ISSN No:-2321-1776

International Journal in IT & Engineering

Volume No. 13

Issue No. 2

May - August - 2025

ENRICHED PUBLICATIONS PVT. LTD

S-9, IInd FLOOR, MLU POCKET,
MANISH ABHINAV PLAZA-II, ABOVE FEDERAL BANK,
PLOT NO-5, SECTOR-5, DWARKA, NEW DELHI, INDIA-110075,
PHONE: - + (91)-(11)-47026006

ISSN No:-2321-1776

International Journal in IT & Engineering

Aims and Scope

International Journal in IT and Engineering is a double blind peer reviewed, refereed monthly international journal that provides rapid publication of articles in all areas of Information Technology (IT) and Engineering through research and its relevant appropriation and inferential application. The journal hopes to accelerate development and governance in both developed and developing countries. The maximum length of intended articles for publication in the journal is 5000 words. A short abstract of 150-250 words with 4-5 key words should precede the introduction. We appreciate innovative and evolutionary contemplation over popular management ethics, differing from the humdrum bulk of monotonous content. The journal welcomes publications of high quality papers, book reviews and reports.

ISSN No:-2321-1776

ISSN No:-2321-1776

International Journal in IT & Engineering

(Volume No. 13, Issue No. 2, May - August 2025)

Contents

High-Voltage Switch Using Series-Connected IGBTs With Simple Auxiliary Circuit

*Gaurav Trivedi

ABSTRACT

For high-voltage applications, the series operation of devices is necessary to handle high voltage with limited voltage rating devices. In the case of self turn-off devices, however, the series operation of devices is very difficult. The main problem associated with series-connected devices is how to guarantee the voltage balance among the devices both at the static and the dynamic transient states. This paper presents a simple and reliable voltage-balancing circuit for the series operation of devices to overcome the disadvantages of solutions presented so far, such as complex control or circuit, low reliability, and limited number of devices to be connected. The proposed balancing circuit realizes a complete Voltage balancing at both static and dynamic states and allows series operation of an almost unlimited number of devices. The operation principle and analysis are presented and tested on 16 series connected insulated gate bipolar transistors to handle 20-kV/400-A switching.

1. INTRODUCTION:

POWER semiconductor device technology has been continually developed far to get higher voltage/current ratings, lower conduction/switching losses, and easier drive. As a result, the performance of devices has been much improved and new devices such as insulated gate bipolar transistors (IGBTs), integrated gate commutated thyristors (IGCTs), etc. have been presented. Among various power devices, the IGBT is becoming the best candidate from low- to highpower applications because it has advantages which include high voltage/current rating, fast switching, and easy drive capabilities. The recently presented IGBT has a 6.5-kV/3-kA rating. In recent years, the demand for high-voltage conversion applications, such as high-voltage inverters, high-voltage pulse generators, high-voltage dc transmission systems (HVDC),flexible ac transmission systems (FACTS), etc., have been increased. Since the voltage rating of these applications usually ranges several tens of kilovolts, the power processing cannot be accomplished with any single device. To do this, several devices should be connected in series and operated simultaneously. For the self turn-off device, however, the series operation of devices is very difficult because of tolerances in device characteristic and/or the mismatching of the driving circuit. Recently, the series operation technique for power semiconductor devices, especially IGBTs, has been introduced and discussed in [1]–[4]. One of the most important aspects in series operation of devices is to equalize the static and dynamic balancing of the voltage. The static voltage balancing can be simply achieved by connecting small balancing resistors in parallel with each device. The dynamic voltage balancing during the switching transient is much more difficult to achieve. Two dynamic voltage-balancing techniques are available: load-side balancing and gate— side balancing. The load-side balancing employs a snubber circuit and/or a clamp circuit. The snubber circuit and/or clamp circuit provide dynamic voltage balancing by limiting the device voltage rising rate dv/dt and/or clamping the peak voltage. This technique, however, cannot be used for high-power applications since much loss is involved in the snubber and clamp circuits which is proportional to the switching frequency. To solve this problem, an active gate control technique has been presented in the last few years, which does not degrade switching transient characteristic

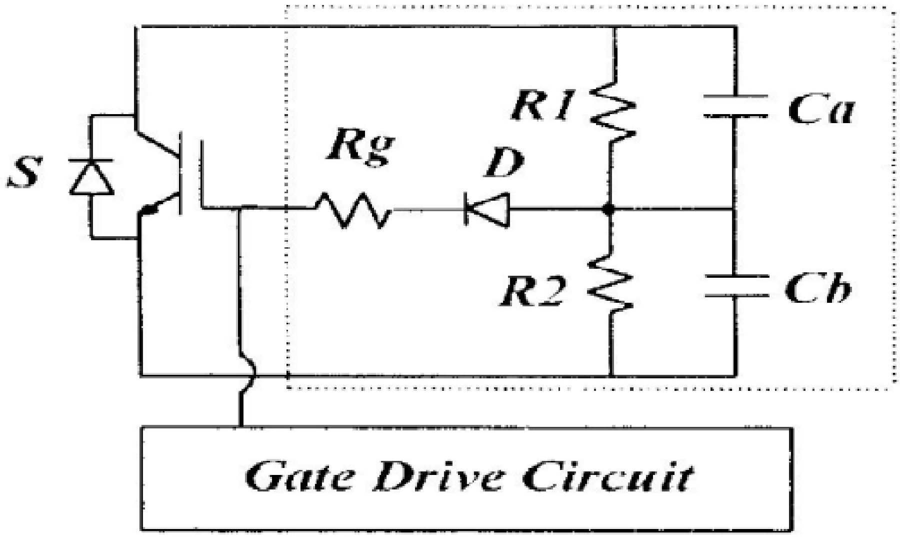


Fig.1:Proposed auxiliary circuit for series operation of devices (inside dashed line)

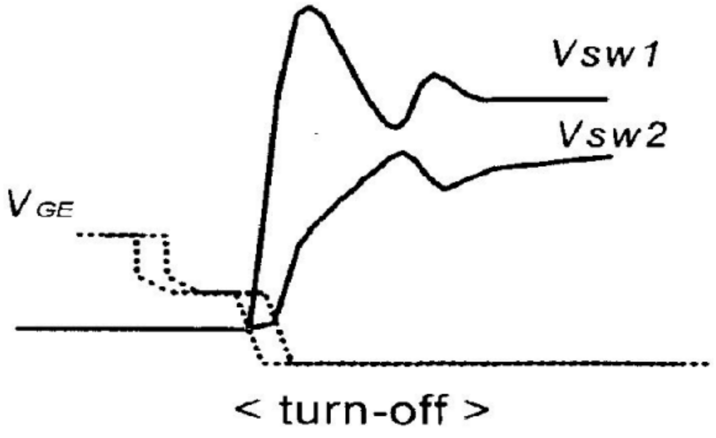
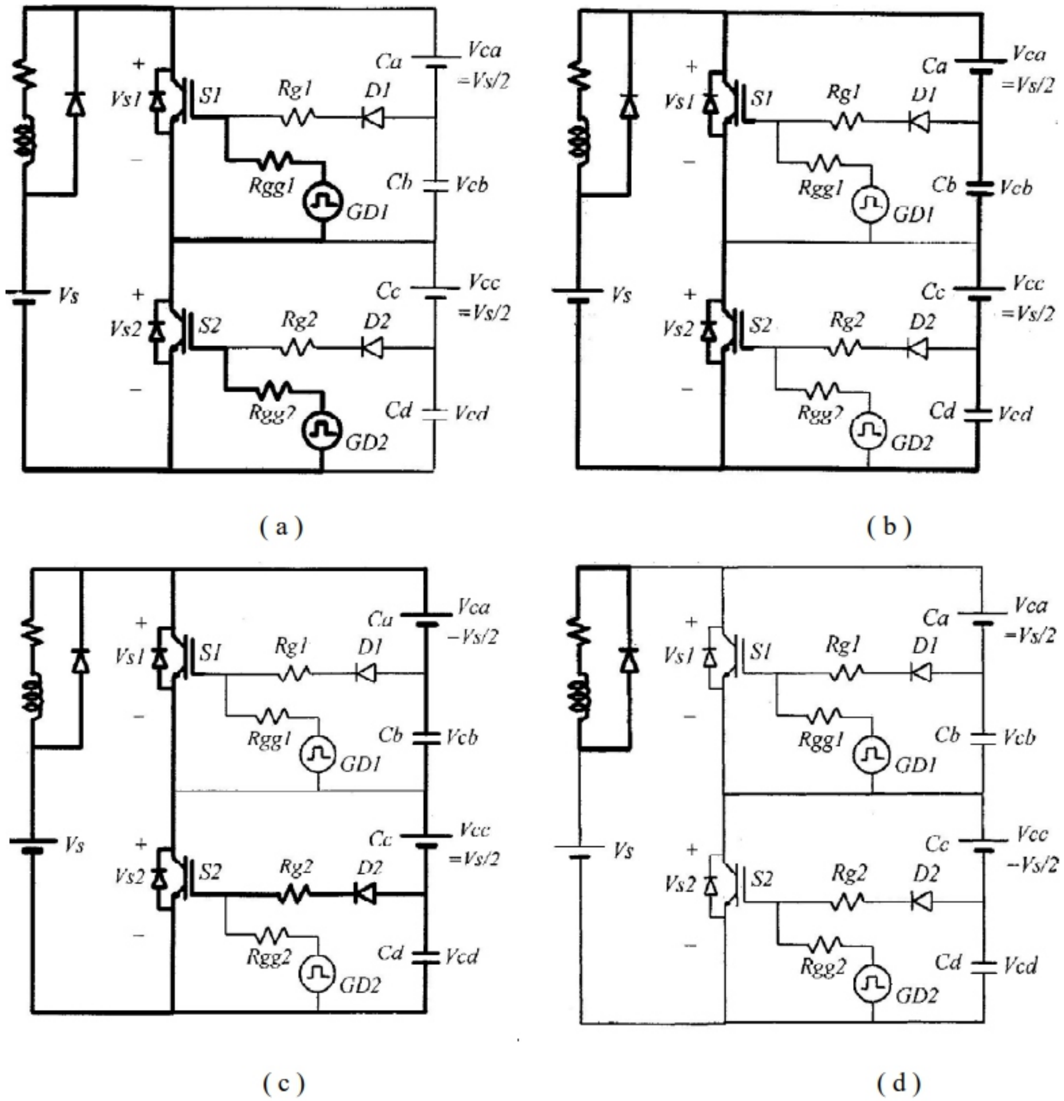


Fig. 2. Typical voltage waveforms of IGBTs during a switching transient

Each gate drive circuit should be actively controlled so that all device voltages are increased or decreased at the same rate. To do this, each voltage of the devices has to be sensed and fed back to the active gate control circuit, resulting in a complex drive circuit, low reliability, and increased switching loss [6]. Therefore, this technique may not be an economical and practical solution. In this paper, a new simple voltage-balancing circuit is presented for both the static and dynamic voltage balancing as shown in Fig. 1. This circuit, which consists of two small capacitors, three small resistors, and one small diode, is attached to each device and provides an active gate control effect. Additional snubber circuits or a special complex gate drive are not required. In addition, the proposed scheme gives a minor effect on the switching time so that it has much lower switching loss compared to the conventional active gate control technique. Therefore, the proposed technique is simple, low in cost, with high reliability and an unlimited number of devices to be connected in series.



(a)

(b)

(c)

(d)

The operation principle and analysis are presented and tested on 16 series-connected IGBTs to handle 20-kV/400-A switching. The experimental results with and without the proposed auxiliary circuit are compared.

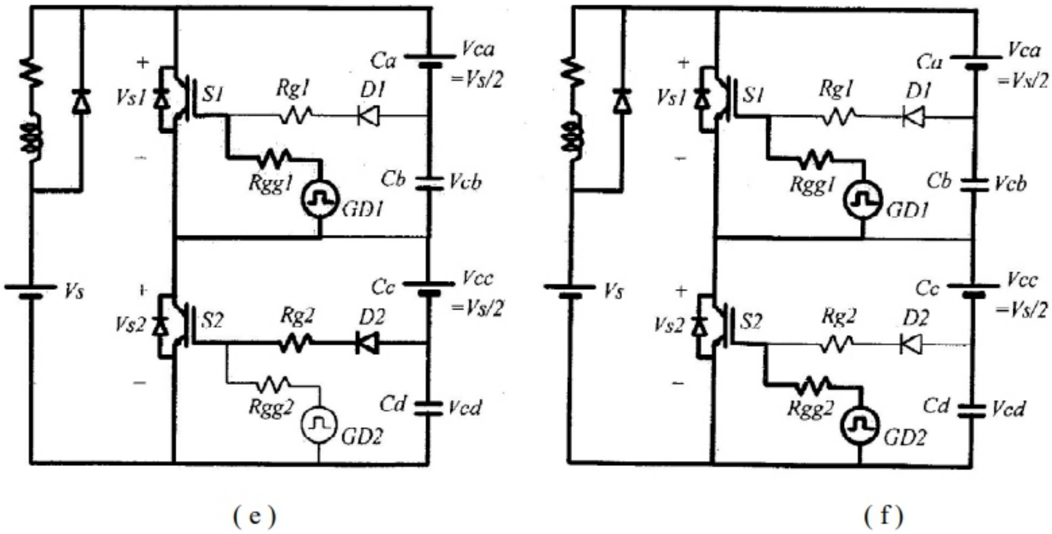


Fig. 3. Operational modes. (a) Mode 1. (b) Mode 2. (c) Mode 3. (d) Mode 4. (e) Mode 5. (f) Mode 6.

II. SERIES OPERATION OF DEVICES:

The series operation of self turn-off devices is not easy because of the following reasons:

- unequal device switching characteristics;
- unequal device leakage current;
- unequal stray inductance in the series circuit;
- unequal gate drive delay.

Fig. 2 shows the typical waveforms of two series-connected IGBTs. After the gate signal goes off, the device voltages are increased in different dv/dt rates and reach unbalanced peak and steady state value. The difference of dv/dt and the peak mainly depend on the difference of device switching characteristics, stray inductance, and gate drive delay time, while the difference of steady-state voltage depends on the difference of the leakage current and the output capacitance of each device. If the peak voltage of one device goes higher than the device rating, that device will be broken and the overall system will fail. Therefore, the voltage-balancing technique is necessary to balance the device voltage, even when all bad conditions are encountered.A simple resistive voltage-dividing circuit guarantees the voltage balance of devices in the static conditions. The dynamic balancing of devices, however, is much more difficult to achieve. Using a snubber circuit for dynamic voltage balancing is not practical, since much loss should be involved . The active gate control technique achieves dynamic voltage by device voltage feedback . This, however, has a reliability problem and additional switching loss. The proposed technique achieves dynamic voltage balance with a simple auxiliary circuit, which is a simple, low-cost, and reliable technique.

III. OPERATION PRINCIPLE:

The proposed voltage-sharing circuit consists of two capacitors, three resistors, and one diode, and all these components have a very small rating compared to those of the main switching devices R1, R2 are voltage-sharing resistors, obviously for static voltage balancing. The other components are for the dynamic voltage balancing. The operation of the static voltage balancing is obvious and, thus, omitted here. The operational mode diagrams and waveforms of the proposed circuit are shown in Figs. 3 and 4. To simplify operation of the dynamic voltage balancing, voltage-dividing resistors are omitted and two series-connected IGBTs are considered. It is assumed that Ca and Cc are charged with Vs/2and are much bigger (about ten times) than Cb and Cd . Therefore, Ca and Cc are considered here as constant voltage sources, Vs/2 and the switch S2 is turned on earlier and turned off later than S1 for any reason. GD1 and GD2 are basic gate drive signals. The proposed circuit has six operating modes within each switching period.Mode 1: S1 and S2 are turned on, the gate voltages of GD1 and GD2 are high. Because the voltage of Ca and Cc is Vs/2 , the voltages of Cb and Cd are charged with – Vs/2 . Diodes Da and Db block the reverse voltage of Vcb and Vcd .

Mode 2: The gate drivers of S1 and S2 go off but the gate driver of S2 is off a little bit earlier. The switch current is decreasing gradually and, at the same time, the switch voltage of S2 starts increasing first and that of S1 follows Cb and Cd are charged up from – Vs/2. The voltage of S2 is increased more rapidly than that of S1 and reaches the steady-state value Vs/2 first. The voltage of Cd also reaches zero first. Mode 3: Since the voltage of S1 is still lower than Vs/2, both voltages of S1 and S2 are continually increased, and then the voltage of S2 is increased to more than Vs/2. At the same time, the voltage of Cd goes positive, and this voltage is applied to the gate terminal of S2 through D2 and Rg2 resulting in slightly turning on of S2. Therefore, the rising voltage of S2 is decreased sharply, and then the voltage of Cd is also decreased trying to turn off of S2 again. At the end of this mode, the voltage of S1 reaches Vs/2 and then all switches are well balanced.

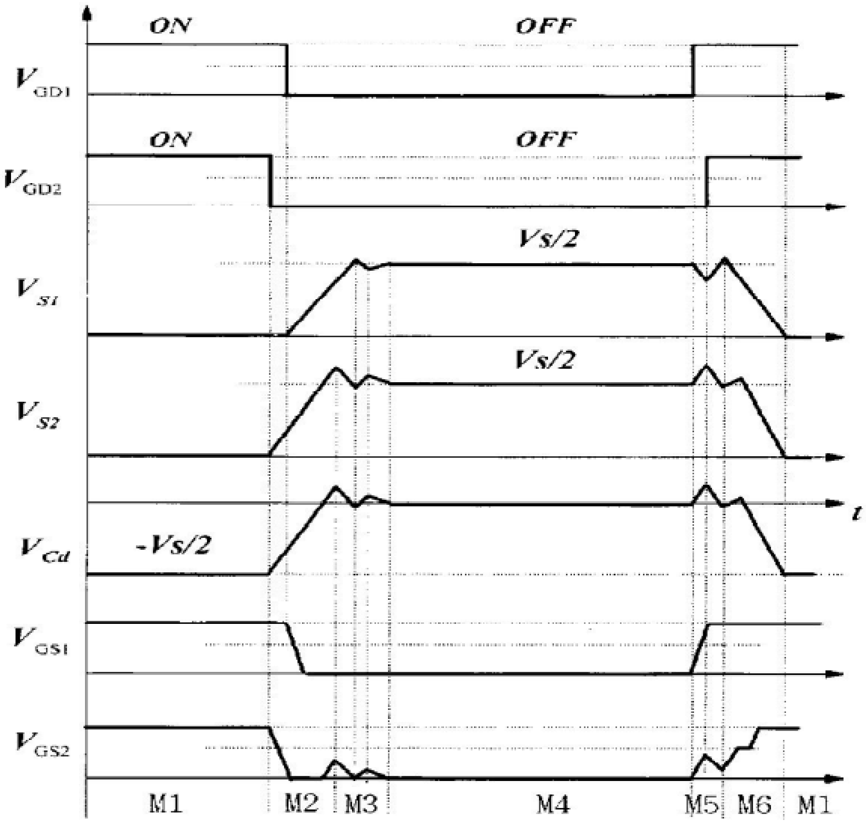


Fig. 4. Operational waveform

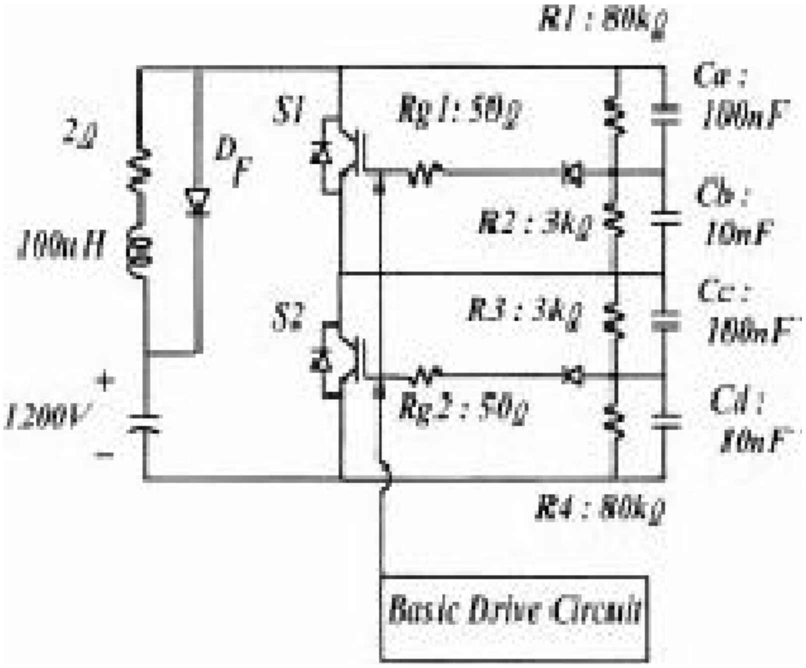
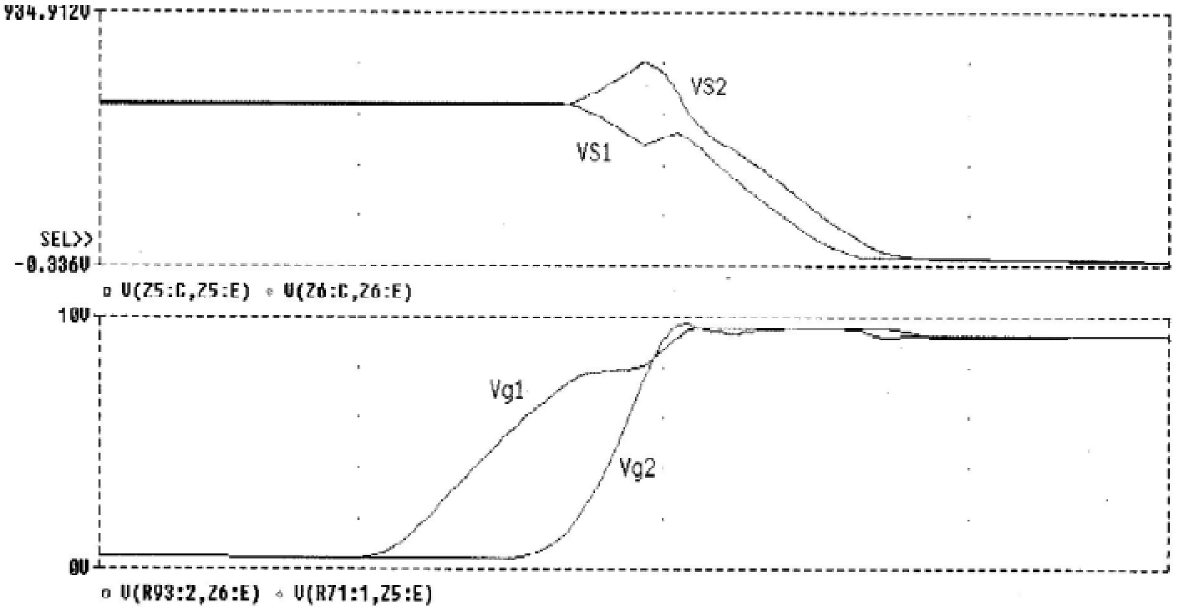


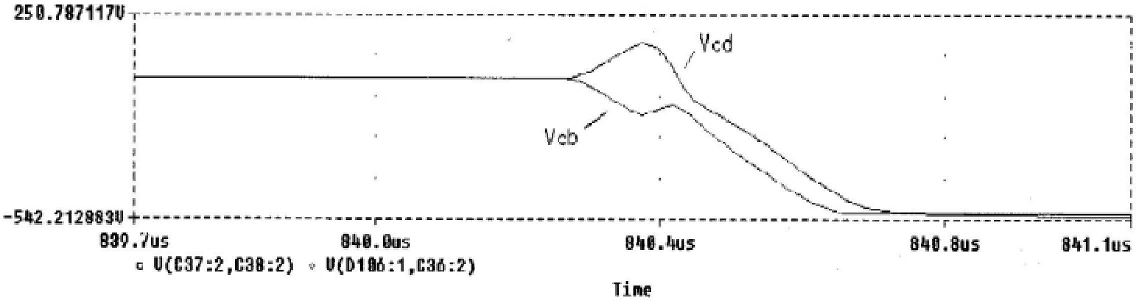
Fig. 5. Simulation circuit

Mode 4: The switch S1 and S2 are turned off with the balanced voltage Vs/2. Load current freewheels through the diode.Mode 5: Now, the gate driver of S1 is on first and that of S2 follows a little bit later. When S1 starts turning on, the overvoltage is applied to switch S2. Then, the voltage of Cd is increased to positive as that of Mode 3, which turns on S2 slightly and reduces the voltage of S2. Both voltages of S1 and S2 reach zero at the end of this mode.Mode 6: Both switches are turned on completely. The Cb and Cd are charged to – Vs/2, again. This is the end of one switching cycle. The dynamic voltage balancing is achieved at any condition of layouts, devices, and gate drivers.

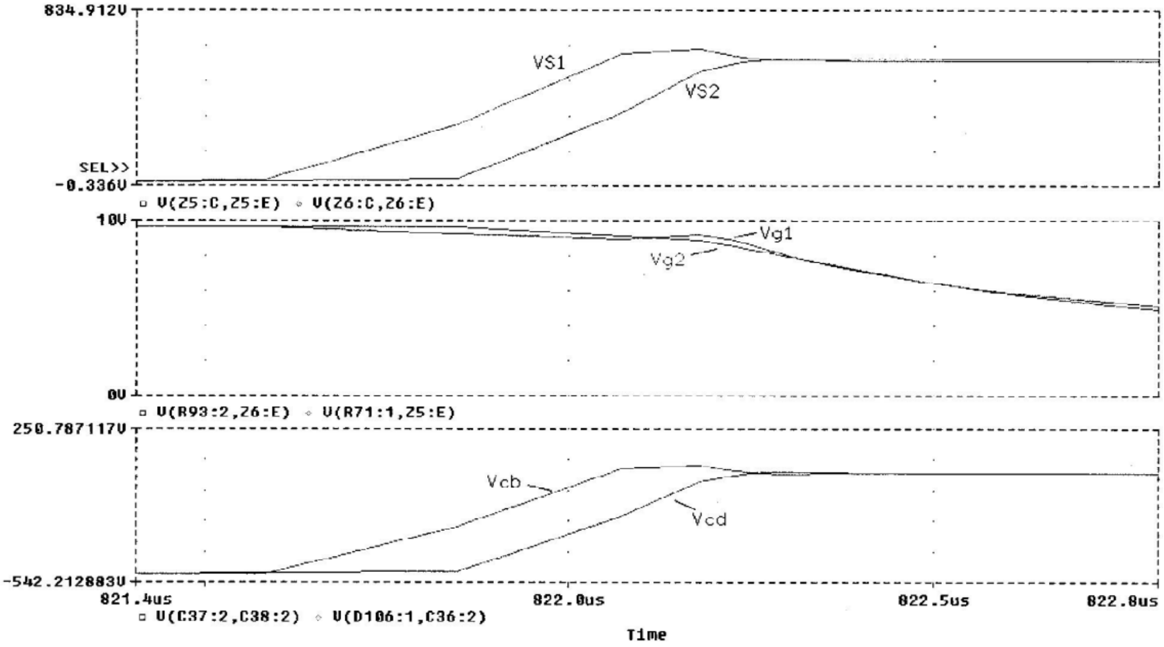
IV. FEATURES OF THE PROPOSED CONVERTER: A. Automatic Voltage Balancing

The static voltage balancing is simply achieved by the voltage-dividing resistors, as in the other balancing techniques[1]–[5]. The dynamic voltage balancing is automatically achieved by the action of the simple auxiliary circuit. The switch voltage fed back through - - (–D2–), which slightly turns on the switch again, limiting the switch voltage with the normal voltage. This action is just like the active voltage clamping. Therefore, the auxiliary circuit provides the dynamic voltage balancing at any condition, including unequal device switching characteristics, unequal stray inductance, unequal gate drive delay time, etc. Neither additional control circuit nor special gate drive is necessary. There is no additional switching loss, either. The number of devices to be connected is not limited




250.787117V
-542.212883V
Vcd
Vcb
839.7us
840.0us
840.4us
840.8us
841.1us
V(C37:2,C38:2)
V(D106:1,C36:2)
Time

(a)


834.912V
-0.336V
SEL>>
VS1
VS2
V(Z5:C,Z5:E)
V(Z6:C,Z6:E)
10V
0V
Vg1
Vg2
V(R93:2,Z6:E)
V(R71:1,Z5:E)
250.787117V
-542.212883V
Vcb
Vcd
821.4us
822.0us
822.5us
822.8us
V(C37:2,C38:2)
V(D106:1,C36:2)
Time

(b)

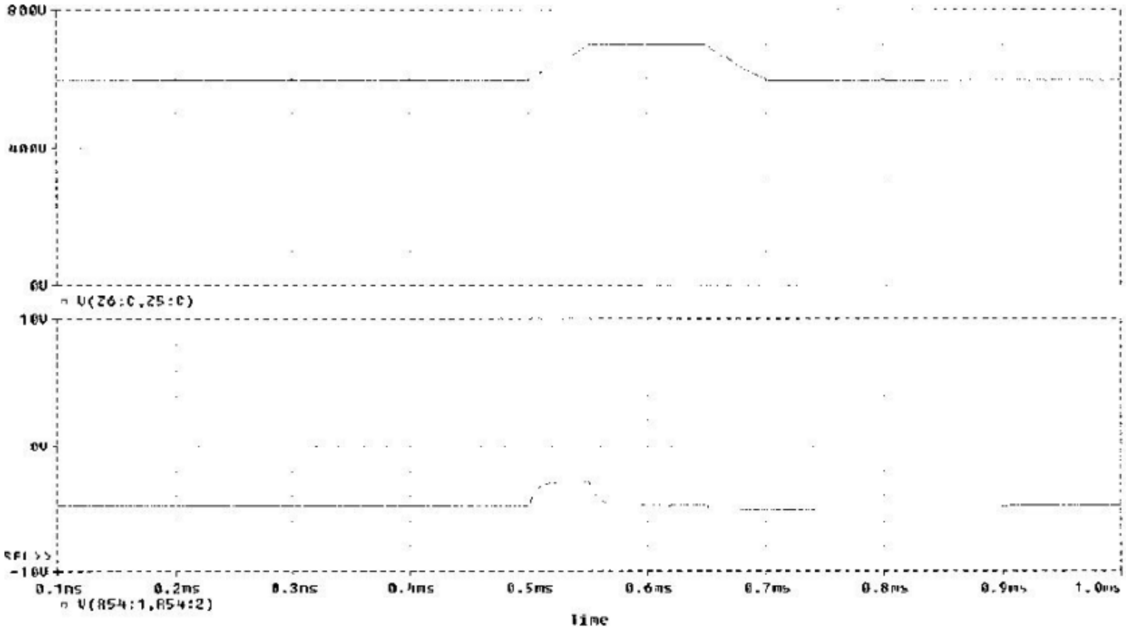

800V
400V
0V
V(Z6:C,Z5:C)
10V
0V
SEL>>
-10V
0.1ns
0.2ms
0.3ns
0.4ms
0.5ms
0.6ms
0.7ms
0.8ms
0.9ms
1.0ms
V(R54:1,R54:2)
Time

Fig. 7. Simulated waveforms when the dc-link voltage is abruptly changed(top: dc-link voltage; bottom: gate voltage).

B. Simple and Low Loss:

The auxiliary circuit consists of all passive components and all small power ratings compared to the main devices. The loss involved with the auxiliary circuit is almost negligible. Therefore, the proposed technique is a very efficient, reliable, and economic solution.

V. DESIGN CONSIDERATIONS:

A. Decision of Capacitors

To detect the overvoltage, the voltage of capacitor Ca (Cc) has to be almost constant during a short switching period. Therefore, Ca (Cc) should be much bigger than capacitor Cb (Cd). The empirical range of Ca (Cc) is about 100 nF. The Cb (Cd) is charged and discharged repeatedly at every switching period. In order to get proper operation and to reduce loss, Cb (Cd) should be much smaller, although it depends on the switching frequency. At several kilohertz switching frequency range, 10% of Ca (Cc) is enough for Cb (Cd).

B. Design of Resistors

If the voltage-dividing resistors are too small, the static balancing is well achieved, but the loss is increased. If the resistor are too big, the static balancing will fail. Therefore, the voltage-dividing resistors should be designed by considering the leakage current of devices and loss. The gate resistor Rg1 (Rg2) should also be designed carefully. The device voltage is fed back to the gate through Ca (Cc) and Rg1 (Rg2), which provides the dynamic voltage balancing. The feedback effect is not so sensitive with Rg1 (Rg2) , but the dynamic voltage balancing is not properly achieved if Rg1 (Rg2) is too high or too low. (If Rg1 (Rg2) is too high, the feedback effect is reduced and so is the voltage balancing or vice versa.) The empirical range of Rg1 (Rg2) is about ten times that of Rgg1 (Rgg2).

C. DC-Link Voltage Variation

Ca (Cc) is constantly charged with the voltage of Vs/2 and Cb (Cd) is charged with – Vs/2 and discharged to zero according to the switching state. If the dc-link voltage is increased, the voltage of Ca (Cc) should be increased to allow proper operation. The main charging path of Ca and Cb is the Rg and the gate-emitter junction during the turn-off state of switches. If the dc-link voltage is increased abruptly, the voltage of Cb (Cd) can be positive and switches S1 and S2 can be turned on without the turn-on gate signal, resulting in undesirable operation. Therefore, the dc-link voltage should not be changed abruptly. This effect, however, can normally be ignored since the dc-link capacitance is usually very high and the voltage is changed very slowly.

VI. SIMULATION RESULTS

To verify the operation of the proposed circuit, an example circuit, two series-connected IGBTs, is designed as shown in Fig. 5 and simulated using PSPICE. To give an intentional difference in switching conditions, the gating signal of S2 is delayed 0.2 us. Fig. 6 shows the simulated waveforms during turn-on and turn-off transients. The feedback through auxiliary circuits is shown in Fig. 6. During turn-on transient, the gating signal of S1 is applied first and the voltage of S1 starts decreasing, as shown in Fig. 6(a). This means that the voltage of S2 is increasing over the steady-state voltage Vs/2. This overvoltage charges Cd and applies a positive voltage to the gate of S2 and, thus, S2 is turned on slightly, even though the real gating signal of S2 is not yet applied. Therefore, the dynamic voltage balancing is achieved during the turn-on transient. During the turn-off transient, S1 is turned off first and the voltage of S1 is increased and reaches Vs/2 first. If Vs1 is increased over the steady-state voltage Vs/2, a positive voltage is applied to the gate of S1 and the voltage of S1 is decreased and stays at Vs/2 until the voltage of S2 reaches Vs/2, as shown in Fig. 6(b). Therefore, the dynamic voltage balancing is also achieved at the turn-off transient.

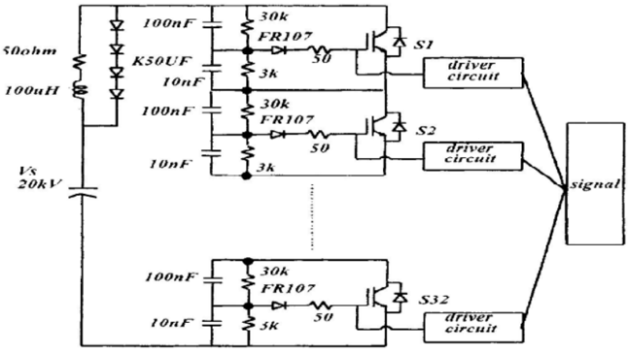


Fig. 8. Experimental circuit diagram for series operation of 16 IGBTs.

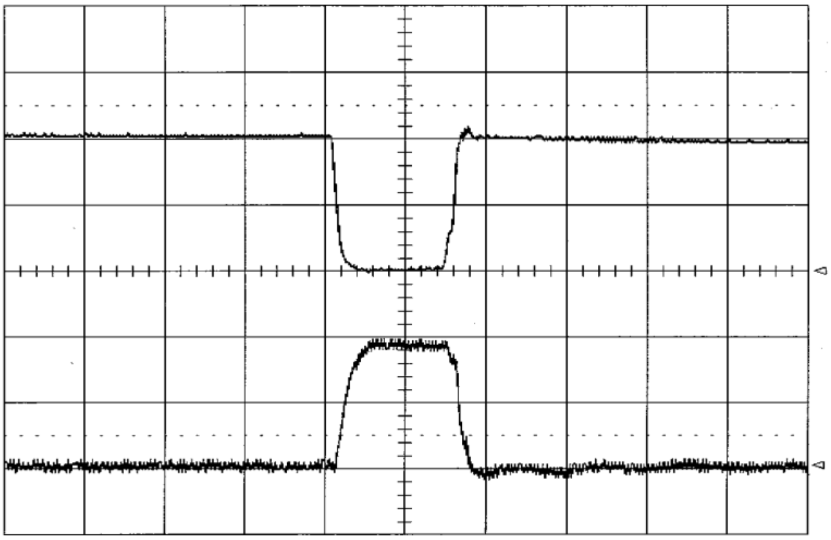
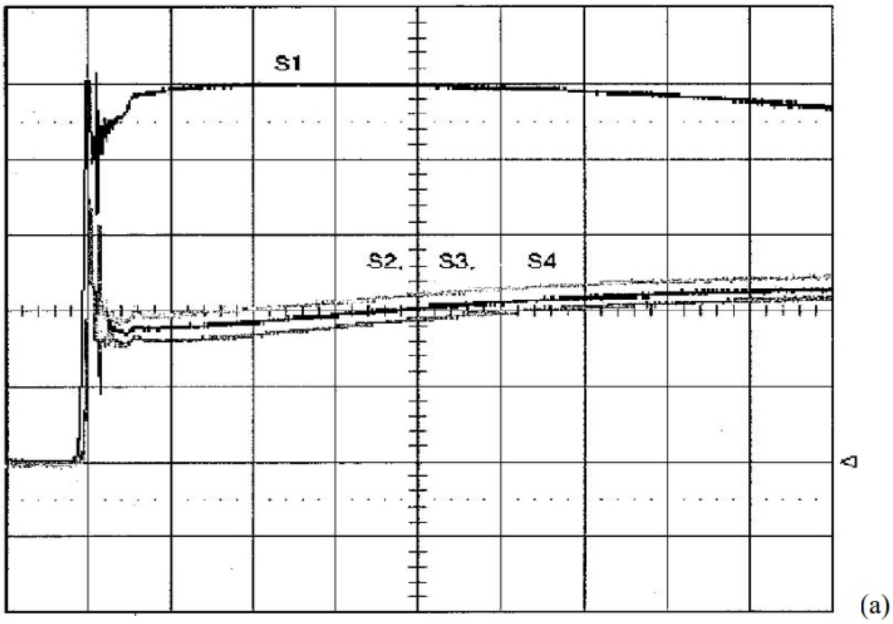


Fig. 9. Voltage and current waveforms of series-connected switches. Top:voltage (10 kV/div); bottom: current (200 A/div). Time (5 s/div).

Fig. 7 shows the simulated waveforms when the dc-link voltage is abruptly changed to see the effect of dc-link voltage variation in the turn-off steady state. With a 100-V rise of dc-link voltage in 50 s, the gate voltage is a little increased but remains under the threshold voltage. Therefore, the unwanted turn-on effect of IGBTs does not occurr, unless the dc-link voltage is not changed too abruptly.



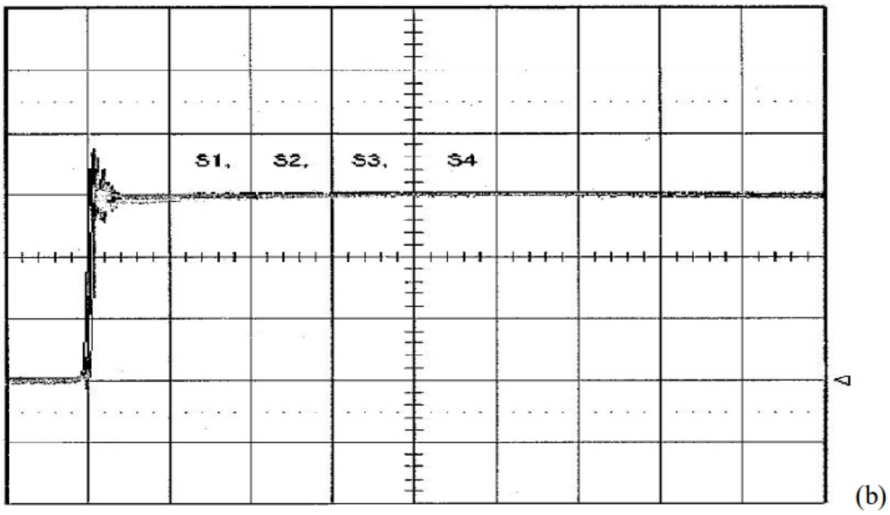


Fig. 10. Voltage waveforms of switches during turn-off transient. (a) Withoutauxiliary circuit. (b)With auxiliary circuit.Voltage (200 V/div). Time (5 s/div).

VII. EXPERIMENTAL RESULTS

To verify the operation of the proposed circuit, a 20-kV 400-A single-pole switching circuit has been built and tested. Fig. 8 shows the experimental circuit diagram with the parts numbers of the components used. Sixteen IGBT modules (1200 V/400 A, SKM400GB124D from Semikron) are series connected with the proposed auxiliary circuit. As a loadR = 50ohms, and L= 100µH are used. All gate drivers have the same characteristics except those of S1. S1 is turned on a little bit later and turned off a little bit earlier than the others to give an intentional difference in switching conditions.

Fig. 9 shows the voltage and current waveforms of the switches connected in series. It can be seen that the switching waveforms are clean. just like the waveforms of a single-switch circuit, thanks to the voltage-balancing function of the proposed auxiliary circuit. Fig. 10 shows the voltage waveforms of four interesting switches during the turn-off transient period with and without the auxiliary circuit, and Fig. 11 shows the extended waveforms of Fig. 10. As shown in Figs. 10(a) and 11(a), there exists a big imbalance among the switch voltages since the auxiliary circuits are not included. The voltage of S1 is increased much higher than the others since S1 is turned off early. In addition, the other voltages of the switches are not the same, either due to small differences of characteristics and stray inductances among devices. The transient voltages of switches when the auxiliary circuits are included are almost the same, even though S1 is turned off early, thanks to the balancing action of the auxiliary circuit. The dynamic voltage balancing is done well. Fig. 12 shows the voltage waveforms of switches during the turn-on transient. When the auxiliary circuits are not included, there exists a high voltage peak across S1 since S1 is turned on later. When the auxiliary circuits are included, however, there is no voltage peak, as shown in Fig. 12(b). The voltage imbalance of switches is less than 15% during the turnoff transient and less than 5% during the turn-on transient. The dynamic voltage balancing is performed well for both turn-on and turn-off transients since 20% of voltage imbalance is usually acceptable. Fig. 13 is a photograph of the IGBT stack with gate drivers.

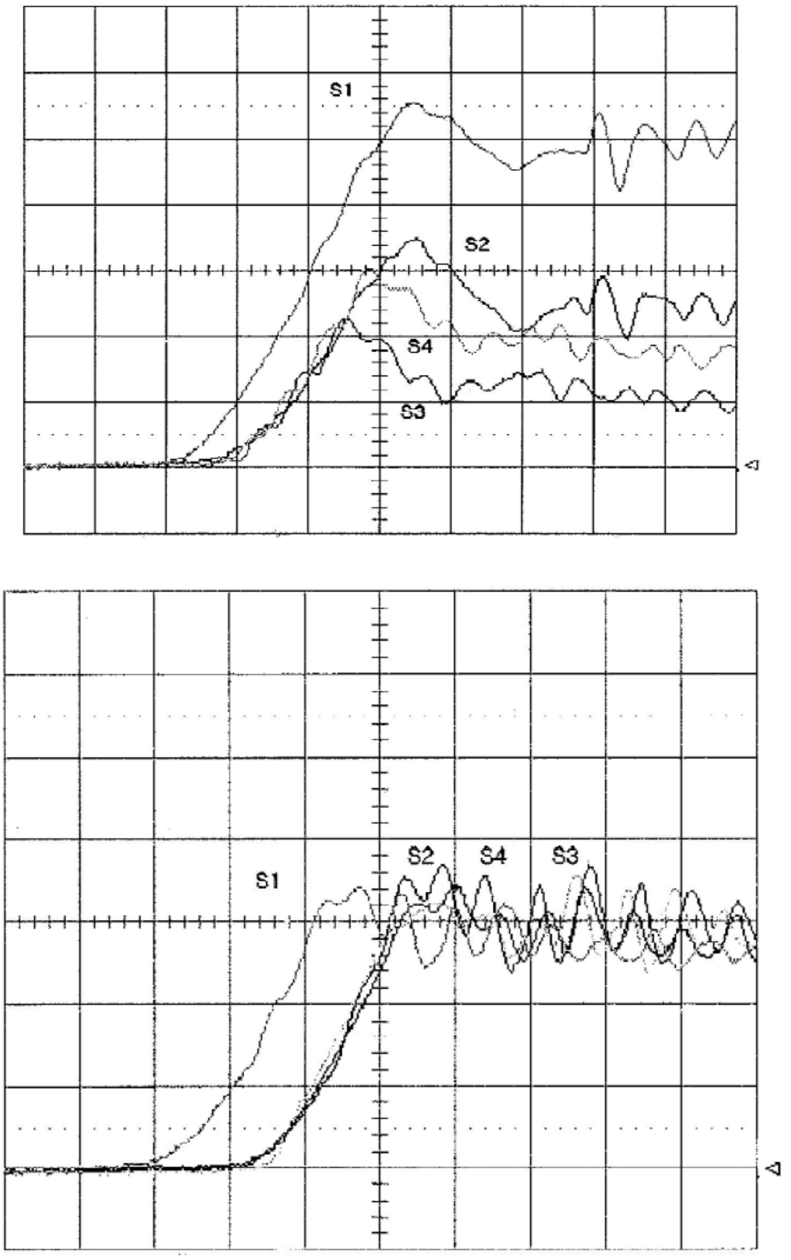


Fig. 11. Extendedwaveforms of Fig. 10. (a)Without auxiliary circuit. (b)With auxiliary circuit. Voltage (200 V/div). Time (0.2 s/div).

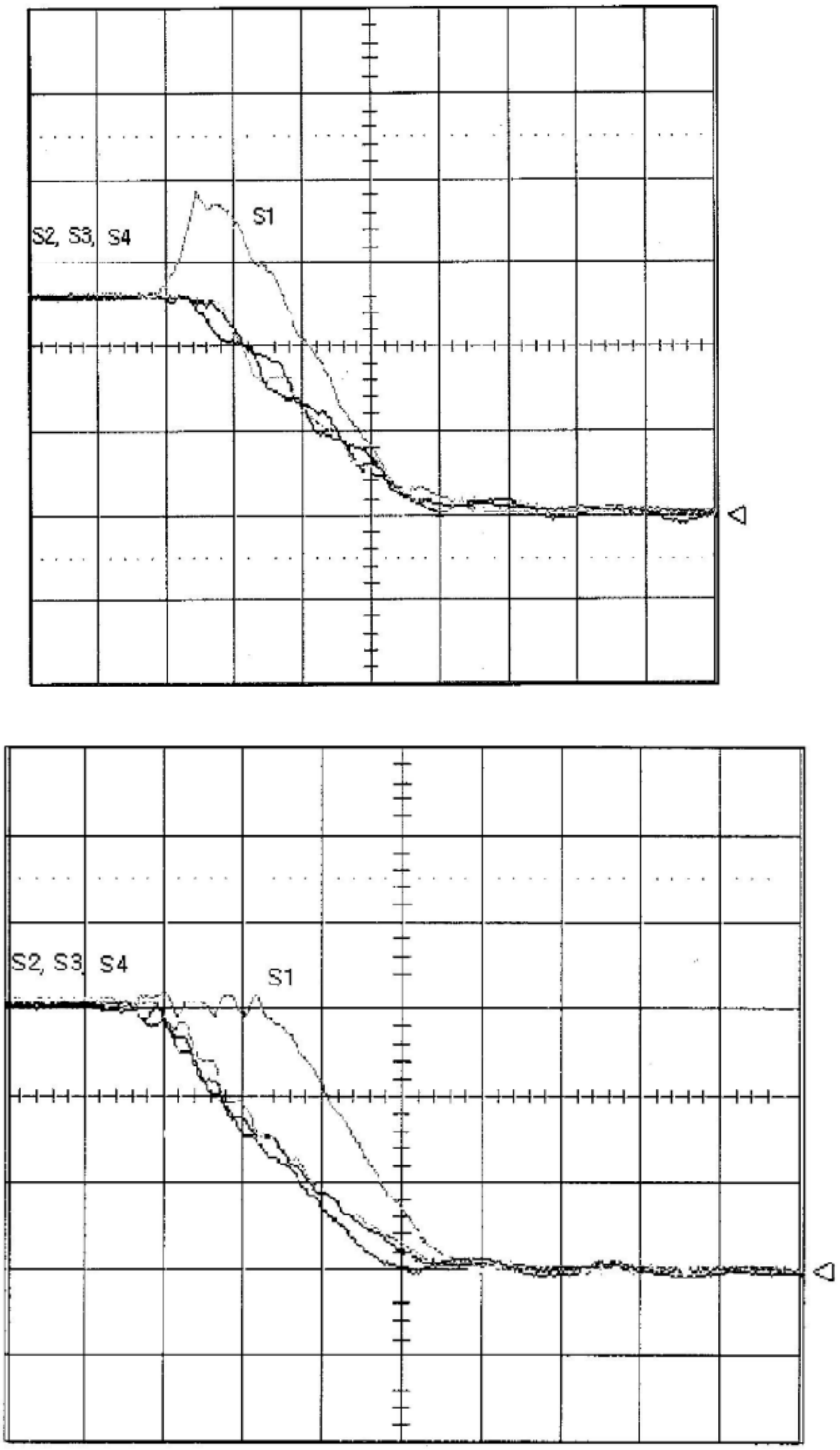


Fig. 12. Voltage waveforms of switches during turn-on transient. (a) Withoutauxiliary circuit. (b)With auxiliary circuit. Voltage (200 V/div). Time (0.2µs/div).

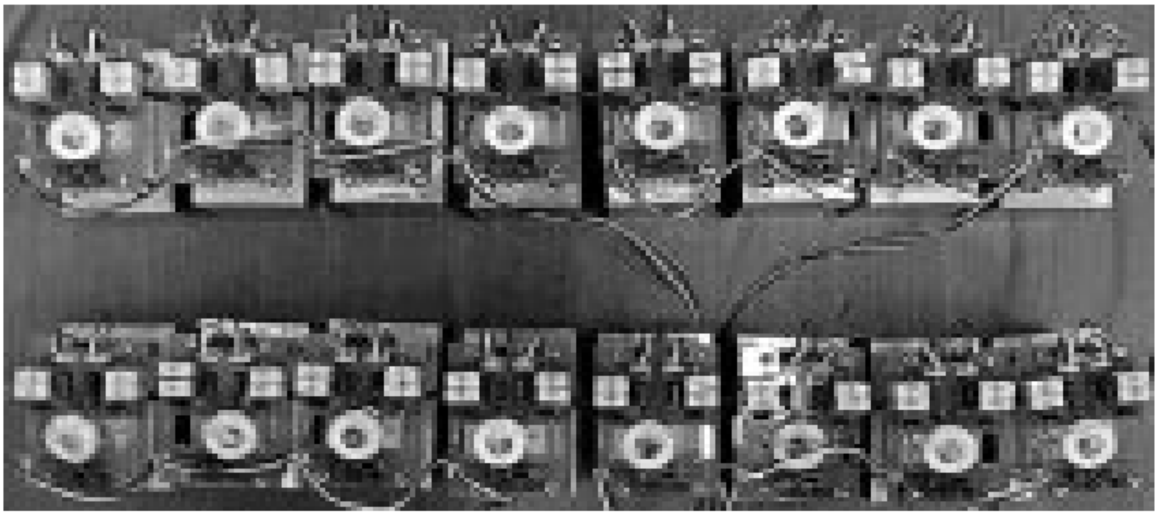


Fig. 13. Photograph of the series-stacked IGBTs with gate drivers.

VIII. CONCLUSION

A novel technique for series operation of IGBTs was presented. The operation, analysis, features, and design considerations were illustrated and verified by the experimental results on a 20-kV/400-A prototype with 16 series-connected IGBTs. It has been shown that the dynamic voltage balancing as well as the static balancing are well achieved with the proposed auxiliary circuit. The proposed technique has many distinctive advantages over those previously presented, as follows:

- simple and low cost;
- high reliability;
- extendibility (unlimited number);
- no additional loss.

These advantages make the proposed technique very promising for high-voltage high-power applications.

PERFORMANCE ANALYSIS IN COMPUTER AIDED DETECTION OF BREAST CANCER BY MAMMOGRAPHY

*R.Bhanumathi
**G.R.Suresh

ABSTRACT

Breast cancer is one of the frequent and leading causes of mortality among woman, especially in developed countries. Early detection and treatment of breast cancer are the most effective method for detecting breast cancer at the early stage. Computer-aided-detection (CAD) system can plays a vital-role in the early detection of breast cancer and can reduce the death rate among women with breast cancer. This paper aims to provide an overview of recent advances in the development of CAD systems and related techniques. Primarily we begin with a detailed introduction of some basic concepts related to breast cancer detection, then focus on the key CAD techniques developed recently for breast cancer, including comparative analysis on detection of masses, calcification, architectural distortion, and bilateral asymmetry in mammograms.

Keywords: Breast cancer, Microcalcification, Computer- aided detection, Mammography.

1. INTRODUCTION:

In recent years breast cancer was found to be the most recurrent form of cancer in women. The use of mammography as a screening tool for the detection of early breast cancer in otherwise healthy women without symptoms continues to be debated. Critic point out that a large number of women need to be screened to locate cancer, two-thirds of the decrease in cancer deaths is due to mammography screening. There is evidence which shows that early diagnosis and treatment of breast cancer can significantly increase the chance of survival for patients [1]–[4]. The earlier the cancer is detected, better the chances that a proper treatment can be arranged. At present, there are no effective ways to prevent breast cancer, because its origin remains unidentified. However, efficient identification of breast cancer in its early stages can give a woman a better chance of full improvement. Therefore, early detection of breast cancer can play an important role in reducing the associated morbidity and death rates.

Computer-aided detection is a system which is specifically planned to spot the abnormalities in mammograms such as calcification, masses, architectural distortion and bilateral asymmetry and aid the radiologist in detecting apprehensive areas on the mammograms. For research scientists, there are more than a few interesting research topics in cancer detection and diagnosis system, such as high-efficiency, high-accuracy lesion detection algorithms, including the detection of masses, calcification, architectural distortion, and bilateral asymmetry in mammograms. This paper deals with the basic concepts related to breast cancer detection and focuses on CAD techniques that are developed recently for breast cancer. As a result, comparison of comparative analysis of masses, calcification, architectural distortion, bilateral asymmetry in mammograms is done. This paper is organized as follows. Section II, presents the related works undergone in CAD systems for breast cancer, including many newly developed algorithms for detection of masses, calcification, architectural distortion and bilateral asymmetry in mammograms. Section III, describes the experimental results and section IV concludes the paper.

2. RELATED WORKS

Even though many techniques have been put forth so far, the growth of new algorithms for Computer-aided-detection of breast cancer is still an active research field, mainly in regard to the detection of slight abnormalities in mammograms [20]. In this section, different techniques for the detection of masses, calcification, architectural distortion, bilateral asymmetry in mammograms is reviewed.

2.1. Microcalcification MC Clusters in Mammograms

By analyzing a mammogram, pathologists could detect the presence of microcalcification in ones breast. Microcalcifications are tiny granule-like deposits of calcium as shown in Fig (1). The occurrence of clustered microcalcification in X ray mammograms is an important display for the detection of breast cancer, particularly for individual microcalcification with diameters of about 0.7 mm and with an average diameter of 0.3mm [5]. Radiologists describe a cluster of microcalcification as the occurrence of three or more visible microcalcification within a square centimetre region of the mammogram [5]. The detection of clustered microcalcification in mammograms has been of great interest to many researchers [6]–[15]. MC detection methods could be broadly separated into four categories: 1) basic image enhancement methods; 2) stochastic modeling methods; 3) multiscale decomposition methods; and 4) machine learning methods.

Wavelet transform is basically a filtering technique that represents images hierarchically on the basis of scale or resolution. Nakayama et al [18] proposed a computerized scheme for detecting early-stage microcalcification clusters in mammograms. It developed a novel filter bank based on enhancement of NC, enhancement of NLC, sub images can be used to reconstruct the original image. It was shown to have potential to detect microcalcification clusters with a clinically acceptable sensitivity and low false positives.

Liyang et al. [19] investigated the use of SVM, KFD, RVM, and committee machines for classification of clustered MCs in digital mammograms. These different classifier models were trained using supervised learning to classify whether a cluster of microcalcification is benign or malignant, based on quantitative image features extracted from the microcalcification.

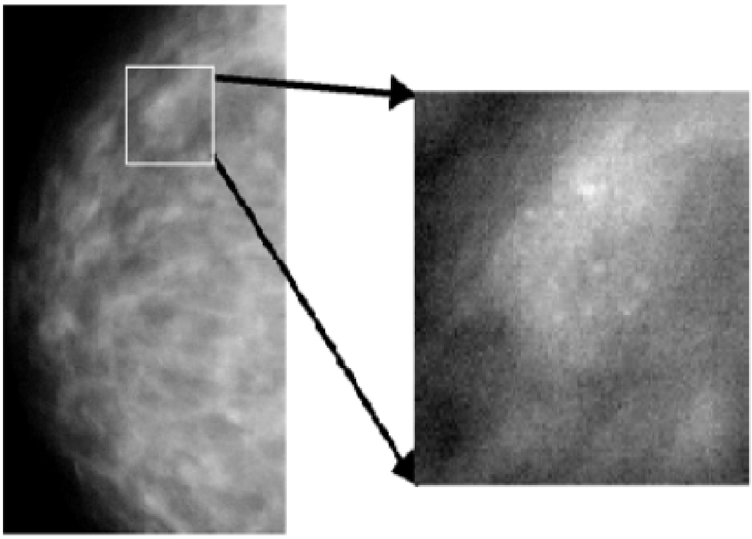


Fig. 1. Left: a CC view mammogram; right: expanded view showing clustered Mcs. MCs is small granule-like deposits of calcium, and appear as bright spots in a mammogram

2.2. Masses in Mammograms

A mass is defined as a space-occupying lesion seen in more than one projection [21]. A mass is regularly characterized by its shape and margin [20], [22]. In general, a mass with a normal shape has a higher probability of being benign, whereas a mass with an unequal shape has a advanced probability of being malignant as shown in Fig (2). In the pixel-based approaches, features are extracted for each pixel and classified as suspicious or normal [20]. The subsequent approach for mass detection is region-based [20]. In the region-based approach, ROIs are segmented, and then, features are extracted from each region, which are then used to classify the regions as suspicious or not suspicious.

Lubomir et al.[23] proposed a hybrid unsupervised and a supervised model to improve classification performance. The classes were separated into two type, individual containing only malignant masses and the supplementary containing a mix of malignant and benign masses. The masses from the malignant classes are classified by ART2 and the masses from the varied classes were input to a supervised linear discriminate classifier (LDA).

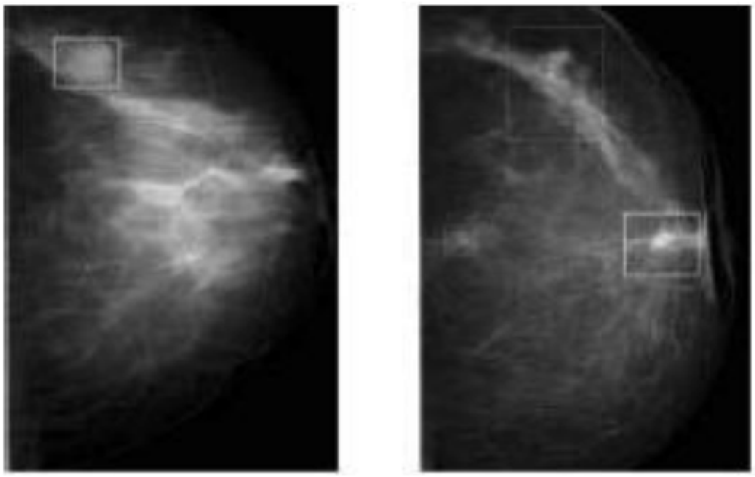


Fig. 2. A Sample Mammographic Image from Our Data Set

2.3. Architectural Distortion in Mammograms

The normal architecture (of the breast) is distorted with no definite mass visible. This includes speculations radiating from a point and focal retraction at the edge of the parenchyma. Architectural distortion also is an associated finding as shown in Fig (3). Architectural distortion is the third most general mammographic sign of nonpalpable breast cancer [25], [26] [27], [28]. But due to its subtlety and changeable presentation, it is often missed during screening.

Sujoy et al. [29] proposed the problem of categorizing a mammographic region-of-interest (ROI) as a two class classification problem as AD or non-AD [29]. The two-layer architecture first collects low-level rotation-invariant textural features at different scales and then learns latent textural primitives from the collected features by GMM.

Rangaraj et al. [30] proposed methods for the detection of architectural distortion in prior mammographic images of interval-cancer cases. The methods are based upon the analysis of spicularity and angular dispersion caused by architectural distortion. Novel measures of spicularity and angular dispersion are proposed for the characterization and detection of architectural distortion using the mammographic image, Gabor magnitude response and Gabor angle response and coherence.

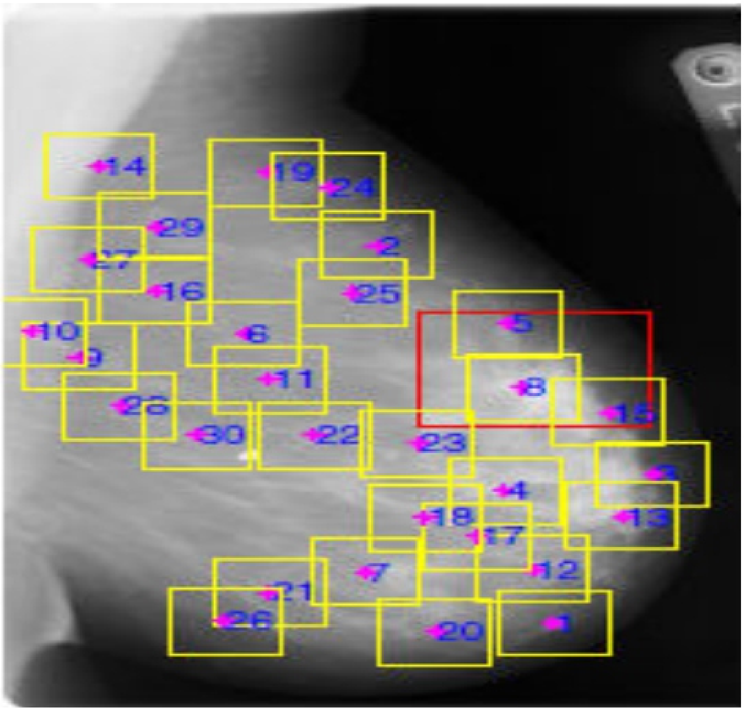


Fig. 3. A prior mammogram of an interval-cancer case with architectural distortion

2.4. Bilateral Asymmetry in Mammograms

Asymmetry between the left and right mammograms of a specified subject is a main sign used by radiologists to diagnose breast cancer [30]. The BI-RADS [21], [25], [31], [32]. Description of asymmetry indicates the occurrence of a greater density of breast tissue not including a distinct mass, in one breast as compare to the corresponding area in the other breast. Examination of asymmetry can give clues about the early signs of breast cancer, such as increasing densities, parenchymal distortion, and tiny asymmetric dense regions as shown in Fig (4).

Ferrari et al. [33] proposed a new scheme based upon a bank of self-similar Gabor functions and the Karhunen–Loève (KL) transform to analyze directional components of images [19]. The method is applied to detect global signs of asymmetry in the fibro-glandular discs of the left and right mammograms of a given subject. Jelena et al. [34] proposed a method for bilateral asymmetry detection in which the left and right breasts were aligned using the B-spline interpolation. After the breast alignment the differential analysis was performed. The difference between the breasts was calculated using simple subtraction technique.

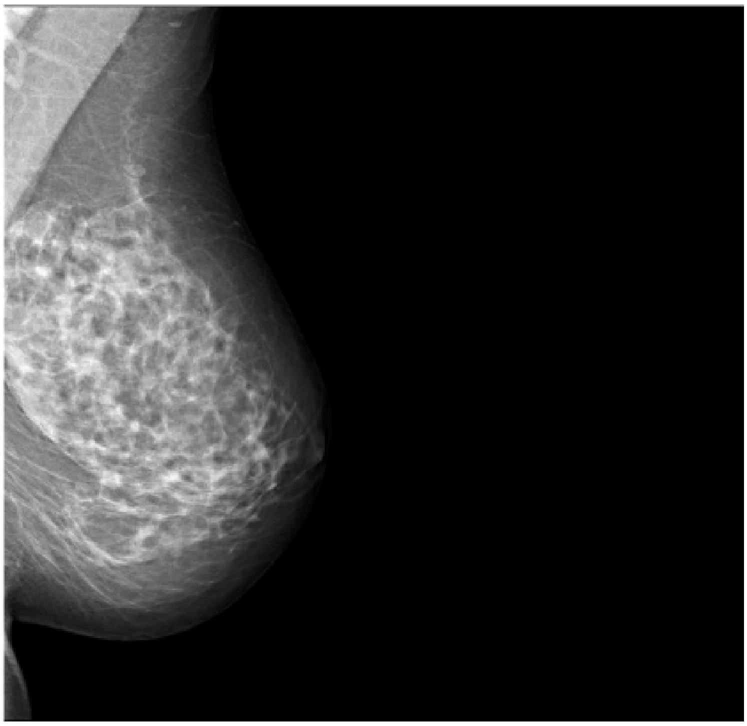


Fig. 4. Bilateral Asymmetry

3. Experimental results and Discussion

3.1. Comparative analysis based on sensitivity

Table 1 displays the Performance of Sensitivity of all the four types of CAD systems namely microcalcification, masses, architectural distortion and bilateral asymmetry. The sensitivity works best in case of both microcalcification and masses and poor in case of architectural distortion and bilateral asymmetry. In fig 5 shows the graphical representation of sensitivity performance in types of CAD system.

Table 1. Performance of Sensitivity in different CAD system

Types of CAD Systems	Sensitivity
Microcalcification	93.7
Masses	94.7
Architectural distortion	84.2
Bilateral Asymmetry	81.8

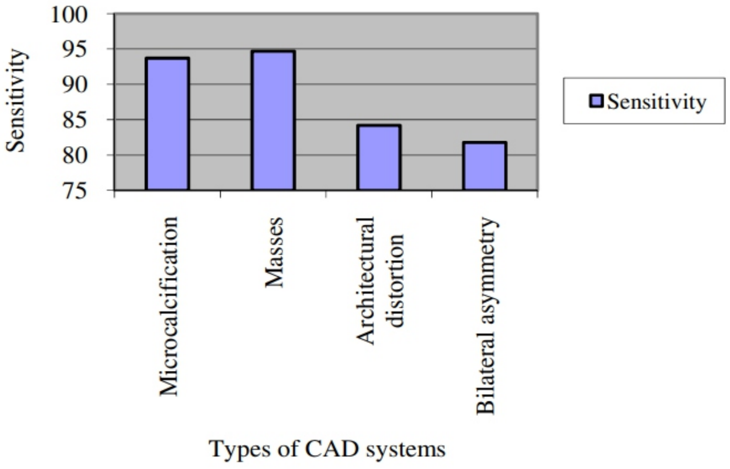
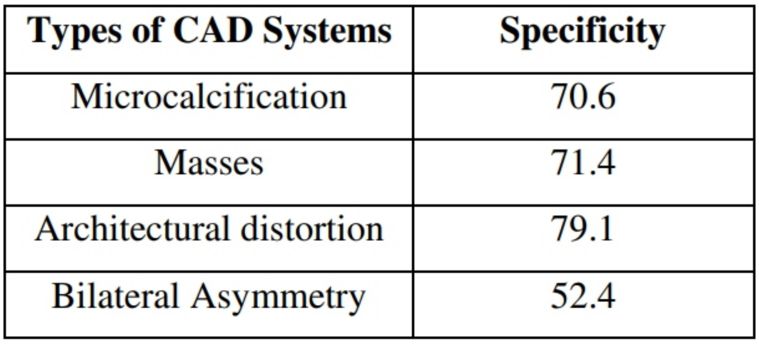


Fig 5: Performance of Sensitivity in different CAD System zz

3.2. Comparative analysis based on sensitivity

In table II shows the Specificity works best in case of architectural distortion and poor in case of microcalcification, masses and bilateral asymmetry. However the corresponding specificity of bilateral asymmetry is 52.4% were incorrectly classified. In fig 6 shows the graphical representation of specificity performance in types of CAD system.

Table 2: Performance of Specificity in different CAD system



Types of CAD Systems	Specificity
Microcalcification	70.6
Masses	71.4
Architectural distortion	79.1
Bilateral Asymmetry	52.4

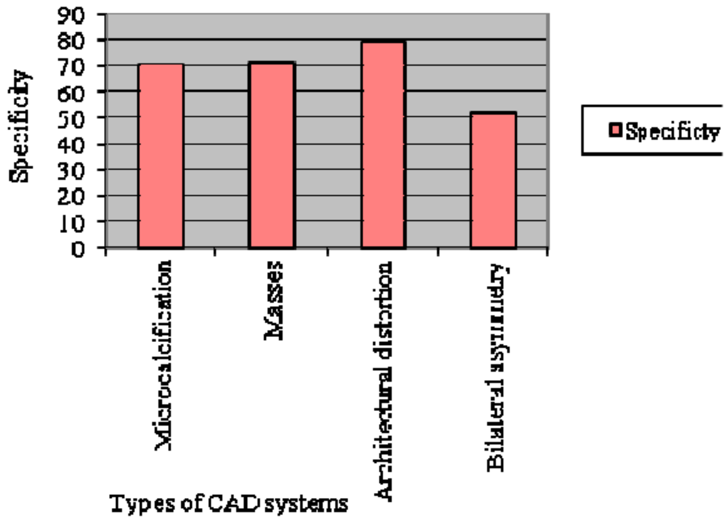
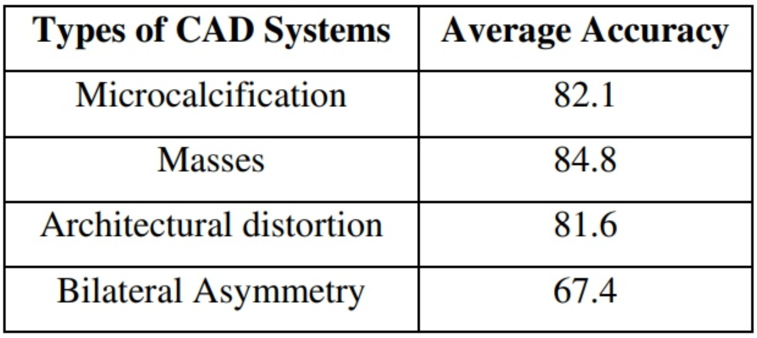


Fig 6: Performance of Specificity in different CAD System

3.3. Comparative analysis based on accuracy

In table III shows the average accuracy of types of CAD system. It was found that accuracy for masses and microcalcification is high when compared to architectural distortion and bilateral asymmetry CAD systems. The masses have high accuracy 84.8% and low accuracy rate of 67.4% in case of bilateral asymmetry. In fig 7 shows the graphical representation of average accuracy in types of CD Systems.

Table 3: Performance of Average Accuracy in different CAD system



Types of CAD Systems	Average Accuracy
Microcalcification	82.1
Masses	84.8
Architectural distortion	81.6
Bilateral Asymmetry	67.4

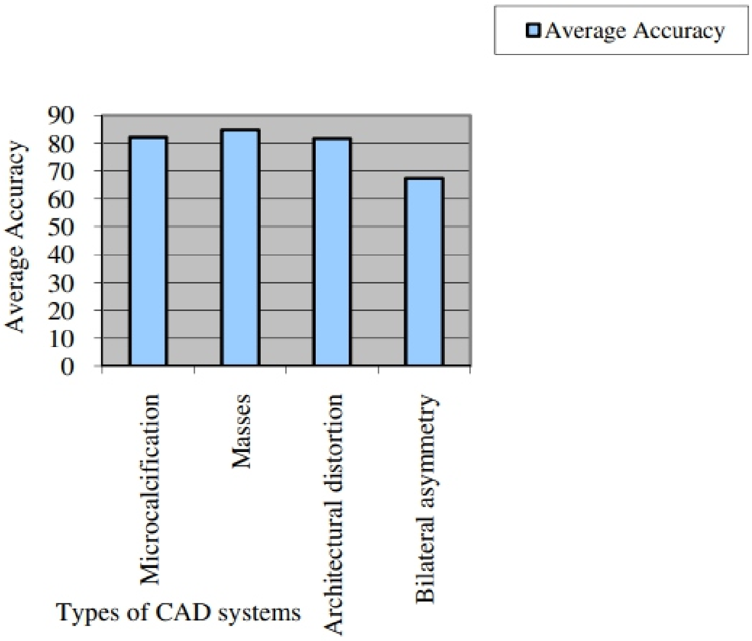


Fig 7: Performance of Average Accuracy in different CAD System

Upcoming work on computer-aided breast cancer detection should focus on the consideration in improving the performance of CAD systems. Even though present CAD systems have not been fully doing well, we believe that advance studies on CAD systems and related technique should help develop their performance, and in this manner facilitate them to gain more widespread adoption in breast care clinics. For MC detection, the last two decades have witnessed a great number of MC detection algorithms developed for mammograms. In current years, several CAD systems that support MC detection have been deployed for clinical use.

4. CONCLUSION

Computer-Aided-Detection (CAD) is a vital system for early detection of breast cancer. A noteworthy amount of work has been done in this area over the past 20 years. On the other hand, the performance of current CAD systems still needs improvement to fully meet up the requirements for everyday clinical applications. This paper has discussed an outline of the recent advances in CAD systems and related techniques, described some fundamental concepts related to breast cancer detection, including comparative analysis of detection of masses, calcification, architectural distortion and bilateral asymmetry in mammograms. Even though important improvement has been made more than the last 20 years, a large amount of work still needs to be done to build up more effective CAD systems.

REFERENCES

[1] S. Shapiro, W. Venet, P. Strax, L. Venet, and R. Roeser, "Ten-to-fourteen- year effect of screening on breast cancer mortality," JNCL, vol. 69, p. 349, 1982.

[2] R. G. Lester, "The contribution of radiology to the diagnosis, management, and cure of breast cancer," Radiology, vol. 151, p. 1, 1984.

[3] M. Moskowitz, Benefit and Risk, Breast Cancer Detection: Mammography and Other Methods in Breast Imaging, 2nd ed, L. W. Bassel and R. H. Gold, Eds. New York: Grune and Stratton, 1987.

[4] R. A. Smith, "Epidemiology of breast cancer categorical course in physics," Tech. Aspects Breast Imaging, Radiol. Soc. N. Amer., pp. 21–33, 1993.

[5] D. B. Kopans, Breast Imaging. Philadelphia, PA: J. B. Lippincoff, 1989, pp. 81–95. [6] H. P. Chan, K. Doi, S. Galhotra, C. J. Vyborny, H. Macmahon, et al., "Image feature analysis and computer-aided diagnosis in digital radiography—1: Automated detection of microcalcifications in mammography," Med. Phys., vol. 14, no. 4, pp. 538–548, 1987.

[7] Y. Wu, K. Doi, M. L. Giger, and R. M. Nishikawa, "Computerized detection of clustered microcalcifications in digital mammograms: Application of artificial neural networks," Med. Phys., vol. 19, no. 3, pp. 555–560, 1992.

[8] D. H. Davies and D. R. Dance, "Automatic computer detection of clustered calcifications in digital mammograms," Phys. Med. Biol., vol. 35, no. 8, pp. 1111–1118, 1990.

[9] H. Yoshida, K. Doi, and R. M. Nishikawa, "Automated detection of clustered microcalcifications in digital mammograms using wavelet transform techniques," Proc. SPIE on Visual Commun. and Image Processing, vol. 2167, pp.868-886, 1994.

[10] M. N. Gurcan, Y. Yardimci, A. E. Centin, and R. Ansari, "Detection of microcalcifications in mammograms using nonlinear subband decomposition and outlier labeling," Proc. SPIE on Visual Commun. and Image Processing, vol. 3024, pp. 909–918, 1997.

[11] J. K. Kim, J. M. Park, K. S. Song, and H. W. Park, "Detection of clustered microcalcifications on mammograms using surrounding region dependence method and artificial neural network," J. VLSI Signal Processing, vol. 18, pp. 251–262, 1998.

[12] H. P. Chan, K. Doi, C. J. Vyborny, R. A Schmidt, and C. E. Metz, et. al., "Improvement in radiologists' detection of clustered microcalcifications on mammograms," Investigative Radiology, vol. 25, pp. 1102–1110, 1990.

[13] R. M. Nishikawa, D. E. Wolverton, R. A. Schmidt, and J. Papaioannou, "Radiologists' ability to discriminate computer-detected true and false positives from an automated scheme for the detection of clustered microcalcifications on digitized mammograms," Proc. SPIE Med. Imag., vol. 3036, pp.

198–204, 1997.

[14] K. Doi, M. L. Giger, R. M. Nishikawa, K. R. Hoffmann, and R. A. Schmidt, et. al., "Prototype clinical 'intelligent' work station for computer-aided diagnosis," RSNA, no. PH087, pp. 1–10, 1995.

[15] H. Kobatake, K. Okuno, M. Murakami, M. Ishida, and H. Takeo, et. al., "CAD system for full-digital mammography and its evaluation," Proc. SPIE Med. Imag., vol. 3034, pp. 745–752, 1997.

[16] S. Mallat, "Multifrequency channel decompositions of images and wavelet models," IEEE Trans. Acoust. Speech Signal Process., vol. 37, no. 12, pp. 2091–2110, Dec. 1989.

[17] S. Mallat, "A theory for multiresolution signal decomposition: The wavelet representation," IEEE Trans. Pattern Anal. Machine Intell., vol. 11, no. i7, pp. 674 –693, Jul. 1989.

[18] Ryohei Nakayama and Yoshikazu Uchiyama, "Computer-Aided Diagnosis Scheme Using a Filter Bank for Detection of Microcalcification Clusters in Mammograms," IEEE Trans. on Bio. Engineering, vol. 53, no. 2, pp. 273-283 Feb 2006.

[19] Liyang Wei and Yongyi Yang, "A Study on Several Machine-Learning Methods for Classification of Malignant and Benign Clustered Microcalcifications," IEEE Trans. on Med. Imaging, vol. 24, no. 3, pp. 371-380 March 2005.

[20] M. P. Sampat, M. K. Markey, and A. C. Bovik, "Computer-aided detection and diagnosis in mammography," in Handbook of Image and Video Processing, A.C. Bovik, Ed., 2nd ed. New York: Academic, 2005, pp. 1195–1217.

[21] American College of Radiology, ACR BI-RADS—Mammography, Ultrasound & Magnetic Resonance Imaging, 4th ed. Reston, VA: Amer. Coll. Radiol., 2003.

[22] S.Timp and N.Karssemeijer, "A new 2D segmentation method based on dynamic programming applied to computer aided detection in mammography," Med. Phys., vol. 31, no. 5, pp. 958–971, 2004.

[23] Lubomir Hadjiiski and Heang-Ping Chan "Classification of Malignant and Benign Masses Based on Hybrid ART2LDA Approach," IEEE Trans on Medical Imaging, vol. 18, no. 12, pp. 1178-1187, December 1999.

[24] Pelin Gorgel and Ahmet Sertbas, "Mammographic Mass Classification Using Wavelet Based Support Vector Machine," Journal Of Electrical & Electronics Engineering, vol. 9, no. 1, pp. 867-875, 2009.

[25] R. M. Rangayyan, F. J. Ayres, and J. E. L. Desautels, "A review of computer-aided diagnosis of breast cancer: Toward the detection of early signs," J. Franklin Inst., vol. 344, no. 3/4, pp. 312–348, 2007.

[26] A. M. Knutzen and J. J. Gisvold, “Likelihood of malignant disease for various categories of mammographically detected, nonpalpable breast lesions,” Mayo Clin. Proc., vol. 68, no. 5, pp. 454-460,1993.

[27] B. C. Yankaskas, M. J. Schell, R. E. Bird, and D. A. Desrochers, “Reassessment of breast cancers missed during routine screening mammography: A community based study,” Amer. J. Roentgenol., vol. 177, no. 3, pp. 535–541, 2001.

[28] H. Burrell, A. Evans, A. Wilson, and S. Pinder, “False-negative breast screening assessment: What lessons we can learn?,” Clin. Radiol., vol. 56, no. 5, pp. 385–388, 2001.

[29] Sujoy Kumar Biswas and Dipti Prasad Mukherjee, "Recognizing Architectural Distortion in Mammogram: A Multiscale Texture Modeling Approach with GMM," IEEE Trans. on Biom. Engineering, vol. 58, no. 7, pp. 2023-2030, July 2011.

[30] Rangaraj M Rangayyan Shantanu Banik, and J. E. Leo Desautels, "Detection of Architectural Distortion in Prior Mammograms," IEEE Transactions on Medical Imaging, vol. 30, pp 279-294, Feb2011.

[31] M. J. Homer, Mammographic Interpretation: A Practical Approach. Boston, MA: McGraw-Hill, 1997.

[32] R.M.Rangayyan, R.J.Ferrari, and A.F.Fr`ere, “Analysis of bilateral asymmetry in mammograms using directional, morphological, and density features,” J. Electron. Imag., vol. 16, no. 1, pp. 013003-1–013003- 12, 2007.

[33] R. J. Ferrari, R. M. Rangayyan, J. E. L. Desautels, and A. F. Fr`ere, “Analysis of asymmetry in mammograms via directional filtering with Gabor wavelets,” IEEE Transactions on Medical Imaging., vol. 20, no. 9, pp. 953–964, Sep. 2001.

[34] Jelena Bozek, Emil Dumic and Mislav Grgic, "Bilateral Asymmetry Detection in Digital Mammography Using B-spline Interpolation," IEEE 16th Internal Conference on Signals and Image Processing, pp 1-4,June 2009.

[35] Siemens, Mammomat NovationDR, Available at: www.medical. siemens.com.

EFFICIENT FAULT DETECTION CODES

*M. Palaniappan
**B. Manikandan

ABSTRACT

The technology advancements in scaling-smaller dimensions, higher integration densities, and lower operating voltages-has lead to reduction of reliability not only in extreme radiation environments like spacecraft and avionics , but also in terrestrial environments. SRAM memory failure rates are increasing significantly, thereby raising a major reliability problem for many applications. This paper presents an error-detection method for difference-set cyclic codes with majority logic decoding. Majority logic decodable codes are suitable for memory applications due to their capability to correct a large number of errors. However, they require a large decoding time that impacts memory performance. The proposed fault-detection method significantly reduces memory access time when there is no error in the data read. The technique uses the majority logic decoder itself to detect failures, which makes the area overhead minimal and keeps the extra power consumption low. This technique will tend to correct burst errors of any length.

Index Terms : Error correction Schemes (ECC), Majority Logic Decoding (MLD), Low Density Parity Check Codes (LDPC).

1. INTRODUCTION:

The general idea for achieving error detection and correction is to add some redundancy (i.e., some extra data) to a message, which receivers can use to check consistency of the delivered message, and to recover data determined to be corrupted. Error-detection and correction schemes can be either systematic or non-systematic: In a systematic scheme, the transmitter sends the original data, and attaches a fixed number of *check bits (or parity data),* which are derived from the data bits by some deterministic algorithm. If only error detection is required, a receiver can simply apply the same algorithm to the received data bits and compare its output with the received check bits; if the values do not match, an error has occurred at some point during the transmission. In a system that uses a non-systematic code, the original message is transformed into an encoded message that has at least as many bits as the original message. Error-detecting and correcting codes can be generally distinguished between random-error-detecting / correcting and burst-error-detecting/correcting. Some codes can also be suitable for a mixture of random errors and burst errors.

The various error correction schemes available are Hash function, Repetition codes, Parity bits, Check sums, Cryptographic Hash function, Cyclic redundancy Checks and etc.,.

TMR, a error correcting mechanism having complexity overhead three times plus the complexity of the majority voter and consumes more power. ECC codes are the best way to mitigate memory soft errors. The usual multi error correction codes, such as Reed–Solomon (RS) or Bose–Chaudhuri–Hocquenghem (BCH) are not suitable for this task. The reason for this is that they use more sophisticated decoding algorithms. Cyclic block codes have been identified as good candidates, due to their property of being majority logic (ML) decodable and it is very simple to implement. But the drawback of ML decoding is that, for a coded word of N -bits, it takes N cycles in the decoding process, posing a big impact on system performance. The simplest way to implement a fault detector for an ECC is by calculating the syndrome, but this generally implies adding another very complex functional unit. Among the ECC codes that meet the requirements of higher error correction capability and low decoding complexity, cyclic block codes have been identified as good candidates, due to their property of being majority logic (ML) decodable [7], [8].

In this paper, we will focus on one specific type of LDPC codes, namely the difference-set cyclic codes (DSCCs), which is widely used in the Japanese tele text system or FM multiplex broadcasting systems [12]-[14]. The main reason for using ML decoding is that it is very simple to implement and thus it is very practical and has low complexity. The drawback of ML decoding is that, for a coded word of N-bits, it takes N cycles in the decoding process. One way of coping with this problem is to implement parallel encoders and decoders. This solution would enormously increase the complexity and, therefore, the power consumption. As most of the memory reading accesses will have no errors, the decoder is most of the time working for no reason. This has motivated the use of a fault detector module [11] that checks if the codeword contains an error and then triggers the correction mechanism accordingly. In this case, only the faulty code words need correction, and therefore the average read memory access is speeded up, at the expense of an increase in hardware cost and power consumption. A similar proposal has been presented in [15] for the case of flash memories. This paper explores the idea of using the ML decoder circuitry as a fault detector so that read operations are accelerated with almost no additional hardware cost. The results show that the properties of DSCC-LDPC enable efficient fault detection.

II. EXISTING ERROR CORRECTION METHODOLOGIES

A. Plain ML Decoder

The ML decoder is a simple and powerful decoder, capable of correcting multiple random bit-flips depending on the number of parity check equations. It consists of four parts: 1) a cyclic shift register; 2) an XOR matrix; 3) a majority gate; and 4) an XOR for correcting the codeword bit under decoding, as illustrated in Fig. 2. The input signal is initially stored into the cyclic shift register and shifted through all the taps. The intermediate values in each tap are then used to calculate the results of the check sum equations from the XOR matrix. In the cycle, the result has reached the final tap, producing the output signal (which is the decoded version of input). As stated before, input might correspond to wrong data corrupted by a soft error. To handle this situation, the decoder would behave as follows.

After the initial step, in which the codeword is loaded into the cyclic shift register, the decoding starts by calculating the parity check equations hardwired in the XOR matrix. The resulting sums are then forwarded to the majority gate for evaluating its correctness. If the number of 1's received in is greater than the number of 0's that would mean that the current bit under decoding is wrong and a signal to correct it would be triggered. Otherwise, the bit under decoding would be correct and no extra operations would be needed on it. In the next step, the content of the registers are rotated and the above procedure is repeated until all codeword bits have been processed. Finally, the parity check sums should be zero if the codeword has been correctly decoded. Further details on how this algorithm works can be found in [6]. The whole algorithm is depicted in Fig. 3. The previous algorithm needs as many cycles as the number of bits in the input signal, which is also the number of taps, in the decoder. This is a big impact on the performance of the system, depending on the size of the code. For example, for a codeword of 73 bits, the decoding would take 73 cycles, which would be excessive for most applications.

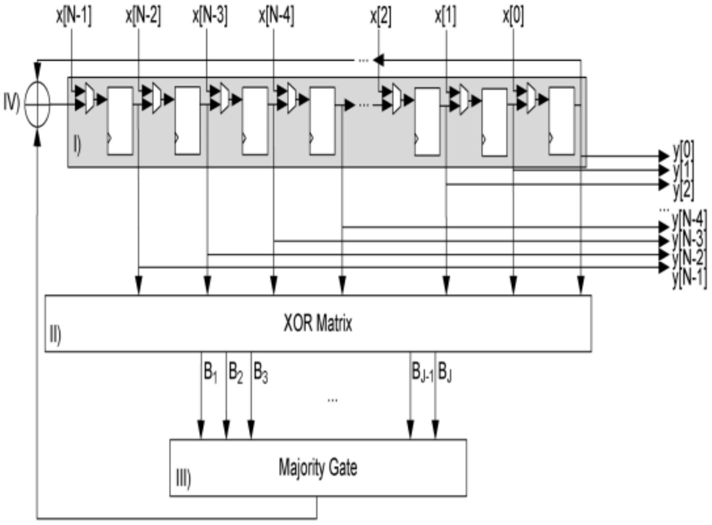


Fig.1 Schematic of plain ML decoder

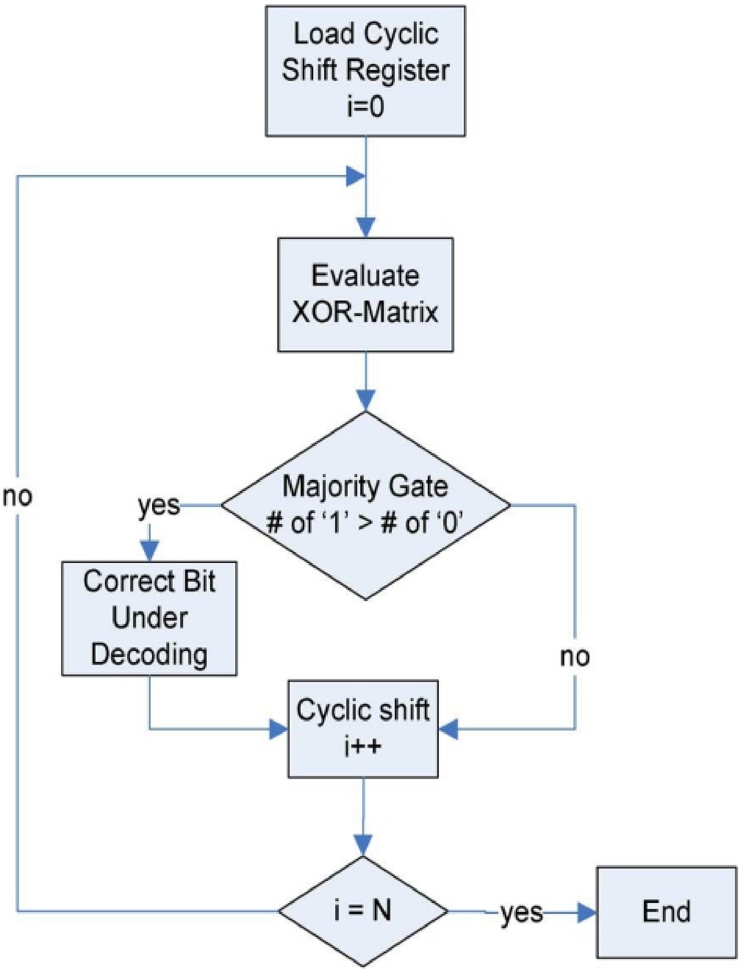

Load Cyclic Shift Register i=0
Evaluate XOR-Matrix
Majority Gate # of '1' > # of '0'
yes
no
Correct Bit Under Decoding
no
Cyclic shift i++
i = N
yes
End

Fig.2 Flow diagram of MLD

B. Plain MLD with Syndrome Fault Detector (SFD)

In order to improve the decoder performance, alternative designs may be used. One possibility is to add a fault detector by calculating the syndrome, so that only faulty code words are decoded [11]. Since most of the code words will be error-free, no further correction will be needed, and therefore performance will not be affected. Although the implementation of an SFD reduces the average latency of the decoding process, it also adds complexity to the design (see Fig. 4). The SFD is an XOR matrix that calculates the syndrome based on the parity check matrix. Each parity bit results in a syndrome equation. Therefore, the complexity of the syndrome calculator increases with the size of the code.

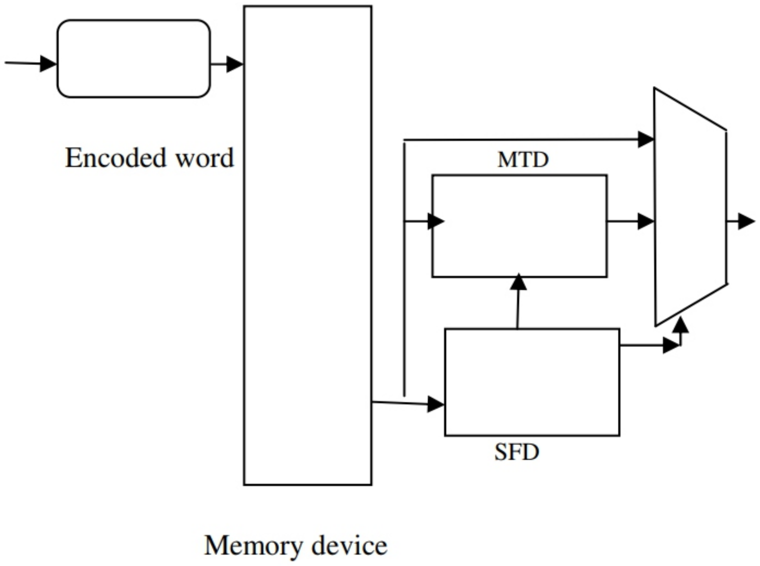


Fig.3 Plain ML decoder with SFD

A faulty code word is detected when at least one of the syndrome bits is "1." This triggers the MLD to start the decoding, as explained before. On the other hand, if the codeword is error -free, it is forwarded directly to the output, thus saving the correction cycles. In this way, the performance is improved in exchange of an additional module in the memory system: a matrix of XOR gates to resolve the parity check matrix, where each check bit results into a syndrome equation. This finally results in a quite complex module, with a large amount of additional hardware and power consumption in the system.

III. PROPOSED METHODOLOGY

This section presents a modified version of the ML decoder that improves the designs presented before. Starting from the original design of the ML decoder introduced in [8], the proposed ML detector/decoder

(MLDD) has been implemented using the difference-set cyclic codes (DSCCs) [16]–[19]. This code is part of the LDPC codes, and, based on their attributes, they have the following properties:

- ability to correct large number of errors;
- sparse encoding,
- decoding and checking circuits synthesizable into simple hardware;
- modular encoder and decoder blocks that allow an efficient hardware implementation;
- systematic code structure for clean partition of information and code bits in the memory.

An important thing about the DSCC is that its systematical distribution allows the ML decoder to perform error detection in a simple way, using parity check sums (see [6] for more details). However, when multiple errors accumulate in a single word, this mechanism may misbehave, as explained in the following. In the simplest error situation, when there is a bitflip in a codeword, the corresponding parity check sum will be "1," .However, in the case of the code word is affected by two bit-flips in bit 42 and bit 25, which participate in the same parity check equation. So, the check sum is zero as the parity does not change. Finally if there is three bit-flips which again are detected by the check sum (with a "1"). As a conclusion of these examples, any number of odd bit flips can be directly detected, producing a "1" in the corresponding equation.

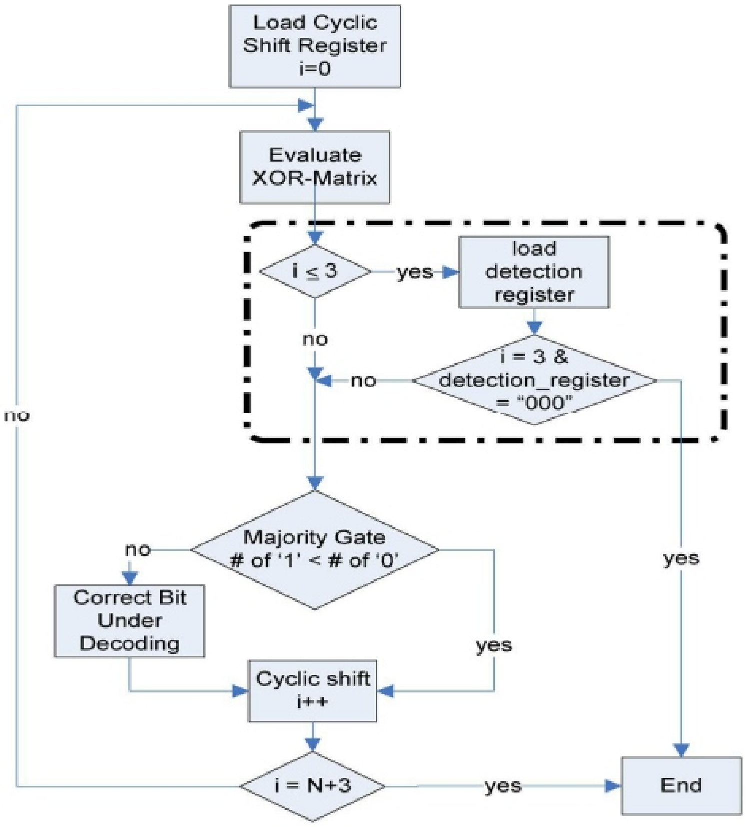

Load Cyclic Shift Register i=0
Evaluate XOR-Matrix
i ≤ 3
yes
load detection register
no
i = 3 & detection_register = "000"
no
no
Majority Gate # of '1' < # of '0'
no
Correct Bit Under Decoding
yes
yes
Cyclic shift i++
i = N+3
yes
End

Fig.4 Flow diagram of proposed method

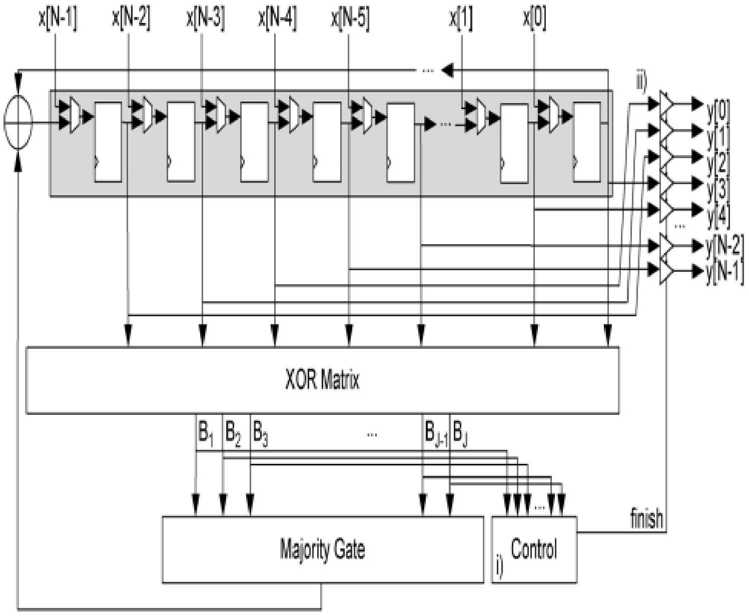


Fig.5 Schematic of MLDD

The problem is in those cases with an even numbers of bit-flips, where the parity check equation would not detect the error. In this situation, the use of a simple error detector based on parity check sums does not seem feasible, since it cannot handle “false negatives” (wrong data that is not detected).

However, the alternative would be to derive all data to the decoding process (i.e., to decode every single word that is read in order to check its correctness), as explained in previous sections, with a large performance overhead. Since performance is important for most applications, we have chosen an intermediate solution, which provides a good reliability with a small delay penalty for scenarios where up to five bit-flips may be expected (the impact of situations with more than five bit-flips will be analyzed in Section IV-A).

This proposal is one of the main contributions of this paper, and it is based on the following hypothesis:

Given a word read from a memory protected with DSCC codes, and affected by up to five bit - flips, all errors can be detected in only three decoding cycles. This is a huge improvement over the simpler case, where decoding cycles are needed to guarantee that errors are detected.

In general, the decoding algorithm is still the same as the one in the plain ML decoder version. The difference is that instead of decoding all codeword bits by processing the ML decoding during cycles, the proposed method stops intermediately in the third cycle, as illustrated in Fig. 6. If in the first three cycles of the decoding process, the evaluation of the XOR matrix for all is "0," the codeword is determined to be error-free and forwarded directly to the output. If it contains in any of the three cycles at least a "1," the proposed method would continue the whole decoding process in order to eliminate the errors. A detailed schematic of the proposed design is shown in Fig. 7. The figure shows the basic ML decoder with an -tap shift register, an XOR array to calculate the orthogonal parity check sums and a majority gate for deciding if the current bit under decoding needs to be inverted. Those components are the same as the ones for the plain ML decoder shown in Fig. 2.

The additional hardware to perform the error detection is illustrated in Fig. 6 as: i) the control unit which triggers a finish flag when no errors are detected after the third cycle. The output tri state buffers are always in high impedance unless the control unit sends the finish signal so that the current values of the shift register are forwarded to the output. The control schematic is illustrated in Fig. 8. The control unit manages the detection process. It uses a counter that counts up to three, which distinguishes the first three iterations of the ML decoding. In these first three iterations, the control unit evaluates the by combining them with the OR1 function. This value is fed into a three-stage shift register, which holds the results of the last three cycles.

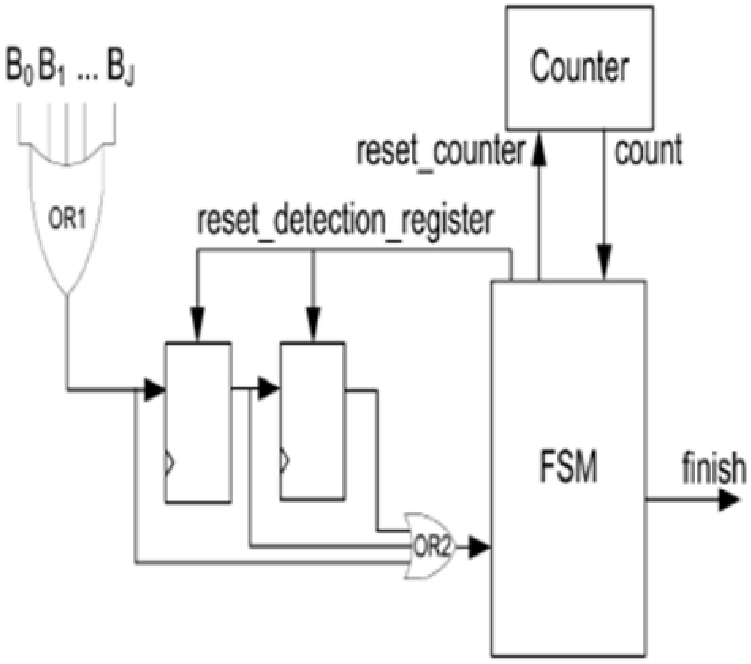
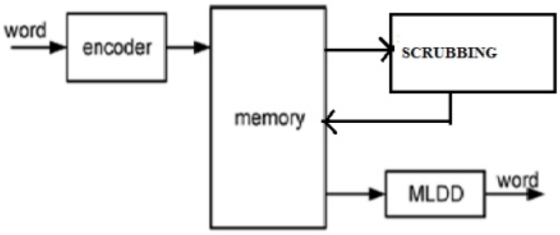
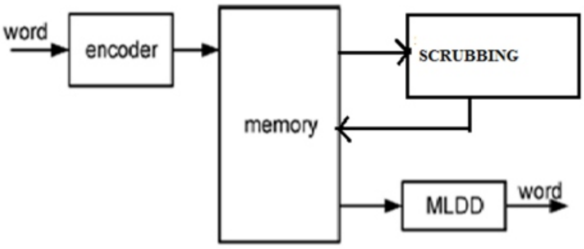


Fig.6 Control unit of MLDD

In the third cycle, the OR2 gate evaluates the content of the detection register. When the result is “0,” the FSM sends out the finish signal indicating that the processed word is error-free. In the other case, if the result is “1,” the ML decoding process runs until the end. This clearly provides a performance improvement respect to the traditional method. Most of the words would only take three cycles (five, if we consider the other two for input/output) and only those with errors (which should be a minority) would need to perform the whole decoding process. The schematic for this memory system is very similar to the one in Fig. 1, adding the control logic in the MLDD module.





FAULT SECURE MEMORY SYSTEM

Scrubbing of memory enables the periodic error detection and correction procedure to be repeated, thereby preventing error propagation to unaffected locations. It also increases the probability of reading the data without errors, which takes only five cycles for MLDD decoding ensuring safety and timely information.

IV.SIMULATION RESULTS

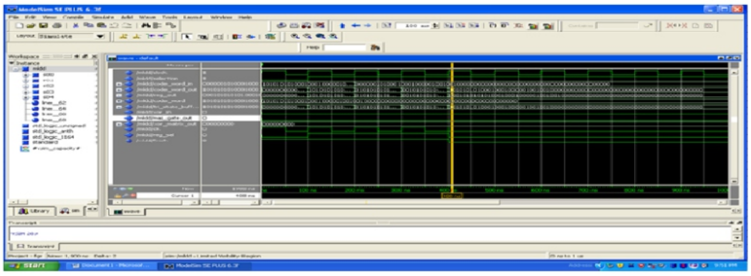


Fig.7 Model sim wave editor showing error detection within 3 cycles.

V. CONCLUSION

In this paper, a fault-detection mechanism, MLDD, has been presented based on ML decoding using the DSCCs. Exhaustive simulation test results show that the proposed technique is able to detect any pattern of up to five bit-flips in the first three cycles of the decoding process. This improves the performance of the design with respect to the traditional MLD approach. On the other hand, the MLDD error detector module has been designed in a way that is independent of the code size. This makes its area overhead quite reduced compared with other traditional approaches such as the syndrome calculation (SFD). In addition, a scrubbing technique is included with the proposed MLDD scheme for preventing error propagation and reducing iterations needed for decoding.

VI. REFERENCES

[1] Shih Fu Liu, Pedro reviriego & Juan Antonio Maestro, "Efficient Logic Fault detection with Difference –Set cyclic codes for Memory Applications," IEEE Trans. VLSI systems., vol.2, no. 1, Jan. 2012.

[2] R. C. Baumann, "Radiation-induced soft errors in advanced semiconductor technologies," IEEE Trans. Device Mater. Reliabil., vol. 5, no.3, pp. 301–316, Sep. 2005.

[3] J. von Neumann " Probabilistic logics and synthesis of reliable organisms from unreliable components" Automata Studies, pp. 43–98, 1956.

[4] M. A. Bajura et al., " Models and algorithmic limits for an ECC-based approach to hardening sub-100-nm SRAMs" IEEE Trans. Nucl. Sci., vol.54, no.4, pp. 935–945, Aug. 2007.

[5] R. Naseer and J. Draper, "DEC ECC design to improve memory reliability in sub-100 nm technologies," in Proc. IEEE ICECS, 2008, pp. 586–589.

[6] S. Lin and D. J. Costello, Error Control Coding, 2nd ed. Englewood Cliffs, NJ: PrenticeHall, 2004.

[7] I. S. Reed, "A class of multiple-error-correcting codes and the decoding scheme" IRE Trans. Inf. Theory, vol. IT-4, pp.38-49, 1954.

[8] J. L. Massey, Threshold Decoding. Cambridge, MA: MIT Press, 1963.

[9] S. Ghosh and P. D. Lincoln, " Low-density parity check codes for error correction in Nano scale memory " SRI Comput. Sci. Lab. Tech. Rep. CSL-0703, 2007.

[10] B. Vasic and S. K. Chilappagari, " An information theoretical framework for analysis and design of Nano scale fault-tolerant memories based on low-density parity-check codes " IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 54, no. 11, pp. 2438–2446, Nov. 2007.

[11] H. Naeimi and A. DeHon, "Fault secure encoder and decoder for Nano Memory applications" IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 17, no. 4, pp. 473–486, Apr. 2009.

[12] Y. Kato and T. Morita, " Error correction circuit using difference-set cyclic code" in Proc. ASP-DAC, 2003, pp. 585–586.

[13] T. Kuroda, M. Takada, T. Isobe, and O. Yamada, " Transmission scheme of highcapacity FM multiplex broadcasting system" IEEE Trans. Broadcasting, vol. 42, no. 3, pp. 245–250, Sep. 1996.

[14] O. Yamada, "Development of an error-correction method for data packet multiplexed with TV signals" IEEE Trans. Commun., vol. COM-35, no. 1, pp. 21–31, Jan. 1987.

[15] P. Ankolekar, S. Rosner, R. Isaac, and J. Bredow, " Multi-bit error correction methods for latency-contrained flash memory systems " IEEE Trans. Device Mater. Reliabil., vol. 10, no. 1, pp. 33–39, Mar. 2010.

[16] E. J.Weldon, Jr., " Difference-set cyclic codes" Bell Syst. Tech. J., vol. 45, pp. 1045–1055, 1966.

[17] C. Tjhai, M. Tomlinson, M. Ambroze, and M. Ahmed, "Cyclotomic idempotent-based binary cyclic codes," Electron. Lett., vol. 41, no. 6, Mar. 2005.

[18] T. Shibuya and K. Sakaniwa, " Construction of cyclic codes suitable for iterative decoding via generating idempotents" IEICE Trans. Fundamentals, vol. E86-A, no. 4, pp.928-939, 2003.

AN EFFICIENT DATA HIDING IN ENCRYPTED IMAGE

PL.Subramanian
B.Manikandan

ABSTRACT

Data transmission is boon to communication. In having secured and efficient data transfer within allotted bandwidth, the compression and encryption technology are of vital importance. The way in which data is compressed and encrypted also plays major role for optimization. Having compression after encrypting the source yields better result than with other case. Security is enhanced by having two separate keys for data and image.

With an encrypted image containing additional data, if a receiver has the data-hiding key, it can extract the additional data though it does not know the image content. If the receiver has the encryption key, it can decrypt the received data to obtain an image similar to the original one, but cannot extract the additional data. If the receiver has both the data-hiding key and the encryption key, it can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image when the amount of additional data is not too large.

Index Terms: Data Hiding, Encryption, Decryption, correlation.

1. INTRODUCTION:

Encryption is the process of transforming information (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is information (in cryptography, referred as cipher text). The reverse process, i.e., to make the encrypted information readable again, is referred as decryption (i.e., to make it unencrypted).

The objective of image compression is to reduce irrelevance and redundancy of the image data in order to be able to store or transmit data in an efficient form. Image compression may be lossy or lossless. Lossless compression is preferred for archival purposes and often for medical imaging, technical drawings, clip art, or comics. This is because lossy compression methods, especially when used at low bit rates, introduce compression artifacts. Lossy methods are especially suitable for natural images such as photographs in applications where minor (sometimes imperceptible) loss of fidelity is acceptable to achieve a substantial reduction in bit rate. The lossy compression that produces imperceptible differences may be called visually lossless. Encryption, by itself, can protect the confidentiality of messages, but other techniques are still needed to protect the integrity and authenticity of a message; for example, verification of a message authentication codes (MAC) or a digital signature. Standards and cryptographic software and hardware to perform encryption are widely available, but successfully using encryption to ensure security may be a challenging problem. A single slip-up in system design or execution can allow successful attacks. Sometimes an adversary can obtain unencrypted information without directly undoing the encryption. See, e.g., traffic analysis, TEMPEST, or Trojan horse.

When doing compression before the encryption there is not improvement in compression gain. Moreover the information security plays a vital role than any other parameters in network communication. Considering all the factors in mind a solution must be attained that could satisfy security transmission as well as data compaction, which facilitates freer bandwidth for additional data transfer in the same time interval. The source is first compressed to its entropy rate using a standard source coder. Then, the compressed source is encrypted using one of the many widely available encryption technologies. At the receiver, decryption is performed first, followed by decompression. In this paper, we investigate the novelty of reversing the order of these steps, i.e., first encrypting and then compressing the encrypted source, as shown in Fig. 2. The compressor does not have access to the cryptographic key, so it must be able to compress the encrypted data (also called ciphertext) without any knowledge of the original source. At first glance, it appears that only a minimal compression gain, if any, can be achieved, since the output of an encryption will look very random.

However, at the receiver, there is a decoder in which both decompression and decryption are performed in a joint step. A significant compression ratio can be achieved if compression is performed after encryption. This is true for both lossless and lossy compression. In some cases, we can even achieve the same compression ratio as in the standard case of first compressing and then encrypting. The fact that we can still compress the encrypted source follows directly from distributed source-coding theory.

II.EXISTING METHODS

As an effective and popular means for privacy protection, encryption converts the ordinary signal into unintelligible data, so that the traditional signal processing usually takes place before encryption or after decryption. However, in some scenarios that a content owner does not trust the processing service provider, the ability to manipulate the encrypted data when keeping the plain content unrevealed is desired.

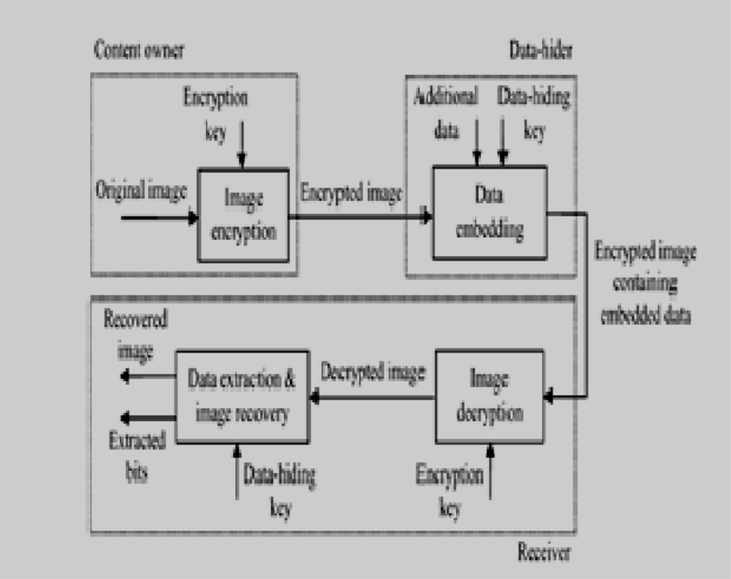


Fig.1 Existing encryption methodology

For instance, when the secret data to be transmitted are encrypted, a channel provider without any knowledge of the cryptographic key may tend to compress the encrypted data due to the limited channel resource. While an encrypted binary image can be compressed with a lossless manner by finding the syndromes of low-density parity-check codes [3], a lossless compression method for encrypted gray image using progressive decomposition and ratecompatible punctured turbo codes is developed in [2]. With the lossy compression method an encrypted gray image can be efficiently compressed by discarding the excessively rough and fine information of coefficients generated from orthogonal transform.

When having the compressed data, a receiver may reconstruct the principal content of original image by retrieving the values of coefficients. The computation of transform in the encrypted domain has also been studied. Based on the homomorphic properties of the underlying cryptosystem, the discrete Fourier transform in the encrypted domain can be implemented. A composite signal representation method packing together a number of signal samples and processing them as a unique sample is used to reduce the complexity of computation and the size of encrypted data. In a buyer–seller watermarking protocol, the seller of digital multimedia product encrypts the original data using a public key, and then permutes and embeds an encrypted fingerprint provided by the buyer in the encrypted domain. After decryption with a private key, the buyer can obtain a watermarked product. This protocol ensures that the seller cannot know the buyer's watermarked version while the buyer cannot know the original version.

III. PROPOSED METHODOLOGY

The proposed scheme is made up of image encryption, data embedding and dataextraction/image-recovery phases. The content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image. Then, the data-hider compresses the least significant bits (LSB) of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. At the receiver side, the data embedded in the created space can be easily retrieved from the encrypted image containing additional data according to the data-hiding key. Since the data embedding only affects the LSB, a decryption with the encryption key can result in an image similar to the original version.

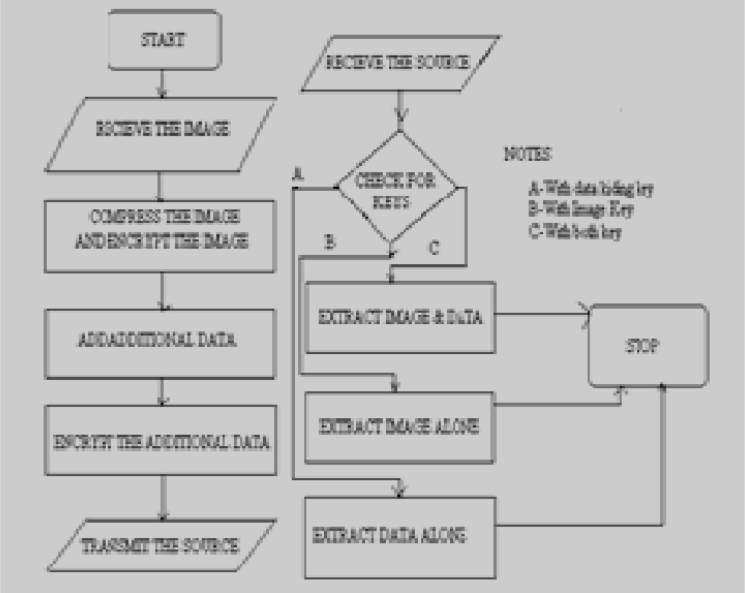


Fig.2 Flow diagram of proposed method

When using both of the encryption and data-hiding keys, the embedded additional data can be successfully extracted and the original image can be perfectly recovered by exploiting the spatial correlation in natural image. Fig. 2 shows the three cases at the receiver side.

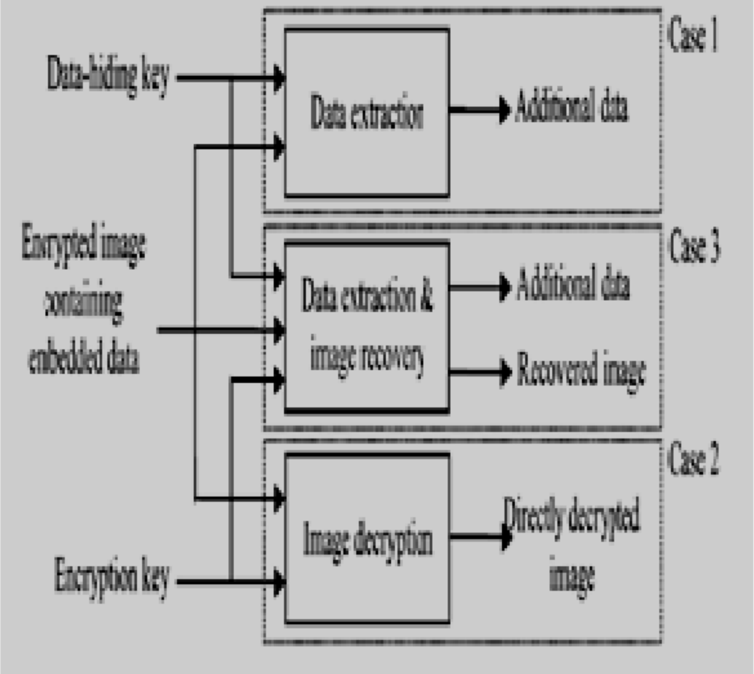


Fig.3 Proposed receiver architecture

We will consider the three cases as in fig 3 that a receiver has only the data-hiding key, only the encryption key, and both the data-hiding and encryption keys, respectively. With an encrypted image containing embedded data, if the receiver has only the data-hiding key, he may first obtain the values of the parameters M,L and S from the LSB of the Np selected encrypted pixels. Then, the receiver permutes and divides the other N-Np pixels into (N-Np)/L groups and extracts the S embedded bits from the M LSB-planes of each group. When having the total (N-Np)*(S/L) extracted bits, the receiver can divide them into Np original LSB of selected encrypted pixels and (N-Np)*(S/L) - Np additional bits. Note that because of the pseudo-random pixel selection and permutation, any attacker without the data-hiding key cannot obtain the parameter values and the pixel-groups, therefore cannot extract the embedded data. Furthermore, although the receiver having the data-hiding key can successfully extract the embedded data, he cannot get any information about the original image content. Consider the case that the receiver has the encryption key but does not know the data-hiding key. Clearly, he cannot obtain the values of parameters and cannot extract the embedded data.

However, the original image content can be roughly recovered. Denoting the bits of pixels in the encrypted image containing embedded data as $B'_{i,j,0}$, $B'_{i,j,1}$, ……$B'_{i,j,}(1<=i<=N_1$ and $1_{<=}j_{<=}N_2$), the receiver can decrypt the received data

$$b'_{ij,n}=B\oplus_{j,n} \quad r_{ij,n}$$

where $r_{ij,n}$ are derived from the encryption key. The gray values of decrypted pixels are

$$P'_{ij},n=2^n(b'_{ijo+}b'_{ij1+}\ldots\ldots+b'_{ij}).$$

Since the data-embedding operation does not alter any MSB of encrypted image, the decrypted MSB must be same as the original MSB. So, the content of decrypted image is similar to that of original image. The probability of this case is $(1/2^s)$, and, in this case, the original(M*L-S) bits in the M LSB-planes can be correctly decrypted. Since S is significantly less than M*L, we ignore the distortion at other S decrypted bits. If there are nonzero bits among B(k,M*L-S+1), B(k,M*L-S+2),…… B(k,M*L), the encrypted data in the M LSBplanes have been changed by the data-embedding operation, so that the decrypted data in the M LSB-planes differ from the original data. The distortion in the N_p selected pixels is also ignored since their number is significantly less than the image size N. So, the value of PSNR in the directly decrypted image is

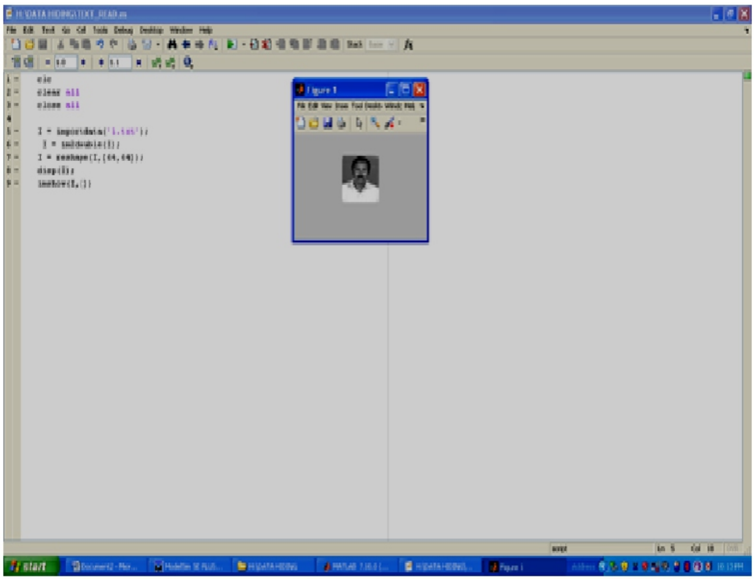
$$PSNR=10*(\log_{10}(A_E))$$

Where A_E is average energy of distortion. Table I gives the theoretical values of PSNR with respect to S and M.

If the receiver has both the data-hiding and the encryption keys, he may aim to extract the embedded data and recover the original image. According to the data-hiding key, the values of M, L and S, the original LSB of the N_p selected encrypted pixels, and the $(N- N_p).(S/L)- N_p)$ additional bits can be extracted from the encrypted image containing embedded data. By putting the N_p LSB into their original positions, the encrypted data of the N_p selected pixels are retrieved, and their original gray values can be correctly decrypted using the encryption keys. In the following, we will recover the original gray values of the other $(N- N_p)$ pixels. For each vector, we attempt to put the elements in it to the original positions to get an encrypted pixel-group and then decrypt the pixel-group using the encryption key. Denoting the decrypted pixel-group as Gk and the gray values in it as $t_{i,j}$, calculate the total difference between the decrypted and estimated gray values in the group. The estimated gray values is generated from the neighbors in the directly decrypted image.

Clearly, the estimated gray values in (16) are only dependent on the MSB of neighbor pixels. Thus, we have 2S different D corresponding to the 2^S decrypted pixel-group Gk. Among the 2^S decrypted pixel-group, there must be one that is just the original gray values and possesses a low D because of the spatial correlation in natural image. So, we find the smallest D and regard the corresponding vector as the actual vector and the decrypted $t_{i,j}$ as the recovered content. A$_S$ long as the number of pixels in a group is sufficiently large and there are not too many bits embedded into each group, the original content can be perfectly recovered by the spatial correlation criterion. Since the 2_S different D must be calculated in each group, the computation complexity of the content recovery is O(N.2_S). On the other hand, if more neighboring pixels and a smarter prediction method are used to estimate the gray values, the performance of content recovery will be better, but the computation complexity is higher.

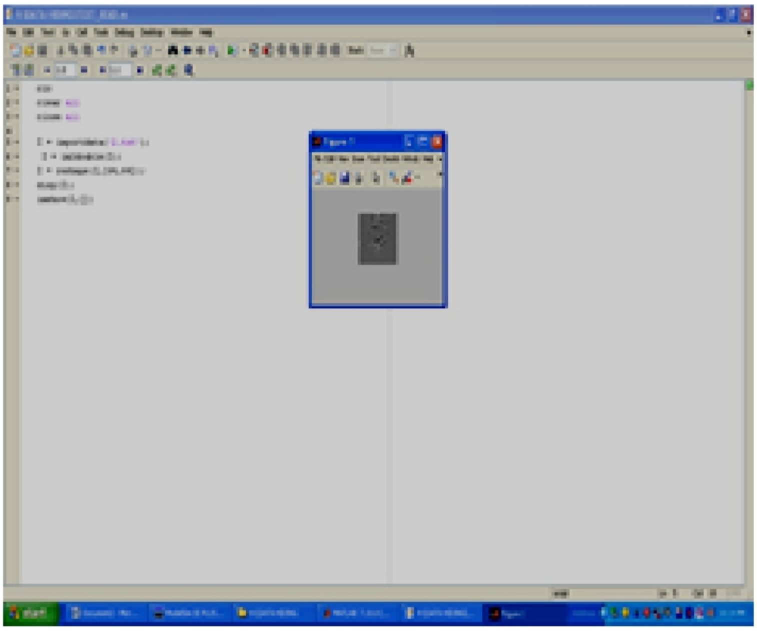
IV.SIMULATION RESULTS



```
clc
clear all
close all

I = importdata('1.txt');
 I = im2double(I);
I = reshape(I,[64,64]);
disp(I);
imshow(I,[])
```

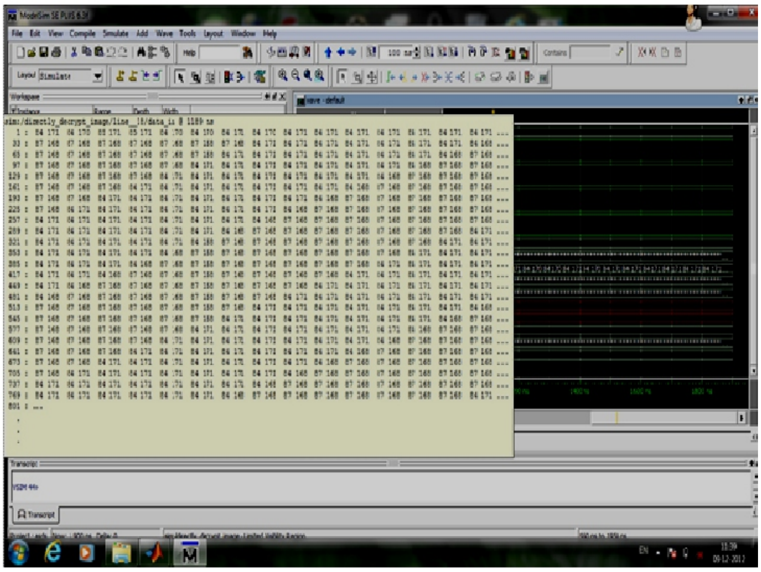
Fig.4 image before encryption and data hiding



```
clc
clear all
close all

I = importdata([illegible]);
 I = [illegible]
I = reshape([illegible]);
disp(I);
imshow([illegible])
```

Fig.5 View of encrypted and data hided image



```
sim:/directly_decrypt_image/line__1/data_in @ 1189 ns
  1 : 84 171 84 170 85 171 85 171 84 170 84 170 84 171 84 170 84 171 84 171 84 171 84 171 84 171 84 171 84 171 ...
 33 : 87 168 87 168 87 168 87 168 87 168 87 168 87 168 84 171 84 171 84 171 84 171 84 171 84 171 84 171 84 168 ...
 65 : 87 168 87 168 87 168 87 168 87 168 87 168 84 171 84 171 84 171 84 171 84 171 84 171 84 171 84 168 87 168 ...
 97 : 87 168 87 168 87 168 87 168 87 168 84 171 84 171 84 171 84 171 84 171 84 171 84 171 84 168 87 168 87 168 ...
129 : 87 168 87 168 87 168 87 168 84 171 84 171 84 171 84 171 84 171 84 171 84 171 84 168 87 168 87 168 87 168 ...
161 : 87 168 87 168 87 168 84 171 84 171 84 171 84 171 84 171 84 171 84 171 84 168 87 168 87 168 87 168 87 168 ...
193 : 87 168 87 168 84 171 84 171 84 171 84 171 84 171 84 171 84 171 84 168 87 168 87 168 87 168 87 168 87 168 ...
225 : 87 168 84 171 84 171 84 171 84 171 84 171 84 171 84 171 84 168 87 168 87 168 87 168 87 168 87 168 87 168 ...
257 : 84 171 84 171 84 171 84 171 84 171 84 171 84 171 84 168 87 168 87 168 87 168 87 168 87 168 87 168 87 168 ...
289 : 84 171 84 171 84 171 84 171 84 171 84 171 84 168 87 168 87 168 87 168 87 168 87 168 87 168 87 168 84 171 ...
321 : 84 171 84 171 84 171 84 171 84 171 84 168 87 168 87 168 87 168 87 168 87 168 87 168 87 168 84 171 84 171 ...
353 : 84 171 84 171 84 171 84 171 84 168 87 168 87 168 87 168 87 168 87 168 87 168 87 168 84 171 84 171 84 171 ...
385 : 84 171 84 171 84 171 84 168 87 168 87 168 87 168 87 168 87 168 87 168 87 168 84 171 84 171 84 171 84 171 ...
417 : 84 171 84 171 84 168 87 168 87 168 87 168 87 168 87 168 87 168 87 168 84 171 84 171 84 171 84 171 84 171 ...
449 : 84 171 84 168 87 168 87 168 87 168 87 168 87 168 87 168 87 168 84 171 84 171 84 171 84 171 84 171 84 171 ...
481 : 84 168 87 168 87 168 87 168 87 168 87 168 87 168 87 168 84 171 84 171 84 171 84 171 84 171 84 171 84 171 ...
513 : 87 168 87 168 87 168 87 168 87 168 87 168 87 168 84 171 84 171 84 171 84 171 84 171 84 171 84 171 84 168 ...
545 : 87 168 87 168 87 168 87 168 87 168 87 168 84 171 84 171 84 171 84 171 84 171 84 171 84 171 84 168 87 168 ...
577 : 87 168 87 168 87 168 87 168 87 168 84 171 84 171 84 171 84 171 84 171 84 171 84 171 84 168 87 168 87 168 ...
609 : 87 168 87 168 87 168 87 168 84 171 84 171 84 171 84 171 84 171 84 171 84 171 84 168 87 168 87 168 87 168 ...
641 : 87 168 87 168 87 168 84 171 84 171 84 171 84 171 84 171 84 171 84 171 84 168 87 168 87 168 87 168 87 168 ...
673 : 87 168 87 168 84 171 84 171 84 171 84 171 84 171 84 171 84 171 84 168 87 168 87 168 87 168 87 168 87 168 ...
705 : 87 168 84 171 84 171 84 171 84 171 84 171 84 171 84 171 84 168 87 168 87 168 87 168 87 168 87 168 87 168 ...
737 : 84 171 84 171 84 171 84 171 84 171 84 171 84 171 84 168 87 168 87 168 87 168 87 168 87 168 87 168 87 168 ...
769 : 84 171 84 171 84 171 84 171 84 171 84 171 84 168 87 168 87 168 87 168 87 168 87 168 87 168 87 168 84 171 ...
801 : ...
  .
  .
  .
```

Fig.6 Image and data recovery in bit format

V. CONCLUSION

A novel scheme for separable reversible data hiding in encrypted image is proposed, which consists of image encryption, data embedding and data-extraction/image-recovery phases. In the first phase, the content owner encrypts the original uncompressed image using an encryption key. Although a data-hider does not know the original content, he can compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. With an encrypted image containing additional data, the receiver may extract the additional data using only the data-hiding key, or obtain an image similar to the original one using only the encryption key. When the receiver has both of the keys, he can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image if the amount of additional data is not too large. If the lossless compression method in [1] or [2] is used for the encrypted image containing embedded data, the additional data can be still extracted and the original content can be also recovered since the lossless compression does not change the content of the encrypted image containing embedded data. However, the lossy compression method in [3] compatible with encrypted images generated by pixel permutation is not suitable here since the encryption is performed by bit-XOR operation. In the future, a comprehensive combination of image encryption and data hiding compatible with lossy compression deserves further investigation.

VI. REFERENCES

[1] Xinpeng Zhang, "Separable Reversible Data Hiding in Encrypted Image" IEEE Transactions on information Forensics and Security,vol .7 No. 2, April 2012.

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

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

[4] T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain," IEEE Trans. Inform. Forensics Security, vol. 4, no. 1, pp. 86–97, Feb. 2009.

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

[6] N. Memon and P. W. Wong, "A buyer-seller watermarking protocol," IEEE Trans. Image Process., vol. 10, no. 4, pp. 643–649, Apr. 2001.

[7] M. Kuribayashi and H. Tanaka, "Fingerprinting protocol for images based on additive homomorphic property," IEEE Trans. Image Process., vol. 14, no. 12, pp. 2129–2139, Dec. 2005.

[8] M. Deng, T. Bianchi, A. Piva, and B. Preneel, "An efficient buyer-seller watermarking protocol based on composite signal representation," in Proc. 11th ACM Workshop Multimedia and Security, 2009, pp. 9–18.

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

[10] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. B. Natale, and A. Neri, "A commutative digital image watermarking and encryption method in the tree structured Haar transform domain," Signal Processing: Image Commun., vol. 26, no. 1, pp. 1–12, 2011.

[11] D. Kundur and K. Karthik, "Video fingerprinting and encryption principles for digital rights management," Proceedings IEEE, vol. 92, no.6, pp. 918–932, Jun. 2004.

[12] X. Zhang, "Reversible data hiding in encrypted image," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2010.

[13] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.

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

[15] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized- LSB data embedding," IEEE Trans. Image Process., vol. 14, no. 2, pp. 253–266, Feb. 2005.

[16] W. Hong, T.-S. Chen, Y.-P. Chang, and C.-W. Shiu, "A high capacity reversible data hiding scheme using orthogonal projection and prediction error modification," Signal Process., vol. 90, pp. 2911–2922, 2010.

[17] C.-C. Chang, C.-C. Lin, and Y.-H. Chen, "Reversible data-embedding scheme using differences between original and predicted pixel values," IET Inform. Security, vol. 2, no. 2, pp. 35-46, 2008.

Increasing Security of Images through Image Steganography: A Review

Prof. Pankaj Nandan
Associate Professor in Computer Science
Govt. College for women, Kathua (J&K)
Rakhi Billawaria
Lecturer in Computer Science
GDC Reasi, J&K.

ABSTRACT

The image processing is the method which is employed to process the image pixels for different objectives. The image data is very sensitive. In order to provide security to image data, various techniques has been proposed in the present times. Among these numerous proposed methods, image steganography is one of the most efficient techniques and methods which provide greater protection to the image data. In the image steganography the sensitive data can be hidden inside the image. The two steps are involved to implement image steganography, in the first step properties of the image are analyzed and in the second phase encoding scheme is implemented to generate final steganography image. In this paper, various techniques of an image steganography are discussed and reviewed in terms of various parameters.

Keywords: Steganography, Information hiding, image properties.

1. INTRODUCTION:

Digital image processing is a quickly growing technology which is employed in medical, defense, agriculture, transmission and encoding and many other fields. The method processes digital images as input to extract some significant aspects from it as an output. Image processing is an important process of analysis and manipulation of the digital images to advance image quality by submitting some efficient algorithms on it.

1. Steganography is very famous and unique instrument for concealing any kind of information into cover media (audio, video, image, text) in such a way that no one can imagine that a secret data exists behind the cover media.

2. It provides more protective communication between two intended parties. Performance of steganography depends on two important factors. The first one, embedding efficiency deals with the

amount of secret data can be hidden in the cover media. The second one is embedding payload, refers to the capacity of the cover media to hide as much as data with minimum distortion.

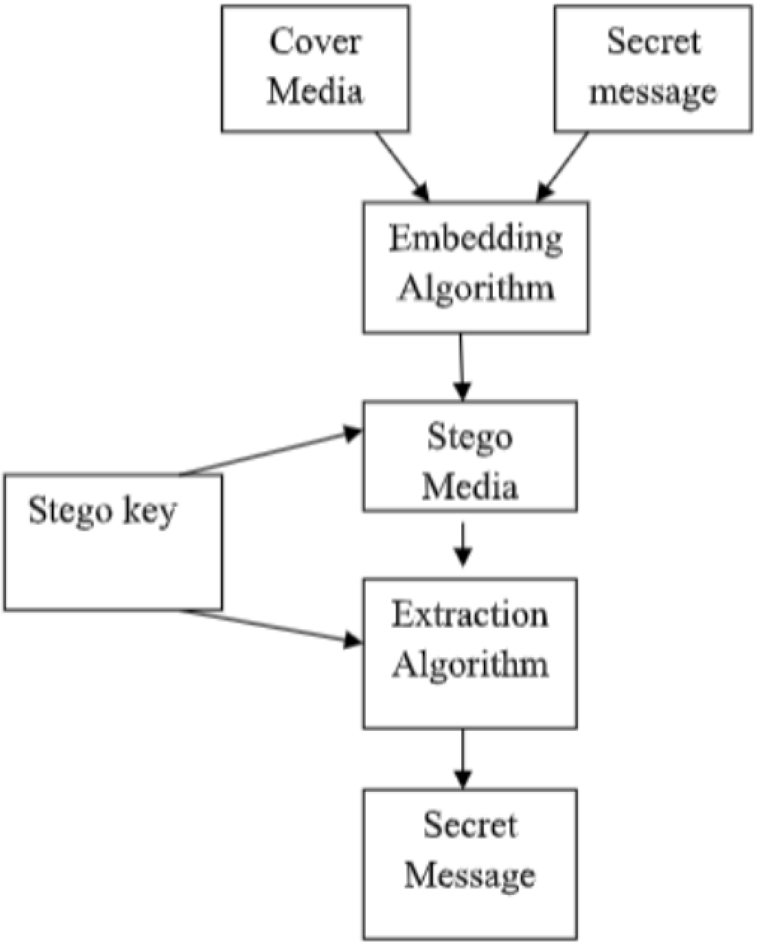


Figure:Common Stegangraphic Model

Video Steganography

In video steganography, a secret data is concealed into a cover video. Video has an enormous capacity to hide secret data than a cover image. Video decomposes into a number of frames and then the encoded secret message is implanted into a selected video frame which bestows greater security than image steganography. The process of message embedding dependsupon two techniques i.e. spatial domain and transform domain.

Spatial Domain VideoSteganography: There are multiple methods which are extensively employed for video steganography, based on spatial domain. These methods change the image pixel values for hiding secret data.

A. Least Significant Bit (LSB)

It is one of the famous techniques for hiding the bits of secret message in the least significant bits of cover image pixels. The resulted stego image looks very similar to the original image [3]. The concealing ability of LSB method can be enhanced by employing up to 4 least significant bits of each pixel which is also quite hard to detect. This method is very simple and less robust. It has high embedding capacity, high visual quality and high detectability.

B. Pixel Value Differencing (PVD)

In this method, for inserting a secret message, the cover image is divided into nonoverlapping blocks of two consecutive pixels. To determine how many bits of secret message should be embedded inside a cover image, the difference between two consecutive pixels values is computed [4]. Large difference value is to be considered in edge area and small difference value is to be considered in smooth area. Human eyes are very sensitive to the noise in smooth area rather than in the edge area. So the difference value is replaced by another value to embed the secret message bits. This method has high imperceptibility and high embedding capacity.

C. RGB based Steganography

A digital image is a collection of pixels that shows light intensities at various points. An image can be stored as 24-bit (RGB) or 8-bit (Gray scale) files. A 24-bit colored image is quite large, however it provides more space for hiding sensitive data. Each pixel is the amalgamation of three primary colors (Red, Green, and Blue), which are individually represented by 1 byte (8 bits). RGB steganography method overcomes the problem of sequential fashion and the use of stego key for selection of pixels [5].

Transform Domain Video Steganography

Transform domain technique does not hide the secret databehind the image pixels [6]. This method is basically used for transforming image pixels from time domain to frequency domain before hiding a secret data. There are two most widely used steganography techniques as follows:

A. Discrete Cosine Transform (DCT)

In this transformation method, inserting of secret message depends on the DCT coefficients. If any DCT coefficient value is above from a specific threshold then that will be a possible location for the insertion of secret data. This technique is employed in general image compression formats like JPEG and MPEG. It divides an image into a number of spectral sub-bands along with its visual quality (high, middle and low frequency components). It is more suitable for low frequency sub-band.

B. Discrete Wavelet Transform (DWT)

DWT is a well-known transformation domain method in which wavelets are discretely tested [7]. There are two operations i.e. horizontal and vertical. Firstly, scan the pixels from left to right in horizontal plane. Then, perform addition and subtraction operations on neighboring pixels. Store the sum on the left that shows the low frequency part denoted as L and collect the variation on the right which highlights the high frequency part of the original image, denoted as H. Repeat these operations until all rows are covered. Secondly, scan the pixels from top to bottom in vertical plane. Then, perform additional and subtraction operations on neighboring pixels. Store the sum on the top and the difference on the bottom. Reiterate these operations until all the columns are covered. Finally we will get 4 sub-bands indicated as LL, LH, HL and HH respectively. The LL is a low frequency sub-band that looks analogous to the original image. LH, HL and HH are the middle and high frequency sub-bands that comprises detailed information about an image i.e. edges and textures of an image [8]. It is more suitable for embedding without being notice by the human eyes.

EVALUTION AND ANALYSIS

Mapping Study Plan Execution:

The various data bases like IEEE Xplore and Springer are searched with numerous strings and it is find out that total number of 328 research papers have been published in the recent years. In the table 2, the individual database results are given.

A. Conduction of Search

The various data bases like IEEE Xplore and Springer are searched with different strings and it is found that total number of 328 research papers have been published in the recent years. In the table 2, the individual database results are given.

TABLE 2: SEARCH STRING RESULT OF VARIOUS DATABASES

Index	Database	Result
1	IEEE Xplore	143
2	Springer	185
Total		328

B. Criteria for Efficient Result Extraction

The study is being conducted to check the authentication of the 328 papers which are searched with the search string criteria from the different databases. The 328 papers have been put into the plagiarism checker tool andleft with 223 papers which are unique and not copied from anywhere. The unique papers are analyzed manually and it is found that only 115 papers which represent divergent video steganography methods for concealing secret message behind the cover video and remaining papers are based on other steganography techniques. The search string is based on video steganography. In the end result we achieved only 40 papers which represent the security concerns of the video steganography.

4. CONCLUSION

In this paper, it is been concluded that various techniques has been recommendedin the recent times to execute image steganography. The image steganography comprises of two phases. In the first phase, image properties are analyzed and in the second step method of image encoding will be applied which will produce final stego image. In future, numerous techniques of video steganography will be reviewed and analyzed in terms of various parameters.

Bibliography

H. Yuh-Ming and J. Pei-Wun, "Two improved data hiding schemes," in Image and Signal Processing (CISP), 2011 4th International Conference on, 2011, pp. 1784-1787.

Shashikala Channalli and Ajay Jadhav, "Steganography an art of hiding data", International Journal of Computer Science and Engineering Vol. (3), pp.137-14I, 2009.

Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav, (2012): Steganography Using Least Significant Bit Algorithm, International ournal of Engineering Research and applications, vol.2, issue 3, pp: 338-341, May-June2012.

H.C. Wu, N.I.Wu, C.S. Tsai, and M.S. Hwang, “An Image Steganography Scheme Based on Pixel Value Differencing and LSB Replacement Methods”, IEEE Proceedings- Vision, Image and Signal Processing, vol. 152, no. 5, pp. 611–615, Oct 2005.

Mandep Kaur, Surbhi Gupta, Parvinder S. Sandhu, Jagdeep Kaur “A Dynamic RGB Intensity Based Steganography Scheme” World Academy of Science, Engineering and Technology, pp. 630-633, 2010 .

Niels Provos, Peter Honeyman.(2003): “Hide and Seek: An Introduction to Steganography”, IEEE SECURITY and PRIVACY, MAY/JUNE 2003.

D. Baby, J. Thomas, G. Augustine, E. George, and N. R. Michael, “A novel dwt based image securing method using steganography,” Procedia Computer Science, vol. 46, pp.

612 – 618, 2015, proceedings of the International Conference on Information and Communication Technologies, ICICT, 2014, 3-5 December 2014 at Bolgatty Palace and Island Resort, Kochi, India.

Ramadhan J. Mstafa and Khaled M. Elleithy, “A highly secure video steganography using hamming code (7,4)”, 2014.

Remah Alshinina, Khaled M.Elleithy et al. "A High Payload Video Steganography algorithm in DWT Domain based on BCH (15, 11)". IEEE, 2015, doi: 10.1109/WTS.2015.7117257.

Bhagya Pillai, Mundra Mounika, Pooja J Rao, Padmamala Sriram,” Image steganography method using K-means Clustering and Encryption techniques”, 2016, IEEE, 978-1-5090-2029-4

Instructions for Authors

Essentials for Publishing in this Journal

1 Submitted articles should not have been previously published or be currently under consideration for publication elsewhere.

2 Conference papers may only be submitted if the paper has been completely re-written (taken to mean more than 50%) and the author has cleared any necessary permission with the copyright owner if it has been previously copyrighted.

3 All our articles are refereed through a double-blind process.

4 All authors must declare they have read and agreed to the content of the submitted article and must sign a declaration correspond to the originality of the article.

Submission Process

All articles for this journal must be submitted using our online submissions system. http://enrichedpub.com/ . Please use the Submit Your Article link in the Author Service area.

Manuscript Guidelines

The instructions to authors about the article preparation for publication in the Manuscripts are submitted online, through the e-Ur (Electronic editing) system, developed by **Enriched Publications Pvt. Ltd**. The article should contain the abstract with keywords, introduction, body, conclusion, references and the summary in English language (without heading and subheading enumeration). The article length should not exceed 16 pages of A4 paper format.

Title

The title should be informative. It is in both Journal's and author's best interest to use terms suitable. For indexing and word search. If there are no such terms in the title, the author is strongly advised to add a subtitle. The title should be given in English as well. The titles precede the abstract and the summary in an appropriate language.

Letterhead Title

The letterhead title is given at a top of each page for easier identification of article copies in an Electronic form in particular. It contains the author's surname and first name initial .article title, journal title and collation (year, volume, and issue, first and last page). The journal and article titles can be given in a shortened form.

Author's Name

Full name(s) of author(s) should be used. It is advisable to give the middle initial. Names are given in their original form.

Contact Details

The postal address or the e-mail address of the author (usually of the first one if there are more Authors) is given in the footnote at the bottom of the first page.

Type of Articles

Classification of articles is a duty of the editorial staff and is of special importance. Referees and the members of the editorial staff, or section editors, can propose a category, but the editor-in-chief has the sole responsibility for their classification. Journal articles are classified as follows:

Scientific articles:

1. Original scientific paper (giving the previously unpublished results of the author's own research based on management methods).

2. Survey paper (giving an original, detailed and critical view of a research problem or an area to which the author has made a contribution visible through his self-citation);

3. Short or preliminary communication (original management paper of full format but of a smaller extent or of a preliminary character);

4. Scientific critique or forum (discussion on a particular scientific topic, based exclusively on management argumentation) and commentaries. Exceptionally, in particular areas, a scientific paper in the Journal can be in a form of a monograph or a critical edition of scientific data (historical, archival, lexicographic, bibliographic, data survey, etc.) which were unknown or hardly accessible for scientific research.

Professional articles:

1. Professional paper (contribution offering experience useful for improvement of professional practice but not necessarily based on scientific methods);
2. Informative contribution (editorial, commentary, etc.);
3. Review (of a book, software, case study, scientific event, etc.)

Language

The article should be in English. The grammar and style of the article should be of good quality. The systematized text should be without abbreviations (except standard ones). All measurements must be in SI units. The sequence of formulae is denoted in Arabic numerals in parentheses on the right-hand side.

Abstract and Summary

An abstract is a concise informative presentation of the article content for fast and accurate Evaluation of its relevance. It is both in the Editorial Office's and the author's best interest for an abstract to contain terms often used for indexing and article search. The abstract describes the purpose of the study and the methods, outlines the findings and state the conclusions. A 100- to 250-Word abstract should be placed between the title and the keywords with the body text to follow. Besides an abstract are advised to have a summary in English, at the end of the article, after the Reference list. The summary should be structured and long up to 1/10 of the article length (it is more extensive than the abstract).

Keywords

Keywords are terms or phrases showing adequately the article content for indexing and search purposes. They should be allocated heaving in mind widely accepted international sources (index, dictionary or thesaurus), such as the Web of Science keyword list for science in general. The higher their usage frequency is the better. Up to 10 keywords immediately follow the abstract and the summary, in respective languages.

Acknowledgements

The name and the number of the project or programmed within which the article was realized is given in a separate note at the bottom of the first page together with the name of the institution which financially supported the project or programmed.

Tables and Illustrations

All the captions should be in the original language as well as in English, together with the texts in illustrations if possible. Tables are typed in the same style as the text and are denoted by numerals at the top. Photographs and drawings, placed appropriately in the text, should be clear, precise and suitable for reproduction. Drawings should be created in Word or Corel.

Citation in the Text

Citation in the text must be uniform. When citing references in the text, use the reference number set in square brackets from the Reference list at the end of the article.

Footnotes

Footnotes are given at the bottom of the page with the text they refer to. They can contain less relevant details, additional explanations or used sources (e.g. scientific material, manuals). They cannot replace the cited literature.

The article should be accompanied with a cover letter with the information about the author(s): surname, middle initial, first name, and citizen personal number, rank, title, e-mail address, and affiliation address, home address including municipality, phone number in the office and at home (or a mobile phone number). The cover letter should state the type of the article and tell which illustrations are original and which are not.