined as follows: substitution attackers and impersonation attackers, in order to show that the receiver can assure the owner of the public key, and its authenticity as well as freshness.For a substitution adversary, it is computationally infeasible to find a substitution $PK_i' \| I\ D_i \| t$ such that $H(PK_i' \| I\ D_i \| t) = h$.Here, PK_i' is a false public key. This is implied from the assumption that the adversary cannot modify the information (i.e., h) transmitted over the narrow-band authenticated channel.

What is more, H is a collision resistant hash function. In order to resist birthday attack, the size of the authenticated information h is greater than 160 bits.According to the two-channel cryptography, an adversary cannot forget the authentication information sent over the narrow-band authenticated channel. Then, for an impersonation adversary, in order to convince the receiver that a public key $PK_i' \| I\ D_i' \| t$ is sent from a target sender, it has to replay the authentication information previously sent by the target sender, such as $h' = H(PK_i' \| I\ D_i' \| t')$. Here note that t is the current time and t' represents the preceding time. Factually, this type of attacks are successful with negligible probability, because it is computationally infeasible to find a forged $PK_i' \| I\ D_i' \| t$ such that $H(PK_i' \| I\ D_i' \| t) = h'$, even if $PK_i' \| I\ D_i' = PK_i \| I\ D_i$. This is derived from the assumption that H is a collision resistant hash function and the size of the hash value is greater than 160 bits.

V. EXPERIMENTAL RESULTS AND DISCUSSION

To examine the performance of the proposed scheme, simulations have been conducted to evaluate the convergence speed. In this simulation, convergence speed is considered as a metric for the performance measurement. The convergence means that every node achieves the public keys of all the other nodes during a

key exchange period. The convergence speed is measured by the minimum number of slots during which all nodes in the network complete public key exchange. In this simulation, the experiment is repeated for multiple times and obtained the average values of this metric. Randomly a time-evolving network is generated via random graph model.

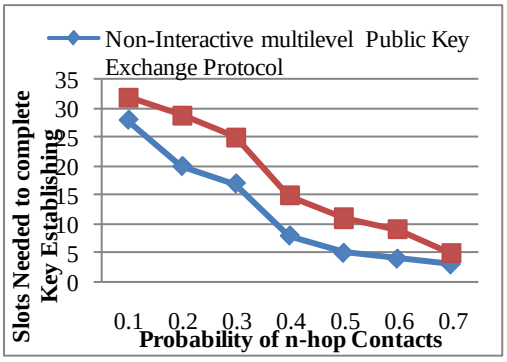


Fig.5. Convergence Speed Comparison

First a sequence of static random graphs is gnerated in order to represent the time-evolving DTN with 100 nodes. Then, the space-time graph corresponding to this time-evolving network is generated, and thereafter the public key exchange process is performed on this spacetime graph. In this experiment, probability *p*increasedfrom 0.1 to 0.99 which significantly increses network density. For each probability, 100 random networks and get an average value is generated, which is presented in Fig.5.

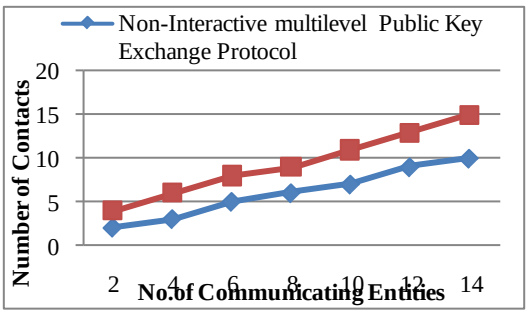


Fig.6.Simulation result for Number of Contacts

Fig. 6 shows the simulation result for the number of contact of the communicating entities with proposed system. From the figure when the number of communicating entities increases the number of contacts also increases. The proposed system hasfewer contacts when compared to the existing one. The reason is that the convergence speed of theproposed system is high

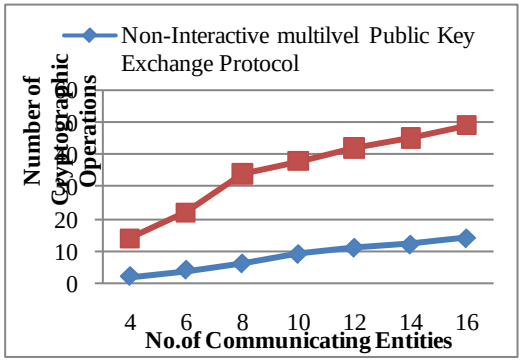


Fig.7.Simulation result for Number of Cryptographic Operations

Fig.7 shows the number of cryptographic operations carried out by proposed system during bundle transmission. The number of communicating entities include one sender, one destination and as many intermediate nodes (DM) as possible. While the proposed scheme has zero contact and zero cryptographic operations by the proposed system, the number of contacts and cryptographic operations by proposed system reduces with increase in the number of communicating entities.For every contact establish proposed work carries out three cryptographic operations of public key decryption, signature verification and symmetric key encryption.

VI. CONCLUSION

In this paper, a novel approach non interactive public key exchange protocol is proposed along with some directions for addressing the challenging problem of Non-Interactive multilevel Key establishment in space DTN environments and establishing secure context to support for BSP of space DTNs. As the DTN is relatively new, the current state of the art is mainly limited to the "language" the security nodes should speak upon which the security services would be built. Limited work has been done in the area of key management and more specifically in key exchange. In the proposed protocol, the space-time graph is utilized to model the predictable property of space networks. This makes the key establishment process scheduled and not opportunistic. The performance of the proposed protocol is measured by means of convergence speed, cryptographic operations and number of context. The experimental results shows that the proposed protocol is better than the existing public key exchange protocols in delay tolerant networks

REFERENCES

[1] Artemios G. Voyiatzis, "A survey of delay – disruption tolerant networking applications", Journal of Internet engineering, Vol 5 no 1, pp: 331-343, June 2012.

[2] Farrell, S., Symington, S., Weiss, H., Lovell, P.: Delay-Tolerant Networking Security Overview. IETF Internet Draft, draft-irtf-dtnrg-sec-overview-06 (2009)

[3] Symington, S., Farrell, S., Weiss, H., Lovell, P.: Bundle Security Protocol Specification. IETF Internet Draft, draft-irtf-dtnrg-bundle-security-15 (2010)

[4] Farrell, S., Cahill, V.: Security Considerations in Space and Delay Tolerant Networks. In: Second IEEE International Conference on Space Mission Challenges for Information Technology (2006)

[5] Jia, Z., Lin, X., Tan, S. H., Li, L., & Yang, Y. (2012). Public key distribution scheme for delay tolerant networks based on two-channel cryptography. Journal of Network and Computer Applications, 35(3), 905-913.

[6] Basha, J. A., & Mozhi, D. A. (2014). Detection of Misbehaviour Activities in Delay Tolerant Network Using Trust Authority, Volume 2, Issue 2, pp.1864-1868.

[7] Johari, R., & Gupta, N. (2011, October). Secure query processing in delay tolerant network using java cryptography architecture. In Computational Intelligence and Communication Networks (CICN), 2011 International Conference on (pp. 653-657). IEEE.

[8]Fall, K..: A Delay-Tolerant Network Architecture for Challenged Internets. In: SIGCOMM' 03, August 25-29, 2003, Karlsruhe, Germany

[9] Asokan, N., Kostiainen, K., Ginzboorg, J. Ott and C. Luo.: Towards Securing DisruptionTolerant Networking. Nokia Research Centre, NRC-TR-2007-007 (2007)

[10] Mashatan and D. Stinson, "Practical unconditionally secure twochannel message authentication," Designs, Codes Cryptogr., vol. 55, no. 2, pp. 169–188, 2010.

[11] R. Kainda, I. Flechais, and A. Roscoe, "Usability and security of outof-band channels in secure device pairing protocols," in Proc. 5th Symp.Usable Privacy Sec., 2009, pp. 1–12.

[12] Balfanz, D. Smetters, P. Stewart, and H. Wong, "Talking to strangers: Authentication in ad-hoc wireless networks," in Proc. 9th Annu. NDSS, 2002, pp. 7–19.

[13] M. Huang, S. Chen, Y. Zhu, and Y. Wang, "Cost-efficient topology design problem in time-evolving delay-tolerant networks," in Proc. IEEE Global Telecommun. Conf., Dec. 2010, pp. 1–5.

DETECTION OF ANATOMICAL STRUCTURES IN OPTICAL FUNDUS IMAGES

B.Vinoth Kumar[1], P.Swathika[2], M.Pradhiba Selvarani[3] , S.Karpagam[4]

[1] *Department of Computer Science and Engineering, RVCE (Sivakasi), India.*
[2,3,4] *Department of Computer Science and Engineering, KCET(Virudhunagar), India.*

ABSTRACT

To implement a computer system for the automatic detection of important anatomical structures in digital fundus retinal images such as blood vessels, Optic Disc (OD) and macula. Blood vessel tracking provides a map of the retinal vessel of the eye, from which a reference frame may be derived that can ease the process of positioning other fundus objects and lesions with respect to a natural "co ordinate systems". Segmenting the OD is key-processing element in many algorithms designed for automatic extraction of anatomical structures and detection of retinal lesions. Macula encircling helps establishing statistics regarding lesions position for disease gradation. Diabetic retinopathy is considered as the root cause of vision loss for diabetic patients. However, if the symptoms are identified earlier and a proper treatment is provided through regular screenings, blindness can be avoided. Exudates are a major indicator of diabetic retinopathy that can possibly be quantified automatically. The purpose of the work is to describe and evaluate a machine learning-based, automated system to detect exudates in digital color fundus photographs, for early diagnosis of diabetic retinopathy.

Keywords--Diabetic retinopathy, Fundus image analysis, Macula detection, Optic nerve detection, Optic Disc Detection

I. INTRODUCTION

The World Health Organization estimates that 135 million people have diabetes mellitus worldwide and that the number of people with diabetes will increase to 300 million by the year 2025 . More than 18 million Americans currently have diabetes and the number of adults with the disease is projected to more than double by the year 2050. Visual disability and blindness have a profound socioeconomic impact upon the diabetic population and diabetic retinopathy (DR) is the leading cause of new blindness in working-age adults in the industrialized world.

Retinal image analysis is a key element in detecting retinopathies in patients. It assists in the automatic detection of pathologies such as diabetic retinopathy (DR), macular degeneration, and glaucoma. Optic Disc (OD), macula and retinal vasculature are all important anatomical structures in the retina. Diabetic-related eye diseases are the most common cause of blindness in the world.

II. RELATED WORKS

The method described in [1] was used to detect Optic Disc Detect From Retinal Images by a Line Operator. This orientation can be used to locate the optic disc accurately. The drawback in this technique is, it can't handle small

images having OD darker than the surrounding pixels. This technique can't handle retinal images that do not have a clear circular brightness structure around their OD.

The method described in [2] was used to detect Optic Disc from Normalized Digital Fundus Images by Means of a Vessel. The drawback in this technique is, OD was not detected correctly due to uneven crescent-shaped illumination.

The method described in [3] was used to detect Optic Disc in Retinal Images by Means of a Geometrical Model of Vessel Structure**.** The drawback in this technique is, the model based on the availability of a good portion of the structure, and independent of the actual visibility.

The method described in [4] was used to detect Anatomic Structures in Human Retinal Imagery. In this technique the segmentation of the vasculature(retina) followed by the determination of spatial features describing the density, average thickness, and average orientation of the vasculature in relation to the position of the optic nerve. The algorithm fails due to slight misdetection in optic nerve and macula.

The method described in [5] was used to detect Optic Disc (OD), Blood Vessels and Macula in digital fundus retinal images. OD localization was done using Principle Component Analysis (PCA) followed by an active contour based approach for accurate segmentation of its boundary

III. PROPOSED SYSTEM

In this paper, there is an increasing interest for setting up medical systems that can screen a large number of people for sight threatening diseases, such as diabetic retinopathy. This paper presents a method for automated identification of exudates pathologies in retinopathy images based on Machine Learning Algorithm. The color retinal images are segmented using following some preprocessing steps, i.e., color normalization and contrast enhancement. The entire segmented images establish a dataset of regions. To classify these segmented regions into exudates and non-exudates, a set of initial features such as color, size, edge strength, and texture are extracted.

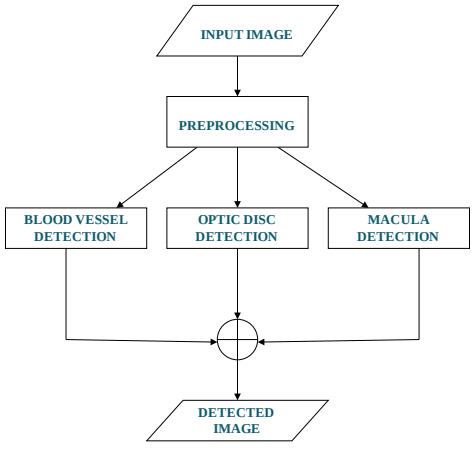


Fig. 1 : Block diagram for overall system

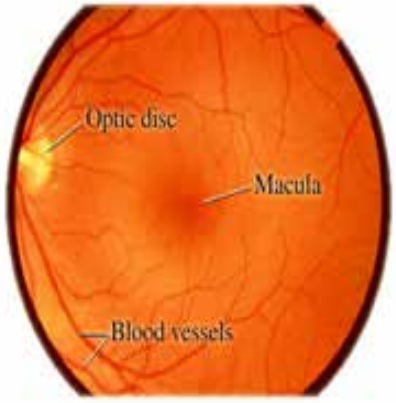


Fig. 2: Anatomical structure of retina

IV. BLOOD VESSEL DETECTION

Blood vessel detection in an essential step in medical diagnosis of fundus images as it aids in the diagnosis of ocular diseases. Other applications of retinal vasculature extraction include the treatment of age related macular degeneration, registration algorithms and personal identification in security application. Vessels appear darker than the background, their width is always smaller than a certain value, they are piecewise hold only approximately. Due to the presence of noise, the vessels are often disconnected, and not each pixel on a vessel appears darker than the background. The vessel borders appear often unsharp.

Diabetic retinopathy is influenced particularly by the disorders in the blood vessels which are very thin and fragile. quantitative analysis of retinal blood vessel images in terms of length, width, twists and turns branching pattern, can provide new intuitive understanding of the truth about vessels provide valuable information for diagnosis and study the stage of disease. With the advent of computing techniques, the automated segmentation an d analysis is expected to support the ophthalmologist in the clinical decision making process.

V. OPTIC DISK DETECTIOIN

The OD localization and segmentation is a crucial task in an automated retinal image analysis system. It is required as a prerequisite for the detection of exudates and also helps in macula detection, as macula is the darkest area in the neighborhood of OD. OD region is found by means of a multi-scale analysis pyramidal approach using a simple haar-based wavelet transforms. The brightest pixel that appears in a coarse resolution image at an appropriate resolution level depending on the initial image resolution and the OD average dimension is assumed to be part of the OD. This global OD localization serves as the starting point for a more accurate OD localization obtained from a template-based matching that uses the hausdorff distance measure on a binary image of the most intense canny edges.

VI. MACULA DETECTION

Macula is highly sensitive region of the ratina responsible for detailed central vision. Macular oedema is a special of DR caused by the leakage of blood vessels in the macula region. Macula oedema can be treated with laser if detected early en ough. Identifying the macular oedema. Macula encircling helps establishing statistics regarding lesions position for disease gradation. The relatively constant distance between the OD and the macula center can b e used as a priori knowledge to help positioning the macula. This darkest pixel in the coarse resolution image corresponds to the region occupied by the macula in the origin al image. The exact center to the macula is then found by searching in the vicinity for the darkest pixel on the original fine resolution image. A circle with a diameter equals to twice the OD diameter is then drawn around that point.

VII. EXUDATES DETECTION

The exudates can be noticed on the ophthalmoscope as areas with hard white or yellowish colors and varying sizes, shapes and locations, near the leaking capillaries within the retina. Hard and soft exudates can be distinguished due to their colour and the sharpness of their borders. There is an extra feature in the images that appear as bright

patterns, like the optic disc and – because of changes in illumination – ordinary background pixels. Besides, they are not the vessels is high as the one caused by the exudates. Exudates detection is our main purpose. We have developed a machine learning algorithm that can detect bright lesions in retinal colour photographs and can differentiate among exudates.

VIII. MACHINE LEARNING ALGORITHM

The machine learning algorithm is as so-called supervised algorithm, and therefore needs a set of annotated lesions to learn how to detect bright lesions. For this purpose, DR images originally read as containing bright lesions were selected. All pixels in all these images were segmented by retinal specialist as to whether they were (part on) an exudates or background retina.

IX. EXPERIMENTAL RESULTS

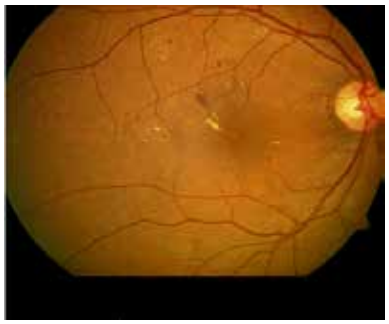


Fig. 3: Input Fundus Image of an Affected Person

Fig. 4: Optic Disc Detected Image

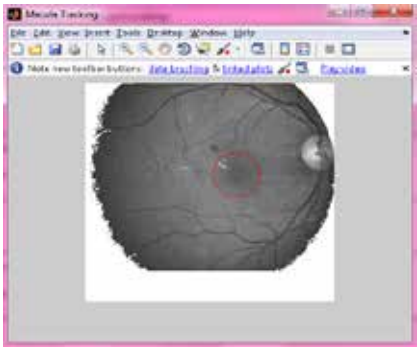


Fig. 5: Macula Detected Image

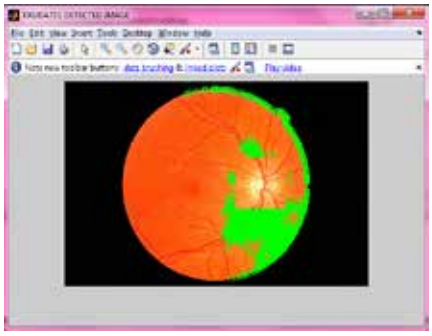


Fig.6 : Exudates Detected Image

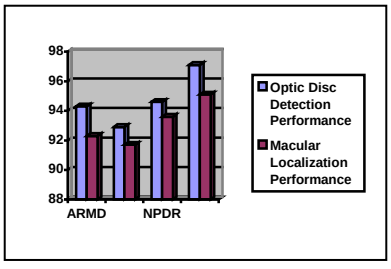


Fig. 7: Performance comparison for different Pathologies

X. CONCLUSION AND FUTURE ENHANCEMENT

In this work all important anatomical structures in color retinal images, the optic disk, the macula and the blood vessel and exudates are detected. The procedure has been tested on a database of more color fundus images which is a combination of normal, diabetic retinopathy and age related macular degeneration affected images acquired from a low resolution digital non-mydriatic fundus camera. The size of the images are 1280×1024. Test results show robustness against visual quality of the images and independently on the fact that the acquisition is macular optic disk-centered.

The proposed work helped in establishing the performance of the vascular network extractor, optic disc detection and macula detection. Future works include other extensive tests on other types of fundus images acquired from different fundus cameras.

REFERENCES

[1] Shijian Lu*, Member, IEEE, and Joo Hwee Lim, Member, IEEE "Automatic Optic Disc Detection From Retinal Images by a Line Operator" IEEE TRANSACTIONS ON BIOMEDICAL ENGINEERING, VOL. 58, NO. 1, JANUARY 2011

[2] M. Foracchia, E. Grisan, and A. Ruggeri*, Senior Member, IEEE "Detection of Optic Disc in Retinal Images by Means of a Geometrical Model of Vessel Structure" IEEE TRANSACTIONS ON MEDICAL IMAGING, VOL. 23, NO. 10, OCTOBER 2004

[3] Aliaa Abdel-Haleim Abdel-Razik Youssif, Atef Zaki Ghalwash, and Amr Ahmed Sabry Abdel-Rahman Ghoneim* "Optic Disc Detection From Normalized Digital Fundus Images by Means of a Vessels" Direction Matched Filter" IEEE TRANSACTIONS ON MEDICAL IMAGING, VOL. 27, NO. 1, JANUARY 2008

[4] Kenneth W. Tobin*, Senior Member, IEEE, Edward Chaum, V. Priya Govindasamy, Member, IEEE, and Thomas P. Karnowski, Member, IEEE "Detection of Anatomic Structures in Human Retinal Imagery " IEEE TRANSACTIONS ON MEDICAL IMAGING, VOL. 26, NO. 12, DECEMBER 2007.

[5] Procedure to detect anatomical structures in optical fundus images – L. Gagnon, M.Lalonde.

[6] Gray-level grouping (GLG): An automatic method for optimized image contrast enhancement-part I:The Basic Method – Zhiyu chen.

[7] Gray-level grouping (GLG): An automatic method for optimized image contrast enhancement-part II: The Variations Zhiyu chen.

[8] Using a patient image archive to diagnose retinopathy – Michael D, Matthew T.S.

[9] Centers for Disease Control and Prevention National Diabetes Fact Sheet [Online]. Available: http://www.cdc.gov 2003

[10] A. A. Cavallerano, J. D. Cavallerano, P. Katalinic, A. M. Tolson, and L. P. Aiello, "Use of Joslin vision network digital-video nonmydriatic retinal imaging to assess diabetic retinopathy in a clinical program," *Retina*, vol. 23, pp. 215–223, April 2003.

[11] M. Larsen, J. Godt, and M. Grunkin, "Automated detection of diabetic retinopathy in a fundus photographic screening population," *Invest. Ophthal. Vis. Sci.*, vol. 44, pp. 767–771, 2003.

DESIGN OF CATEGORY-WISE FOCUSED WEB CRAWLER

Monika[1], Dr. Jyoti Pruthi[2]

[1]M.tech Scholar, [2]Assistant Professor, Department of Computer Science & Engineering, MRCE, Faridabad, (India)

ABSTRACT

The exponential growth of World Wide Web is rapid and it has scaled to large volume which is difficult to handle, index and search. Due to this increase in the size and diversity of information available on web, it is becoming difficult for traditional crawlers to efficiently crawl the web. Traditional, web crawlers retrieve all the pages that match the query, whether they are relevant for the user or not. So there is a need to develop efficient crawlers. Focused crawler is a crawler which retrieves only the relevant information for the user and discards the information which is irrelevant. In this paper we modify the proposed architecture of category-wise focused crawler which was earlier proposed by us and define the design of Category-Wise Focused Web Crawler.

Keywords: Focused Web Crawler, Relevant page, Web Crawler

I. INTRODUCTION

Web is a fast growing hypermedia database. In 90's the amount of data generated in a year is now generated every day. This availability of data is both structured and unstructured. So, it is very difficult to handle this amount of data. A web crawler is a program that visits Web sites and reads their pages and other information in order to create entries for a search engine index. With the exponential growth of information on the World Wide Web, there is a great demand for developing efficient and effective methods to organize and retrieve the information available and to develop a web crawler that retrieves most relevant pages. Because of limited computing resources and limited time, focused crawler has been developed.

II. RELATED WORKS

Focused crawling was introduced by Soumen Chackrabarti in 1999[7]. The goal of a focused crawler is to selectively seek out pages that are relevant to a pre-defined set of topics. Fish Search Algorithm for collecting topic-specific pages was proposed by P.M.E DeBra[9]. The algorithm simulates a school of fish, breeding and searching for food. Based on improvement of fish-search algorithm, M.Hersovici et al[8] proposed the shark-search algorithm. Shark-Search is a more aggressive version of Fish-Search. A Generic Framework for Focused Crawler was given by Martin Ester, Matthias Grob, Hans-Peter Kriegel[6]. The framework consists of 2 major components. First component consists of specification of user interest and measuring the relevance of webpage. Second component consists of ordering the links in the crawl frontier. Focused Crawler based on link structure and contents is discussed by Mohsen Jamali, Hassan Sayyadi, Babak Bagheri Hariri and Hassan Abolhassani[5]. They maintain Link Structure of pages and also introduce metric for measuring similarity of a page to a domain. A major problem faced by the above focused crawlers is that it is frequently difficult to learn that some sets of off-topic documents lead reliably to highly relevant documents. For solving this problem Anshika Pal, Deepak

singh tomar[4] proposed a method. For improving the Prediction of Page Relevance of Focused Crawlers Mejdl S. Safran, Abdullah Althagafi[3] proposed a Focused Crawler which uses Naïve Bayesian as the base Prediction Model. Approaches of Focused Web Crawler is discussed by Jay Sampat and Dharmeshkumar Mistry[2].

III. PROBLEM STATEMENT

The objective is to design a crawler that is efficient, fast, user friendly and improves the search based on focused category, so that best matched results will be displayed.

IV. PROPOSED ARCHITECTURE

In this paper we are modifying the proposed architecture of category-wise focused crawler which we have proposed in [1]. The Category-wise Focused Web Crawler crawl a website on the basis of a category and retrieve most relevant pages based on that category. The proposed system architecture has two main modules: Crawl Module & Search Module.

- ***Crawl Module:*** This module will crawl the WebPages using focused approach and store the result in the database. In this module first the user will provide a Domain to crawl, For example- '.com' domain, then user will also provide URL to start crawler. At last the user will choose a category on which crawler will focus while crawling, For example- 'News', 'Education' etc.
- ***Search Module:*** In this module, we will develop a search page. The user can give his/her query under any specified category and best matched results of the query from that category will be retrieved.

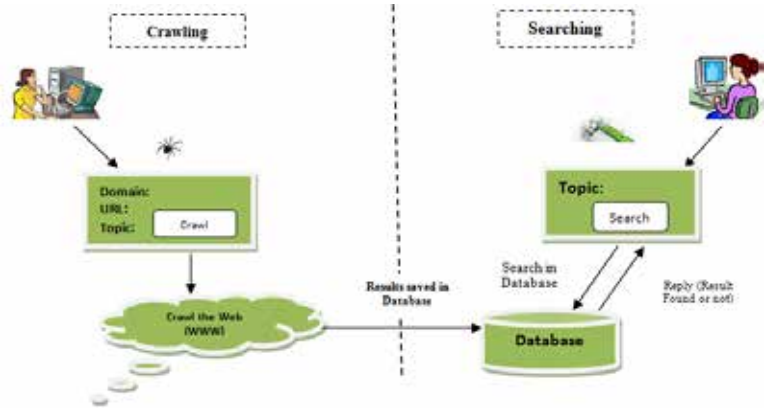


Figure 4.1: Proposed System Architecture

The proposed system crawls the WebPages recursively and stores the relevant data in database. This data includes Title, Meta keywords, Meta title, Meta Description etc of the webpage. When a query is submitted to the Search Engine, it searches its own database in response to it. In Focused Search, a category is also chosen. The WebPages are then retrieved as per the field chosen.

V. DESIGN OF CATEGORY-WISE FOCUSED WEB CRAWLER

The design of the Category-wise Focused Web Crawler is explained with the help of UML Diagram, basic Flowchart and ER Diagram.

5.1 UML Diagram

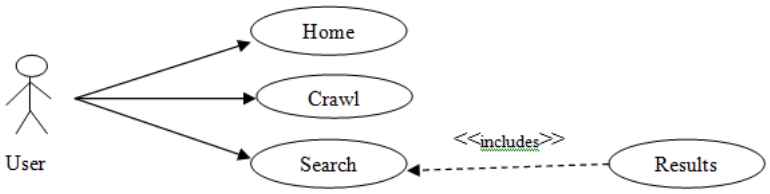


Figure 5.1: UML Diagram

The UML Diagram in Figure 4.2, we have an actor which is the user, the use cases for this actor can be the Home page(which provides basic linking of Crawl and Search Page), Crawl Module and the Search Module. In the Search use case, we have a include relationship with the Results, which specifies that searching includes displaying of results, whether found or not found.

5.2 Flowchart of Category-wise Focused Web Crawler

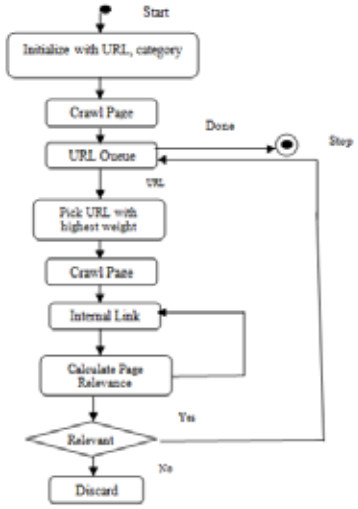


Figure 5.2: Flowchart

The Flowchart in Figure 4.3 explains the basic flow of Category-wise Focused Web Crawler. Here, first we initialize the crawl with Domain, URL and Category. Initially, only single page is crawled and add to the URL Queue. From the URL Queue the webpage with highest Relevance Score is picked and further links of that webpage is explored only. For every internal link Relevance Score or the Page Relevance is calculated. If the webpage is found to be relevant it is stored in database and URL is also added to the URL Queue, otherwise it is discarded. In the next round the URL Queue will have all the relevant internal links of the starting URL. This process will continue until we reach a stopping condition or there are no more webpage's in the URL Queue to crawl.

5.3 ER Diagram

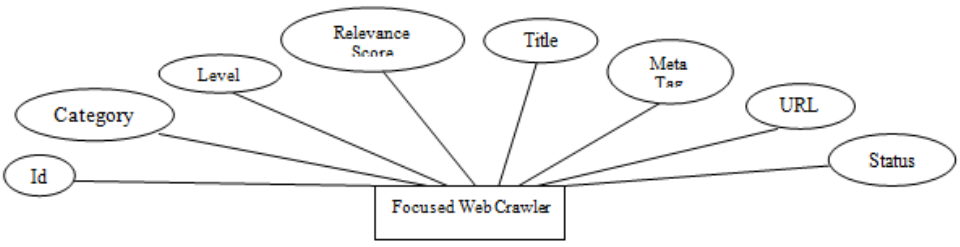


Figure 5.3 ER Diagram

ER Diagram in Figure 4.3, in this diagram we have:

Id: It is a Random Number associated with every crawl. So for every crawl we have a id associated with it. Id will be same for all the URL's of a single crawl.

Category: It is the Area or Field chosen to focus upon while crawling.

Level: It is the depth of the tree constructed by the exploring URL's.

Relevance Score: It is the measure to which a webpage is relevant to a specified category. The Relevance Score is calculated by the counting the frequency of the category in the webpage

Title: Title of the webpage.

Meta Tag: Meta Description of the webpage. In Meta Description, we are storing the keywords of the webpage.

URL: Complete URL of the webpage.

Status: There can be 2 types of Status that we can set:

1. Pending: The URL which is examined, but yet not explored.
2. Done: The URL which is examined and also explored.

VI. CONCLUSION

In today's world of Big Data, we need to prioritize our crawl and search, so that we can more useful data in less time. As there is limited time and resources available there is a need to develop efficient crawlers. So, Focused Crawlers came into existence, which crawl only the relevant page for the user. The modified architecture and also the basic design of the Category-wise Focused Web Crawler are discussed in this paper. We are working on the implementation of this Web Crawler.

VII. ACKNOWLEDGEMENT

I express my sincere and deep gratitude to my guide Dr. Jyoti Pruthi, Assistant Professor, Department of Information Technology, Manav Rachna College of Engineering, Faridabad, for the invaluable guidance, support and encouragement. She provided me all resource and guidance for this work.

REFERENCES

[1] Monika, Dr. Jyoti Pruthi, "Focused Web Crawler: Proposed Architecture", 2nd International Conference on "Innovation and Sustainability: Managing for Change", Jan 2015, 433-437.

[2] Jay Sampat, Anmol Jain, D. Mistry, "Focused Web Crawler and its Approaches", International Journal of Current Engineering and Technology, Volume-4, No.-5, Oct 2014

[3] Mejdl S. Safran, Abdullah Althagafi and Dunren Che, "Improving Relevance Prediction for Focused Web Crawlers", IEEE 11 International Conference on Computer and Information Science, 2012

[4] Anshika Pal, Deepak singh tomar, S.C. Shrivastava, "Efficient Focused Crawling Based on Content and Link Structure analysis", International Journal of computer science and information security, vol. 2, No.-1, June 2009.

[5] Mohsen Jamali, Hassan Sayyadi, Babak Bagheri Hariri and Hassan Abolhassani," A Method for Focused Crawling Using Combination of Link Structure and Content Similarity", IEEE International Conference on Web Intelligence, December 2006, Pages 753-756.

[6] Filippo Menczer, Gautam Pant, Padmini Srinivasan, "Topical Web Crawlers: Evaluating Adaptive Algorithms", ACM Transactions on Internet Technology, Vol. 4, No. 4, November 2004, Pages 378–419.

[7] S. Chakrabarti, M. van den Berg, B. Dom, "Focused crawling: a new approach to topic-specific Web resource discovery," in 8th International WWWConference, May 1999.

[8] Hersovici, M., Jacovi, M., Maarek, Y. S., Pelleg, D., Shtalhaim, M., and UR, S. 1998, " The sharksearch algorithm—An application: TailoredWeb site mapping", 7th International World-Wide Web Conference.

[9] P.M.E. De Bra, R.D.J. Post, "Information Retrieval in the World Wide Web: Making Client-based searching feasible", Computer Networks and ISDN Systems, 27(2) 1994 183-192.

ECG DATA COMPRESSION USING WAVELET FAMILY

Hemlata Shakya[1], Shiru Sharma[2]

[1,2] *School of Biomedical Engineering, IIT BHU, Varanasi, U.P., (India)*

ABSTRACT

In this paper we have done ECG data compression using wavelet family. ECG compression methods classified into three categories: Direct compression method, Parameter extraction method and transform method. ECG is a diagnostic tool that records the electrical activity of the heart. Large amount of ECG signal data needs to stored and transmitted so, it is necessary to compress the ECG signal data. Wavelet methods are very powerful tools for signal and data compression. This paper evaluated the compression ratio (CR) and percent of root mean square difference (PRD). A high compression ratio is achieved with a relatively, low percent root mean square difference (PRD).

Keywords: Electrocardiogram, Compression ratio, PRD.

I. INTRODUCTION

ECG data compression is playing a vital role in biomedical application. An ECG is a diagnosis tool that records the electrical activity of the heart. It is used to measure the heart electrical conduction system. ECG is a simple and non invasive. Electrodes are placed on the skin of the chest and connected in a specific order and machine that, when turned on measure electrical activity all over the heart. The Output found on a long scroll of papers that displays a printed graph of activity on a computer screen. ECG signal has been extended for heart disease diagnosis and ambulatory monitoring for storage and transmission of large signal data, it is necessary to compress the ECG signal data [4].

ECG is a simple painless test that records the electrical activity. Shows on an example of a normal ECG waveform, which consist of a p wave, a QRS complex and a T wave. The u wave also some time visible. The p wave marks the activation of atria. This is the chamber of the heart that receives blood from the body, which collect oxygen rich blood from the lungs and the right atrium. The QRS complex represents the activation of the left ventricle. The T wave represents the repolarization of the ventricle.

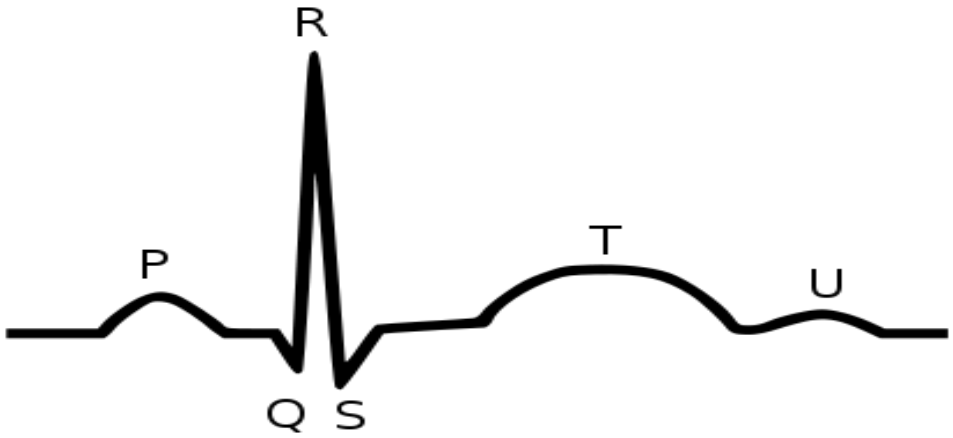


Fig.1 ECG Waveform

II. ECG DATA COMPRESSION

The goal of ECG compression techniques is to achieve a reduce information rate. A compressor can reduce the size of a file by deciding which data is more frequent by assigning it less bit than to less frequent data. To save time when transmitting and to save space when storing it.

ECG data compression methods are:

2.1 Lossless Compression

Lossless compression is a data compression algorithm that allows the original data to be perfectly reconstructed from the compressed data. Ex-It is used zip file format.

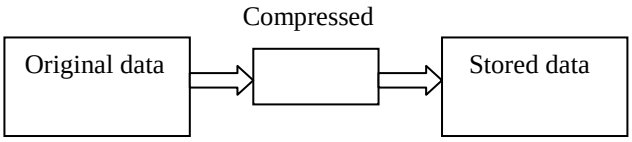


Fig.2 Lossless compression

2.2. Lossy Compression

Lossy compression is commonly used to compress multimedia data (audio, video and still images). It is the rate of the difference between original signal and the reconstructed signal.

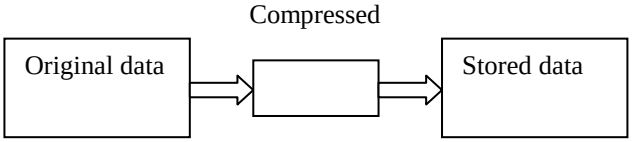


Fig.3 Lossy Compression

Wavelet transform is an excellent tool, an analyze the time and frequency signal. A number of time and

frequency methods are currently available for the high resolution decomposition the time frequency plane useful for signal analysis. The wavelet analysis procedure is to adopt a wavelet prototype function called an analyzing wavelet or mother wavelet. Wavelet was first introduced in seismology to provide a time dimension to seismic analysis that Fourier analysis lacked. Wavelets are used in a wide range of applications such as signal analysis, signal compression, differential equations and integral equations.

The wavelet transform is similar to the Fourier transform. Wavelets are better suited represent functions which are localized both in time and frequency signal.

The applications of wavelet transform are:

- Data and image compression
- Pattern recognition
- Partial Difference equation solving
- Texture analysis
- Transient detection

ECG signal is non stationary signal which includes different frequency component and different time location. Wavelet transform may localize the signal analysis in time and frequency domain simultaneously.

Wavelet families are Daubechies, Mexican, symlet, haar, Meyer wavelet, but I have taken two wavelet daubechies wavelet and symlet wavelets are used ECG data compression

2.3 Daubechies Wavelet

A family of wavelet transform discovered by Ingrid daubechies. This wavelet is similar to the haar wavelet. One of the brightest stars in the world of wavelet research invented what are called compactly supported orthonormal wavelet thus making discrete wavelet analysis. The names of the daubechies wavelet family dbN, where N is the order and db the surname of the wavelet.

2.4. Symlet Wavelet

The symlet wavelets are nearly symmetrical wavelet proposed by daubechies as modifications to the db family. The properties of the two wavelets families are similar.

III. COMPRESSION MEASUREMENT

To measure the performance for different compression methods, the original signal and reconstructed signal is measured by PRD.

3.1. Compression Ratio

The compression ratio defined as the ratio of bit rate of original signal to the bit rate of reconstructed signal.

CR= Original signal / Reconstructed signal

3.2. Percent of root mean square difference (PRD)

It is used for ECG signal reconstruction. It is the rate of difference between the original signals to the reconstructed signal [5].

$$PRD = \sqrt{\frac{\sum_{I=1}^{n}[X_{org(i)} - X_{rec(i)}]}{\sum_{I=1}^{n}[X_{org(i)}]}} * 100$$

IV. RESULT AND DISCUSSION

Wavelet family based ECG data compression proposed in this paper. The proposed wavelet based compression algorithm has been tested for the following parameters. In this paper two wavelet family daubechies and symlet wavelet are used. ECG data has been taken from the physionet database on the internet. I have taken the original ECG data and then decomposition of ECG signal. The daubechies wavelets (db3, db4) and symlet wavelet (sym2, sym3) are used. It is used for decomposition and then reconstruction of ECG signal. The work proceeds by taking the ECG signals and applies the wavelet transform and then calculate the compression ratio and percent root mean square difference. This processing is done with the help of matlab tool.

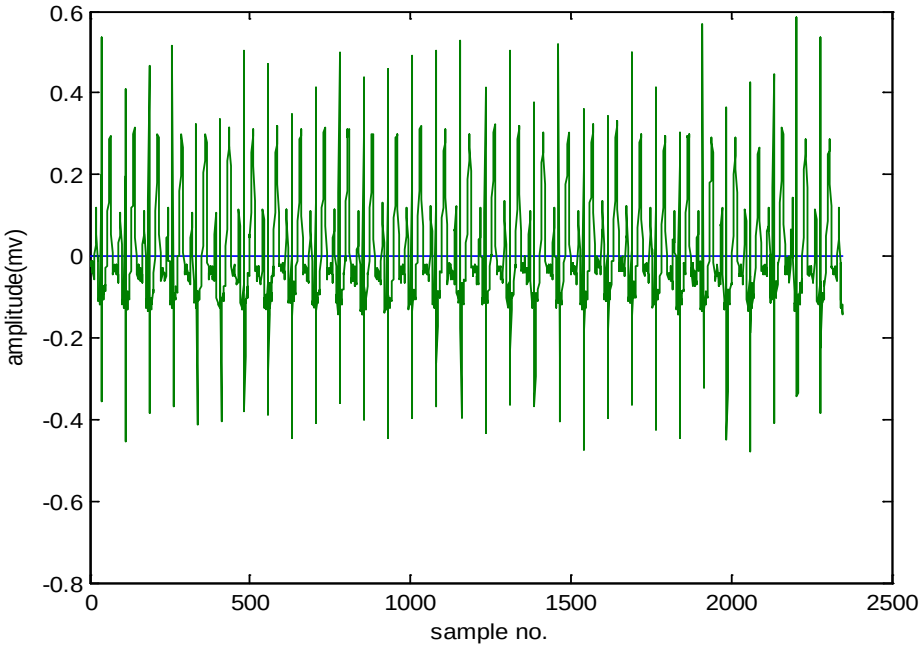


Fig.4 Original signal of ECG

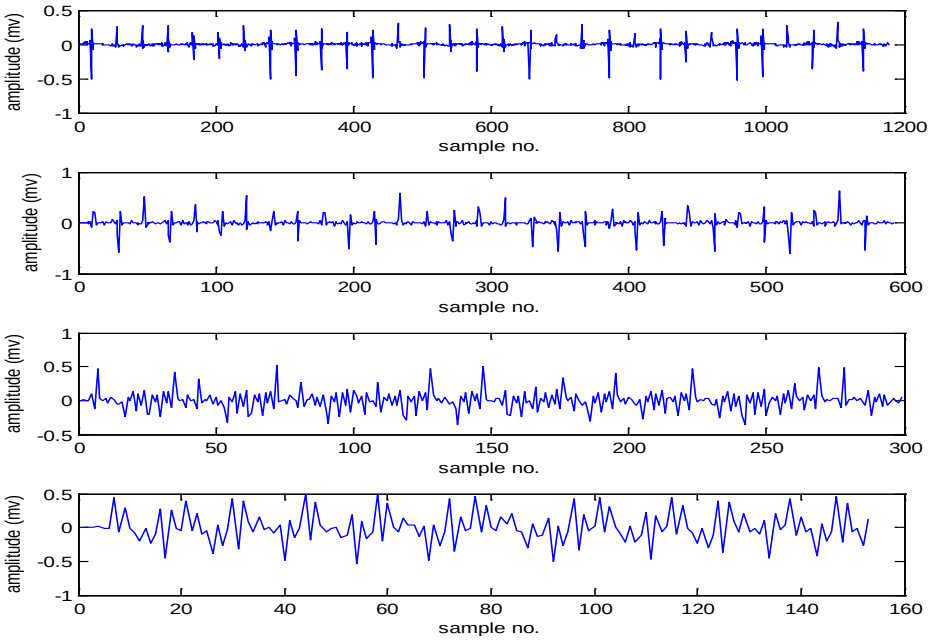


Fig.5 Decomposition of ECG signal

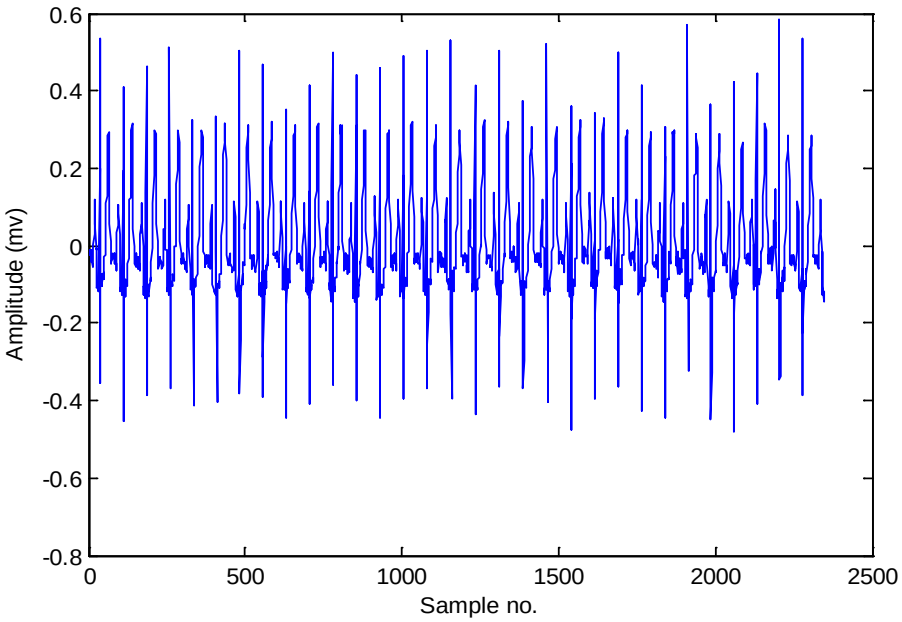


Fig.6 Reconstruction of ECG Signal

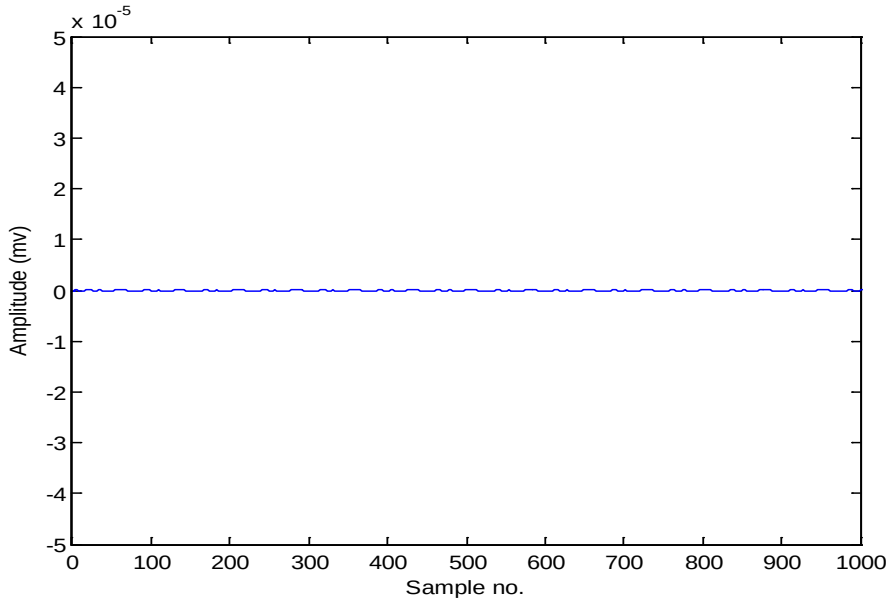


Fig.7 Error of ECG Signal

Table I

Wavelet Family	**Compression Ratio (CR)**	**Percent of root mean square difference (PRD)**
Db3	4.31	2.31
Db4	**5.00**	**1.99**
Sym2	1.02	9.78
Sym3	2.83	3.52

V. CONCLUSIONS

Wavelet transform is a powerful tool for signal compression and decompression. The proposed wavelet based compression algorithm has been tested for the following parameter. The use of daubechies wavelet and symlet wavelet (db2, db3, db4, sym1, sym2). The evaluated compression ratio and percent root mean square difference. The daubechies wavelet high compression ratio and low PRD value, and symlet wavelet is low compression ratio and high PRD value.

REFERENCES

[1] Priyanka, indu saini "Analysis ECG data compression techniques- A Survey Approach" Ijeat trans. Vol. 3, issue 2, February 2013.

[2] J. P. abenstien and W.J. Tompkins, "New Data reduction algorithm for real time ECG analysis," IEEE Trans. Biomed. Eng.,

Vol.BME- 29, pp-43-48, jan. 1982.

[3] Nidhal K. EI Abbadi, Abbas M. AI- Bakery "New Efficient Techniques for Compression of ECG Signal" Vol. 10 Issue 4,
July 2013.

[4] Abdelaziz Ouamri "ECG compression method using Lorentzian functions model",Science Direct, Digital Signal Processing 17(2007),8th August 2006..

[5] Mrs.S.O. Rajankar, Dr. S.N. Talbar "An Optimized Transform for ECG signal Compression" vol.01, No.03, Dec 2010.

[6] M. L. Hilton "Wavelet and Wavelet Packet Compression of Electrocardiograms" IEEE. Trans. Biomed.Engg., vol.44, pp. 394-402, 1997.

[7] Zhelong, Wang Ying Chen "ECG Signal Compression based on MPSHIT Algorithm" International Conference on information technology and application in biomedicine , pp.30-31, may 2008,

[8] B. R. S. Reddy and I. S. N. Murthy, "ECG Data Compression using Fourier descriptor," *IEEE Trans. Biomed. Eng.*, vol. BME-33, pp. 428–434, 1986.

[9] Robert S. H. Istepanian, Leontios J. Hadjileontiadis "ECG Data Compression using Wavelets and Higher Order Statics Method" IEEE Trans.on Information Technology in medicine, vol.5, June 2001.

[10] I. Daubechies, "The Wavelet Transform, Time-Frequency Localization and Signal Analysis" IEEE Trans. Inform. Theory 36 (5) pp.961–1005, 1990.

[11] Ahmad Reza A. Moghaddam and Kambiz Nayebi "A Two Dimensional Wavelet Packet Approach for ECG Compression" International Symposium on Signal Processing and its applications, pp-13-16 August, 2001.

[12] L. N. Sharma, S. Dandapat and Anil Mahanta "Multichannel ECG Data Compression Based on Multiscale Principal Component Analysis" IEEE Transaction on Information Technology in Biomedicine, Vol.16, No.4, july 2012.

[13] Jie chen, shuichi Itoh "A Wavelet Transform based ECG Compression Method Guaranteeing desired signal quality" IEEE Trans. Biomed. Engg., vol.45, pp-1414-1419,dec. 1998.

[14] Robert S. H. Istepenian , Arthur A. Petrosian " Optimal Zonal Wavelet Based ECG Data Compression For mobile Telecardiology System" IEEE Transaction On Information Technology in Biomedicine, vol.4 no.3, sept. 2000.

REVISITING SOCIAL MEDIA A REVIEW OF VARIOUS PERSPECTIVES FOR MODERN ERA MARKETING

Meenakshi Tomar[1], Dr. Anirban Sengupta[2], Dr. Krishan .K. Pandey[3], Dr. Devendra K. Punia[4]

[1,2,3,4] *Comes, University of Petroleum & Energy Studies,(India)*

ABSTRACT

The purpose of this research is to see various perspectives of Social Media that shall give a meaning to companies to implement it in their marketing strategies. The study also highlights the roles that social media has to play in today's dynamic landscape of Marketing. Rigorous literature review using existing existing literature, journals and articles has been done. The findings indicate that there are many logical reasons for marketers to incorporate Social Media in their IMC construct. The findings are of interest to academicians and marketers to understand significant reasons why Social Media is different from other marketing tools and also address the uniqueness of Social Media.

Keyword: Social Media, Marketing

Background

Social Media is not an unknown phenomenon. The initial use of Social Media was made by Individuals, family members and relatives with an aim to converse with each other and later on sharing of videos and other pictures made it the center of attraction to the people who saw associations happening over this platform without a motive. Therefore companies have taken advantage of this opportunity where the attraction was visible and the companies could easily inject their promotions which were accepted at least by the people who have an association with the company.

I. INTRODUCTION

With the pace of growth that social media has seen over past few years it has shrinked the space for people to breathe an air without any kind of promotions. Speaking about the comparison that social media has with other communication elements we cannot rank it as the best medium but we can definitely say that if Social Media is incorporated in the Marketing Communication Strategies of a company along with the other experienced and experimented mediums it will surely give positive results. Within this Literature review we shall cover the advantages that make social media a preference tool for any company.

II. LITERATURE REVIEW

The first association that any company will look with a customer is the emotional attachment. If the consumer are attracted and targeted by their emotions the power of loyalty and Brand can be seen for a company. Social Media is an easy tool which can be used to create emotional attachment with the consumers. (Quy Huy, 2012) This further enhances community building among those people who share emotional attachments with each

other. From the perspective of customer relationship, companies are adopting Social Media to increase their customer base either by original new additions to the existing customer's base or by importing contacts of the existing customers to widen up the reach. (Heller, 2011)

One very important thing for a company is to ensure spread of information weather related to product, brand, service or corporate. Dissemination of this information is targeted at a very low cost revolving around the idea of growing public relations. It becomes essential for a company to change its branding mechanisms from overall branding and be focused towards personal branding. This aspect is possible only at a platform like Social Media. (Nadia Yusuf, 2014)

Analysis of the growth of Social Media has led down certain perspective which is of great value to the marketers. The platform has been explored for benefits in advertising, positive Word of mouth marketing, effective branding activities, focused promotion, engaging customers in meaningful messages, developing fruitful campaigns which are revenue targeted, active marketing research and other benefits of communication tool. The author has also focused that Social Media is beneficial when integrated with traditional mediums. (Parsons, 2013)

If a company has an objective to see only the branding activities the inference that will come out is of course in the favor of the Marketer. Social Media has been able to create expected Brand equity. The platform is equally promising when used only for Branding activities. Marketing communication of any goal and motive can certainly be placed over Social Media ensuring positive Word of Mouth. (Manfred Bruhn, 2012)

One of the most interesting features of Social Media is using it for customer relationship management. Over Social Media people with some kind of association with other people tend to create a community. This community includes people with like needs or preferences at times. Social Media tends to boost community relationship by making it more attractive through conversations that happen among the community members already established. This helps in relationship marketing too. Over here individuals within a community have a tendency of sharing certain information and posts that have created interest in their mindsets and they further tend to share it within the group. Certainly there is an expectation that some people out of the group with whom the information got shared will try to seek more information by connecting with the company. This enhances relationship marketing. On the other hand individuals also go in depth search of the product or service which has been communicated over Social Media and try to learn or seek specific information from other people too. Therefore the experience sharing scenario converts an individual engagement to many to many interactions (Ang, 2011) .When the focus is particularly on information sharing the company has to be very careful on what is going out from its desk. Social Media ensures collaboration by opening two way communications between company and individuals or rather prospective customers thereby enhancing their knowledge management boxes (Vilma Vuori, 2012) .

When we talk about Social Media platforms like Pininterst or Twitter the targeted communication comes out in the form of images thereby branding the product or service effectively (Sharon Kiely, 2013). If there is something that an organization has to communicate with the help of Audio and Visual both the wonder area here is how to do it within a specified amount? With the evolution in technology platforms like you tube and their use over Social media has given new edge to connectivity and reach among customers, aside to proving itself as one of the most cost effective medium. The method is very simple. Create something on You Tube and share it

on Social Media. The conversations that take place after the rolling out of a video over Social Media is the attention catching stuff. (Lee, 2013)

One of the prominent factors while using Social Media which a marketer considers is the existing perceptions and would be perceptions of the targeted audience. Any communication weather aided with a visual or a stand along creative, campaign or a sales discount event will always influence the intentions of the consumers and shall lead to some additions in perceptions in such people .Literature shows that people perceive Social Media as a mode of enjoyment and also believes that it is very easy to use with any focused purpose. (N.DLODLO, 2013) A marketer may also be interested in looking at the behavior of consumers online. Social Media helps companies to track the behavior of people involved in shopping or sourcing knowledge about a product or service through online data. A company can always take an opportunity to segment such kind of people. This leads to online segmentation (Simona Vinere, 2013).

Social Media also helps in creating differentiation for the product or services by using the data of the consumers who leave information online. Since it is an established mechanism of spreading greater awareness positive brand associations are an obvious outcome of such differentiation. The platform is equally good at promoting brands. This is backed by a fact that companies get an opportunity to raise their spell and speak for their Brand as and when needed. (Yan, 2011)

Psychology says that people remember those things with which their associations are regular and continuous in nature, therefore giving them a lesser chance to forget about the product or a service. Social Media has proven itself to be platform showing a rise in the customer lifetime value. The Customers lifetime value here means the active connectivity of a customer with a company or its brands. This happens when a consumer is continuously assessing information, leaving comments, appreciating product or giving ideas for further innovation. His connectivity is a factor that goes in the calculation of customer lifetime value. (Bruce D Weinberg, 2011)

Viral advertising is one of the most targeted mechanisms of spreading awareness and information about a product. Social Media promotes viral advertising heavily. (Paquette, 2013)

In order to spread an information the companies leave a link spelling to know more and asking people to click it where information pertaining to products and services can be assessed therefore increasing web traffic for that particular website. This ensures website attractiveness. (Bernd W. Wirtz, 2013)

With the attraction of people using social media specifically for marketing purposes the companies have now gone deep into media marketing strategies along with other marketing plans. (Neti, 2011)

After assessing a lot of information pertaining to products, people are expected to react therefor smoothing their decision making and making wise decisions. Social Media is an actor towards influencing consumer decisions. It ensures efficiency in the cost even while dealing with different roles like initiator, influencer, decider, buyer , user. (Anas Khan, 2012)

The success of any business depends on sales and profit that come out from the number of people who have opted to buy that product. This figure is attained by spreading the information and executing advertising to the market so targeted thereby widening population .Social Media promises a quality reach which when converted into quantitative terms is much larger as compared with other mediums. Therefore ensuring effectiveness over variable cost also, Social media has been a promising tool. (Joel Indrupati, 2012)One very important aspect of any marketing communication lies in the personal touch that it can ensure with the targeted audience. Social Media has been able to create positive brand image and has also enhanced loyalty among people by personalized

marketing.(Saadia Shabnam, 2013). Social Media is one tool which promises overall brand management and single handedly ensures embedment of all the 7 p's of marketing. (Hall, 2012)

Social Media has been an interesting tool for conducting market research even without conducting it. People tend to share their opinions in the form of Status, posts, pictures or just my iconic expression. This allows marketer to use the analytics pertaining to what he requires from such status that pertain to a marketers questions. (Report, 2013)

Taking about Indian scenario people love to converse, share and express. This leads to valuable engagements that are otherwise not possible to be tracked on other mediums. These way social media platforms affect and impact on current business as well as marketing activities.(Pandya, 2012) With the help of the feedbacks that are generated and the reviews that are shared along people over Social Media company's tend to use these reviews towards research and development for getting a new product in the product line or may be launching a new product altogether through the information collected over social media. Therefore social networks are beneficial if appropriately used for innovation. (Toni Ahlqist, 2010)

Every company expects some sort of return over any kind of investments made. In marketing terms if a company promotes a product or service over social media, it is bound to give a rate of return. The existing literature shows us that the rate of return assured by Social media is slightly higher than what traditional mediums claim. Another aspect to this is the use of technology like Web.2.0. This is a user interface mechanism which makes the access of Social Media useful meaningful and understandable. With the advent of technologies Social Media has now become measurable too. (David M Gilfoil, 2012)

Apart from developing brand communities, social media also offers avenues for Email Marketing. The platform also enables the marketer to perform effective search engine optimization. Social media is a virtual place for events based marketing. The closest tool to social media is mobile marketing. (Castronovo, 2012)

Any brand awareness is represented by positioning where Social media has been to meet both Brand positioning and repositioning in a desired manner.(Kumar, 2003) A new approach for providing value addition to customers is the heterogeneity of the product endorsed by celebrity over social media. (Alexander Zauner, 2012) Social Media also helps in developing meaningful content by using user generated content in the communities. (Lucenko, 2012) A company can also target community services by telling people how the product purchased by them contributed to the welfare of the society. (Kang, 2011)

III. FINDINGS

The Literature review presented gives us an insight to various reasons for using Social Media. The advantages have been highlighted that make Social Media a preference tool for the company. These preferences also act as the differentiators when compared with other tools of marketing.

IV. CONCLUSION

The features highlighted can be used to implement Social Media when the communication targets specification for inclusion in IMC. However Social Media works best when combined with other tools of marketing although it can perform single handedly.

REFERENCES

1. Alexander Zauner, M. K. (2012). Sponsering , Brand Value and Social Media. RAE .
2. Anas Khan, R. K. (2012). Embracing new Media in Fiji : The way forward for Social network marketing & Communication Strategies. Strategic Direction (Emerald).
3. Ang, L. (2011). Is SCRM really a good Social Media Strategy ? Journal of Database Marketing & Customer Strategy Management.
4. Bernd W. Wirtz, R. P. (2013). Determinants of Social Media Websites Attractiveness. Journal of Electronic Commerce Research .
5. Bruce D Weinberg, P. D. (2011). Connected Customer Lifetime Value : The Impact of Social Media. Journal of Direct Data & Digital marketing Practice.
6. Castronovo, C. (2012). Social Media in an Alternative Marketing Communication Model. Journal of Marketing Development & Competitiveness .
7. David M Gilfoil, C. J. (2012). Return on Investment for Social Media : A proposed framework for understanding , Implementing & measuring the return. Journal of Business & Economics Research .
8. Hall, m. K. (2012). Social Marketing at the Right Place & right time with new Media. Journal of Social Marketing (Emerald).
9. Heller, C. (2011). From Social Media to Social Customer relationship Management. Emerald .
10. Joel Indrupati, T. H. (2012). Entrepreneurial Success using Online Social Networking Evaluation. Education , Business & Society Contemporary Middle Eastern Issues (Emerald).
11. Kang, J. (2011). Social Marketing in Hospitality Industry : The Role of Benefits in increasing Brand Community participation and the Impact of Participation on Consumer Trust and Community towards Hotel & Restraunts Brands. UMI .
12. Kumar, S. R. (2003). Branding Strategies in a changing Marketing Environment (Indian Context). Journal of Brand Management .
13. Lee, D. H. (2013). Social Media and Youtube as an attractive Marketing Tool. The Journal of American Business Review Cambridge.
14. Lucenko, K. (2012). Integrated Marketing Communication and Social Media . UMI.
15. Manfred Bruhn, V. S. (2012). Are Social Media replacing traditional Media in terms of Brand Equity Relations. Emerald Management Research.
16. Michelle B.Kunz, B. A. (2011). Are consumers Following Retailers to Social Networks ? Academy of Marketing Studies Journal .
17. N.DLODLO, M. D. (2013). Selected Social Media Antecendents: Attitude Towards Behavioural Impacts on its Usage among Consumers in a developing Country. STUDIA UBB.
18. Nadia Yusuf, N. A. (2014). The Social Media as Echo Chambers.The Digital Impact. Journal of Business and Economics Research.
19. Neti, S. (2011). Social Media and its Role in Marketing. International Journal of Enterprise Computing & Business Systems.
20. Pandya, K. (2012). Social Media Marketing in India--Creating new grownd work in Marketing Innovation. International Journal of Multi Disciplinary Management Studies .
21. Paquette, H. (2013). Social Media as a Marketing Tool : A Litrature Review. Digital Commons @ URI.

22. Parsons, A. (2013). Using Social Media to reach Consumers: A content analysis of Official FB pages. Academy of Marketing Studies.
23. Quy Huy, A. S. (2012). The Key to Social Media Success within Organizations. MIT SLOAN Management Review.
24. Report, A. (2013). Social Media & Public Opinion. Labger Research .
25. Saadia Shabnam, A. C. (2013). An Emerging method of Communication : Social Media Marketing & its Social and Managerial Implications. World Review of Business Research .
26. Sharon Kiely, A. L. (2013). Blogging Around the Twittersphere: Has Social Media Changed the way a destination is developed. The Business Review Cambridge.
27. Simona Vinere, I. C. (2013). The effects of Social Media Marketing on Online Consumer Behaviour. International Journal of Business & Management.
28. Toni Ahlqist, A. ,. (2010). Road Mapping the Societal Transformation potential of Social Media . Foresight (Emerald).
29. Vilma Vuori, J. O. (2012). Refining Information & Knowledge by Social Media Applications. Journal Of Information & Knowledge Management System.
30. Yan, J. (2011). Social Media in Branding : Fulfilling a Need. Journal of Brand Management .

THE COMPUTATIONAL ANALYSIS OF SEDAN CAR WITH VORTEX GENERATOR

G.Sivaraj[1], D.Lakshmanan[2], R.Veeramanikandan[3]

[1,2,3] *Department of Aeronautical Engineering, Bannari Amman Institute of Technology, (India)*

ABSTRACT

The main cause of pressure drag is the separation of air flow at the top surface of car. So this invention aims to delay flow separation by keeping Vortex Generators. The experimental investigations were performed on BLWT, while computational analysis was carried out using Standard computational software. Pressure measurements were made for the model when the wind was flowing parallel to the length of the car, with and without Vortex generators. As per the computational and experimental analysis it's observed and proved that, the drag co-efficient of car model was reduced by keeping Vortex Generators.

Keywords: Flow Separation, Sedan Car, Vortex Generator, Wind Tunnel.

I. INTRODUCTION

Automobile industry aims at producing car's which will have reduced drag, so as to improve performance and fuel consumption of the car. The cars adopt airfoil shape in order to produce high speed. This airfoil shape cannot be completely achieved due to the various aspects of car such as passenger seats, engine spaces, rear deck etc. In commercial cars, aesthetic appearance and comfort also plays a very important role to earn market. Thus the cars body will be made entirely with aerodynamic aspects; it tends to become aerodynamically bluffed. Due to this, it faces flow separation at the rear end. The car design is the key aspect for the success of the automobile industry producing cars.

II. VEHICLE AERODYNAMICS

Vehicle aerodynamics is the study of the aerodynamics of road vehicles. The main concerns of vehicle aerodynamics are reducing drag , reducing wind noise, minimizing noise emission, and preventing undesired lift forces and other causes of aerodynamic instability at high speeds. For instance the flow separation increases the drag in the car, these vehicle aerodynamics are necessary to identify the techniques to delay the flow separation. An aerodynamic automobile will integrate the wheel arcs and lights into the overall shape to reduce drag. It will have a flat and smooth floor to support the Venturi effect and produce desirable downwards aerodynamic forces**.**

The air that rams into the engine bay, is used for cooling, combustion, and for passengers, then reaccelerated by a nozzle and then ejected under the floor. For mid and rear engines air is decelerated and pressurized in a diffuser, loses some pressure as it passes the engine bay, and fills the slipstream. The cars needs a seal between the low pressure region around the wheels and the high pressure around the gearbox. They all have a closed engine bay floor. The suspension is either streamlined or retracted. Door handles, the antenna, and roof rails can have a

streamlined shape. Streamline are uniform curves similar to the pictorial representation of air flow below.The side mirror can only have a round fairing as a nose. Air flow through the wheel-bays is said to increase drag, though race cars need it for brake cooling and a lot of cars emit the air from the radiator into the wheel bay.Vehicle aerodynamics differs from aircraft aerodynamics in several ways. First, the characteristic shape of a road vehicle is much less streamlined compared to an aircraft. Second, the vehicle operates very close to the ground, rather than in free air. Third, the operating speeds are lower and aerodynamic drag varies as the square of speed. Fourth, a ground vehicle has fewer degrees of freedom than an aircraft, and its motion is less affected by aerodynamic forces. Fifth, passenger and commercial ground vehicles have very specific design constraints such as their intended purpose, high safety standards.The factors on which Vehicle Aerodynamic depends are Aerodynamic Forces, Laminar Separation, Tripping of Boundary Layer, Pressure Distribution, Wake, Tires, Glass and Trim, General Improvements and Unconventional Features

III. FLOW SEPARATION

Flow separation occurs when the boundary layer travels far enough against an adverse pressure gradient that the speed of the boundary layer relative to the object falls almost to zero. The fluid flow becomes detached from the surface of the object, and instead takes the forms of eddies and vortices.

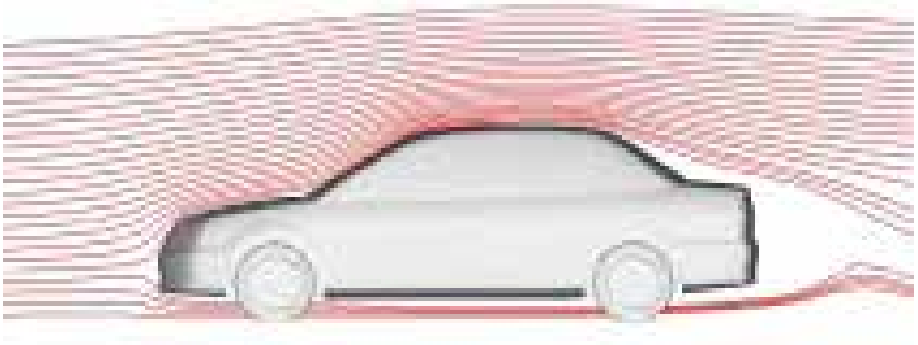


Fig 1: Flow separation over an sedan car

In aerodynamics, flow separation can often result in increased drag, particularly pressure drag which is caused by the pressure differential between the front and rear surfaces of the object as it travels through the fluid. For this reason much effort and research has gone into the design of aerodynamic and hydrodynamic surfaces which delay flow separation and keep the local flow attached for as long as possible. Fig 1 schematically shows the flow around a sedan car. Flow separation increases drag and hence the coefficient of drag vary in accordance to the design of the car. It occurs when the boundary layer travels against an adverse pressure gradient that the speed of the boundary layer to the object is almost zero. The fluid flow tends to detach from the surface of the object, and takes the forms of eddies and vortices. The scope of this paper is to improve the performance and reduce fuel consumption of a sedan type car .This increase in performance can be achieved by using an aerodynamic tool called vortex generator to the roof of the car and the constraints faced are Shape of the vortex generator and Size of the vortex generator.To improve the performance and efficiency of the car, we have done the following changes in the car.

1. Placing nine number ofVGs at the roof of the car.
2. Comparing the performance by using delta wing shaped and right angled shape vortex generator.
3. Considering the height of the vortex generator as 10mm.

IV. VORTEX GENERATOR

Vortex generator (VG) is an aerodynamic surface, consisting of a small vane or bump that creates a vortex. Vortex generators delay flow separation and aerodynamic stalling, thereby improving the effectiveness of wings and control surfaces. We have chosen vortex generator as our aerodynamic device to be implemented in the sedan car to enhance the performance of the car. VGs were developed for the aircraft sector, this technology has made it's way into car design. The main function of this device is to delay air flow separation. Air flow separation is when the airflow of an object detaches from the surface and creates eddies and vortexes. So vortex generator over the rear of the roof, effectively helps to reduce drag.

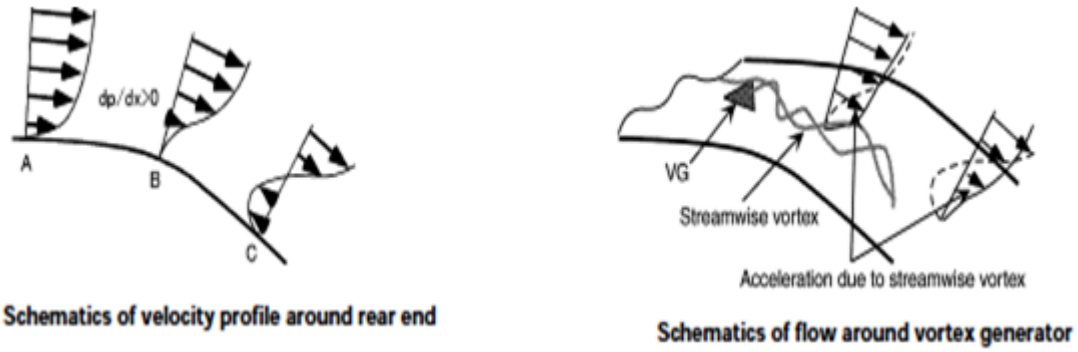


Fig 2.VG at the rear end of the car

The fig shows a flow velocity profile on the vehicle's centerline plane near the roof end. Since the vehicle height in this section becomes progressively lower as the flow moves downstream, an expanded airflow is formed there. This causes the downstream pressure to rise, which in turn creates reverse force acting against the main flow and generates reverse flow at downstream Point C.No reverse flow occurs at Point A located further upstream of Point C because the momentum of the boundary layer is prevailing over the pressure gradient (dp/dx). Between Points A and C, there is separation Point B, where the pressure gradient and the momentum of the boundary layer are balanced. Here the airflow quickly loses momentum as it moves downstream due to the viscosity of air. The purpose of adding VGs is to supply the momentum from higher region to lower region. This allows the separation point to shift further downstream. So it enables the expanded airflow to persist proportionately longer. It reduces drag by increasing g the back pressure. It provides dual advantage in drag reduction: one is to narrow the separation region in which low pressure constitutes the cause of drag another is to raise the pressure of the flow separation region. As to the location of VGs, a point immediately upstream of the flow separation point was assumed to be optimum, and a point 100 mm in front of the roof end was selected.

V. RESULT AND ANALYSIS

GAMBIT is a general purpose preprocessor for CFD analysis.**G**eometry **A**nd **M**esh **B**uilding **I**ntelligent **T**oolkit is a meshing software package which is used to generate the model of car and mesh it with the domain.Fluent software contains the broad physical modeling capabilities needed to model flow. It is an integral part of design and optimization phases of the product. It provides accurate CFD results, flexible moving and deforming meshes and superior parallel scalability. The interactive solver setup, solution and post-processing capabilities of Fluent make it easy to handle a calculation, examine results with integrated post-processing, change any setting, and then continue the calculation within a single application.

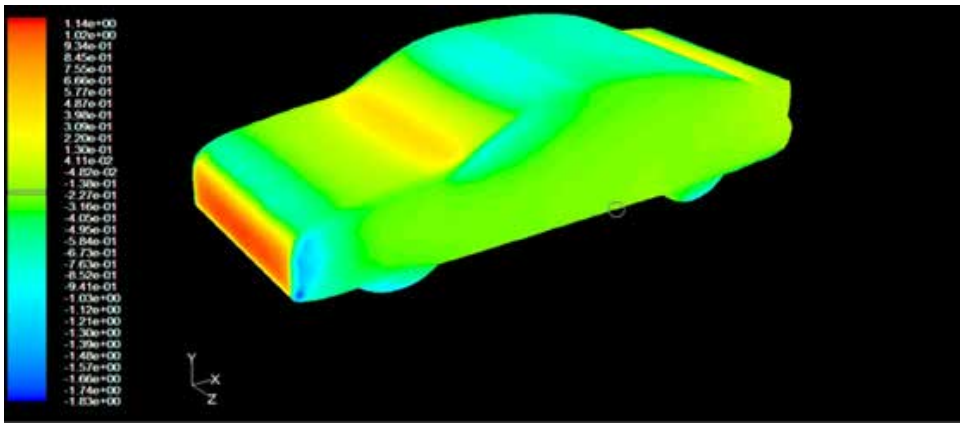


Fig .3: Pressure Coefficient Generated Without Vortex Generator

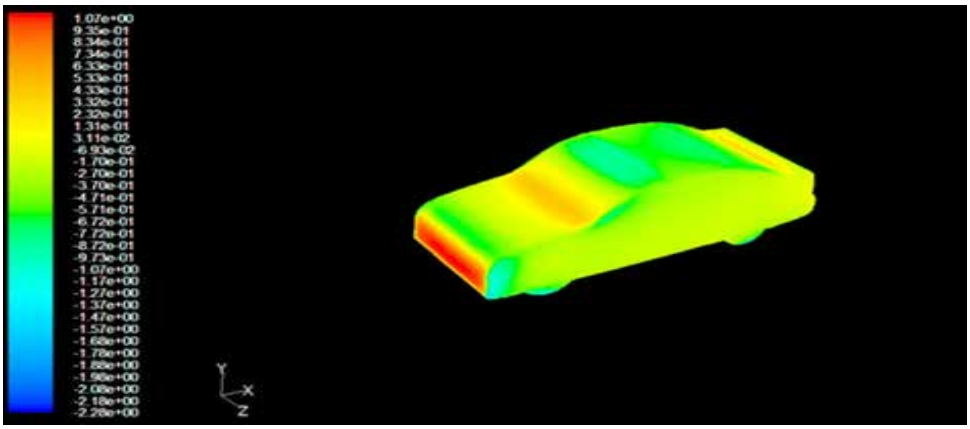


Fig .4: Pressure Coefficient Generated with Vortex Generator

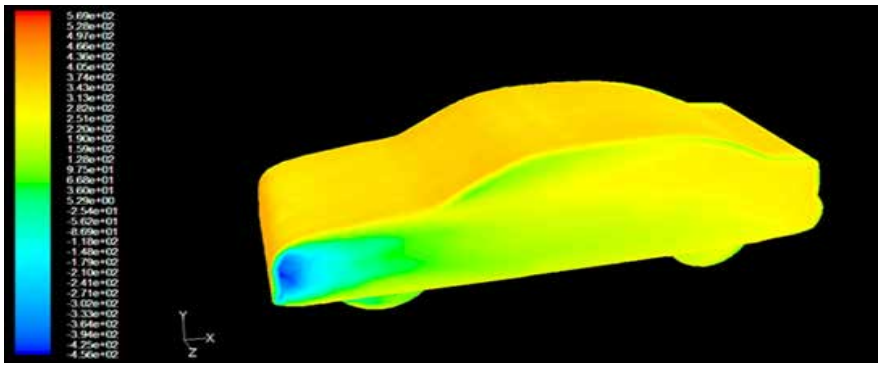


Fig .5: Total Pressure Generated without Vortex Generator

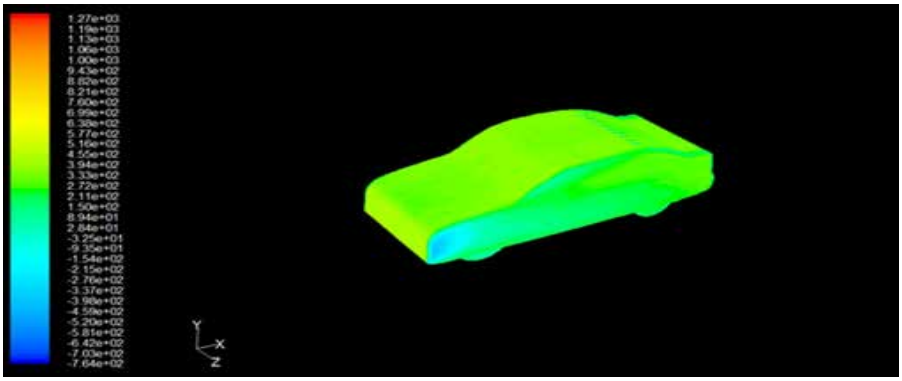


Fig 6: Total Pressure Generated with Vortex Generator

Zone name	Pressure force	Viscous force	Total force	Pressure coefficient	Viscous coefficient	Total coefficient
Car	4.08E+08	8308778.2	4.16E+08	1.05E+00	21952.466	1069634
Car with VG	3.93E+08	8174012.2	4.02E+08	1.03E+00	21352.469	1049013.7

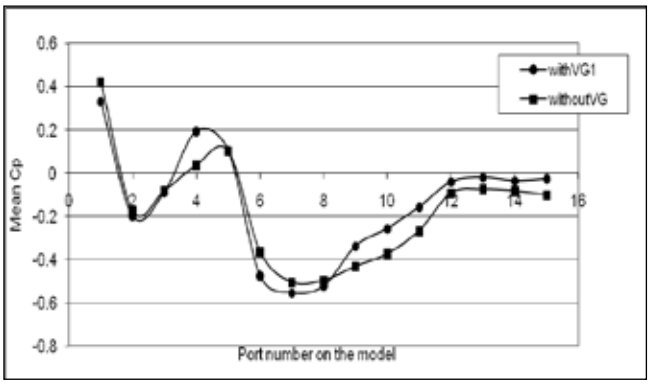
Table 1 :Comparison of Forces with and without Vortex Generator

The enhanced performance of the vortex generator was determined and the comparison was made between right angle shape and delta wing shape vortex generators. The addition of the vortex generators at the rear end of the car gave an average reduction of drag by -0.006. Vortex generator is a viable method of performance enhancement in cars. Vortex generators can be added to other standard enhancement techniques by varying the size, shape, thickness and height. The results in reducing the drag, shifting the flow separation point and narrow the flow separation

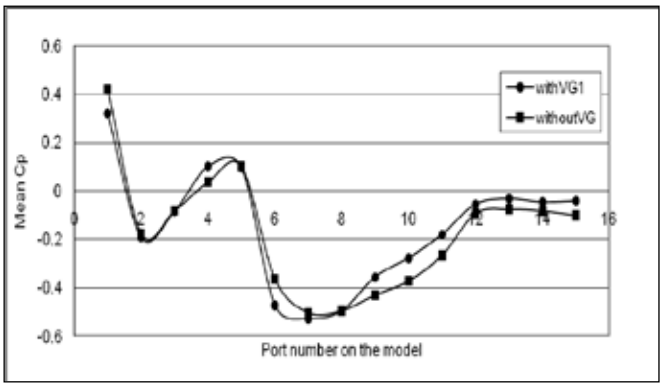
region. This project focused on the enhancement of the performance of cars using different shapes of vortex generators and the comparison results that the right angle shape vortex generator gave the better performance.

5.1 Comparison of Model With Vg

C_p curve for 19.01m/s for model:



Graph.1: delta shaped VG



Graph.1: right angle VG

The co-efficient of drag for the model with delta shaped VG for 19.01m/s is estimated as,

C_d with reference to maximum height from ground = 0.086614

C_d with reference to individual port height = 0.326612

C_d with reference to maximum height excluding ground clearance = 0.102774

The co-efficient of drag for the model with right angle shaped VG for 19.01m/s is estimated as,

C_d with reference to maximum height from ground = 0.090216

C_d with reference to individual port height = 0.332263

C_d with reference to maximum height excluding ground clearance = 0.11002

VI. CONCLUSION

It is concluded that both the vortex generators i.e. delta shaped and right angle shaped have the significance effect in reducing the drag force and also it is concluded that both the positions i.e. after front wind shield and top roof end has considered as the significant place in delaying the flow separation region. But there is an optimum position in the car model that should have to be found out and also the optimum shaped Vortex Generator in which the drag force is said to be least. Considering all the results and graph, the optimum shaped vortex generator and position is,Flow gets reattached in the areas of back wind shield, boot, and rear end by keeping Delta Shaped Vortex Generator at beginning of Front wind shield. But in the model those above said regions show there is no reattachment of flows that contributes more drag in the car.As a result of the verifications, it is confirmed that VG create stream wise vortices, the vortices mix higher and lower layers of boundary layer and the mixture causes the

flow separation point to shift downstream, consequently separation region is narrowed. From this, we could predict that VGs cause the pressure of the vehicle's entire rear surface to increase and thereby decreasing the drag.

REFERENCES

1. Hoerner, S. F., Fluid-dynamic Drag, Published by the author, 1958
2. Hoerner, S. F., Fluid-dynamic Lift, Published by the author,1985
3. Shibata, H., MMC's Vehicle Wind Tunnel, Automobile Research Review (JARI) Vol. 5, No. 9, 1983
4. Hucho, W. H., Aerodynamics of Road Vehicles, Fourth Edition, SAE International 1998
5. J. P. Brzustowicz, T. H. Lounsberry, and J. M. Esclafer de la Rode, Experimental and Computational Simulations Utilized During the Aerodynamic Development of the Dodge Intrepid R/T Race Car, SAE2002-01-3334, Indianapolis, IN, 2002
6. L. T. Duncan, Wind Tunnel and Track Testing an ARCA Race Car, SAE 901867, Detroit, 1990
7. lF. K. Schekel, The Origins of Drag and Lift Reductions on Automobiles With Front and Rear Spoilers, SAE Paper 77-0389, Detroit, 1977
8. Anderson, John D. (2007). Fundamentals of Aerodynamics (4th ed.). McGraw-Hill. ISBN 0071254080.
9. Bertin, J. J.; Smith, M. L. (2001). Aerodynamics for Engineers (4th ed.). Prentice Hall. ISBN 0130646334.
10. Craig, Gale (2003). Introduction to Aerodynamics. Regenerative.
11. J. Katz, Race-Car Aerodynamics, 2d ed., Robert Bentley Inc., Cambridge, Massachusetts, 2006
12. J. Katz, Aerodynamics of race cars, Annu. Rev. Fluid Mech., 38:27–64, 2006
13. W. F. Milliken and D. L. Milliken, Race Car Vehicle Dynamics, SAE International, Warrendale, Pennsylvania, 1995
14. www.sedancar/aerodynamics/flow.187.com
15. Buckley M Used Car Buying Guide: Range Rover Channel 4 (UK) 24 Jan 2005

DESIGN AND OPTIMIZATION OF OUTLET SHAPE ON COAXIAL TURBULENT JETS USING CFD

G.Sivaraj[1], D.Lakshmanan[2], S.Nithish[3]

[1,2,3] *Department of Aeronautical Engineering, Bannari Amman Institute of Technology, (India)*

ABSTRACT

The computational analysis was carried out to investigate the effect of flow field generated by two coaxial jets using Ansys Fluent software. The area ratio between the external and internal nozzle was varied as well as the velocity issuing from each of the nozzles. The distribution of the mean velocities, turbulence intensities, and shear stresses were determined for the various cases. The development of the flow field and its approach to a self-preserving state is discussed. The Reynolds numbers based on various shape of nozzle outlet such as Circle, square, and polygon shapes and the velocities were low enough that the flow can be considered incompressible.

Keywords: Annular, Coaxial Jet, Nozzle, Turbulence Intensities

1. INTRODUCTION

A nozzle is a device designed to control the direction or characteristics of a fluid flow as it exits an enclosed chamber or pipe via an orifice. Nozzles are frequently used to control the rate of flow, speed, direction, mass, shape, and/or the pressure of the stream that emerges from them

A computational study was carried out to investigate the effect of co-axial nozzle technology with varying cross sections. The co-axial design can be used with water, Class A foam, or compressed air foam. It is especially valuable in CAFS applications because the unobstructed smooth-bore passageway produces a tight stream that maintains a good bubble volume with an excellent reach. This allows firefighters to keep a safer standoff distance when making a direct attack or to effectively coat all parts of a threatened structure from a position on the ground in a defensive mode.

The background study was carried out about co-axial nozzles with their applications. The computational and experimental results were also carried out. Based on the literature survey coaxial nozzle were a designed with varying cross sections. Computations were performed to understand the flow field around a scaled down model of a typical nozzle with annular. Computations using the commercially available software FLUENT 6.3.26 were carried out for two dimensional and three dimensional fully developed flows. A validation test was performed by referring to the same type of model at a same inlet velocity

II. COAXIAL NOZZLES

Much data have been accumulated for laser cutting using various nozzle shapes with various standoff distances and pressures. But it appears to be little agreement on methods for obtaining a consistently high cutting quality. Usually the nozzle is positioned close to the work piece (0.3-1.3 mm) and with low nozzle pressures. When higher nozzle pressure is used, the cutting speed is raised but the cutting repeatability cannot be ensured.

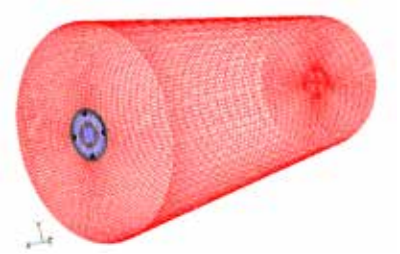
III. DESIGN OF NOZZLE

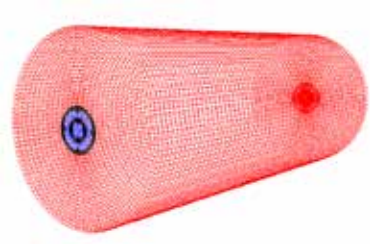
Frequently the goal is to increase the kinetic energy of the flowing medium at the expense of its pressure and internal energy. Nozzles can be described as convergent (narrowing down from a wide diameter to a smaller diameter in the direction of the flow) or divergent (expanding from a smaller diameter to a larger one). A de Laval nozzle has a convergent section followed by a divergent section and is often called a convergent-divergent nozzle ("con-di nozzle").

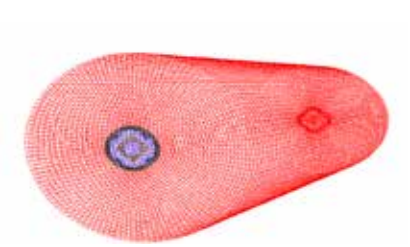
3.1 Different Shapes of Nozzle Outlet Cross Sections

There are nozzle outlet shapes classified by circle and square shapes with annular.

1. Circle without annular
2. Square without annular
3. Square with annular







Fig(1). Circular without annular **Fig(2). Square with annular** **Fig(3): Square without annular**

IV. COMPUTATIONAL ANALYSIS

For thorough understanding of the complex flow field around typical Co-axial Nozzle with annular, axi-symmetric computational simulation of the flow field can be made useful along with the experimental testing. This can be done either by developing a code or by available commercial CFD software. In the present study computation has been attempted for flow over a nozzle with different types of cross section model with the commercially available software FLUENT 6.3.26. Present chapter describes briefly about the solver, solution methodology, preprocessing, solver settings and post processing.

4.1 Geometry Design

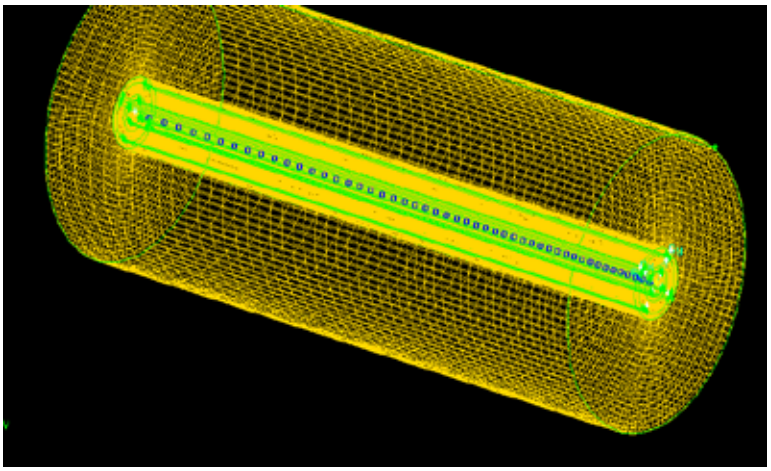
Any CFD analysis can be divided into three broad categories namely, preprocessing, solver settings and post processing. GAMBIT is an aid for preprocessing of the problem in FLUENT. It is a software package designed to help analysts and designers build a mesh around the geometry under consideration. GAMBIT receives user input by means of its graphical user interface (GUI). Geometry creation in GAMBIT is done with the help of required commands from the geometry creation tool pad. The geometry creation tool pad contains command buttons that allows performing operations which include creating vertices, lines, faces, volumes etc.

Meshing in GAMBIT can be done in various forms namely edge meshing, face meshing and volume meshing. Meshed edges, faces and volumes can be copied, moved, linked or disconnected from one another.Creation of the geometry can also be done in any of the available software like AutoCAD, CATIA, and PRO-E etc. Created geometry can then be imported into GAMBIT and meshed. After meshing is completed and the zone types are specified, the created mesh can be exported as a mesh file in to various different solvers like FLUENT 5/6,

FLUENT 4, POLYFLOW, ANSYS etc. The exported mesh is ready to be fed into the solver for obtaining a solution of the given problem.

4.2 Grid Generation for Nozzle Model

A structured grid was generated for 2D simulation of flow around the nozzle model. The grid was made very fine at the geometry surfaces and coarsens away from the body. The overall domain was selected based on several iterations, boundary conditions and finally a domain extending 5 times the major length of the nozzle model. The extents of the domain were evaluated from inviscid simulation of the problem. A total of 50,000 cells were used in the grid system. Figure shows the grid system with boundary conditions, in the vicinity of the geometry and a close up surface grid near main body and strap-on nose regions respectively. In order to capture the shocks more accurately, finer mesh cells were created near the surface of the model using appropriate edge mesh distribution.



Fig(4).Solid View of Entire Domain With Model

4.3 Boundary Conditions

Pressure far field boundary condition was set for the pressure outlet (outer domain), where it is needed to specify the atmospheric pressure. Inlet 1 and inlet 2 boundary condition was set to the velocity inlet (surface from which the flow enter), Wall boundary condition is assigned for the model surfaces and domain boundary extents other than interior.

V. COMPUTATIONAL RESULTS

Computations were performed to understand the flow field around a scaled down model of a typical nozzle with annular. Computations using the commercially available software FLUENT 6.3.26 were carried out for two dimensional and three dimensional fully developed flows. A validation test was performed by referring to the same type of model at a same inlet velocity. The details of the computations are discussed in this chapter.

Two dimensional and three dimensional computational simulations were carried out for studying the flow field around typical nozzle geometry at 30 m/s inlet 1 and 25 m/s inlet 2. in detail in the following sections.

5.1 Validation of Computational Procedure

Verification and validation are the primary means to assess accuracy and reliability in computational simulations.

Several computational tests were performed on a typical nozzle at a 30 m/s inlet 1 and 25 m/s inlet 2 for verifying and validating the computational grid and turbulence model that are going to be adopted for the present work.Inviscid, laminar, S-A, standard k-ε and standard k-ω models were tested for verifying the most suitable turbulence model for present case of a typical nozzle configuration. The solver settings operational conditions, material properties, and boundary conditions were set according to the present typical space launch vehicle problem. The problem was iterated till the residuals of continuity, momentum, and energy converged to a value of 10^{-3} and the scalars nut (SA) residuals converged to a value of 10^{-5}.

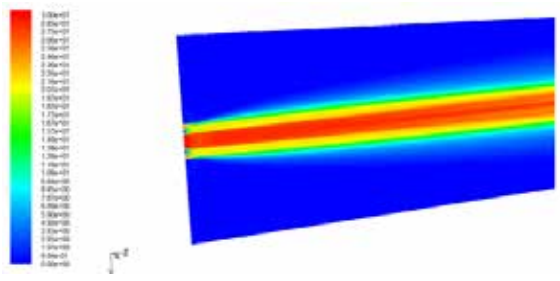
5.1.1 Comparison of Circular Cross Section with and Without Annular

Force Report						
zone name	pressure Force	Viscous Force	total force	pressure coefficient	viscous coefficient	total coefficient
Without Annular	35984.81	0.024961	35984.83	65.27856	4.53E-05	65.278608
With Annular	29511.12	0.03901	29511.16	77.09026	0.000102	77.090366

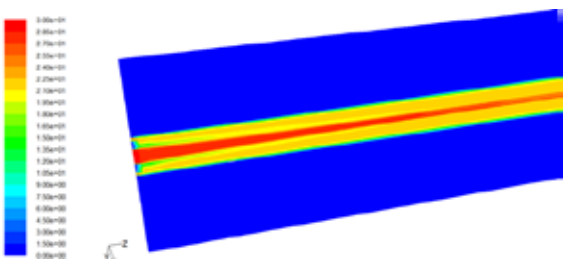
5.1.2 Comparison of Rectangular Cross Section with and Without Annular

Force Report						
zone name	pressure Force	Viscous Force	total force	pressure coefficient	viscous coefficient	total coefficient
Without Annular	30332.31	0.038046	30332.35	49522.14	0.062116	49522.2
With Annular	30282.81	0.0437046	30282.85	59622.17	0.062116	59622.5

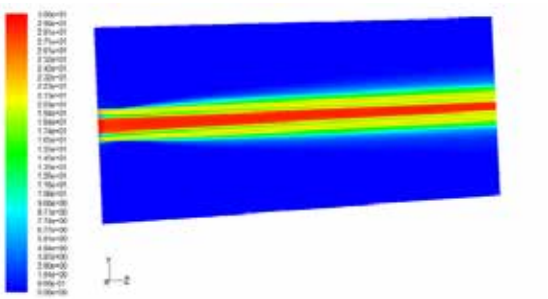
VI. VELOCITY MAGNITUDE OF JET STREAM



Fig(5).Circular Cross Section Without Annular



Fig(6).Rectangular Cross Section With Annular



Fig(7). Rectangular Cross Section Without Annular

VII. CONCLUSION

Based on computational investigations of co axial circular flow jet using annular, the following conclusions have been observed:

- The potential core length of Circular cross section without annular jet was less than the Circular cross section with annular Co-axial jet and it was longer for circular co-flow jet when compared to the non-circular co-flow.
- The velocity decay of single jet was less than the Co-axial jet. It was significant in size for crusi form jet. The velocity decay along the radial direction of single circular jet was lesser than the Co-axial circular jet, and it was faster for non-circular co-flow jet when compare to circular co-flow jet compared with circular jet and related to vortices generated at the corner of jetting.

REFERENCE

[1]. Nob hide Kasagi, “Jsme International Journal”, Publication Year:2006

[2]. ParvizBehrouzi And James J, McGuirk ,”Journal Of Fluid Science And Technology”, Publication Year:2007

[3]. Toru KosoAnd Takuya Kinshasa, “Journal Of Fluid Science And Technology”, Publication Year:2008

[4]. Truong V.V, Hideyuki Takakura, Jonn.C.Wells And Takashi Minemot,“Journal Of Solid Mechanics And Materials Engineering”, Publication Year:2010

[5]. Jeff Kastner, Chris Harries And Ephraim Gut mark,”Journal Of Fluid Science And Technology”, Publication Year:2011

MELANOMA DETECTION USING HYBRID CLASSIFIER

D.Selvaraj[1], D.Arul Kumar[2], D.Dhinakaran[3]

[1,2] *Associate Professor, Department of ECE, Panimalar Engineering College, Tamilnadu, (India)*

[3] *Assistant Professor, Department of CSE, Peri Institute of Technology, Tamilnadu, (India)*

ABSTRACT

In our proposed method an automatic melanoma classification system is developed. The input image is pre-processed, segmented and features are extracted. Based on the calculated features, the image is classified as cancerous or non-cancerous using KNN and SVM classifier. In the pre-processing stage noise is removed using Median filter and the image is enhanced using Adaptive Histogram Equalization. Later the image is segmented using Otsu thresholding, a novel method for acquiring accurate border of tumour of the selected images. Then features like entropy, mean, variance, skewness, kurtosis, correlation, energy, contrast, area and homogeneity are calculated from the segmented images. Later, SVM Classifier is trained with the extracted features. A total of 100 images have been used, out of which 45 are used for training and remaining images for testing. SVM classifier classifies the input image to be cancer affected or normal based on features extracted. If the image is cancer affected, then type of cancer is detected as malign tumor or benign tumor using KNN Classifier.

Keywords: ***KNN Classifier, Median Filter, Melanoma, Skin Cancer And SVM Classifier***

I. INTRODUCTION

Melanoma is named after the type of skin cell from which they arise. Basal cell cancer originates from the lowest layer of the epidermis, and is the most common but least dangerous skin cancer. Squamous cell cancer originates from the middle layer, and is less common but more likely to spread and, if untreated, become fatal. Melanoma, which originates in the pigment-producing cells (melanocytes), is the least common, but most aggressive, most likely to spread and become fatal if untreated. Most cases are caused by over-exposure to UV rays from the sun or sun beds. Treatment is generally via surgical removal. Melanoma has one of the higher survival rates among cancers. Most melanomas consist of various colors from shades of brown to black. A small amount of melanomas are pink, red or fleshy in color; these are called amelanotic melanomas which tend to be more aggressive. Warning signs of malignant melanoma include change in the size, shape, color or elevation of a mole. Other signs are the appearance of a new mole during adulthood or pain, itching, ulceration, redness around the site, or bleeding at the site.

Image segmentation plays a vital role in biomedical image processing to segment the medical input images in to meaningful regions. Even though several image segmentation and classification methods like otsu thresholding, region growing, region split and merge, active contour, Fuzzy C-means (FCM), Self Organizing Map (SOM), Support Vector Machine (SVM), Artificial Neural Networks are available, till image segmentation and classification remains a challenging problem.

In our proposed technique, initially the input melanoma image is preprocessed in order to remove the noise and make the image fit for the rest of the processes. Here we use median filter for removing the noise and CLAHE for image enhancement. Subsequently, the preprocessed image is segmented using the OTSU thresholding

technique. After segmentation process, the feature such as mean, variance, Correlation, energy, Entropy, Skewness, Kurtosis, Contrast and Homogeneity are extracted from the regions and given to the SVM classifier for training. Later, the inage is classified as tumourous or normal with the help of trained SVM. Finally, the type of cancer is detected using KNN classifier.

The paper is organised as follows, A brief review of researches relevant to the melanoma detection and segmentation technique is presented in section 2. The proposed segmentation and classification technique is presented in section 3. The detailed experimental results and discussions are given in section 4. The conclusions are summed up in section 5.

II. REVIEW OF RELATED WORK

Many research works have been performed for the segmentation and classification of melanoma images. Some of the related works regarding the segmentation and classification of melanoma images are reviewed in the following section.

PaulWighton et al., [1] presented many sub problems in automated skin lesion diagnosis (ASLD) can be unified under a single generalization of assigning a label, from a predefined set, to each pixel in an image. The first model is based on independent pixel labeling using maximum a-posterior (MAP) estimation. The second model is based on conditional random fields (CRFs), where dependencies between pixels are defined using a graph structure. But the discrepancy between the objective and subjective performance of the CRF model implies that evaluation metric (pixel-wise sensitivity and specificity) is less than ideal.

Ho Tak Lau et. al.,[2] developed an automatic skin cancer classification system describing the relationship of skin cancer image across different type of neural network with different types of preprocessing. The collected images are fed into the system, and across different image processing procedures to enhance the image properties. Then the normal skin is removed from the skin affected area and the cancer cell is left in the image. The paper presented a study which can be concluded that there are some possible factors of low classification result. The image database is not feasible and too small; the variation between dermoscopy and digital image is large. The imaging processing methods are not unique and their variation is large.

SookpotharomSupot et. Al.,[3] proposed a new method of segmentation to locate the skin lesion is proposed by. The method consists of two stages; image pre-processing and image segmentation. As the first step of image analysis, pre-processing techniques are implemented to remove noise and undesired structures for the images using median filtering. In the second step, the fuzzy c means (FCM) thresholding technique is used to segment and localize the lesion. The border detection results are visually examined by an expert dermatologist and are found to be highly accurate. The proposed method gives more reliability and visually precise boundary tracing for a range of images. It is robust from noise and unwanted objects that gave the challenged problem in the most of the segmentation methods.

Thresholding is a simple but effective method to separate objects from the background. A commonly used method, the Otsu method improves the image segmentation effect obviously. It’s simpler and easier to implement. Its half belongs to object and half belongs to background. Then a new weight to the Otsu method is applied by Kritika Sharma, Chandrashekhar Kamargaonkar, Monisha Sharma [4]. This weight can make sure that the result threshold value will always reside at the valley of the two peaks or at the bottom rim of a single peak. Moreover, it ensures that both the variance of the object and the variance of the background keep away

from the variance of the whole image. The components of the histogram cover a broad range of the gray scale and it is reasonable to conclude that an image, whose pixels tend to occupy the entire range of possible gray levels and, in addition, tend to be distributed uniformly, will have an appearance of high contrast and will exhibit a large variety of gray tones.

A new segmentation method that combines the advantages of fuzzy C mean algorithm, thresholding and level set method is presented by AmmaraMasood, Adel Ali Al-Jumaily[5]. 3-class Fuzzy C mean thresholding is applied to initialize level set automatically and also for estimating controlling parameters for level set evolution. The proposed method showed reasonably good accuracy for segmentation of skin lesion images with an average true detection rate of 92.6% and quite reduced false positive and false negative error i.e. 4.66% and 7.34% respectively. Comparative analysis proved that it works well even in the presence of different artifacts present in skin images.

According to Howard Lee .Yi-Ping Phoebe Chen [6], a new approach to segment different types of skin cancers using fuzzy logic approach is developed. An optimum threshold segmentation algorithm based on type-2 fuzzy sets algorithms to delineate the cancerous area from the skin images is proposed. By using the 3D color constancy algorithm, the effect of color changes and shadows due to skin tone variation in the image can be significantly reduced in the preprocessing stage. The proposed method showed more tolerance at the border. Proposed skin cancer segmentation using the fuzzy algorithm approach demonstrated a good segmentation result while utilizing global features such as RGB color features. However, biological properties of different skin cancer types have not yet been utilized to fine tune the segmentation result.

One application of image processing is to reconstruct the original scene from the low quality images. Considering the idea of histogram, many histogram analyzing based methods have been studied recently. However, some methods require users to set some parameters or condition, and cannot get the optimal results automatically. To overcome those short come, Qieshi Zhang, Hiroshi Inaba andSei-ichiroKamata [7] presented an Adaptive Histogram Separation and Mapping (AHSM) method for Backlight image enhancement. First, the histogram by binary tree structure with the proposed Adaptive Histogram Separation Unit (AHSU) is separated. And then mapping the LowDynamic Range (LDR) histogram partition into High Dynamic Range (HDR). By doing this, the excessive or scarcity enhancement can be avoided. The experimental results show that the proposed method can gives better enhancement results, also compared with some histogram analyzing based methods and get better results.

The value of ‘k’ in KNN classifiers based on a n-sized training set is evaluated by C.Alippi, M.Fuhrman and M.Roveri [8]. The paper relates the generalization error of a k-nn classifier with k and n through a functional that allows identifying the optimal k. It depends on the application itself and cannot be solved in a closed form. However the functional can be numerically solved and an approximation of the optimal k derived. This method provides optimal results and it is seen that when the number of training samples increases the generalization error becomes more robust with respect to k.

III. PROPOSED METHOD

Our proposed method consists of 4 phases namely preprocessing, segmentation, feature extraction and classification. In preprocessing phase, the noise is removed using median filter and the image is enhanced using CLACHE. We have used OTSU thresholding technique for segmentation. After segmentation process, the

features such as mean, variance, Correlation, energy, Entropy, Skewness, Kurtosis, Contrast and Homogeneity are extracted from the regions and given to the SVM classifier for training. Later, the inage is classified as tumourous or normal with the help of trained SVM. Finally, the type of cancer is detected using KNN classifier. The block diagram of the proposed technique is shown in Fig. 1.

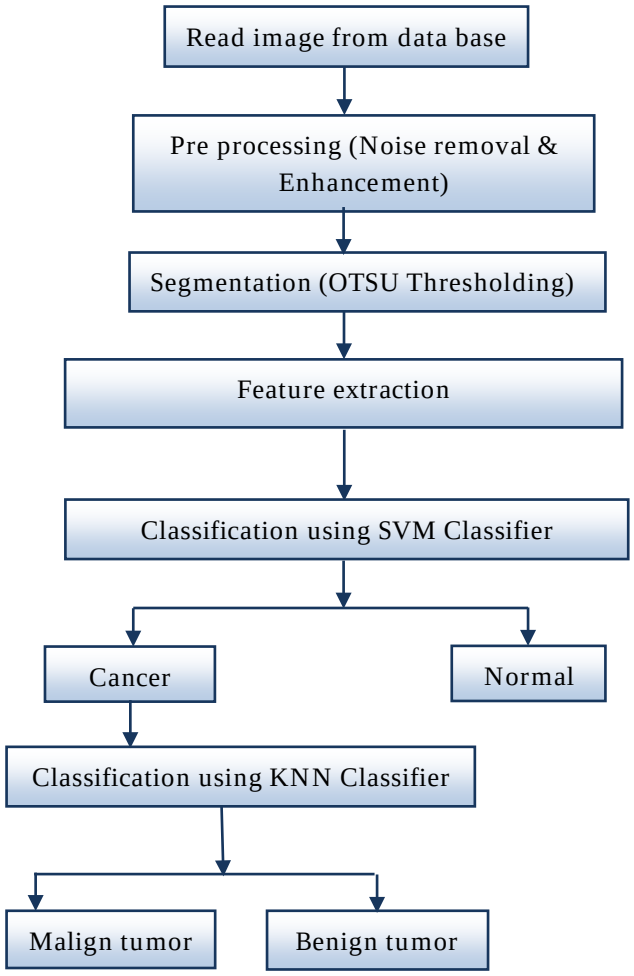


Fig. 1 Block diagram of proposed approach

3.1 Preprocessing

The first step in image processing is to read an image from data base. Select an image which is to be detected as cancerous or not from database available. Steps which are done prior to processing of an image are called pre processing. It includes processes like noise removal, image enhancement, resizing of image and equalization of image. These are done in order to make the image suitable than original image for specific applications. If the image selected is a color image, it is converted to gray scale image using 'rgb to gray conversion' command. Then the intensity variation of gray level image is shown in graph as in Figure 3. Its value varies from 0 to 255.

Resizing of image is done for accurate processing of image. Image can be resized to any size of our interest. There are many factors which cause noise in an image. It may be due to environmental conditions, quality of image sensing elements or interference in transmission channel. In order to avoid this, "filtration" is done. Here, median filter is used for removing noise. The median filter replaces each pixel in the input image by the median of gray levels in neighborhood. This filter is a type of smoothing spatial filter.

Median filter is useful for removing isolated lines or pixels while preserving spatial resolutions. It provides less blurring than linear filters. The filtering procedure consists of three steps:

- Arrange the pixel values in the window in increasing or decreasing order.
- If window size is odd, the middle value is the median. If the window size, K is even, the average of two values in the middle is the median.

Once noise is removed, we go for image enhancement. We use CLAHE (Contrast Limited Adaptive Histogram Enhancement) for this purpose. Histogram equalization also known as histogram linearization is a process of automatically determining a transformation function which produces an output image with uniform histogram. The transformation function modifies the pixels based the gray level content of an entire image. These techniques are used to enhance details over small areas in an image.

3.2 Segmentation

Otsu thresholding technique is used for segmenting the enhanced melanoma image. Otsu method is the commonly used thresholding technique. Otsu method is simple and effective to implement. Otsu's thresholding technique is based on a discriminant analysis which partitions the image into two classes C_1 and C_2 at gray levels 'k' such that C_1 = { 0,1,2,3,…, k} and C_2 = { k+1, k+2,…, L-1}where, 'L' is the total number of gray levels of the image. Let 'n' be the total number of pixels in the given image and 'n_i' be the number of pixels at the i^{th} gray level.

3.2.1 Algorithm

Step1: Compute probabilities of each intensity level

Step2: Compute various thresholds T = 1, 2, ….. , max intensity and i) upgrade w_i and η ii) Compute

$$s_B^2(k)$$

Step 3: Select threshold value having max $s_B^2(k)$

3.3 Feature Extraction

Feature is a parameter of interest to describe an image. Transforming the input data into the set of features is called feature extraction. If the features extracted are carefully chosen it is expected that the features set will extract the relevant information from the input data in order to perform the desired task using this reduced representation instead of the full size input. Feature extraction involves simplifying the amount of resources required to describe a large set of data accurately. There are many features we can extract from an image such as energy, entropy, mean, standard deviation, variance, color, texture etc.; we have considered extracting features like entropy, mean, contrast, correlation, energy, homogeneity, skewness, kurtosis and variance.

3.4 Classification

Two classifications are done here using two different efficient classifiers and hence the name "hybrid classifier". First classifier, SVM (Support Vector Machine) classifies the image to be cancerous or not depending on the

features extracted. If the outcome of SVM classifier says that the input image is diseased, then second classifier KNN classifier is used. It classifies severity stage of skin cancer as malign or benign tumor.

3.4.1 SVM Classifier

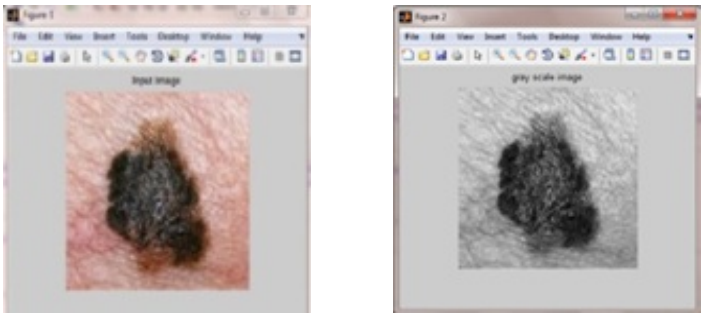
In machine learning, support vector machines are supervised learning models with associated learning algorithms that analyze data and recognize patterns, used for classification and regression analysis. Given a set of training examples, each marked as belonging to one of two categories, an SVM training algorithm builds a model that assigns new examples into one category or the other, making it a non-probabilistic binary linear classifier. An SVM model is a representation of the examples as points in space, mapped so that the examples of the separate categories are divided by a clear gap that is as wide as possible. New examples are then mapped into that same space and predicted to belong to a category based on which side of the gap they fall on.

3.4.2 k-NN Classifier

In pattern recognition, the *k*-Nearest Neighbors algorithm (*k*-NN) is a non parametric method used for classification. Here the input consists of the *k* closest training examples in the feature space. In k-NN classification, the output is a class membership. An object is classified by a majority vote of its neighbors, with the object being assigned to the class most common among its *k* nearest neighbors (*k* is a positive integer, typically small). If $k = 1$, then the object is simply assigned to the class of that single nearest neighbor. *KNN* is a type of instance-based learning, or lazy learning, where the function is only approximated locally and all computation is deferred until classification. The *k*-NN algorithm is among the simplest of all machine learning algorithms. Based on the output of KNN classifier, the severity stage of skin cancer is detected.

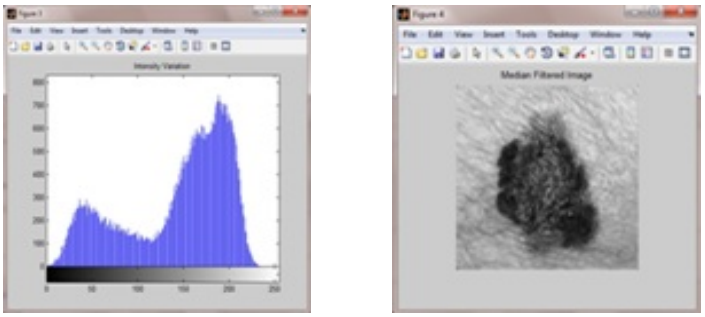
IV. EXPERIMENTAL RESULTS AND DISCUSSION

Here, totally 100 images have been used out of which 45 are taken for training and remaining have been used for testing. Calculated feature values of various input skin images are tabulated. Results show that 27 images are detected to be normal, 13 are benign tumor and 15 images are malign tumor. Comparison of various features for normal, benign and malign tumor images are shown in figure.



(A) (B)

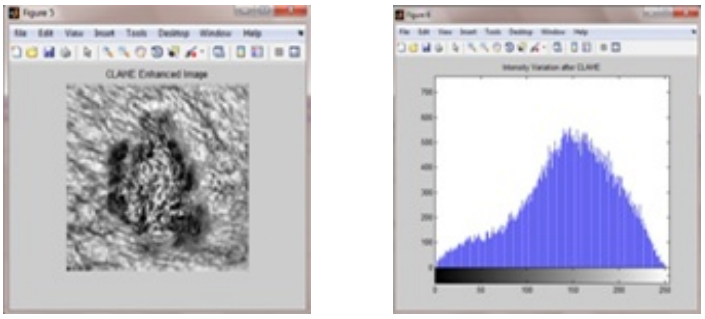
Fig. 2: (a) Input skin cancer image, (b) Converted gray scale image of input melanoma image



(A) **(B)**

Fig. 3: (a) Intensity variation before filtering, (b) Input melanoma image after median filtering

The input image is first preprocessed by converting color image to gray scale image, resizing it to required size and later filtering it using median filter as shown in Fig. 2 and Fig. 3. The enhanced image and segmented image is shown in figure 4 and 5. The intensity variation of the melanoma image before and after median filtering is shown in Fig. 3 (A) and Fig. 4(B).



(A) **(B)**

Fig. 4: (A) Enhanced melanoma image after filtering, (B) Intensity variation after median filtering

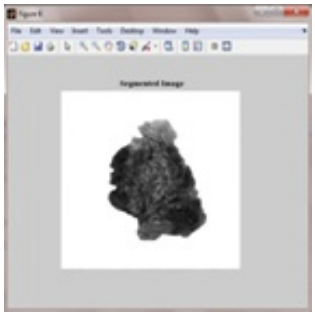


Fig. 5: Segmented melanoma image

Fig. 6: First order gradient features of melanoma image

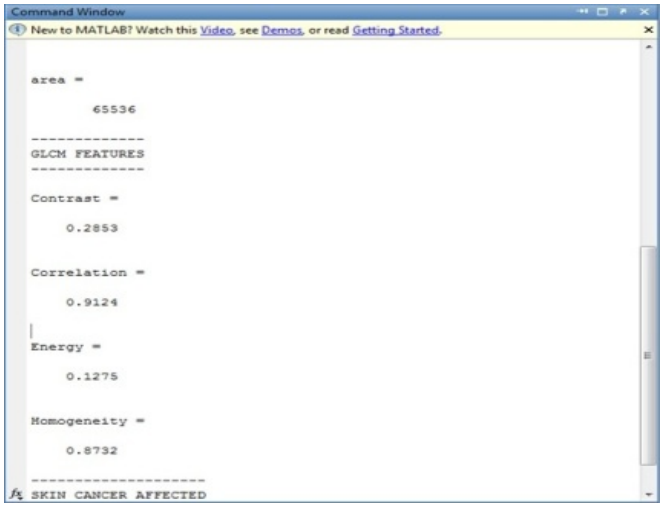


Fig. 7: GLCM features of melanoma image

The calculated first order gradient and GLCM feature values are shown in Fig. 6 and Fig. 7. Based on the calculated features values, the SVM classifer classified the image as a cancer image. so, the input image is fed to the KNN classifer for further classification. This classfier classified the image as Benign. The screensot of the final result is shown in Fig. 8.

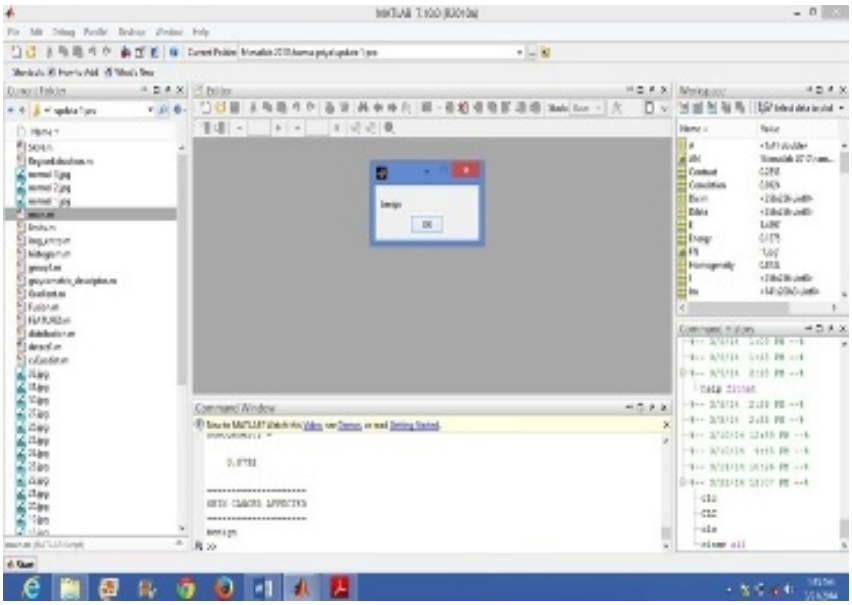
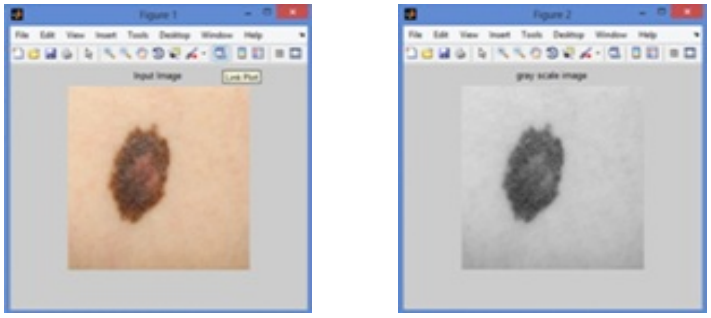
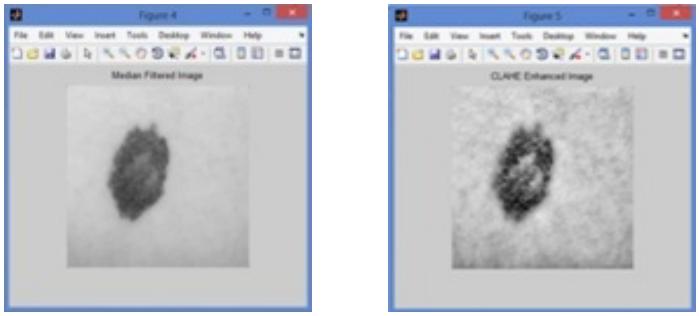


Fig. 8: The screenshot of the classified result



(A) **(B)**

Fig. 9: (a) input skin cancer image, (b) converted gray scale image of input melanoma image



(A) **(B)**

Fig. 10: (a) input image after median filtering, (b) input enhanced image

Fig. 11: Segmented image

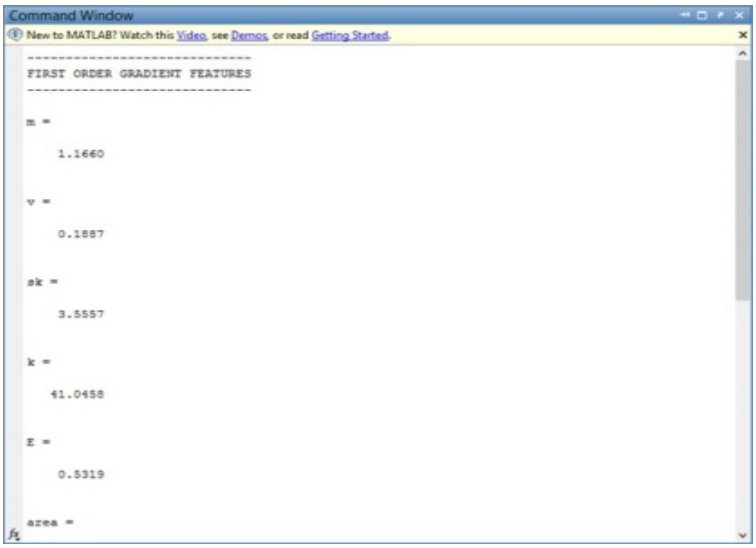


Fig. 12: First order gradient features of melanoma image

Fig. 13:GLCM features of melanoma image

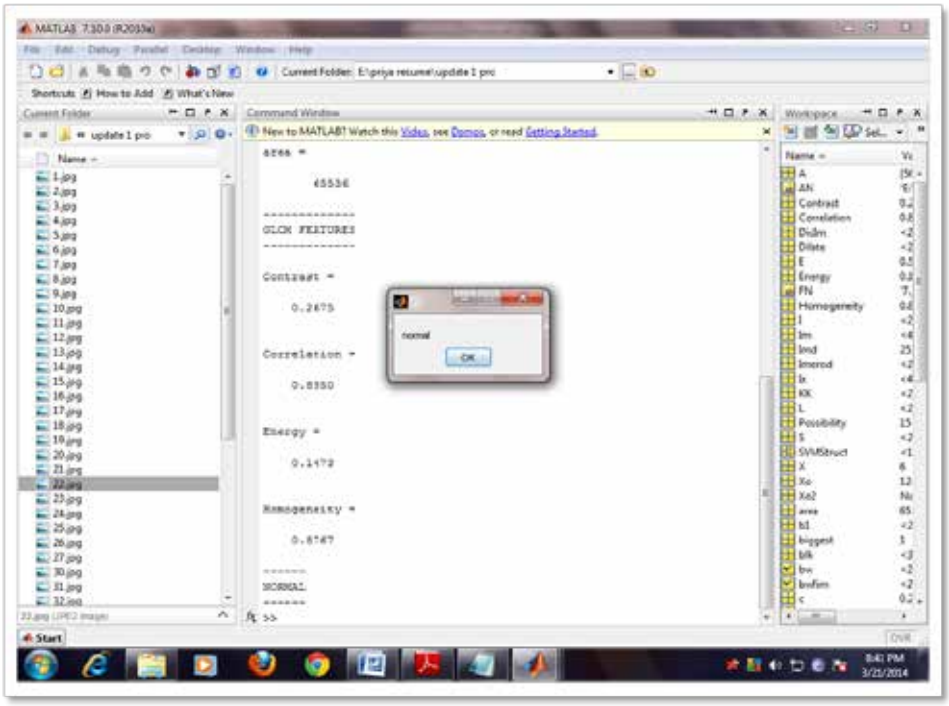


Fig. 14: The screenshot of the classified result

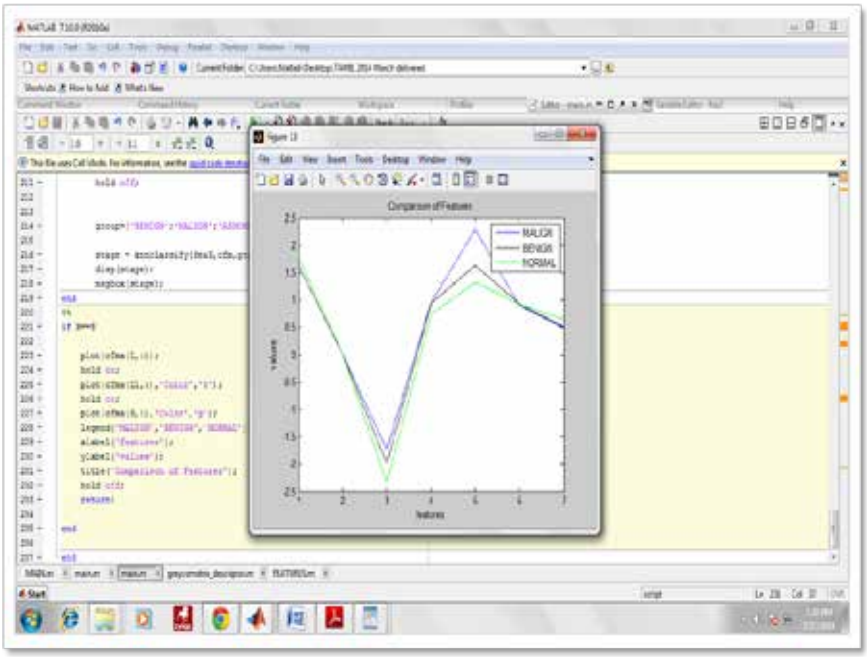


Fig. 15: Comparison between feature values of normal, benign and malignant images

Table 1 calculated feature values of different melanoma and non- melanoma images

IMAGES	M	V	E	ENE	S	CNT	COR	K	H	RESULT
	1.5976	0.5531	0.5197	0.7275	5.5098	0.2853	0.9124	109.9113	0.8732	Benign
	1.6624	0.6188	0.8557	0.5279	4.2582	0.0946	0.9617	43.5705	0.9531	Benign
	2.2224	1.1146	1.7452	1.1284	0.9545	0.2961	0.9092	12.1516	0.8731	Malign
	1.7791	0.7159	0.6141	0.5085	1.9156	0.1952	0.9064	21.3572	0.9080	Benign
	1.0002	0.0578	0.1259	0.2837	0.5599	0.0725	0.9705	9.6587	0.9649	Normal
	1.1660	0.1887	0.2319	0.1473	3.5557	0.2675	0.8950	41.0458	0.8767	Normal
	1.1115	0.1527	0.0147	0.2484	0.2662	0.0607	0.9755	5.2423	0.9697	Normal
	1.2462	0.2571	0.2150	0.2119	2.3509	0.2453	0.8364	36.7244	0.8874	Normal

IMAGES	M	V	E	ENE	S	CNT	COR	K	H	RESULT
	1.5702	0.5420	0.7486	0.7311	2.1349	0.1810	0.9578	8.2059	0.9133	Benign
	1.0975	0.2918	0.1341	0.2309	3.1586	0.3044	0.7607	42.1937	0.8640	Normal
	2.3432	1.1153	1.5673	1.1279	2.3867	0.1442	0.9754	59.1696	0.9312	Malign
	2.4261	1.2338	1.4644	1.2105	2.2530	0.1615	0.9153	15.2236	0.9206	Malign
	1.8322	0.6131	0.8422	0.6390	1.0508	0.1039	0.9513	11.2167	0.9486	Benign
	2.1439	1.2239	1.6632	1.1249	0.5898	0.2216	0.9479	16.4620	0.9029	Malign
	1.7584	0.5970	0.5873	0.5889	-0.9255	0.1358	0.9442	2.2801	0.9329	Benign
	2.4144	1.2315	1.3929	1.1289	0.4272	0.2231	0.9544	7.1833	0.8996	Malign

IMAGES	M	V	E	ENE	S	CNT	COR	K	H	RESULT
	2.4830	1.1100	1.2766	1.1676	1.3286	0.1265	0.9662	11.3186	0.9419	Malign
	1.7076	0.7374	0.6137	0.7135	5.3478	0.2609	0.9481	41.8162	0.8884	Benign
	2.5435	1.0784	1.7586	1.2365	3.2266	0.1411	0.9260	54.3418	0.9386	Malign
	1.2578	0.0528	0.1082	0.2464	1.5375	0.1472	0.9122	7.9463	0.9282	Normal
	1.7584	0.5970	0.5873	0.5889	-0.9255	0.1358	0.9442	2.2801	0.9329	Benign
	1.2853	0.0287	0.2852	0.1899	0.7658	0.1628	0.9272	5.3689	0.9204	Normal
	2.2224	1.1146	1.7452	1.1284	0.9545	0.2961	0.9092	12.1516	0.8731	Malign
	1.1085	0.1649	0.1931	0.0266	0.0502	0.0570	0.9471	4.0766	0.9741	Normal

IMAGES	M	V	E	ENE	S	CNT	COR	K	H	RESULT
	1.7923	0.6210	0.8803	0.7710	5.1837	0.3173	0.8687	77.1542	0.8627	Benign
	1.8667	0.8213	0.7190	0.6934	1.0656	0.2148	0.9247	0.1934	0.8990	Benign
	1.2233	0.0086	0.1577	0.2202	-0.5770	0.0985	0.9868	0.2202	0.9668	Normal

The feature values for different cancer and non-cancer images are calculated and tabulated in table 1. The same process as image 1 is repeated for the second image. Now, the second image is considered as normal image. The output of the image 2 at various stages are shown in figure 9 to 14. Similarly, various images can be processed.

V. CONCLUSION

This paper presents a method to detect type of cancer using hybrid classifier. Input image is subjected to pre processing stages like noise removal and enhancement. Here, totally 100 images have been used out of which 45 have been used as training images and 55 images are used as testing images. After enhancement, image is segmented using OTSU Thresholding. Features like mean, variance, entropy, energy, etc., are calculated. Based on the features extracted, image is classified to be cancer affected or not using SVM (Support Vector Machine) classifier. If the image is detected to be cancerous, then the severity of cancer is classified using KNN classifier. The severity of cancer is classified to be malignant or benign. From the results obtained, we can see our proposed hybrid method received a better quantity rate for all input images.

REFERENCES

1. Alippi.C, Fuhrman.M and Roveri.M, (2008), ‘k-NN classifiers: Investigating the k=k (n) relationship’hoi, Mihwa. “Contesting Imaginaires in Death Rituals during the Northern Song Dynasty.” PhD thesis., University of Chicago, 2008.
2. AmmaraMasood and Adel Ali Al-Jumaily, (2013), ‘Fuzzy C Mean Thresholding based Level Set for Automated Segmentation of Skin Lesions’.
3. Ho Tak Lau and Adel Al-Jumaily, (2009) ‘Automatically Early Detection of Skin Cancer: Study Based on Neural Network Classification’.
4. Howard Lee · Yi-Ping Phoebe Che, (2013), ‘Skin cancer extraction with optimum fuzzy thresholding technique’.

5. Kritika Sharma,ChandrashekharKamargaonkar and Monisha Sharma, (2012), 'An Improved Image Segmentation Algorithm Based on Otsu Method'.
6. PaulWighton, Tim K. Lee, GregMori, Harvey Lui, David I. McLean and Stella Atkins, (2011) 'Conditional Random Fields and Supervised Learning in Automated Skin Lesion Diagnosis'.
7. Qieshi Zhang, Hiroshi Inaba and Sei-ichiroKamata, (2010), 'Adaptive Histogram Analysis for Image Enhancement'.
8. SookpotharomSupot, (2009), 'Border Detection of Skin Lesion Images Based on Fuzzy C-Means Thresholding'

MULTI-LAYERED SECURITY FOR PRIVATE COMMUNICATION (USING STEGANOGRAPHY AND CRYPTOGRAPHY)

[1]Sahil Agarwal, [2] Barkha Khattar , [3] Dr. Inder Singh

[1,2] Scholar, [3]Assistant Professor (Senior Scale),

Centre for Information Technology- COES, UPES-Dehradun, (India)

ABSTRACT

Communication has always been an integral part of human existence and innovation. In this age of technology, data transmission has become important in order to communicate. This paper proposes the use of enhanced form of Least Significant Bit method for Steganography and Triple Data Encryption Standard algorithm for encrypting the message. The proposed method will encrypt the message and embed it into the cover image in the red, green and blue channels of each pixel in random method, making use of linked list data structure. We are making use of the least significant bit and also one bit before it in each pixel, chunking three pixels, to store the message and the address of the next pixel and those chunked together along with it. The recipient, on receiving the image will have to log in using a valid username and password and then can de-embed the message, followed decrypting the message. We are using the enhanced version of steganography and the classical method for cryptography, making it a multi-layered secured system for private communication, which can be used the secret agencies or government agencies or even by the defence to communicate in a secret way even if the network is unsecured.

Keywords: Cryptography, Linked-List, LSB Technique, Secret communication, Steganography, triple-DES

I. INTRODUCTION

In this age of cyberspace revolution, people are diving into the world of internet that can be used without any restriction or strict regulation. There are some people, known as intruders, who secretly keep an eye on the communication which is taking place between the sender and the receiver. Intruders, having malicious intention or purpose can reveal the message to others or can alter it to mislead the recipient. For the purpose of secretly transmitting the message over the network, steganography and cryptography has been used from a long time. Steganography[1], a term which was first recorded in the year 1499, is the type of information hiding method[2], that conceals a message or a file into a cover object, such as digital image[3]. Cryptography is the practice and study of techniques for secure communication, so that the third party cannot read the message. Cryptography allows data to be hidden from the third party, whereas steganography is to keep others from thinking that the information even exists.

II. PROPOSED SYSTEM

2.1. Cryptographic Techniques

Cryptography is the science of keeping the transmitted data secure [4]. It provides data encryption for secure communication [5]. There are two basic types of cryptographic algorithms, which are, symmetric key algorithm and public key algorithm. Algorithm which uses same key for encryption and decryption is known as symmetric key algorithm and algorithm which uses different keys for encryption and decryption is known as public-key encryption.

In this system, the encryption process is achieved using triple Data Encryption Standard algorithm. Triple DES algorithm is a symmetric-key block cipher, which applies Data Encryption Standard three times to each data block. Triple DES provides a relatively simple method of increasing the key size of DES to protect against brute force attacks, without requiring a completely new block cipher algorithm. The encryption algorithm using 3DES is:

ciphertext = EK3(DK2(EK1(plaintext)))

i.e., DES encrypts with K1, DES *decrypt* with K2, then

DES encrypt with K3. The decryption algorithm using 3DES

is:

plaintext = DK1(EK2(DK3(ciphertext)))

i.e., decrypt with K3, *encrypt* with K2, and then decrypt with K1.

The standards define three keying options:

- Keying option 1: All three keys are independent.
- Keying option 2: K1 and K2 are independent, and K3 = K1.
- Keying option 3: All three keys are identical, i.e. K1 = K2 = K3.

Keying option 1 is the strongest, with 3 x 56 = 168 independent key bits.

Keying option 2 provides less security, with 2 x 56 = 112 key bits. This option is stronger than simply DES encrypting twice, e.g. with K1 and K2, because it protects against meeting- the-middle attacks.

Keying option 3 is no better than DES, with only 56 key bits. This option provides backward compatibility with DES, because the first and second DES operations simply cancel out. It is no longer recommended by the National Institute of Standards and Technology (NIST) and not supported by ISO/IEC 18033-3.

In general Triple DES with three independent keys (keying option 1) has a key length of 168 bits (three 56-bit DES keys), but due to the meet-in-the-middle attack the effective security it provides is only 112 bits. Keying option 2 reduces the key size to 112 bits. However, this option is susceptible to certain chosen-plaintext or known-plaintext attacks and thus it is designated by NIST to have only 80 bits of security.

2.2. Image Steganography

Steganography is the art of hiding that the communication is even taking place as the original information is buried into the cover digital medium. Different types of carrier formats can be used, but digital images are more popular because of their frequency over the network. Before selecting an image as a cover image, precaution should be taken to check that the image is of good quality. There are three types of steganography techniques

used for image, which are: 1) LSB Techniques; 2) Masking and filtering Techniques; 3) Algorithms and transformation techniques.

In this system, enhanced version of Least Significant Bit method is being used. It is widely used method for embedding message into an image. To understand this method, we shall be clear about the least significant bit. LSB is the bit of lowest value. In the proposed system, we shall be using LSB and also a bit before the LSB, chunking it together to make a linked list containing the message bit and also the address to the next bit chunked together to hold the same.

When using a 24-bit image, a bit of each of red, green, blue channels can be used, since they are each represented by a byte. In other words, one can store three bits in each pixel. Representing a grid for three pixels of 24-bit image:

(00101010 10110100 10101111)

(10001011 01011101 00010100)

(11110010 11010001 00010010)

A number, suppose 180, before being embedded into the above grid using the LSB method has to be converted into the binary form. The binary form of 180 is 10110100. Embedding this into the above grid:

(00101011 10110100 10101111)

(10001011 01011100 00010101)

(11110010 11010000 00010010)

On an average, only half of the pixels in an image are modified using this method. On changing the least significant bit no changes are visible in the image as the intensity of change is very less. One of the disadvantages of LSB method is that it is easily detectable [7]. A slight secure method will be sharing of the key by the sender with the receiver that specifies alteration in certain bits only, making it difficult for the adversary as he would not know which bits to target [8].

III. IMPLEMETATION OF THE PROPOSED SYSTEM

In the proposed system, we shall be making use of the above mentioned techniques for implementation, that is, for encryption and decryption, triple-Data Encryption Standard and for embedding and de-embedding an image, Least Significant Bit method. The proposed system targets to overcome the difficulty faced in the classical method, making it a multi-layered secured system.

3.1. Authentication

First step of this multi-layered secured system is providing the valid username and password for authentication of the sender. Any individual or organization (private, government, military) can make an account, to log into the system. Hence, people having username and password can only send secret message over the network.

3.2. Sender

The sender has to type the message into a text box provided for the message to be typed. 'Encrypt' button has be pressed. On pressing that button the message typed in the text box will be encrypted using the triple- Data Encryption Standard algorithm mentioned above.

The sender then has to load an image into the image box from the saved images. Any image can be selected of good quality. On pressing the 'embed' button, the message is embedded into the cover image in the following manner: the least significant bit and second to the least significant bit, of each channel (red, green, blue) are to be taken together. We will now take the pixel, adjacent pixel and next to the adjacent pixel, that is, three pixels are chunked together to hold the message and the address in coordinate form of the next pixel. It can be represented as follows:

(00101*01* 10110*00* 10101*11*)

(10001*11* 01011*01* 00010*00*)

(11110*01* 11010*01* 00010<u>10</u>)

The italics bits hold the address in coordinate form(x,y). The value for the 'x' coordinate is stored evenly in the 8th bit of each byte of the channel and the value for 'y' coordinate is stored in the 7th bit of each byte. The underlined bits hold the message in both 7th and 8th bit.

Suppose the coordinates of the next pixel holding the message is (0,255). It will be converted into the binary form as: 0 will be 00000000 and 255 will be 11111111. It will be evenly distributed as:

(00101*01* 10110*11* 10101*10*)

(10001*01* 01011*10* 00010*10*)

(11110*01* 11010*01* 00010010)

The underlined bit shall hold the message bit as required.

The start pixel will be used as key and will be sent to the receiver separately. The message will then be transmitted over the network.

3.3. Receiver

On receiving the image, the recipient will be required to login for authentication. The encrypted message from the cover image can then be retrieved using the reverse technology. The message has to be de-embedded after the key has been received. The encrypted message can then be decrypted by the algorithm provided above using triple-DES.

IV. PRECAUTIONS

- The image that the sender is selecting as the cover image should be of good quality.
- The key should be sent separately by the sender.
- Valid username and password has to be provided by the sender.

V. CONCLUSION

We have seen the paradigm shift from batch processing to this era of internet in everything. Hence it has become important to secure communication from being attacked during a secret transmission. The formulation that we have made through this paper may have already been discovered but our implementation is different and involves use of both technologies in a distinct way.

VI. ACKNOWLEDGEMENT

We owe a great debt of gratitude to Dr. Inder Singh, our mentor and guide who helped us to make this project a success. We would also like to thank all our friends and classmates who helped us in the coding.

REFERENCES

[1] R.J. Anderson and F.A.P. Petitcolas, “On the Limits of Steganography”, IEEE Journal of Selected Areas in Communications, Special Issue on Copyright and Privacy Protection, vol. 16(4), pp. 474−481, 1998.

[2] Petitcolas, FAP; Anderson RJ; Kuhn MG (1999). "Information Hiding: A survey" (pdf).*Proceedings of the IEEE (special issue)* 87 (7): 1062– 78. doi:10.1109/5.771065. Retrieved 2008-09-02.

[3] Fridrich, Jessica; M. Goljan and D. Soukal (2004). "Searching for the Stego Key".*Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VI* 5306: 70–82. Retrieved 23 January 2014.

[4] Obaida Mohammad Awad Al-Hazaimeh, (2013) "A New Approach for Complex Encrypting and Decrypting Data" International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.2.

[5] Xinpeng Zhang and Shuozhong Wang, (2005), "Steganography Using MultipleBase Notational System and Human Vision Sensitivity", IEEE signal processing letters, Vol. 12, No. 1.

SYNTHESIS, CHARACTERIZATION AND DEVELOPMENT OF NANOCOMPOSITE

Mintu Mary Mathew [1], Jemimah Carmichael. M [2], Prince Arulraj.G[3],

[1]PG student, [2]Assistant Professor(S.G), School of Civil Engineering,
Karunya University, Coimbatore, Tamilnadu(India)
[3]Dean of Civil Engineering, S.N.S. College of Technology,
Vazhiyampalayam, Coimbatore, Tamilnadu (India)

ABSTRACT

Nano Technology is one of the areas which is gaining prominence in the field of civil engineering. Application of the concepts of nano technology is steadily growing [(1)]. Materials at nano stage results in new materials which can change the entire property of the composites to which nano materials are added. Literature reveals that nano particles enhance the strength and durability of concrete [(3)]. Studies on nano particles added cement paste indicate that stronger and durable concrete can be made by adding particles at nano scale to concrete. At present, many investigations are being carried out to understand the hydration of nano sized cement particles and the use of nano-size ingredients such as alumina [(4)], fly ash and silica particles for production of concrete. During the present study, an attempt has been made to understand the influence of adding two nano materials on the consistency, setting time and strength of cement mortar. Cement was replaced with nano-cement (NC) and nano-flyash (NFA). It is found that the consistency is not affected due to the presence of nano materials. The setting time and the compressive strength are influenced by the presence of nano materials to a greater extent. It is found that addition of nano particles decreases the initial and final setting time of the cement mortar. Also the compressive strength is increased compared to cement mortar without nano materials

Keywords: Nano Technology, Cement Mortar (NCM), Nano-Cement (NC), Nano- Fly Ash (NFA), Consistency, Setting Time, Compressive Strength. .

I INTRODUCTION

Nanotechnology is one of the most active research areas that encompass a number of disciplines including Civil Engineering and construction materials. Currently this technology is being used for the creation of new materials, devices and systems at molecular, nano and micro-level. Nanomaterials show unique physical and chemical properties that can lead to the development of more effective materials than the ones which are currently available. The use of nano-materials can improve the function and properties of many types of elements. Recently, nanotechnology has attracted considerable scientific interest due to the new potential uses of particles in nano scale. The nano-scale particles can result in dramatically improved properties from conventional grain size materials of the same composition.

Application of nano-materials into the production of cement and concrete can lead to significant improvements in the field of Civil engineering since the mechanical strength and life of concrete structures are determined by the micro-structure and by the mass-transfer in nano-scale. Due to the materials very small size, they have some remarkable, and in some cases, novel properties. Significant enhancement of optical, mechanical, electrical, structural and magnetic properties are commonly found with these materials. ***Hasan Biricik et.al.***[1] conducted a study between nano silica, silica fume, and flyash incorporated cement mortars using Fourier transform infrared spectrometer (FTIR), thermogravimeter-differential thermogravimeter (TG-DTG) and scanning electron microscope (SEM), wherein the mechanical strengths of the specimens were determined at early (7^{th} day) and standard (28^{th} day) curing ages**..** The compressive strengths developed in the mortar specimens containing NS particles was found to be considerably higher than those of the corresponding specimens of SF and FA at early and standard ages. Parallel to the increase in the amount of NS from 5 wt% to 10 wt%, the increases in compressive strength at both ages were observed. ***Yilmaz kocak***[2] experimentally determined the mutual influence of fly ash and silica fume on Portland cement. Fly-ash and silicafume slowed down hydration speed, decreased hydration heat and temperature and hence were effective against contraction by increasing the setting time. Properties such as compressive strength, modulus of elasticity, free and restrained shrinkage, measurement of internal relative humidity, isothermal calorimetry, and semi-adiabatic temperature rise of cement replaced with class C flyash was evaluated by ***Igor De la Varga et.al*** [3]. HVFA mixtures with w/cm of 0.30 had higher strength at later ages (28 d, 91 d, and 365 d) compared to the reference mortar**.** ***K. Thomas Paul et.al***[4] characterized nano structured fly ash for its particle size by using particle size analyzer, specific surface area with the help of BET surface area apparatus, structure by X-ray diffraction studies and FTIR, SEM and TEM was used to study particle aggregation and shape of the particles which revealed that the surface of the nano structured fly ash is more uneven and rough and shape is irregular, as compared to fresh fly ash which are mostly spherical in shape. ***Maile Aiu***[5] conducted an experiment focusing on synthesizing the components of Portland cement type I using nano-particles and comparing their properties with that of commercial cement. Scanning electron microscopy (SEM) and X-ray diffraction (XRD) tests were conducted to study the morphology and structure of synthesized tricalcium silicate (C3S) components. The results showed conglomerated Nano-particles with crystalline structures containing quantities of tri- and di- calcium silicate compounds as well as copper oxide. Hydration testswere also performed and the results show that the Nano-cement has a more rapid hydration rate than Portland cement. ***V.R.Rath et.al***[6] reviewed the efforts, current status, and effect of various nano materials on properties of cement mortar and concrete due to its large surface area concluding that nanoparticle addition improves compressive, flexural strength, hydration characteristics and reduced porosity and water absorption. Nano materials can also reduce the cement content in concrete while maintaining same strength characteristics, which will lead into the production of 'greener' concrete. ***Jemimah Carmichael et.al*** [7] investigated the effect of nano-flyash on the strength of concrete. It was found that the 28 day strength of 10% nano-flyash was higher than normal cement concrete.

II EXPERIMENTAL PROGRAMME

In this experimental study cement mortar cubes with and without nano particles was used. A combination of nanofly ash and nanocement with various percentage was used as a replacement of cement. Normal consistency,

setting time and compressive strength tests were done. Scanning Electron Microscope (SEM) was used to study the morphology of the nano fly ash and nano cement.

III MATERIAL

The materials used are the ordinary Portland cement of grade 5 conforming to IS 10269:1982, fine aggregate of specific gravity 2.67 belonging to zone II, nano flyash and nano cement. For making the composite mortar, ordinary Portland cement and class F fly ash was scaled down to nano level with the help of high intensity ball milling. High impact collisions are used to reduce microcrystalline materials down to nano crystalline structure without chemical change. The Scanning Electron Microscope (SEM) was used to determine the particle size of the nano materials. The SEM images of cement, nano-cement, flyash and nano-flyash are shown in figure 1,2,3 and 4 respectively.

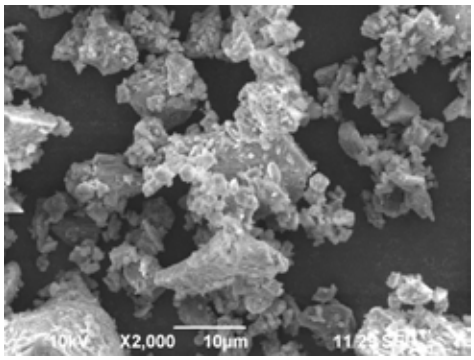


Figure 1: SEM picture of cement

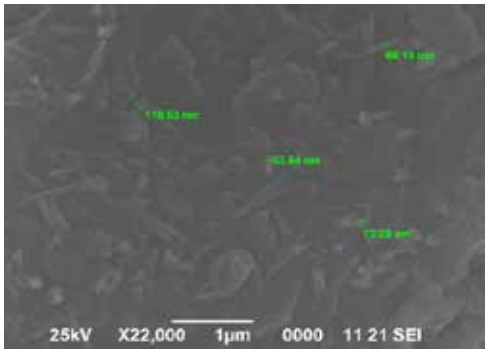


Figure 2: SEM picture of nano cement

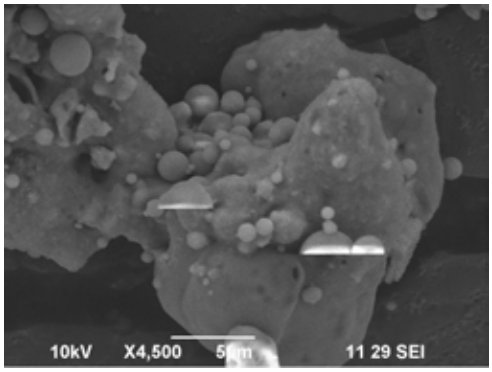


Figure 3: SEM picture of fly ash

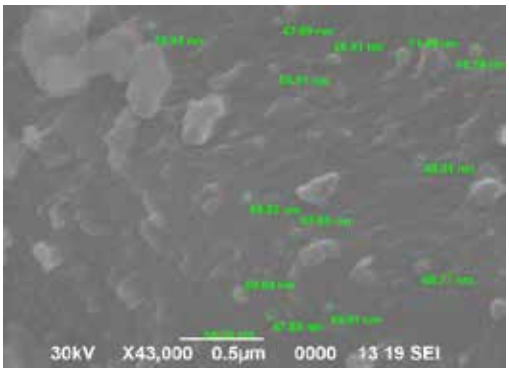


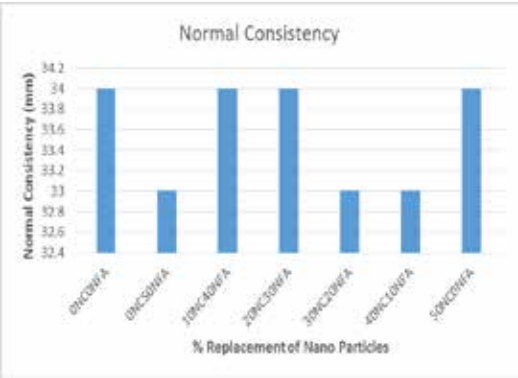
Figure 4: SEM picture of nano flyash

IV RESULTS AND DISCUSSION

The normal consistency, initial setting time, final setting time and compressive strength results are shown in table 1

Table 1: Normal Consistency, Initial Setting Time, Final Setting Time and Compressive Strength

% Replacement of Nano Particles		Normal Consistency (mm)	Setting Time(mins)		Compressive Strength		
Nanocement	Nanoflyash		initial	final	3 days	7days	21 days
0	0	34	70	510	52.5	67	73
0	50%	33	155	920	51.5	64.86	81.75
10%	40%	34	110	730	52.76	65.42	80.02
20%	30%	34	85	640	52.9	68.75	81.78
30%	20%	33	70	530	58.98	73.12	84.64
40%	10%	33	55	370	63.84	74	86.22
50%	0	34	30	245	68	75.53	88



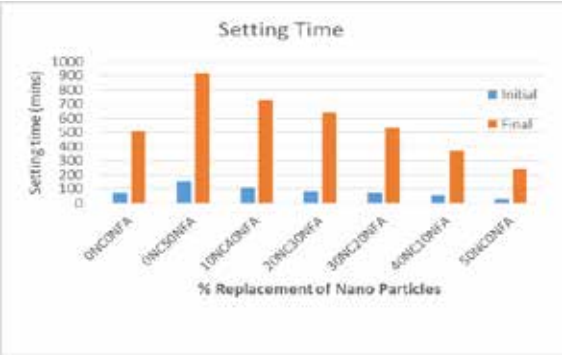


Figure 5:Chart depicting normal consistency **Figure 6: Chart depicting initial and final setting time**

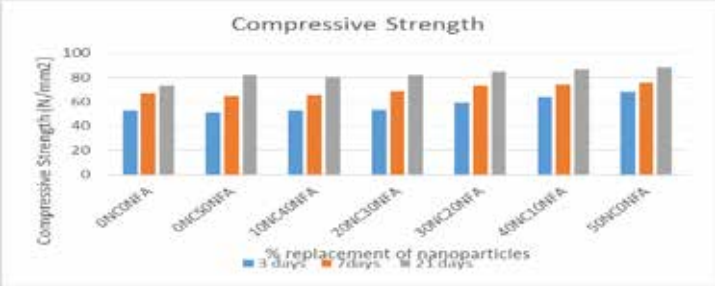


Figure 7: Chart depicting compressive strength

4.1 Discussion of normal consistency, initial setting time and final setting time.

1. The percentage of normal consistency for 0% replacement of Nano-cement and 50% replacement of Nano-flyash was found to decrease by 2.94 % whereas initial setting time and final setting time of cement was found to increase by 121. 4 % and 80.9 % than Normal Cement respectively.

2. The percentage of normal consistency for 10% replacement of Nano-cement and 40% replacement of Nano-flyash was found to be the same whereas initial setting time and final setting time was found to increase by 57.1% and 43.1% that of Normal Cement respectively.

3. The percentage of normal consistency for 20% replacement of Nano-cement and 30% replacement of Nano-flyash was found to be the same whereas initial setting time and final setting time of cement was found to increase by 21. 4 % and 25.4 % that of Normal Cement respectively.

4. The percentage of normal consistency for 30% replacement of Nano-cement and 20% replacement of Nano-flyash was found to decrease by 2.94 % whereas final setting time was found to increase by 3.9% that of Normal Cement respectively. The initial setting time was the same.

5. The percentage of normal consistency of cement for 40% replacement of Nano-cement and 10% replacement of Nano-flyash was found to decrease by 2.94 % whereas the initial setting and final setting time was found to decrease by 21.94 % and 27.4 % than Normal Cement respectively.

6. The percentage of normal consistency of cement for 50% replacement of Nano-cement and 0% replacement of Nano-flyash was found to be the same whereas the initial setting and final setting time was found to decrease by 57.1% and 51.9% that of Normal Cement respectively.

4.2 Compressive Strength

4.2.1 3 days compressive strength

1. The percentage increase of compressive strength of cube for 0% replacement of Nano-cement and 50% replacement of Nano-flyash was found to decrease by 0.961% than Normal Cement mortar for 3 days.
2. The percentage increase of compressive strength of cube for 10% replacement of Nano-cement and 40% replacement of Nano-flyash was found to increase by 1.46% than Normal Cement mortar for 3 days.
3. The percentage increase of compressive strength of cube for 20% replacement of Nano-cement and 30% replacement of Nano-flyash was found to increase by 1.73% than Normal Cement mortar for 3 days.
4. The percentage increase of compressive strength of cube for 30% replacement of Nano-cement and 20% replacement of Nano-flyash was found to increase by 13.42% than Normal Cement mortar for 3 days.

5. The percentage increase of compressive strength of cube for 40% replacement of Nano-cement and 10% replacement of Nano-flyash was found to increase by 22.769% than Normal Cement mortar for 3 days.
6. The percentage increase of compressive strength of cube for 50% replacement of Nano-cement and 0% replacement was found to increase by 0.769% than Normal Cement mortar for 3 days.

4.2.2 7 days compressive strength

1. The percentage increase of compressive strength of cube for 0% replacement of Nano-cement and 50% replacement of Nano-flyash was found to decrease by 3.194% than Normal Cement mortar for 7 days.
2. The percentage increase of compressive strength of cube for 10% replacement of Nano-cement and 40% replacement of Nano-flyash was found to decrease by 2.35% than Normal Cement mortar for 7 days.
3. The percentage increase of compressive strength of cube for 20% replacement of Nano-cement and 30% replacement of Nano-flyash was found to increase by 2.61% than Normal Cement mortar for 7 days.
4. The percentage increase of compressive strength of cube for 30% replacement of Nano-cement and 20% replacement of Nano-flyash was found to increase by 9.13% than Normal Cement mortar for 7 days.
5. The percentage increase of compressive strength of cube for 40% replacement of Nano-cement and 10% replacement of Nano-flyash was found to increase by 10.44% than Normal Cement mortar for 7 days.
6. The percentage increase of compressive strength of cube for 50% replacement of Nano-cement and 0% replacement was found to increase by 12.73% than Normal Cement mortar for 7 days.

4.2.3 21 days compressive strength

1. The percentage increase of compressive strength of cube for 0% replacement of Nano-cement and 50% replacement of Nano-flyash was found to increase by 11.194% than Normal Cement mortar for 21 days.
2. The percentage increase of compressive strength of cube for 10% replacement of Nano-cement and 40% replacement of Nano-flyash was found to increase by 9.61% than Normal Cement mortar for 21 days.
3. The percentage increase of compressive strength of cube for 20% replacement of Nano-cement and 30% replacement of Nano-flyash was found to increase by 12.61% than Normal Cement mortar for 21 days.
4. The percentage increase of compressive strength of cube for 30% replacement of Nano-cement and 20% replacement of Nano-flyash was found to increase by 15.13% than Normal Cement mortar for 21 days.
5. The percentage increase of compressive strength of cube for 40% replacement of Nano-cement and 10% replacement of Nano-flyash was found to increase by 18.44% than Normal Cement mortar for 21 days.

6. The percentage increase of compressive strength of cube for 50% replacement of Nano-cement and 0% replacement was found to increase by 20.73% than Normal Cement mortar for 21 days.

V CONCLUSION

An experimental investigation has been carried at to find out at the effect of replacing cement with nano-cement and nano-flyash on the strength, consistency, initial and final setting times of cement mortar. It was found that replacement of nano materials had insignificant effect on the consistency of cement paste. The initial and final setting times of cement mortar containing nano-cement was found to decrease with addition of nano-flyash increase in the replacement percentage. The strength varies between 1-20% compared to cement mortar without nano particles.

REFERENCES

1. Hasan Biricika, Nihal Sarier. Comparative Study of the Characteristics of Nano Silica–, Silica Fume– and Fly Ash–Incorporated Cement Mortars. Materials Research. 2014; 17(3): 570-582.
2. Yilmaz kocak. A study on the effect of fly ash and silica fume substituted cement paste and mortars.Scientific Research and Essays Vol. 5(9), pp. 990-998, 4 May, 2010.
3. Igor De la Varga, Javier Castro, Dale Bentz, Jason Weiss. Application of internal curing for mixtures containing high volumes of fly ash. Cement & Concrete Composites 34 (2012) 1001–1008.
4. K. Thomas Paul,S. K. Satpathy ,I. Manna, K. K. Chakraborty, G. B. Nando.Preparation and Characterization of Nano structured Materials from Fly Ash: A Waste from Thermal Power Stations, by High Energy Ball Milling. Nanoscale Res Lett (2007) 2:397–404.
5. Maile Aiu. The Chemistry and Physics of Nano-Cement NSF-REU,University of Delaware August 11, 2006.
6. V.R.Rathi, Dr.C.D.Modhera, An overview on the Influence of NanoMaterials on Properties of Concrete journal on International Journal of Innovative Research in Science,Engineering and Technology,Vol. 3, Issue 2, February 2014
7. Jemimah Carmichael, Prince Arulraj.G, Effect of NanoFlyash on Strength of Concrete, International Journal of Civil and Structural Engineering Volume 2, No 2, 2011