A Challenge in E-Passport: 2D Human Skull Recognition using Mutual Information Algorithm with Passport Display Screen

C.V.Arulkumar
PG Scholar
Dept of Information Technology
SNS College of Technology
arulkumaran.ckpc@gmail.com

Prof.G.Selvavinayagam
Asst.Professor
Dept of Information Technology
SNS College of Technology
ohmselva@gmail.com

ABSTRACT

In today's world, security plays a vital role in all areas. In past few years terrorist attacks and illegal transportation across country borders has increased which cannot be controlled unless the present passport system is updated. Though tough passport verification processes are introduced in some European countries, still illegal passport exists. So in the motive to give hundred percent efficiency and assured security to passport, this paper proposes the much secured means of passport features through skull scanning in the area of biometric that can never be broken. Biometric, provides one of the most secure methods of authentication and identification. According to this paper it is designed in such a way that it is more efficient with Skull authentication comparing the existing e-passport with the biometric information like face recognition, Iris scan, Retina scan, Voice Matching of a person, RFID, Retina scan, Contactless smart cards. The RFID have some drawbacks in terms of cost, privacy and lack of standards. This paper proposes an idea that, every passport holder is given an own unique Login ID and password to access his passport through Reporting Centers. Once he lost his passport, he can update the status as INACTIVE, so that nobody can make use of passports by changing the face through plastic surgery or by modifying Iris, voice, etc so theft of passport can be prevented. For security enhancement in e-passport, certain reporting centers are localized in cities where e-passport holder's account is maintained and it is accessed by the e-passport holder by using his unique login ID & Password after skull scanning authentication at Reporting Centers. Biometric security feature electronic skull recognition and Passport Display Screen (PDS), adds security enhancement to e-passport.

This paper illustrates the need of skull structure biometric by mitigating the existing biometric techniques and thus we can avail the low cost and high secure e-passport design methodology.

Keyword: *Human Skull, ePassport, Prenology, MATLAB, 2D Rigid Body, PDS, Passport Display Screen*

INRTODUCTION

There are two types of passports, the normal passport and the ePassport. The difference between is that with the normal passports is utilized globally, every country has it but with the ePassport, only in some countries people are allowed to possess. These two passports serve the same purpose but in different ways. When you are traveling with the normal passport, the airline attendants will perform a passport number search to ensure that you are the right full owner of the passport. With an ePassport, due to the fact that it is biometric, they do not have to do a passport search to identify you they can use your thumb prints, or even scan your eyes as a way of identifying[2]. ePassports are preferable because they are a safeguard against people, who are out to steal your identity. The security ePassport provides to it's so thick in that it is highly unlikely for one to penetrate and try and make an exact replica of your passport. The only disadvantage with ePassport is that it is offered in a few countries so not everyone benefits from their fineness.

The word "biometrics" comes from the Greek language and is derived from the words bio (life) and metric (to measure)[3]. This paper will refer to biometrics as the technologies used to measure and analyze personal characteristics, both physiological and behavioral. These characteristics include fingerprints, voice patterns, hand measurements, irises and others, all used to identify human characteristics and to verify identity.

These biometrics or characteristics are tightly connected to an individual and cannot be forgotten, shared, stolen or easily hacked[2]. These characteristics can uniquely identify a person, replacing or supplementing traditional security methods by providing two major improvements: personal biometrics cannot be easily stolen and an individual does not need to memorize passwords or codes. Since biometrics can better solve the problems of access control, fraud and theft, more and more organizations are considering biometrics a solution to their security problems. However, biometrics is not a panacea and has some hurdles to overcome before gaining widespread use[3].

This paper will discuss the recent history of biometrics, benefits of biometrics over traditional authentication methods, some of the most widely used biometric technologies and the issues surrounding biometrics to include issues standing in the way of widespread biometric implementation.

The past development of two disciplines, Phrenology and Anthropometry, helped to pave the way for biometrics. Phrenology, the study of the structure of the skull to determine a person's character and mental capacity, was founded by Franz Joseph in early nineteenth century Germany. Although long considered a pseudoscience lacking real scientific merit, Phrenology remained popular, especially in the United States, throughout the 19th century and still has advocates today.

The Digital image processing is the use of computer algorithms to perform image processing on digital images[1]. It allows a much wider range of algorithms to be applied to the input data and can avoid problems such as the build-up of noise and signal distortion during processing.

Since images are defined over two dimensions (perhaps more) digital image processing may be modeled in the form of Multidimensional Systems[2]. In particular, digital image processing is the only practical technology for Classification and Feature Extraction. A learning classifier is able to learn based on a sample.

Here, the median filter is one of the basic building blocks in many image processing situations. However, its use has long been hampered by its algorithmic complexity of O(r) in the kernel radius. With the trend toward larger images and proportionally larger filter kernels, the need for a more efficient median filtering algorithm becomes pressing. In this correspondence, a new, simple yet much faster algorithm exhibiting O(1) runtime complexity is described and analyzed. It is compared and benchmarked against previous algorithms.

The median filter is a canonical image processing operation, best known for its salt and pepper noise removal aptitude. It is also the foundation upon which more advanced image filters like unsharp masking, rank-order processing, and morphological operations are built[2]. Higher-level applications include object segmentation, recognition of speech and writing, and medical imaging. shows an example of its application on a high-resolution picture.

In this correspondence we propose a simple $O(1)$ median filtering algorithm. We show a few straightforward optimizations which enable it to become much faster than the classic algorithm[1]. We take the opportunity to examine why lower bound of $O(\log r)$ does not seem to hold. Then we explore extensions to the new filter, namely application to higher-precision or higher-dimensional data as well as a circular kernel approximation[2]. Finally, timing results are shown, asserting the practicality of this approach.

Thresholding with hysteresis requires two thresholds – high and low. Making the assumption that important edges should be along continuous curves in the image allows us to follow a faint section of a given line and to discard a few noisy pixels that do not constitute a line but have produced large gradients.

EXISTING SYSTEM

Finger-Scan Technology

Finger-scan technology is the most commonly deployed biometric technology, used in a broad range of physical access and logical access applications. A normal fingerprint pattern is made up of lines and spaces. These lines are called ridges while the spaces between the ridges are called valleys. It is through the pattern of these ridges and valleys that a unique fingerprint is matched for verification and authorization [4].

Though Finger-scan technology is proven and capable of high levels of accuracy, there are some weaknesses to finger-scanning. There are certain ethnic groups that have lower quality fingerprints than the general populations. Another problem is that over time, sometimes in as short a period as few months, the fingerprint characteristics of an individual can change, making identification and verification difficult[4].

Facial-Scan Technology

This technology is considered a natural means of biometric identification since the ability to distinguish among individual appearances is possessed by humans. Facial-scan systems can range from software-only solutions that process images processed through existing closed-circuit television cameras to full fledged acquisition and processing systems, including cameras, workstations, and backend processors. Facial-scanning technology has a poor record in verifying a subject who has had plastic surgery to alter their appearance[5].

Retinal-Scan Technology

Retina-scan technology makes use of the retina, which is the surface on the back of the eye that processes light entering through the pupil. Retinal Scan technology is based on the blood vessel pattern in the retina of the eye. The principle behind the technology is that the blood vessels at the retina provide a unique pattern, which may be used as a tamper-proof personal identifier[6].

Iris-Scan Technology

Iris scans examine the colored tissue surrounding the eye's pupil. The iris is a muscle within the eye that regulates the size of the pupil, controlling the amount of light that enters the eye. It is the colored portion of the eye with coloring based on the amount of melatonin pigment within the muscle. Although the coloration and structure of the iris is genetically linked, the details of the patterns are not [7].

The iris develops during prenatal growth through a process of tight forming and folding of the tissue membrane. Prior to birth, degeneration occurs, resulting in the pupil opening and the random, unique patterns of the iris. Although genetically identical, an individual's irides are unique and structurally distinct, which allows for it to be used for recognition purposes[7]. Iris scanning technology is far from foolproof however scanners have been fooled by users placing photographs of irises over their own eyes (with holes cut out for their own pupils)[7].

DRAWBACKS OF EXISTING SYSTEMS

Table A (Disadvantage of Existing Systems)

Sl.No	Biometrics	Strengths	Weakness	Suitable Application
1.	Fingerprint	Very stable over time Uniqueness	Potential user resistance Requires user training	IS access control Workstation access Control Physical access
2.	Facial Recognition	Universally present	Cannot distinguish between identical siblings Religious or cultural prohibitions	Physical access control
3.	Voice verification	Good user acceptance Low training	Unstable over time Changes with time	Mobile phones Telephone banking
4.	Retina scanning	Stable over time Uniqueness	Requires user training High user resistance Slow read time	IS access control Physical access control
5.	Iris scanning	Very stable over time Uniqueness	Potential user resistance Requires user training Dependant.	Physical access control ATMs and airline Tickets

To summarize, physiological biometrics is unchanging and unalterable, but is perceived as being more invasive and raises privacy concerns more quickly. On the other hand, behavioural biometrics are partly derived from physiology; an individual's voice depends on the shape of the vocal chords, an individual's signature depends on the dexterity of hands and fingers and an individual's face might depend or change based on the individual's behaviour.

In other words, behavioral biometrics is less stable, changes with stress and sickness and is less secure, but has a significant advantage over physiological-based biometrics because the verification process can be potentially "invisible" to the user. Further state that behavioural-based biometric security systems are more acceptable to users than physiological-based biometric security systems because they are perceived to be less obtrusive and less intrusive e.g.:

1. There have been some concerns over the widespread acceptance of fingerprint verification due to its association with crime. It mentions that although fingerprint verification seems to be socially 1. doubtful, it appears to be legally acceptable[4].

2. It is interesting to note that some characteristic of physiological-based biometric methods makes them more acceptable than behavioral-based biometric methods e.g. voice verification appears to be more acceptable than other behavioral-based biometric methods. The reason could be that the verification of an individual's voice is perceived to have more in common with fingerprint and retina verification procedures (physiological) than signature verification procedures.

PROPOSED SYSTEM

Human Skull Registration

Skull recognition, a biometric, provides one of the most secure methods of authentication and identification thanks to the unique characteristics of the skull. With an ePassport, due to the fact that it is biometric, forensic people do not have to verify your password identity by means of your thumb prints or even scan your retina, iris as a way of identifying the personnel.

Thus the ePassport is designed in such a way that, once it is scanned at the immigration, the login page of the user gets displayed. The Active Status is checked parallel. It is a secure way that alleviates all other existing methods and it can be used as a cost effective way to provide a secure ePassport.

Phrenology

Phrenology is the study of the structure of the skull in Fig.1 to determine a person's character and mental capacity. This pseudoscience is based upon the false assumption that mental faculties are located in brain "organs" on the surface of the brain and can be detected by visible inspection of the skull.

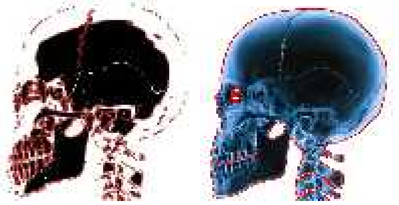


Figure No 1 Human Skull for preprocessing

Although phrenology has been thoroughly discredited and has been recognized as having no scientific merit, it still has its advocates. It remained popular, especially in the United States, throughout the 19th century and it gave rise to several other pseudoscientific characterologies, e.g., craniometry and anthropometry. Phrenology was highly praised by Ralph Waldo Emerson, Horace Mann, Thomas Edison, and Alfred Russell Wallace. For the security reasons for ePassport enhancement, we are extracting the skull structural characteristics from the phrenology concept. It is impossible to change the skull structure when the human is alive, and hence it increases security in biometrics.

Datacenter are used for storing the personal identities of ePassport holder, and the normal way of security algorithms can be implemented in the same networked environments. For securing the database, Database administrators prefer the hashing algorithms and Message Digest 5 (MD5) algorithms in which the original information will not be tracked easily.

The Indian Government has been quite focused on e-governance, on using the Internet to communicate, and other uses of technology. The ePassport was initially introduced by Pranab Mukherjee last year. And this recent news article confirms that the first set of ePassports will soon be doled out to the public. Now, the conventional passport contains, name, address, age proof. But the new ePassport will have all the personal details, including finger-prints of the person carrying it. Currently, the ePassport programme is available to diplomats and Government officials. And now, everyone would have access to it. In accordance with this, we propose the skull scanning biometric for the enhanced security in EPassport, to secure our nation.

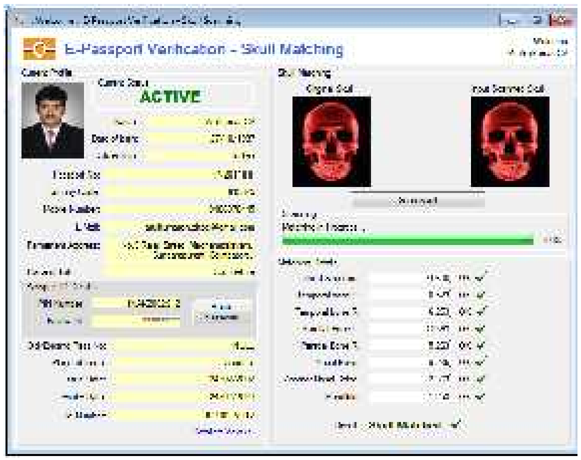
ADVANTAGES OF PROPOSED SYSTEMS

Table B (Advantages of Proposed System)

Sl.No	**Advantages**	Why?	Improvements
1.	No PINs	Cuts down on support costs	Efficiency
2.	Known user	Confidence in information	Decision making
3.	Cannot be sheared	Integrity of information upheld	Reliability
4.	Use of template	Cannot recreate biometric	Security
5.	Levels of security	Adjust to needs of business	Customizability
6.	Increased security	Biometric information cannot be lost	Security
7.	Increased convenience	Biometric information always present	User acceptance
8.	Reduced costs	Eliminate the overhead of password management	Economical

EXPERIMENTAL ANALYSIS

Large-scale biometrics systems such as Automated Fingerprint Identification System (AFIS) have been in use with great success for many years, and provide valuable lessons to developers of ePassport systems. Image quality, enrollment efficiency, data interoperability, and robust networking are challenges that have been addressed in AFIS, and should also be addressed in ePassport systems. Anticipating these issues early in the development of ePassport systems will significantly reduce risks and costs associated with fixing problems after systems have already deployed. The above figure 4.2 depicts the system architecture that must preprocess and stores in trained datasets and to be implemented in the immigration centre and the reporting centre for skull recognition in the passport holder's information to conceive the identity.



E-Passport Verification - Skull Matching

ACTIVE

Fig: 2 Implementation of Skull matching in MATLAB

MATLAB functionality supports for the design of new e-passport design and verification method, the Mutual Information algorithm can be used for these type of medical images. The parameters from the skull can be given into the proposed system and Entropy, mean, variance are calculated for the matching parameters, as given above the e-passport verification can be handled and it may pursuit the profile of the user.

DATAFLOW DIAGRAM

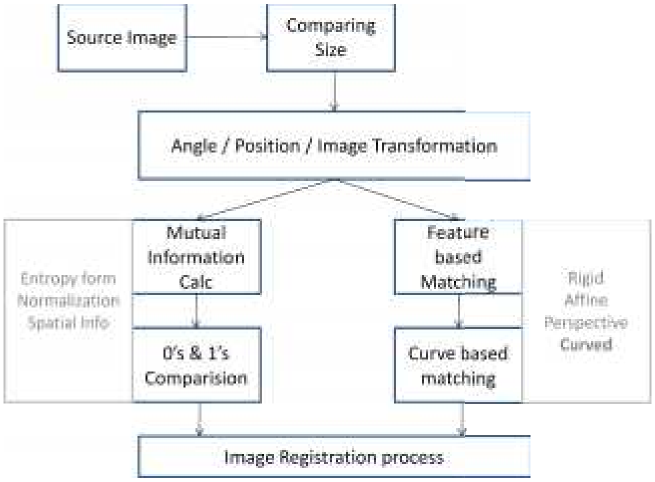


Fig:3 (System Architecture of the proposed Skull Registration using Mutual Information Algorithm)

The benefits, of course are humongous, starting from easy issuing, to enabled verification. It is expected to result in the issue of passports within three days and in cases requiring police verification, within three days after completion of the verification process. Tatkal passports would be issued on the day of submission of the application. The Government has planned to have 68 passport facilitation centres across the country to verify documents and decide on granting the passport. Police verification would be expedited through electronic linkage of these facilitation centres with the police authorities in State capitals.

Mutual-Information-Based Registration

The aim of the survey is threefold: an introduction for those new to the field, an overview for those working in the field, and a reference for those searching for literature on a specific application. Methods are classified according to the different aspects of mutual-information-based registration. The main division is in aspects of the methodology and of the application. The part on methodology describes choices made on facets such as preprocessing of images, gray value interpolation, optimization, adaptations to the mutual information measure, and different types of geometrical transformations. The part on applications is a reference of the literature available on different modalities, on interpatient registration and on different anatomical objects.

ENTROPY

This field concerns the broadcast of a message from a sender to a receiver. The first attempts to arrive at an information measure of a message focused on telegraph and radio communication, sending Morse code or words. However, picture transmission (television) was already considered in the important paper by Hartley [3]. In 1928, he defined a measure of information of a message that forms the basis of many present-day measures. where is a constant depending on the number of symbols . He further assumed that, given messages of length and from and numbers of symbols, respectively, if , i.e., the number of possible messages is equal, then the amount of information per message is also equal. These two restrictions led him to define the following measure of information:

$$H - n \log s - \log s^{n}$$

A drawback of Hartley's measure is that it assumes all symbols (and, hence, all messages of a given length) are equally likely to occur. Clearly, this will often not be the case. In the
previous paragraph, for example, the letter "e" has occurred 229 times and the letter "q" only twice. Shannon introduced an adapted measure in 1948 [4], which weights the information per outcome by the probability of that outcome occurring. Given events occurring with probabilities , the Shannon entropy is defined as

$$H = \sum_i p_i \log \frac{1}{p_i} = \sum_i p_i \log p_i.$$

If we apply to Shannon's entropy the assumption that all outcomes are equally likely to occur, we get

$$H = -\sum \frac{1}{s^n} \log \frac{1}{s^n} = \sum \frac{1}{s^n} \log s^n = \log s^n$$

Data Flow Explanation - Mutual Information

Most books on information theory ([16]–[18], for example) discuss the notion of mutual information. The definition of the term, however, can be presented in various ways. We will next treat three frequently used forms of the definition, because more than one is used in the literature. All three forms are identical; each can be rewritten into the other two1 . Each form of definition, however, explains the relation to registration in a different way. We will describe mutual information for two images, as used in image registration, and not in a general sense. The first form of definition we discuss is the one that best explains the term "mutual information." For two images and, mutual information can be defined as

$$I(A, B) = H(B) - H(B \quad A)$$

where is the Shannon entropy of image , computed on the probability distribution of the gray values. Denotes the conditional entropy, which is based on the conditional probabilities, the chance of gray value in image given that the corresponding voxel in has gray value . When interpreting entropy as a measure of uncertainty, (5) translates to "the amount of uncertainty about image minus the uncertainty about when is known." In other words, mutual information is the amount by which the uncertainty about decreases when is given: the amount of information contains about . Because and can be interchanged, is also the amount of information contains about. Hence, it is mutual information. Registration is assumed to correspond to maximizing mutual information: the images have to be aligned in such a manner that the amount of information they contain about each other is maximal. The second form of definition is most closely related to joint entropy. It is

$$I(A,B) = H(A) - H(B) - H(A,B),$$

This form contains the term , which means that maximizing mutual information is related to minimizing joint entropy. We have described above how the joint histogram of two images' gray values disperses with misregistration and that joint entropy is a measure of dispersion. The advantage of mutual information over joint entropy per se, is that it includes the entropies of the separate images. Mutual information and joint entropy are computed for the overlapping parts of the images and the measures are therefore sensitive to the size and the contents.

E-PASSPORT WITH DISPLAY SCREEN

The proposed idea is to make the passport in the form of a CARD and as a secured one too. Already there are usages and research & development being done on e-passports in some countries like USA, Indonesia etc. These e-passports are used for user data security and to improve accuracy in the verification of the right passenger identification. Even though it is secured than the old passports, here usage of a passport book is repeatable. To make it easier, the smart card can be used as the passport. In SMART Passport each and every passport holder will be given a unique identity number based on some norms which is proposed in this project. The biometrics and RFID tag is used here are for the identification and authentication purposes. Each and every smart passport holder will have their own secret key which is used as a decryption key and based on this key and the data stored in the RFID tag is used to make the passengers as an authenticated person. All the details of the passengers can be centralized throughout the world with the help of Cloud Computing Technique. This SMART PASSPORT will be comparatively good in security, portability and centralization which are the required parameters in the passport for today's world.

The Proposed E-Passport is replaced with RSIM module instead of RFID module, this passport also known as "Digital E-Passport' with PDS (Passport Display Screen).

Fig: 4. E-Passport with Passport Display Screen (PDS)

This passport can be used with the help of satellite communication and the data's are stores in the remote server, so that no one can hack this passport data and there is no way for fake passport. Here is the block diagram of E-Passport is given, in that new proposed circuit is used with the RSIM module, The skull scanning technique provides a way to avoid the use of fake passports. We have also planned to introduce PDS (Passport Display Screens) directly in e-passports which provide the ease of usage. When the passport holder update the status as INACTIVE using his unique PIN (Passport Identification Number) & Password at Reporting Centers after the proposed biometric technique, the e-passport updates the status as LOCKED. So it never gives the chance to any third-parties to steal or to use the lost e-passport illegally. Though this plan gives high-tech tight security, the cost effective implementation is currently under our study.

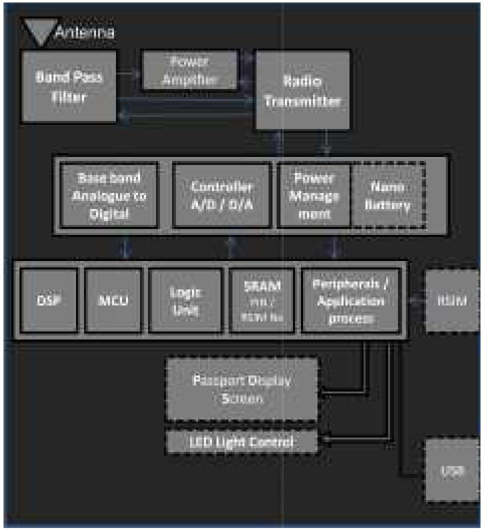


Fig: 5. Proposed E-Passport circuit block diagram

CONCLUSION

This paper proposes the security enhancement in E-Passport to the governing authority. Skull related Biometrics allow for increased security, convenience and accountability while detecting and deterring fraud. One of the continuing challenges for the biometric industry is to define the environment in which the technology provides the strongest benefit to individuals and institutions.

In the same manner, we can implement this in case of issuing E-Passport. In future, we can implement the distributed networked environment for securing the datacenter as well as other secured and commercial applications, we planned to adopt biometrics technique to bring the tight security for the end users and hackers.

REFERENCES

1. Hamdan.O.Alanazi, B.B Zaidan, A.A Zaidan 3D Skull Recognition Using 3D Matching Technique, Journal Of Computing, Volume 2, Issue 1, December 2010, Issn 2151-9617.
2. Xiaoyang Tan and Bill Triggs, Enhanced Local Texture Feature Sets for Face Recognition Under Difficult Lighting Conditions, IEEE Transactions On Image Processing, vol. 19, no. 6, june 2010
3. Fanglin Chen, Jie Zhou, Senior Member, IEEE, and Chunyu Yang, Reconstructing Orientation Field From Fingerprint Minutiae to Improve Minutiae-Matching Accuracy. IEEE Transactions On Image Processing, VOL. 18, NO. 7, JULY 2009.

4. Medha V. Wyawahare, Dr. Pradeep M. Patil, and Hemant K. Abhyankar, Image Registration Techniques: An overview. International Journal of Signal Processing, Image Processing and Pattern Recognition Vol. 2, No.3, September 2011.
5. Satyanadh Gundimada and Vijayan K. Asari*, Senior Member, IEEE.* Facial Recognition Using Multisensor Images Based on Localized Kernel Eigen Spaces. IEEE Transactions On Image Processing, VOL. 18, NO. 6, JUNE 2011
6. Gajanand Gupta, Algorithm for Image Processing Using Improved Median Filter and Comparison of Mean, Median and Improved Median Filter. International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, Issue-5, November 2011.
7. Rishi R. Rakesh, Probal Chaudhuri, and C. A. Murthy, Thresholding in Edge Detection: A Statistical Approach. IEEE transactions on image processing, vol. 13, NO. 7, JULY 2009.
8. Guoping Qiu, An Improved Recursive Median Filtering Scheme for Image Processing. IEEE Transactions On Image Processing, Vol. 5, NO. 4, APRIL 1996.
9. Lin Xu and Justin W.L. Wan, Real-Time Intensity-Based Rigid 2D-3D Medical Image Registration Using RapidMind Multi-Core Development Platform. IEEE transactions on image processing, vol. 13, NO. 7, JULY 2009.