**SYNOPSIS**

Information security is an indispensable requirement in the present scenario, with increasing instances of unauthorized copying, reproduction and fabrication of information. Although many secret information-sharing schemes have been proposed in the recent years, they are vulnerable to impersonation and tapping. Steganography is a promising and popular method that conceals the secret in a multimedia carrier such as image, audio or video, such that it is unintelligible to unintentional recipients. The existing authentication schemes for image steganography do not do well to protect the integrity of the message. Consequently, it is difficult to recover the entire message without distortion and loss, leading to poor image quality and the benefit of doubt to the hacker.

We propose to address the issue of weak authentication, combined with the optimization of available hardware and software resources. Spatial Image Steganography intends to operate based on the physical location of the pixels in an image. So, a grayscale image is acquired and converted into a decimal array using LabVIEW. It is randomized into 2x2 blocks and stored in the SRAM of Altera DE1 Board (EP2C20F484C7). The secret message and authentication bits are embedded into the blocks using hardware. The final stego-image is reconstructed from the blocks, followed by simulation-based hardware architecture verification. FPGA is preferred for embedding, owing to its high-speed block processing, high intrusion resistance, huge internal storage and better performance in comparison to software platforms.

The image acquisition and processing are done using LabVIEW software. The DE1 Control Panel application is used to write/read the contents to/from the 256K x 16 bits *IS61LV25616* CMOSStatic RAM. Quartus II software is used to embed the secret and parity bits into the image blocks stored in the FPGA’s SRAM memory. The reconstruction of the image is accomplished using LabVIEW. Finally, the architecture is verified by simulation in Quartus II.

The proposed project has myriad applications in the field of medicine, defense, politics, banking etc. where confidentiality, integrity and authentication are of utmost necessity. The future feasible additions to this project might include multi-level nesting of secret images in the cover and successful recovery. Eg) Hiding two or more barcodes in one cover image. There is also a good prospect for works including an element to ensure non-repudiation.