ACKNOWLEDGEMENT

I extend my deep respect and gratitude to my research guide/supervisor Dr. Samir Kumar Bandyopadhyay, (Professor, University of Calcutta) for his valuable advises and support throughout the development of this research. I also express my whole-hearted thanks and respect to Prof. Tai-hoon Kim, Hannam University, Republic of Korea, for his unconditional support to make me carry out this research work.

I am grateful to Heritage Institute of Technology, Hannam University and The University of Calcutta, the Institutions I serve in, for its wonderful laboratories where one can culminate oneself. Finally, I thank all my colleagues for their tremendous support and help in creating a very encouraging and creative environment to work in.

I would like express my deepest gratitude to my dear wife Champa. She has been my most important support, giving me the strength to keep going.

Date: March 24, 2011.

Place: Kolkata

Debnath Bhattacharyya
Registration No. 3920 Ph.D. (Tech)
Abstract-In today’s world, many commercial systems work with handwritten signatures and
digital images comprising of a person’s identity which needs to travel through the internet. While
roaming through the internet, these data/images require a security system so that they are
apparently hidden or camouflaged to avoid any possible attack or fraud on them. This data/image
hiding procedure should obviously be reversible and loss-less so that the receiver receives it in
the equivalent integrated form. The handwritten signatures are either scanned or collected
through any suitable input device like Stylus and light pen. Several E-Commerce applications
like Net-banking, online credit card transactions etc and the Copy write protection, require the
above features. Again if the image comprises of any human signature, validation and
authentication of the same after receiving it at the recipient’s side requires a rigorous pattern
matching methodology.

This thesis attempts to present a complete package that will hide and encrypt an image (more
specifically a handwritten signature in BMP format) into another image which is ready to send
over the network from the Sender’s computer, the modified image when received is processed
through an algorithm to extract the original image at the Recipient’s computer. Afterwards,
automatic signature recognition and authentication is also done at the recipient’s side to ensure
either that the signature belongs to the claimed identity or that the data came from the authorized
origin as the case may be.

Thus the whole work can be broadly classified into four sub-parts, namely,

- Scaling of the Training(s) and the input images to a predefined size
- Data/Image Hiding at the Sender’s side
- Data/Image Extraction at the Recipient’s side
• Handwritten signature recognition and authentication at the Recipient’s side

Thus the end user need only install this package in his/her computer system and the rest will be taken care of by this product itself. This work has implemented using JAVA (J2EE as middleware server), so this is platform independent and portable. As this work involves several new developments in the area of image processing (e.g. it is going to introduce a new data/image hiding and extraction technique and a new handwritten signature authentication technique), it is a good candidate for research based project, but at the same time there is enormous scope of the work in both the commercial and non-commercial application areas.

In this thesis, I propose a novel Human Signature Authentication and IRIS Verification scheme; in which users or human can be identified by his/her Handwritten Signature and simultaneously that human also verified by his/her IRIS characteristic. Thus, a double way protection/security can be achieved by this system or scheme. Our authentication schemes also useful for the remote users.

This scheme supports most application environments and input devices, rather than being limited to small mobile devices (PDAs). This scheme will consume less magnetic storage for the sample images, as the images are bi-color images; will be digitized and converted into two-dimensional arrays. These arrays in turn will be used as training data during authentication. In this scheme, extraction of ‘region of interest’, image scaling (compressed or expanded into specific manageable size), thinning and protection during transmission also play a major role in particular.

At end, the Double-way protection will be achieved by these two parallel processes, namely, Handwritten Signature Authentication and IRIS Verification of a person.