

Casino Exclusion Technique Exploration - Framework Development

B. T. DUDLEY MSc (Image Analysis, UNP, Cum Laude)
882207268

Submitted in partial fulfilment of the academic requirements for the degree of
MASTERS IN BUSINESS ADMINISTRATION

882207268

Graduate School of Business, Faculty of Management
University of Natal (Durban)

Supervisor: Adv. L. K. Gibson (B. Com Hons (Bus Econ), LLB, MCSSA)

September 2003

Confidentiality Clause

19 SEPTEMBER 2003

TO WHOM IT MAY CONCERN

RE: Confidentiality Clause

Due to the strategic importance of this research it would be appreciated if the contents remain confidential and not be circulated for a period of two (2) years.


Sincerely

B. T. DUDLEY


Declaration

This research has not been previously accepted for any degree and is not being currently submitted in candidature for any degree.

The opinions expressed in this document are the views of the author alone and do not necessarily reflect those of the views of Intervid, Intervid Technologies, Intervid International, the National Gambling Board, any Provincial Gambling Board, casino, casino management, casino employee or any other party.

Signed.....

B. T. DUDLEY

Date..........2003

Acknowledgements

I would like to thank the following for the loan of biometric systems:

Dex Security Solutions (www.dex.co.za) for a fingerprint reader and software
Identix Incorporated for FACE IT - Debbie, Pam and wonderful Alex Eastwood
Acscs Biometrics Corp. - - Ashley Kelly, for a 3D face recognition system
Intervid for an Iris recognition system

This thesis would not have been possible without the help and support of numerous people, to whom my appreciation is extended:

Lee Gibson: Graduate School of Business

The lecture's from the GSB who often had to work under difficult conditions,

Headley Davidson: Cynaps Access Control,

Dennis De Beer: Gold Reef City Casino Complex Surveillance & Security manager

Rudi Coetzee: Chief Gaming Auditor and his staff from Western Cape Gambling and Racing Board

Johan Van Wyk and Jan Visagie: Grand West Casino

Yagan and Walter: Intervid SA casino division

Rob and Chris Le Seuer: Tech Pro SA

Dr. Clive Putman and Intervid Technologies for the time to do this dissertation

Mark Ross for formatting

Ingrid and David Dudley

My Girlfriend for her critical review, with the promise to make up for lost time

Fellow MBA students and friends at the GSB for their advice and help

Finally, and most importantly, my family, colleagues and friends for their much needed emotional support and encouragement throughout the course of this work.

Abstract

The new National Gambling Bill introduces a system of voluntary and court-ordered exclusion of problem gamblers from casinos. A wide range of exclusion techniques for access control could be applied to South African casinos. However, there are no clear criteria on which to base the decision of which system is to be implemented. Various role players need to be considered to determine what can be deployable in casino applications.

A framework, from a business perspective, is proposed which allows multiple role players and varied criteria to effectively evaluate a range of possible solutions. The framework is applied to the role players affected by the proposed exclusion of problem gamblers from gambling. The main role players evaluated a number of possible exclusion techniques according to a range of important criteria.

The current solution of a security guard at the entrance is superior according to the casino operations department. The casino marketing division places a high emphasis on ease of use for the public. Of the alternative solutions, comparison-based solutions (using an identity book) were preferred by Gambling Anonymous while card-based solutions (proximity card) was found to be preferable by the public. The casino surveillance department preferred non-contact, overt, biometric acquisition (such as iris recognition).

Covert biometric acquisition (face recognition) is found to be the most acceptable to all the role players, with fingerprint recognition being the least acceptable. The application of the framework allowed multimodal exclusion techniques (face recognition linked to casino loyalty cards) to emerge as a promising way forward.

Key words

National Gambling Bill, problem gamblers, casino, framework development, business perspective, evaluate, exclusion techniques, surveillance, face recognition

Table of Contents

	PAGE
Title Page	i
Confidentiality Clause	ii
Declaration.....	iii
Acknowledgements	iv
Abstract.....	v
Key words.....	v
Table of Contents.....	vi
List of Figures.....	viii
List of Tables	ix
Chapter 1 Introduction	1
1.1 Introduction	1
1.2 Problem Statement.....	2
1.3 Objectives of the Study.....	2
1.4 Background of the Research.....	3
1.5 Motivation for the Research	5
1.6 Value of the Project	8
1.7 Establishing the Business Case.....	12
1.8 Limitations of the Project	13
1.9 Assessing the Casino Application	14
Chapter 2 Exclusion Techniques.....	17
2.1 Introduction	17
2.2 Current Solutions.....	18
2.3 Alternative Solutions	19
2.3.1 Comparison Based Solutions.....	19
2.3.2 Card Based Solution	19
2.3.3 Biometrics.....	20
2.3.3.1 Biometrics Defined.....	20
2.3.4 Biometrics' Basic Components and Processes.....	21
2.3.4.1 The Generic Biometric System.....	21
2.3.4.2 Data Collection	22
2.3.4.3 Sensor (Acquisition Device).....	24
2.3.4.4 Transmission.....	25
2.3.4.5 Feature Extraction.....	25
2.3.4.6 Signal Processing.....	26
2.3.4.7 Decision	27
2.3.4.8 Storage	28
2.3.4.9 Template	28
2.3.4.10 Contact Biometrics	30
2.3.4.11 Non-Contact Biometrics	31
2.3.5 Which is the Best Biometric Technology?	31
2.4 Research Methodology	34

2.5	Key performance Metrics.....	35
2.5.1	Cost	36
2.5.2	Ease of Use for the Public	38
2.5.3	Physical Contact	39
2.5.4	Accuracy.....	40
2.5.5	Response Time.....	43
2.5.6	Intrusiveness	43
2.5.7	Distinctiveness (Unique Identifiers)	45
2.5.8	Human Factor Limitations.....	45
2.5.9	Environmental Affects	46
2.5.10	Stability of Trait.....	46
2.5.11	User Acceptability	47
2.5.12	Market Share by Technology	47
2.5.13	Mature Technology.....	48
2.5.14	False Acceptance	48
2.5.15	False Rejection.....	49
2.5.16	Template Size (bytes).....	50
2.5.17	Remove Security Threats	51
2.5.18	Level of Impact on Existing System and Processes.....	52
2.5.19	Compatibility with Existing Data	53
2.5.20	Identification of High Rollers (VIP's).....	53
2.5.21	Verification / Identification	53
2.5.22	Overt / Covert Acquisition	56
2.5.23	Behavioural / Physiological.....	57
2.5.24	Give / Grab Acquisition	57
2.5.25	Privacy Risk Rating	57
Chapter 3	Role Players.....	59
3.1	Introduction	59
3.2	Marketing.....	61
3.3	Operations Management (Process control)	63
3.4	Surveillance	64
3.5	Security	66
3.6	Privacy Rating	67
3.7	Gambling Board	69
3.8	Gambling Anonymous.....	72
3.9	Public	73
3.10	Weighting of Role Player Importance	75
Chapter 4	Results.....	76
4.1	Role Player Rating of Exclusion Techniques.....	76
Chapter 5	Evaluation & Recommendations.....	83
5.1	Most Acceptable Exclusion Techniques.....	83
5.2	Multiple-Exclusion Systems	86
	Bibliography	87
	References	88
	Definitions	93
	Appendices	I
	Appendix I – Results of Role Player Evaluation	I
	Appendix II – Role Player Evaluation of Evaluation Techniques.....	V

List of Figures

	PAGE
Figure 1. 1. Biometric Revenue, 2002-2007	7
Figure 2. 1. Generic biometric system	21
Figure 2. 2. Biometric Matches	29
Figure 2. 3. Biometric template encryption	29
Figure 2. 4. Fingerprint recognition proposed for US entry	31
Figure 2. 5. Zephyr Analysis to determine the “ideal” biometric	32
Figure 2. 6. Example of face and iris recognition	37
Figure 2. 7. Remote optical head for iris recognition	37
Figure 2. 8. Performance matrix by biometric technologies	39
Figure 2. 9. Face recognition accuracy test	42
Figure 2. 10. Market Share by Technology	47
Figure 2. 11. Detection error trade off: FAR VS FRR	49
Figure 2. 12. Failure to enrol rate (based on 3 attempts)	49
Figure 2. 13. Biometric Template size	51
Figure 3. 1. Casino marketing - weighting of selection criteria	62
Figure 3. 2. Casino processing - weighting of selection criteria	64
Figure 3.3. Casino surveillance - weighting of selection criteria	65
Figure 3. 4. Hemingway’s casino excluding problem gamblers.	66
Figure 3. 5. Casino security - weighting of selection criteria	66
Figure 3. 6. Privacy issues - weighting of selection criteria	70
Figure 3. 7. Gambling Board - weighting of selection criteria	70
Figure 3. 8. Gambling Anonymous - weighting of selection criteria	73
Figure 3. 9. Public - weighting of selection criteria	74
Figure 3.10. Weighting of Role Player Importance	75
Figure 4. 1. Casino marketing department evaluation of exclusion techniques	76
Figure 4. 2. Face recognition evaluation by casino role players	76
Figure 4. 3. Casino operations department evaluation of exclusion techniques	77
Figure 4. 4. Guard at the entrance evaluation by casino role players	77
Figure 4. 5. Iris recognition evaluation by casino role players	78
Figure 4. 6. Casino surveillance department evaluation of exclusion techniques	78
Figure 4.7. Casino surveillance department evaluation of exclusion techniques	79
Figure 4. 8 Casino surveillance department evaluation of exclusion techniques	79
Figure 4. 9. Gambling Board evaluation of exclusion techniques	80
Figure 4. 10. Fingerprint recognition evaluation by casino role players	80
Figure 4. 11. Gambling Anonymous evaluation of exclusion techniques	81
Figure 4. 12. Iris recognition evaluation by casino role players	81
Figure 4. 13. Fingerprint recognition evaluation by casino role players	82
Figure 4. 14. Iris recognition evaluation by casino role players	82
Figure 5. 1. Exclusion techniques calculated by role players	83
Figure 5. 2. The most desirable exclusion technique for casinos	84
Figure 5. 4. Surveillance Information Network (Sin) Report	84

Figure	5. 3. Suspect demographics	85
Figure	5. 5. Face recognition match - One of nine	85
Figure	5. 6. Multimodal solution – face recognition linked to a swipe card	86

List of Tables

	PAGE	
Table	1. 1. Benefits of Exclusion Technology in Casinos.....	9
Table	1. 2. Accumulative Monthly Casino Tax	10
Table	2. 1. Sample types associated with each biometric technology	22
Table	2. 2. Acquisition devices associated with biometric technology.....	24
Table	2. 3. Common characteristics used in feature extraction	25
Table	2. 4. Investigated Exclusion and Access Control Solutions.....	34
Table	2. 5. Biometric comparisons.....	35
Table	2. 6. Biometric Technology Comparison.....	41
Table	3. 1. Law enforcement statistics	71
Table	I. 1. Marketing evaluation	I
Table	I. 2. Process evaluation	I
Table	I. 3. Surveillance evaluation	II
Table	I. 4. Security evaluation	II
Table	I. 5. Privacy rating evaluation	III
Table	I. 6. Gambling Board evaluation	III
Table	I. 7. Gambling Anonymous evaluation.....	IV
Table	I. 8. Public perception evaluation	IV
Table	II. 1. Weighted evaluation of multiple exclusion techniques.....	V

Chapter 1 Introduction

1.1 Introduction

The new National Gambling Bill, introduced into parliament on 20 August 2003 introduces a system of voluntary and court-ordered exclusion of problem gamblers from gambling. Parliamentary committee chairman, Rob Davies, says the effect of gambling goes beyond addictive or compulsive gambling and incorporates the social context. As such, the committee would want to strengthen the provisions for the exclusion of problem gamblers from casinos (Minister to get powers to issue casino licences, Business Day, Thursday 21 August 2003, Pg 2). The bill proposes the establishment of norms and standards for provinces as well as and standards for gambling premises. A wide range of exclusion techniques to remove problem gamblers could be applied in South African casinos. However, there are no criteria on which to base the decision as to which technology to apply. Various role players need to be considered to determine what solutions might be acceptable to deploy in casino exclusion applications. From a business perspective which modus operandi for excluding categorised gamblers from South African casinos would be the best to use?

Surveillance and real-time screening applications will inevitably see broader deployment, despite the inherent difficulties encountered in the casino environment. However, a biometric based exclusion technique is uniquely capable of identifying an individual in an automated fashion – and in some circumstances without the individual's knowledge or consent. Historically, decisions concerning exclusion techniques for casinos have been made according to either single criteria or multiple criteria. Single criteria are often legislative reasons while multiple criteria often do not take into consideration the multiple role players involved. A method to evaluate a large number of possible exclusion techniques according to a range of criteria important to the selected role players, is proposed.

1.2 Problem Statement

Problem gamblers, gambling addicts and unwelcome customers are required to be removed from South African casinos. The South Africa casino industry is required to detect the presence of problem gamblers in casinos (National Gambling Act, 1098. 3 of July 1996, 33 of 1996). In addition to legislative requirements, it is also in the best interest of casino management to be able to identify certain already identified gamblers (patrons) in the following three categories:

- 1) Those people with a gambling addiction, who ban themselves from the casino, (as required by Regional Gambling Boards);
- 2) Those who are known card sharks / card counters (undesirables) and
- 3) High rollers (VIP's).

Exclusion techniques, in collaboration with access control, may assist in identifying addicted gamblers, recognise known casino felons and enhance the gambling experience for casino VIP's. Is there an effective substitute to current manual identification, possibly by creating highly accurate digital records of an individual's physiological features? Such a solution must not negatively affect a role player, which would either limit the effectiveness or result in reduced implementation. Furthermore certain criteria may be overlooked, rendering the exclusion technology and technique inefficient. These two aspects are addressed by the study.

This study proposes a "scorecard" framework, which will facilitate casinos' (any of the existing 28 or 12 remaining licenses) selection of exclusion techniques appropriate for their contingent (business and industry) requirements.

1.3 Objectives of the Study

This study sets out to derive the pre-eminent exclusion technique for the casino environment, which would also be the most appropriate for access control in SA casinos.

No pre-developed instrument could be found. Therefore this study set out to develop a theoretical “scorecard” framework upon which the various available exclusion techniques and corresponding technologies) can be evaluated on the basis of clearly defined criteria, by the multiple role players, from an industry and business perspective.

Then in practice to use the “scorecard” for evaluation of a number of possible exclusion techniques (13 in total) by the multiple role players (8 in total) according to a range of important criteria (25 in total).

The “multiple role players” mentioned include the casino divisions, legislature and public affected by the proposed exclusion of problem gamblers from casinos and “exclusion technologies ” include existing and novel access control technologies, used for the exclusion of problem gamblers, available to SA casinos.

1.4 Background of the Research

The system of voluntary and court-ordered exclusion of problem gamblers, which the new National Gambling Bill introduces, provides an incentive for the review of existing exclusion techniques in casinos. An increased understanding of the limitations of today’s exclusion techniques is required, along with a clear definition of criteria which exclusion technologies must meet and exceed in order to be considered deployable in casino applications. Exclusion technologies have been subjected to unsubstantiated claims regarding accuracy, scalability, response time, and real-world effectiveness. Current technologies require a previously absent realism must be injected into the general discourse on exclusion systems. Therefore, an increased emphasis is placed on objective performance data, on real-world as opposed to laboratory-based capabilities, on adherence to standards, and on the ability to impact positively on current systems and processes.

Exclusion techniques may offer effective, low cost solutions that could streamline

traditional, labour intensive processes in access control. All of the access control techniques vary in the degree of intrusiveness and user friendliness. These systems recognise features such as the presence of a card or identity document, an iris, a voice, a signature, a fingerprint, a hand or a face. Will the proffered techniques enable casinos to have control over problem gamblers without inconveniencing or embarrassing the customer?

Determining which exclusion techniques to deploy in controlling access in the casino environment has become a major portion of a casino's overall access control implementation strategy. It is generally understood that access control techniques do not provide 100% accuracy, and are particularly prone to non-matching in one-to-many applications. Exclusion techniques are often difficult to use and operate, incompatible with legacy systems, and their performance often varies according to the gender, ethnicity, demographic group, and age group of the enrolled user. This study will focus on what exclusion techniques can realistically deliver, both from the short and long-range potential, in access control for casinos.

Independent, scenario-based, comparative exclusion technique testing to assess the real-world performance of leading exclusion technologies, and to provide casinos, integrators, technology firms, and government agencies with objective information on biometric system capabilities is required. Understanding exclusion technologies' accuracy and performance under real-world conditions is a precondition of effective deployment. Error rates encountered by actual users, including false match rates, false non-match rates, and failure to enrol rates, often differ from error rates generated in laboratory tests using databases of biometric samples (Comparative Biometric Testing, Available online at: http://www.ibgweb.com/reports/public/comparative_biometric_testing.html).

Testing protocols need to emulate real-world conditions, focusing on cooperative users with little or no biometric experience. Careful control of the testing conditions should be an essential component of biometric testing. Environmental factors, such as background noise and lighting are controlled for different biometric technologies under varying conditions. In addition, systems should be tested at high, medium, and low security thresholds to determine their accuracy under different operating conditions. User perception data gathered during and after testing would provide an

independent, objective view of the public's view of various biometric technologies.

Testing of exclusion devices requires repeat visits with multiple human subjects. The generally low error rates mean that many human subjects are required for statistical confidence. Consequently, exclusion testing is extremely expensive and generally affordable only by government agencies. Few exclusion technologies have undergone rigorous, developer/vendor-independent testing to establish robustness, distinctiveness, accessibility, acceptability and availability in real-world (non-laboratory) applications. All test results must be interpreted in the context of the test application and cannot be translated directly to other applications. Most prior testing has been done in cooperative, overt, habituated, attended, standard environment, private, closed application of the test laboratory. This is the application most suited to decision policies yielding low error rates and high user acceptability. Clearly, people who are habitually cooperating with an attended system in an indoor environment with no data transmission requirements are the most able to give clear, repeatable exclusion measures. Habituated volunteers, often “incentivised” employees (or students) of the testing agency, may be the most apt to see biometric systems as acceptable and non-intrusive.

Performance of a device at a casino to assure the identification of problem gamblers, cannot be expected to be the same as in the laboratory. This use constitutes a non-cooperative, overt, non-habituated, unattended, non-standard environment, public, closed application. Performance in this application can only be predicted from measures on the same device in the same casino application. An increased understanding from a business perspective, of a framework in which to evaluate the vendor information, the possibilities, and inherent limitations, of exclusion techniques that could be applied to South African casinos, is required.

1.5 Motivation for the Research

The choice to gamble is just that . . . a choice. The majority of people in many communities choose to gamble responsibly. Gambling is one option among many

entertainment and recreational options. Problem gambling has an impact on entire communities. To better understand the impact, basic definitions will be helpful. Problem gambling refers to any gambling behaviour, which adversely affects significant areas of a person's life, including their mental health, physical health, employment, family relationships, financial and legal status. Pathological gambling may be defined as a progressive disorder characterised by a continuous or periodic loss of control over gambling; a preoccupation with gambling and with obtaining money with which to gamble; irrational thinking; and a continuation of the behaviour despite adverse consequences. Understanding problem gambling as an impulse control disorder provides one perspective on the nature of the condition. The impacts on the individual and upon community life are very real. Young adults, families, older adults, women and the community feel the impacts at large. The number of lives changed by problem gambling behaviour far exceeds the number of individuals identified in a prevalence rate. Entire families and employers are directly affected by changes that they did not choose to bring upon themselves. The choice to gamble, for some, is a choice to uproot and change forever a landscape of home and community (Ursel, 2001). The choice to gamble is a healthy and enjoyable option for many people. However, for some, the choice to gamble may strip away energy and options from a person's life. His/her family and community will feel the repercussions for a lifetime.

A technique to analyse and evaluate the complex relationships between the role players, the benefits and limitations of the exclusion techniques, and the rating of each, is proposed from a business standpoint. The technique could be applied to any of the new or existing casinos to determine the appropriate exclusion to apply from a business point of view.

Casino security management are well aware that technology could assist with exclusion of problem gamblers (Cape casino security managers, Caledon Casino, Hotel & Health Spa, July 2003, personal communication). Casinos across Canada are installing facial-recognition systems and other biometric security measures to filter out customers due to legal pressures (Keeling, G, 2003). From videotapes and tough security guards to these hi-tech 'Mission-Impossible' style digital systems, is a huge leap. The selection of the correct technology for the South African casino is the crucial aspect that faces the casino security manager. All casino role players require

nonbiased, vendor neutral, assistance in facing the challenge of selecting an appropriate exclusion technique for use in casino access control. The access control industry has historical baggage regarding its inability to deliver on promises and therefore it is important to focus on what exclusion techniques can realistically deliver today, identifying the short and long-range potential, as well as the immediate limitations of the technology. This is a worldwide problem, with the Mississippi Gaming Commission wanting to toughen the rules of its self-exclusion program for problem casino gamblers. Anyone who wants to join the self-exclusion program would have to visit a commission office rather than a casino to complete a consent form. The intention is for Mississippi's self-exclusion list to be shared with the Louisiana and the Choctaw Gaming Commission (Mississippi Wants Tougher Casino Self-Ban Rules, 2003, available online at: <http://www.casinowire.com/news.asp?id=5085>).

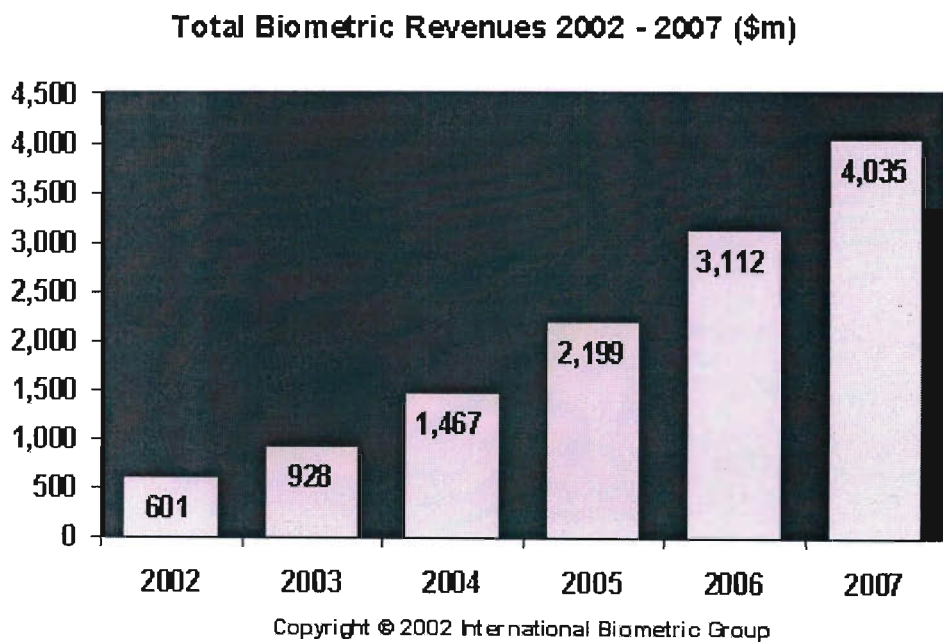


Figure 1. 1. **Biometric Revenue, 2002-2007**

The projected total revenues for 2002–2007 from the Biometric Market Report ([Biometric Market Report 2002-2007](http://www.biometricgroup.com/reports/public/market_report.html), 2003, available online at http://www.biometricgroup.com/reports/public/market_report.html) of biometrics is shown in Figure 1. 1. While this does not indicate that casino applications will increase, it does indicate increased interest in the field of biometric solutions, which may translate to casino

applications.

Despite biometrics' many weaknesses, sales could grow rapidly, according to Figure 1.1 which predicts that global biometric sales will rise more than 500% from 2002 to 2007, reaching revenues of \$4 billion, driven by large-scale public sector biometric deployments, the emergence of transactional revenue models, and the adoption of standardised biometric infrastructures and data formats. Fingerprint-based technologies are projected to account for \$467m of 2002 industry revenues, far-and-away the largest technology segment. This growth is attributable to the wide range of applications in which fingerprint-based solutions operate effectively. Among emerging biometric technologies, facial recognition is projected to reach \$200m in annual revenues in 2005. Iris-recognition is projected to reach \$210m in annual revenue in 2007 (Biometric Market Report 2003-2007, 2003, available online at http://www.biometricgroup.com/reports/public/market_report.html).

1.6 Value of the Project

There has been growing use of digital fingerprint, face recognition and iris recognition systems to confirm identity. There are other technological solutions in the works some that have begun stirring privacy concerns. Casinos, and financial institutions, must now verify the identities of new customers and make records of customer transactions available to law enforcement and money laundering officials upon request. Some casinos are turning to commercial services to authenticate the identities of their customers; others are banding together to create their own verification systems. To date, business has been essentially trying to treat identity theft as a "cost of doing business" and hasn't really taken many serious steps to prevent it (Becker, P 2003a). Internet retailers and security companies have formed a group to battle online identity theft, of which more than 48 000 of those complaints of fraud and that the total dollar loss from those cases was \$54 million, up from \$17 million in 2001 (Reuters, 2002). Identity theft is the most rapidly growing crime in the U.S. (Gilpin, 2003).

ROLE PLAYER	BENEFIT
For employers	Reduced costs – less time required to compare suspect to wanted list
	Increased security – no shared or compromised photographs when a template is used
	Increased security – deter and detect fraudulent gamblers
	Competitive advantage – familiarity with advanced technology
For employees	Convenience – reduced need for staff to deal directly with problem gamblers
	Convenience – updates of problem gamblers and undesirable card counters automatically generated
	Security – much more difficult to remove a template from the system
	Non-repudiation – biometrical transactions difficult to refute
For consumers	Convenience – can be banned from the casino remotely
	Security – personal data can be secured
	Security – safer when enabled by biometric
	Privacy – ability to transact anonymously
For the casino	Reduced costs – biometric users less likely to commit fraud
	Competitive advantage – first to offer secure exclusion method.
	Seen to be addressing socio-economic issues of problem gamblers.
	Security – account access much more secure than via signing

Table 1.1. Benefits of Exclusion Technology in Casinos

Table 1.1 proposes the potential benefits of exclusion technology in casinos. An increased understanding from a business perspective of the possibilities, and inherent limitations, of exclusion techniques or access control that could be applied to South African casinos is required, along with a clear definition of criteria which access control must meet in order to be considered deployable in casino applications.

The Eastern Cape Gambling & Betting Board are the first jurisdiction in South Africa, if not the world, to introduce a provision for the exclusion of persons by third parties. Since its inception the Act (63 of the Eastern Cape Gambling & Betting Act, 1997 (Act No. 5 of 1997) (Eastern Cape)) has had provision for the exclusion of prodigals (spendthrifts) but have found that, in general, families of problem gamblers do not have the finances to bring High Court applications, hence the procedure for the Board

to exclude via third parties. The Eastern Cape Gambling & Betting Board believe this is more practical than the provisions in the National Gambling Amendment Bill. In addition, all provinces except Western Cape and Mpumalanga presently provide for self-exclusions. The Eastern Cape presently has 49 persons who appear on this Board's exclusion list. In addition to this 213 people have, in terms of the contractual provisions between themselves and the relevant Eastern Cape casinos, had themselves excluded from specific casinos. This is a contractual arrangement rather than the statutory provisions contained in Section 63 (Kirton, S, 2003, Legal Affairs Division Eastern Cape Gambling & Betting Board, personal communication).

MONTH	TOTAL ADJUSTED GROSS REVENUE	TOTAL TAX	NUMBER OF TABLES	NUMBER OF MACHINES
Jun 2003	R 86,627,197.92	R 10,069,344.86	91	2,525
May 2003	R 93,920,747.14	R 11,073,895.07	91	2,525
Apr 2003	R 95,678,811.96	R 11,205,583.30	91	2,525
Mar 2003	R 89,995,233.62	R 10,406,974.79	91	2,525
Feb 2003	R 74,909,131.70	R 8,174,072.36	91	2,525
Jan 2003	R 94,270,829.68	R 11,068,076.59	91	2,525
Dec 2002	R 107,669,280.43	R 13,111,077.31	91	2,525
Nov 2002	R 76,989,741.30	R 9,045,040.57	77	2,275
Oct 2002	R 79,135,268.38	R 9,328,946.87	77	2,250
Sep 2002	R 70,512,256.99	R 7,832,803.44	77	2,250
Aug 2002	R 76,046,272.81	R 8,852,863.90	77	2,250
Jul 2002	R 76,954,435.05	R 9,020,543.72	80	2,250
TOTAL	R 1,022,709,206.98	R 119,189,222.78		

Table 1.2. Accumulative Monthly Casino Tax

Table 1.2 details the direct value attributed to the casino industry (last updated: 09 July 2003), excluding the 50 000 direct jobs created and other positive and negative spin offs of the casino industry. Selecting an inappropriate exclusion technique or not utilising an exclusion technique effectively will either negatively affect the revenue

generated or not provide protection for problem gamblers. Casinos are the only businesses, which make money by beating their own customers at games of chance. The operators of the lotto and horse racing or sports betting do not care who wins or loses. With casinos, however, the house cares very much who wins. The casino participates as a player covering the bets of the other players in every hand.

Casinos spend an enormous amount of time and money attempting to foil card-counters. Some of these counter-measures are aimed not only at card-counters, but are part of the industry's continuous attempt to speed up the velocity of money. Among the many tactics casinos have used:

1. Identifying known counters through photo books and face recognition computer technology.
2. Linking computers with imbedded scanners in blackjack tables. The most sophisticated of these systems can even recognise which system a player is using.
3. Dealing out only a few hands before shuffling. Dealers sometimes shuffle whenever players greatly increase the size of their wagers.
4. Changing the rules, often in the middle of a game. These include lowering the stakes, and limiting the right to double-down, split or play more than one hand at a time. Sometimes the restrictions are imposed on the entire table and sometimes only on the card-counter.
5. Harassing skilled players. Skilled players have been subjected to such crude tactics as having drinks spilled on them. One was even arrested in Atlantic City on trumped up charges, leading to a civil suit and a large jury verdict against the casino.
6. Bringing social pressure against the card-counter. Casinos are social settings. Slowing up a game to measure where the cut card is can turn the other players at the table against the card-counter.

It is highly doubtful that any well-run operation has been bankrupted by card-counters. But regulators and legislators do not talk to players; players are not organised, they have no spokespersons. They do hear regularly from casino executives and their lawyers. Government decision-makers thus tend to over-estimate the fiscal impact skilled players can have on a casino. The result is that casinos have sometimes been able to win by lobbying what they had initially lost through regulation (Rose 2002, a).

1.7 Establishing the Business Case

All exclusion systems require the expenditure of time, energy and money. Casino exclusion systems are certainly no different in this regard. They are not free in any sense. Many failed exclusion efforts fail, not because of deficiencies in the technology, but because the business case was not sufficient in the first place to justify the required expenditures. Fascination with the technology is not a sufficient business case. For positive identification applications, alternatives to biometrics exist that might be faster, cheaper and more seamlessly integrated into existing systems. The most successful biometric implementations are those that replace existing systems deemed too expensive or problematic to the casino administrators, or too cumbersome to the users. Successful implementations occur when the system management has carefully assessed the alternatives and is prepared to do the work necessary to make the systems effective.

There is tremendous value in educating the marketplace as there is not as yet broad public, casino and Gambling Board awareness about what exclusion techniques, and especially biometrics, can accomplish and how they operate. At best, this means that consumers might resist using the technologies in place of more antiquated, but familiar, processes. At worst, regulators and legislators may make ill-informed decisions that will stifle the use of exclusion techniques in casinos. The lack of common, and clearly articulated, industry positions on issues such as safety, privacy, and standards further increase the odds that regulatory bodies could react rashly to unfounded accusations about the functions and uses of exclusion technology.

Typical, approximate ballpark costs for a new casino are around R38 million, with R8 million being spent on capital expenditure for surveillance solutions. An exclusion solution, costing more than the entire casino or even the surveillance department capital budget is certainly not feasible. With thousands of people visiting the casino daily just a few Rand per person on an exclusion solution rapidly adds up to a very costly proposition (and few exclusion techniques exist which only cost cents per person).

1.8 Limitations of the Project

An exclusion technique offers a competitive advantage to the casino, which has meant that casinos have not willingly shared the information leading to successes.

The framework developed will be applicable only if the various role players will compromise.

It is not possible to test each access control exclusion technique in the casino environment with a large enough population to determine either the effectiveness or the problems, so decisions are made based on manufacture tests, which are not necessarily valid for casinos.

The small sizes of exclusion databases, which currently exist (less than 100 000) for large-scale projects, mean certain comparisons cannot be made.

The selected solutions are not necessarily the only solutions possible. Others that may yield positive results, such as Palm-recognition, DNA, Ear shape, Odour, Vein-recognition, Finger geometry, Nail bed identification, Gait recognition, etc. do exist.

The different possible exclusion solutions were evaluated, using a Likert scale of 1 - 5 relative to the other exclusion techniques. This is selective, and a full survey of the neighbouring environment would be more applicable to the local situation.

The selection criteria used were based on the relative importance of the different role players, which may not be necessarily the best way to select the systems.

The role players selected, as affected by exclusion, may not be comprehensive.

The weighted score system utilised is selective and should be based on a comprehensive survey of the local environment.

1.9 Assessing the Casino Application

The first task in selecting an exclusion technology is to assess the application environment in a casino. The various technologies are strongly differentiated by their technical applicability to different environments. The conditions in a casino environment are particularly difficult for access control exclusions. The privacy issues in the casino environment are very sensitive, with the casino not wanting to inhibit, or deter, any potential clients. The casino does, however, want to stop known card counters, and con artists without interfering with legitimate gamblers. Most casinos have frequent user cards, which give the gamblers benefits for high usage. Preventing these cards from being used by anyone other than the owner is a beneficial way to introduce the concept of biometrics to the public and the casino. A reference site in an operating casino environment is required which would work over a long period in order to gain real-world experience in the application of exclusion techniques. The claims of vendors are frequently based on tests performed under optimal conditions, making it very hard to draw meaningful conclusions.

Selecting the appropriate technology for a given application is crucial to the success of any exclusion-based deployment. Furthermore, at a conceptual level, exclusion systems can only confirm or determine a claimed identity – one established upon system enrolment – as opposed to revealing a “true” identity. Exclusion systems also must be seen as but one component in an overall system, and do not provide increased security when implemented in conjunction with highly vulnerable or easily circumvented systems.

The lack of information from the other tests and evaluations of exclusion systems in casino applications is disconcerting, as one does not keep a successful solution quiet. An investigation into the alternatives to the current solution to the casino problem may mean remaining with the current solution or some other solution. A system that partially assists could be beneficial, as seen in other cases where manual facial biometrics assisted in sorting through photographs (Miami Police Department Targets Prostitutes 2003 Available online at: <http://www.foxnews.com/story/0,2933,93749,00.html>). Exclusion devices and software are non-intrusive technologies that have been

designed to work effectively under variable and demanding conditions. None of the products present health or safety risks to either users or operators. They do not leave marks or don't take physical samples, and require minimal or no contact by the user. Although biometric technologies are relatively new to the marketplace, they have already earned a reputation for effectiveness in a variety of demanding environments that require high levels of accuracy, robust security and solid customer service. On the customer service side, users have repeatedly expressed complete satisfaction with biometric solutions. Exclusion processes need to be quicker and simpler than those that they replace, and need to be set up to function reliably under difficult conditions.

The savings from converting manual processes to those driven by exclusion devices can be significant. This is especially true in circumstances where safety and security is important, and customer service and accessibility are essential. Systems will certainly cost more than the current, ineffective systems, however, the benefits are much greater. Without knowledge of the current losses suffered by the casinos it is difficult to determine accurately the possible savings. The cost of saving just one problem gambling will never be too high a price to pay, for some role players.

Biometric technology works best in controlled situations, which are hardly the norm in the casino environment. Many examples exist where biometrics have been applied with success (Centre for Criminal Justice Technology 2003 Public On-Line Documentation available online at: http://www.ece.unh.edu/biometric/biomet/public_docs/). At the same time, though, numerous biometric pilot projects around the country and the world have come up short. Many casinos have facial-recognition systems to spot known card counters, but rarely use them due to the high number of false-positive identifications. Plans to use biometrics in national ID cards in the United States did not even get off the ground before concerned lawmakers scrapped them. While dozens of airports around the world have installed, or are running trials, with biometric systems to authenticate IDs for airline employees and even passengers, how many of these systems remain in use is an open question (McMillan, 2003). Trials of facial-recognition technology at Palm Beach International Airport (Willing, R, 2003) never made it to full installation after the airport decided it was not worth the cost. There has been too much hype surrounding the technologies, and as well as fear of the technologies (Krause, 2003).

Biometrics is losing some of its magic-bullet appeal, even among security zealots. Instead, the science and practice of measuring physical characteristics that are unique in each human – such as the sound of a voice, the shape of a hand, or the geography of a retina -- seem to offer limited, but significant hope to those seeking more order in an out-of-control world. All facial-recognition technology does is create a template of a face so we can store it and find it later (Bernard Bailey, CEO of facial-recognition company Viisage Technology (www.viisage.com)). That way, if I'm looking for someone with brown hair, brown eyes, and a wide nose, it will automatically narrow it down for me. I don't have to go through 20 million photos, maybe just 4 million. This is a technology for authentication and verification, not identification.

The key is to understand how technologies and processes create opportunities for the casino to achieve its goals. Those who have focused on security have tended to miss the point that security has meaning only if it is in service of a larger business goal. Today, the market suffers, because neither the vendors nor the prospective buyers understand the value to the business (Becker, 2003b). This is a common failure when things are looked at solely from a technological point of view. This creates urgency for a “better” solution to a very narrowly defined problem, and neglects to see how technology makes business work better. Tends towards technology for technology’s sake, not for the business’s sake. There is a large overlap between what provides security and what provides tremendous business leverage in productivity, response times, empowering the individual closest to the problem, and reducing management overheads. Biometrics is a new language for security professionals, and it is beyond the comfort zone of most IT professionals.

Chapter 2 Exclusion Techniques

2.1 Introduction

The basic parameters of excluding problem gamblers from gambling – including requirements for accuracy, response time, cost, level of impact on existing systems and processes, and compatibility with existing data, and a host of others depending on the role player – define which access control techniques can be effectively deployed. Each exclusion technology has strengths and (sometimes fatal) weaknesses depending upon the manner in which it is used. Although each of the access control exclusion technologies is clearly different, some striking similarities emerge when considering applications as a whole.

The exclusion techniques to be compared for access control were categorised into current solutions (either a guard at the entrance or surveillance operators with a file of photographs) or alternative solutions. The alternative solutions that were investigated were either comparison-based solutions (identity book or a drivers license), card-based solutions (swipe or proximity card) or a biometric. Biometrics was further divided into contact or non-contact biometrics. Contact biometrics were either based on physiological characteristics (such as fingerprint recognition or hand recognition) or behavioural characteristic (such as signature, voice or keystroke). The non-contact biometrics were based on either an overt acquisition (such as iris or retina recognition) or covert acquisition (such as face recognition).

Of the multiple exclusion technologies listed above, all are available for implementation in South African casinos to meet the requirements of the new National Gambling Bill. The decision is rather which would be the most appropriate to exclude problem gamblers from gambling in South African casinos?

2.2 *Current Solutions*

Current exclusion solutions include the use of a guard at the casino entrance trained to identify gamblers who have banned themselves. The guards would have at their disposal a photo file with which to compare the incoming people with those who have banned themselves. When the guard identifies someone who they think is a match they can confirm it with the identity number listed with the photograph. This technique is taken a step further when surveillance operator's use fixed or dome cameras focused on the gamblers and compare this to the file of photographs. This allows the surveillance operators to recognise compulsive gamblers and compare these people to the photos in the files. The guard at the gate only has a single view of short duration of the person while the surveillance operator can zoom in and watch the person for some time from a number of angles. Both techniques suffer from the fact that the file images are taken in a sterile office environment while recognition has to occur under poor or variable lighting conditions. In order to use the current solution based on guards or surveillance operators, the user approaches the entrance, passes the guard and, only if recognised, is prevented from gaining access. The surveillance operator can examine the person from any of the multiple cameras present in the casino and, if recognised, would ask them to leave. Current solutions do not require that every person be enrolled into the system database, only those who wish to be excluded. If the problem gambler is not recognised by the guard or the surveillance operator, they are allowed access.

2.3 *Alternative Solutions*

2.3.1 Comparison Based Solutions

Comparison based exclusion techniques use currently existing pictures, such as those included in an identity book, driver's license or casino loyalty card, and compared with the person identifying themselves. This allows the identity number, or other unique number, to be used for exclusion, as well as a facial biometric, which together create a very powerful exclusion technique. Compared with current techniques this allows the casino to automate the unique number searching of exclusion control. The casino can search initially on the unique number for exclusion, confirm that the holder is identified and possibly search against logged problem gamblers. Comparison based solutions do not require that every person be enrolled on the system database, only those who wish to be excluded. In order to use the comparison based solution the user would approach the turnstile, place the ID book, driver's licence or casino issued card in the scanner, which would read the document and check the database for unique numbers that are currently excluded. If allowed to proceed, the people presenting themselves would be compared manually to the picture in the ID book, driver's licence or card from the casino. If the user passes this comparison they are allowed access to the casino.

2.3.2 Card Based Solution

Access control solutions based on the use of cards, such as a swipe card or a proximity card, have the ability to control access, letting only those who have a card into the casino. Card based solutions require that every person who wishes to gain access to the casino be enrolled into the system database. However, the control of the cards and who can use them is the major limitation with this solution. In order to use the card based solution, the user swipes the card or bring it near the reader in the case of the proximity card, and gain access. If the card number was removed from the database the person could not gain access. However, there would be no way to

prevent the problem gambler from using someone else's card. Only an exclusion system based on biometrics can prevent the abuse of the card system by non-authorised gamblers.

2.3.3 Biometrics

2.3.3.1 Biometrics Defined

Biometric (noun) - one of various technologies that utilise behavioural or physiological characteristics to determine or verify identity

Biometric (adjective) – of, or pertaining to technologies that utilise behavioural or physiological characteristics to determine or verify identity (Association for Biometrics (AfB) and International Computer Security Association (ICSA) 1999).

Biometrics can be used in a wide variety of applications, so it is very difficult to establish an all-encompassing definition. The most suitable definition of biometrics is: The automated use of physiological or behavioural characteristics to determine or verify identity (Association for Biometrics (AfB) and International Computer Security Association (ICSA) 1999). To elaborate on this definition, physiological biometrics is based on measurements and data derived from direct measurement of a part of the human body. Behavioural characteristics are based on an action taken by a person. The term “biometric authentication” refers to the automatic identification, or identity verification, of living individuals using physiological and behavioural characteristics. Biometric authentication is the “automatic”, “real-time”, “non-forensic” subset of the broader field of human identification.

There are two distinct functions of biometric devices:

1. To prove you are who you say you are (one-to-one matching).
2. To determine who you are without knowing (one-to-many matching).

The first function is the act of linking the presenting person with an identity previously registered, or enrolled, in the system. The user of the biometric system makes a “positive” claim of identity, which is “verified” by the automatic comparison of the submitted “sample” to the enrolled “template”. Clearly, establishing a “true” identity at the time of enrolment must be done with documentation external to any

biometric system. The purpose of a positive identification system is to prevent the use of a single identity by multiple people. If a positive identification system fails to find a match between an enrolment template and a submitted sample, a “rejection” results. A match between sample and template results in an “acceptance”. In the latter function, it is suspected that you may be in the database and your biometric is compared to see if there is a match. This compares the suspects biometric to all other records looking for a match. The result may still need to be confirmed by the operator with reference to other information in the database.

2.3.4 Biometrics' Basic Components and Processes

2.3.4.1 The Generic Biometric System

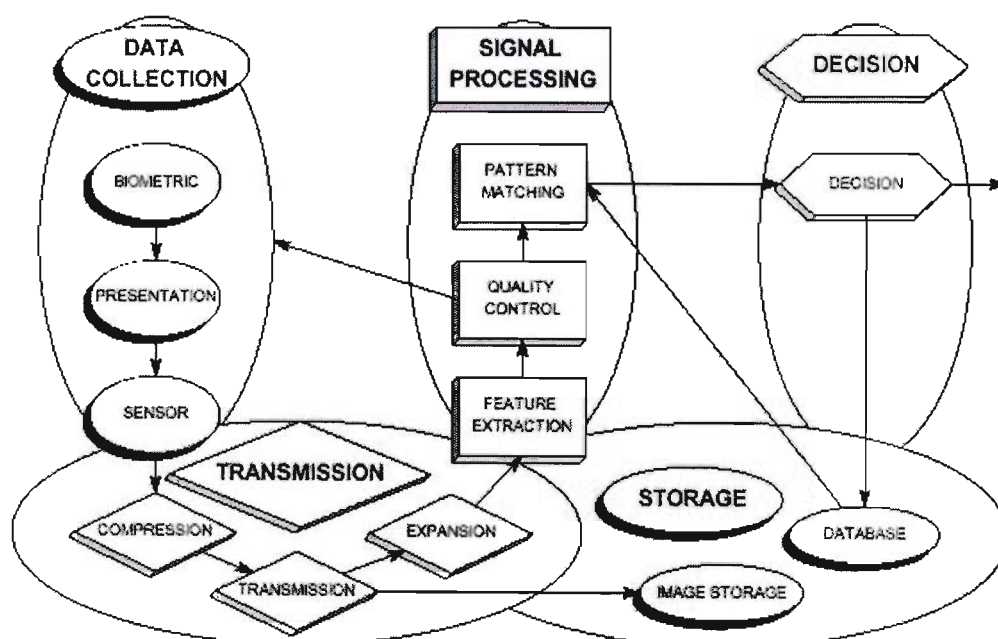


Figure 2. 1. Generic biometric system

Biometric systems convert data derived from behavioural or physiological characteristics into templates, which are used for subsequent matching. This is a multi-stage process as described below in Figure 2.1. Although these devices rely on widely different technologies, much can be said about them in general. Figure 2.1

shows a generic biometric authentication system, divided into five sub-systems: data collection, transmission, signal processing, decision and data storage (Wayman, 2001).

2.3.4.2 Data Collection

Biometric systems begin with the measurement of a behavioural/physiological characteristic. Key to all systems is the underlying assumption that the measured biometric characteristic is both distinctive between individuals, and repeatable over time for the same individual. The problems in measuring and controlling these variations begin in the data collection sub-system.

The user's characteristic must be presented to a sensor. The output of the sensor, which is the input data upon which the system is built, is the convolution of the biometric measure; the way the measure is presented; and the technical characteristics of the sensor. Both the repeatability and the distinctiveness of the measurement are negatively impacted by changes in any of these factors. The process whereby a user's initial biometric sample or samples are collected, assessed, processed, and stored for ongoing use in a biometric system is called enrolment, which takes place in both 1:1 and 1:N systems. If users are experiencing problems with a biometric system, they may need to re-enrol to gather higher quality data.

Technology	Biometric Sample
Fingerprint	Fingerprint image
Voice recognition	Voice recording
Facial recognition	Facial image
Iris-recognition	Iris image
Retina-recognition	Retina image
Hand geometry	3-D image of top and sides of hand and fingers
Signature-recognition	Image of signature and record of related dynamics measurements
Keystroke-recognition	Recording of characters typed and record of related dynamics measurements

Table 2. 1. Sample types associated with each biometric technology

The identifiable, unprocessed image or recording of a physiological or behavioural characteristic, acquired during submission, is used to generate biometric templates. Table 2.1 lists the sample types associated with each biometric technology:

Biometrics are much easier to use than one might expect as demonstrated in the following technology-by-technology summary of how one interacts with biometric systems (Are Biometric Systems Difficult to Use? 2003 available online at http://www.ibgweb.com/reports/public/reports/difficulty_of_use.html).

Fingerprint. The user places his or her finger on a postage stamp-sized optical or silicon surface. The user must hold the finger in place for 1-2 seconds, during which automated comparison and matching takes place. After a successful match, the user has access.

Typical verification time from “system ready” prompt: 2-3 seconds (Harrison, 2003).

Facial recognition. The user faces the camera, preferably positioned within 50 cm of the face. The system will locate the face very quickly and perform matches against the claimed identity. In some situations, the user may need to alter his or her facial aspect slightly to be verified.

Typical verification time from “system ready” prompt: 3-4 seconds.

Voice recognition. The user positions him or herself near the acquisition device (microphone, telephone). At the prompt, user either recites enrolment pass phrase or repeats pass phrase given by the system.

Typical verification time from “system ready” prompt: 4-6 seconds.

Iris-recognition The user positions him or herself near the acquisition device (peripheral or standalone camera). User centres eye on device so as to see the eye’s reflection. The user is between 5-40 cm away. Capture and verification are nearly immediate.

Typical verification time from “system ready” prompt: 3-5 seconds.

Retina-recognition The user looks into a small opening on a desktop or wall-mounted device. User holds head still, looking at a small green light located within the device.

Typical verification time from “system ready” prompt: 10-12 seconds.

Hand geometry. The user places hand, palm-down, on a 15 x 30 cm metal surface with five guidance pegs. Pegs ensure that fingers are placed properly, ensure correct

hand position.

Typical verification time from “system ready” prompt: 2-3 seconds.

Signature-recognition The user positions himself to sign on tablet. When prompted, user signs name in tablet’s capture area.

Typical verification time from “system ready” prompt: 4-6 seconds.

Keystroke-recognition The user types his or her password or pass phrase.

Typical verification time from “system ready” prompt: 2-3 seconds (Are Biometric Systems Difficult to Use? 2003 Available online at: http://www.ibgweb.com/reports/public/reports/difficulty_of_use.html).

If a system is to be used in a covert, non-cooperative application, the user must not be able to wilfully change the biometric or its presentation sufficiently to avoid being matched to previous records.

2.3.4.3 *Sensor (Acquisition Device)*

The sensor is the different hardware is used to acquire biometric samples. The acquisition devices listed below in Table 2.2 are associated with each biometric technology (What Are Biometrics' Basic Components and Processes 2003 Available online at: http://www.ibgweb.com/reports/public/reports/components_processes.html):

Technology	Acquisition Device
Fingerprint	Chip or reader embedded in turnstile
Voice recognition	Microphone
Facial recognition	Video camera, surveillance camera, single-image camera
Iris-recognition	Infrared-enabled video camera
Retina-recognition	Wall-mountable unit
Hand geometry	Proprietary wall-mounted unit
Signature-recognition	Signature tablet, motion-sensitive stylus
Keystroke-recognition	Keyboard or keypad

Table 2.2. Acquisition devices associated with biometric technology

2.3.4.4 *Transmission*

Some, but not all, biometric systems collect data at one location but store and/or process it at another. Such systems require data transmission. If a large amount of data is involved, compression may be required before transmission or storage, so as to conserve bandwidth and storage space. Figure 2.1 shows compression and transmission occurring before the signal processing and image storage. If a system is to be open, compression and transmission protocols must be standardised so that every user of the data can reconstruct the original signal. Standards currently exist for the compression of fingerprint (WSQ), facial images (JPEG), and voice data (CELP).

2.3.4.5 *Feature Extraction*

The automated process of locating and encoding distinctive characteristics from a biometric sample in order to generate a template is known as feature extraction. The feature extraction process may include various degrees of image or sample processing in order to locate a sufficient amount of accurate data. For example, voice recognition technologies can filter out certain frequencies and patterns, and fingerprint technologies can thin the ridges present in a fingerprint image to the width of a single pixel. Furthermore, if the sample provided is inadequate to perform feature extraction, the biometric system will instruct the user to provide another sample, often with some type of advice or feedback.

Technology	Feature Extracted
Fingerprint	Location & direction of ridge endings & bifurcations on fingerprint
Voice recognition	Frequency, cadence and duration of vocal pattern
Facial recognition	Relative position and shape of nose, position of cheekbones
Iris-recognition	Furrows and striations in iris
Retina-recognition	Blood vessel patterns on retina
Hand-recognition	Height and width of bones and joints in hands and fingers
Signature-recognition	Speed, stroke order, pressure, and appearance of signature
Keystroke-recognition	Keyed sequence, duration between characters

Table 2.3. Common characteristics used in feature extraction

The manner in which biometric systems extract features is a closely guarded secret, and varies from vendor to vendor. Common physiological and behavioural characteristics used in feature extraction are included in Table 2.3.

Selecting a biometric based on feature extraction (Table 2.3) would require that sufficient difference existed in the feature extracted to make an accurate comparison. In a one-to-one comparison where the user presents a token or ID and claims to be someone, this is not a concern due to confirming claimed identity on a one-to-one basis. However in one-to-many identity applications where millions of users exist only iris recognition could be used. However, the largest database so far is just over 100 thousand people, so this is still difficult to say for certain. Other biometrics simply do not have enough features for one-to-many comparison, without dividing the database into sub-categories, such as sex, race, age, etc, all of which are difficult to obtain from an uncooperative subject, who may be a problem gambler or a suspected card counter.

2.3.4.6 Signal Processing

Having acquired and possibly transmitted a biometric characteristic, it must be prepared for matching with other like measures. Figure 2.1 divides the signal processing sub-system into three tasks: feature extraction, quality control, and pattern matching. In feature extraction, the technology deconvolves the true biometric pattern from the presentation and sensor characteristics and preserves from the biometric pattern those qualities distinctive and repeatable, and discards those, which are not, or are redundant. Feature extraction is a form of non-reversible compression, meaning that the original biometric image cannot be reconstructed from the extracted features. After feature extraction, the system checks to verify if the signal received from the data collection subsystem, is of good quality. If the features “don’t make sense” or are insufficient in some way, it concludes that the received signal was defective and requests a new sample from the data collection subsystem while the user is still at the sensor. The development of this “quality control” process greatly improves the performance of biometric systems. On the other hand, some users (known as goats) seem unable to present an acceptable signal to the system. If a negative decision by

the quality control module cannot be over-ridden a “failure to enrol” error results.

The feature sample, now of very small size compared to the original signal, is sent to the pattern matching process for comparison to one or more previously identified and stored features. The term “enrolment” refers to the placing of that feature sample into the database for the very first time. Once in the database and associated with an identity by external information provided by the enrollee or others, the feature sample is referred to as the “template” for the individual to whom it refers.

The purpose of the pattern matching process is to compare a presented feature sample to a stored template, and to send to the decision subsystem a quantitative measure of the comparison. An exception is enrolment in systems allowing multiple enrolments. In this application, the pattern matching process can be skipped. In the cooperative case, where the user has claimed an identity or where there is but a single record in the current database (which might be a magnetic stripe card), the pattern matching process only makes a comparison against a single stored template. In all other cases, the pattern matching process compares the present sample to multiple templates from the database one-at-a-time, as instructed by the decision subsystem, sending on a quantitative “distance” measure for each comparison (Wayman, 2001).

2.3.4.7 Decision

The decision subsystem implements system policy by directing the database search, determine matches or non-matches based on the distance measures received from the pattern matcher, and ultimately makes an “accept/reject” decision based on the system policy. Such a policy could be to declare a match for any distance lower than a fixed threshold and “accept” a user on the basis of this single match, or the policy could be to declare a match for any distance lower than a user-dependent, time-variant, or environmentally-linked threshold and require matches from multiple measures for an “accept” decision. The policy could be to give all users three attempts to return a low distance measure and be “accepted” as matching a claimed template. In the absence of a claimed template, the system policy could be to direct the search of all, or only a portion, of the database and return a single match or multiple candidate matches. The decision policy employed is a management decision that is specific to the operational

and security requirements of the casino. In general, lowering the number of false non-matches can be traded against raising the number of false matches. The optimal system policy in this regard depends both upon the statistical characteristics of the comparison distances coming from the pattern matcher and upon the relative penalties for false match and false non-match within the system.

2.3.4.8 Storage

The remaining subsystem to be considered, is that of storage. There will be one or more forms of storage used, depending upon the biometric system. Feature templates will be stored in a database for comparison to incoming feature samples by the pattern matcher. For systems only performing “one-to-one” matching, the database may be distributed on magnetic stripe cards carried by each enrolled user. Depending upon system policy, no central database need exist, although in the application a centralised database can be used to detect counterfeit cards or to reissue lost cards without re-collecting the biometric pattern. The database will be centralised if the system performs one-to-N matching with N greater than one, as in the case of identification or “PIN-less” verification systems. As N gets larger, system speed requirements dictate that the database be partitioned into smaller subsets such that any feature sample need only be matched to the templates stored in one partition.

2.3.4.9 Template

A template is a comparatively small but highly distinctive file derived from the features of a user’s biometric sample or samples, used to perform biometric matches. A template is created after a biometric algorithm locates features in a biometric sample. The concept of the template is one of biometric technology’s defining elements, although not all biometric systems use templates to perform biometric matching. For example, some voice recognition system utilise the original sample to perform a comparison.

Depending on when they are generated, templates can be referred to as enrollment templates or verification templates (Figure 2. 2). Enrolment templates are created upon the user’s initial interaction with a biometric system, and are stored for usage in

future biometric comparisons. Verification templates are generated during subsequent verification attempts, compared to the stored template, and discarded after the comparison. Multiple samples may be used to generate an enrolment template, facial recognition, for example, will utilise several facial images to generate an enrolment template.

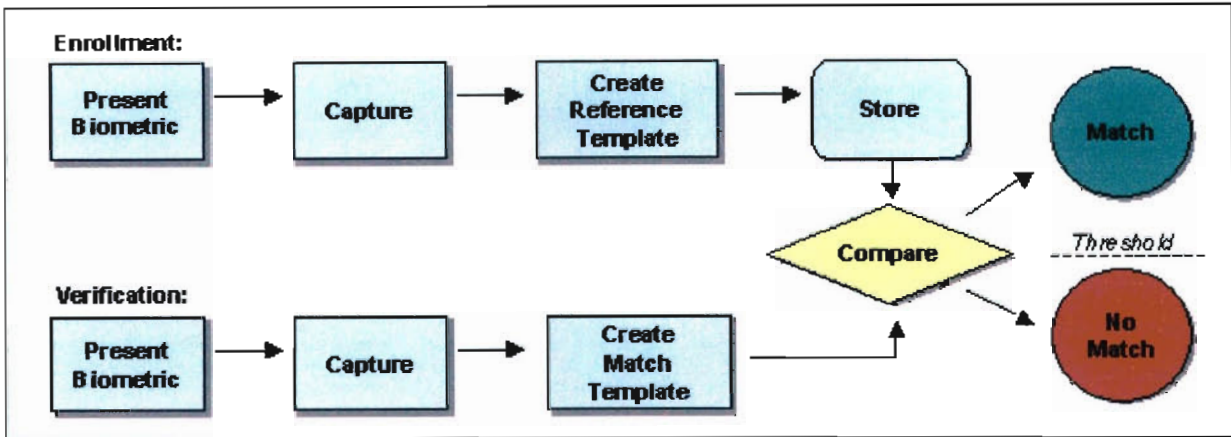


Figure 2.2. Biometric Matches

Verification templates are normally derived from a single sample – a template derived from a single facial image can be compared to the enrolment template to determine the degree of similarity. Just as the feature extraction process is a closely held secret, the manner in which information is organised and stored in the template is proprietary to biometric vendors. Biometric templates are not interoperable a template generated in vendor A’s fingerprint system cannot be compared to a template generated in vendor B’s fingerprint system.

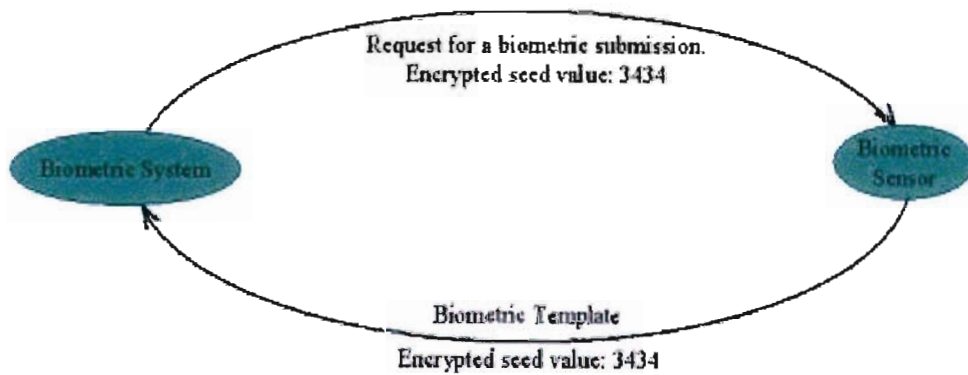


Figure 2.3. Biometric template encryption

Are biometric templates secret? The answer depends on how well a biometric system is designed. If a system allows a template to be inserted into the verification process without ensuring that this template came from an actual placement, a compromised template can pose a problem. However, a well-designed system will ensure that the information it is analysing is not a recording but is, in fact, a new sample.

One-way to assure that a new template is being submitted is to seed the request for a sample. This involves the biometric system sending an encrypted random number (known as a seed) to the biometric sensor. This number can be encrypted such that only the sensor itself can decrypt the message. When returning the biometric template, the sensor also sends the encrypted seed number back. This ensures that the template being sent was created immediately after the request for the template (as opposed to an old template that has been recorded and played back). Figure 2.3 illustrates a request for a biometric sample with a seed value of 3434. Note that biometric templates cannot be used to regenerate original biometric data (How Do Identification and Verification Differ 2003 Available online at: http://www.ibgweb.com/reports/public/reports/identification_verification.html).

2.3.4.10 Contact Biometrics

The manner in which the acquisition of the biometric occurs can be used to remove exclusion techniques. The fact that one has to touch a sensor should remove fingerprint, hand geometry, keystroke recognition and signature recognition as viable options due to the perceived or real transmission of bacteria, viruses and any other health concern.

Contact biometrics can be further subdivided into those based on physiological characteristics, such as fingerprint recognition (Figure 2.4); hand recognition and those contact biometrics where behavioural characteristics are used, such as signature; voice or keystroke. Contact biometrics requires that every person be enrolled into the system database. In order to use the contact biometric solution the user would, present the body part on which the biometric is based either a fingerprint, hand recognition or sign their name, talk into a microphone or key in a certain phrase into the keyboard and gain access. If not recognised the person would not gain access.

2.3.4.11 Non-Contact Biometrics

Non-contact biometrics can either be overt biometric acquisition, such as iris and retina recognition or covert biometric acquisition, such as face recognition. Non-contact biometrics requires that every person be enrolled into the system database. In order to use the non-contact, overt, biometric access control solution, the user presents the iris or retina to the cameras from a distance of about 15-30 cm and gain access if recognised. If not recognised or if not allowed in, the person would not gain access (Havenga, M, 2002).

In order to use the non-contact, covert, biometric access control solution the user would enter the casino, and recognition would occur from any of the multiple cameras currently installed in the casino. The casino surveillance staff would capture an image of the suspected problem gambler from a distance between 1 - 100 m and manually compare that to the database of excluded gamblers. If a high score were obtained the person's identity may be further investigated and if proven to be a banned gambler would be asked to leave the casino. If not recognised nothing would occur as the person may not be in the database. Non-contact, covert, biometric based solutions do not require that every person be enrolled into the system database, only those who need to be excluded.

2.3.5 Which is the Best Biometric Technology?

The primary biometric disciplines include the following:

Fingerprint (optical, silicon, ultrasound) (Figure 2. 4)

Facial recognition (optical and thermal)

Voice recognition (not to be confused with speech recognition)

Iris-recognition

Retina-recognition

Hand geometry



Figure 2. 4. Fingerprint recognition proposed for US entry

Signature-recognition

Keystroke-recognition (Which is the Best Biometric Technology? 2003 Available online at: http://www.ibgweb.com/reports/public/reports/best_biometric.html)

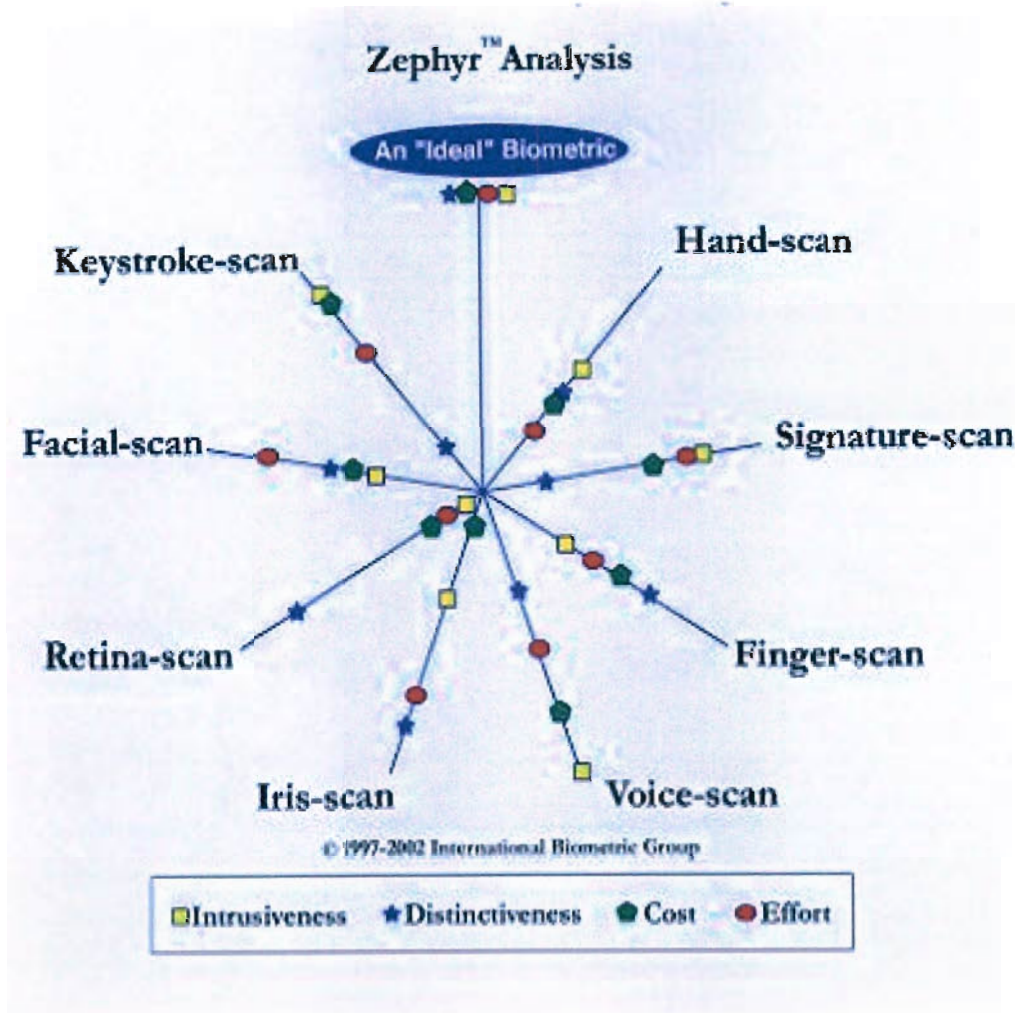


Figure 2. 5. Zephyr Analysis to determine the “ideal” biometric

Despite vendor claims, there is no “ideal” biometric technology, although examples of successful uses of biometric technologies do exist (Embracing New Technology in Health Care: A Case Study 2003 Available online at: http://www.emedicalfiles.com/case_study_1.shtml). If one specifically defines an application, it may be possible to describe the most accurate, easiest to use, easiest to deploy, or cheapest biometric for that particular deployment, but no one biometric technology or set of criteria is right for all situations. The Zephyr chart provided above (Figure 2. 5) is a general comparison of biometric technologies in terms of ease-of-use, cost, accuracy, and perceived intrusiveness. Symbols represent the relative capabilities of each technology. A perfect biometric would have all symbols at the periphery, while a poor biometric would have symbols near the centre of the Zephyr chart.

The primary concerns of which characteristic is best are at least five-fold: the robustness (repeatable, not subject to large changes), the distinctiveness (the existence of wide differences in the pattern among the population), the accessibility (easily presented to an imaging sensor), the acceptability (perceived as non-intrusive by the user) and the availability (some number of independent measures can be presented by each user) of the biometric pattern. The question of “Which biometric device is best?” is very complicated and the answer depends upon the specifics of the application. The Zephyr chart of Figure 2. 5, illustrates remarkably well the challenge faced by the role players in the casino industry in trying to select the appropriate biometric technology. No one biometric technology stands out as the best option, with the best price performance, most secure and easiest to use. If the Gambling Board could persuade the casinos and the public that the use of a biometric was compulsory in order to gain access to the gambling floor, the selection of the best biometric would be far simpler. One could then link the biometric to an access card and perform one-to-one verification, confirming the identity card holder. The biometric information would remain on the card, not in the casino records. The casino would then remove the problem gamblers on entry. This is a legislative solution, which should have occurred when the casinos were first introduced.

2.4 Research Methodology

The methodology is qualitative in nature. The selection of the appropriate exclusion technique for use in access control in the South African casino environment must take into consideration many, often conflicting, business criteria. These include speed, accuracy, ease of use, privacy rating, environmental affects, technology maturity, cost, ease of enrolment, template size, unique identifiers, stability of trait, at different weightings, etc.

A framework, from a business perspective, is proposed which allows multiple role players and varied criteria to effectively evaluate a range of possible solutions (Table 2.4). The framework is applied to the role players affected by the proposed exclusion of problem gamblers from gambling.

The different possible exclusion solutions were evaluated, using a 1-5 Likert scale; with 1 being best, and 5 being worst. The values were decided upon in consultation with various casino role players through personal communication and meetings with casino security managers. They represent no particular casino but could be considered applicable to any casino operating in the South African environment.

Current solutions	Guard at the entrance with a file of photographs Surveillance operators with a file of photographs	
Alternative solutions	Pre-existing identity based solutions Identity book photo and no. Checked automatically Drivers license photo and no. Checked automatically	
Card based solution	Swipe card Proximity card	
Biometrics	Contact biometrics	Physiological characteristic Fingerprint recognition Hand recognition
Behavioural characteristic	Signature Voice Keystroke	
Non-Contact biometrics	Overt biometric acquisition	Iris Recognition Retina
Covert biometric acquisition	Face recognition	

Table 2. 4. Investigated Exclusion and Access Control Solutions

2.5 Key performance Metrics

There are almost as many performance metrics as there are exclusion techniques, as shown in Table 2.5 (Biometrics Market Intelligence, Volume 01, issue 01 2003 Available online at: http://acuity-mi.com/?page=home_biometrics/index).

Unfortunately, there is no single metric that indicates how well a system will perform. Analysis of multiple metrics is necessary to determine the strengths and weaknesses of each technology and vendor under consideration for a given application. It should also be noted that the processes unique to various applications have a great effect on performance metrics. Testing is most valuable when it emulates real-world application environment. Additional partitions might also be appropriate and not all possible partition permutations are equally likely or even permissible.

Factors	Face	Finger Scan	Hand	Iris	Keystroke	Retina	Signature	Voice
Ease of Enrollment	good	fair	good	good	good	fair	good	good/exc
Identification (1:N)	yes	search only	no	search only	no	search only	no	no
Speed (relative)	good	good	excellent	good	good	good	good	good
Cost	medium	medium	medium	med/high	low	medium	low/med	low
Accuracy: relative;	med/high	med/high	med/high	high	med/high	high	medium	med/high
Invasiveness	medium	medium	low	medium	low	high	low	low
Ease of Use	good	good	good	good	excellent	good	good/exc	good/exc
Ease of Integration	good	good	good	good	excellent	good	good/exc	excellent
Existing Infrastructure	yes	no	no	depends on application	yes	yes	yes	yes
Environmental Affects	lighting, position	temperature, moisture, dirt	none	none	none	none	none	noise, acoustics
Physical Con-	none	clean surface	bulky	none	none	light source	none	none
Human Factor Limitations	beards, glasses, skin tone, cosmetics	worn fingertips	missing fingers, young kids, arthritis	blind	alcohol, stress, loss of fingers	none	emotional state	emotional state, laryngitis
Mature Technology (varies by vendor)	no	yes	well established >10years	well established >10years	well established >10years	yes	no	no
User Acceptability	med/high	associated w/criminals	med/high	medium	high	low/med	med/high	high
Template Size (bytes)	84 (1:N) 1,300 (1:1)	250-1200	9	512	1500	96	..	10,000-20,000
Liveness	yes	for some	yes	yes	yes	yes	yes	yes
Unique Identifiers	~128	30-90	96	266 of 400	NA	~192	~10 variables	5 frequencies
Natural Interface	yes	no	no	yes	yes	yes	yes	yes
Stability of Trait	medium	high as adult	high	high	medium	high	medium	medium

Table 2.5. Biometric comparisons

Key performance metrics include the following:

2.5.1 Cost

The cost calculation is not as simple as hardware + software + communication = exclusion implementation cost. There are very significant infrastructure and organisation change management costs that will have to be incurred at the outset in order to make use of exclusion techniques in casinos viable, even if every person had such an ID readily available today.

A full scale costing exercise of each biometric, even if one could standardise an application for the different biometrics, is well beyond the scope of this study. Table 2.5 does show that most biometric solutions are comparatively priced, except for iris recognition, which is a more expensive, but not when the greater accuracy is taken into consideration. Detailed costing of face and iris recognition (Figure 2. 6) is included as these are the most promising solutions. The cost of the front-end biometric technology is a small part of the entire cost of the project. When the computers, networks, training, procedures, software interfaces, maintenance, etc. are brought into the equation, the relative cost of the front end biometric is insignificant compared to the overall cost of the project.

Face recognition implementation costs are upwards of R20 000 for 10 000 users, but one may find many more expensive systems. If one were to go for a limited implementation, and only place the face recognition system in the surveillance department of the casino the extra costs would be limited to the R20 000 indicated, as the users of the system would be the current surveillance operators.

If one opted for a more extensive implementation and placed five of the face recognition biometric systems in the following places:

- With the local Gambling Anonymous office;

- The entrance to the casino and one within the gambling hall;

- At a local shopping mall and a community centre, away from the casino;

- With the surveillance operators.

The costs would then incorporate the hardware (5 x R20 000 = R100 000) plus the networking and database functionality. The additional cost of the database / front end

is not included as the requirements would be detailed by the relevant user.



Figure 2. 6. Example of face and iris recognition

In order for the system to work to full effect, it is essential that the databases be shared with as many casinos as possible. The large number of face recognition vendors would complicate the issue of database sharing, unless all the casinos were to use the same vendor. It is possible that the lowest level of cooperation may only be in terms of the images and not the biometric data extracted from the images. This means the images will need to be enrolled at each casino, leading to different results and possible delays.



Figure 2. 7. Remote optical head for iris recognition

Iris recognition cost is from R50 000 per system upwards (Figure 2. 7), which will process two users per minute, which means for one hundred people to gain access to the casino in 5 minutes one would need 10 systems at a minimum cost of two hundred and fifty million Rand. Iris recognition is certainly the most accurate biometric, a duplicate match never having been found, but due to the inability to capture the biometric from an unwilling subject, the fact that the sensor must be very close to the subject, and finally the cost, iris recognition is unlikely to be implemented in the foreseeable future. There are certainly specific areas in casinos where iris recognition could assist, primarily with regard to access control into areas where the takings are handled and possibly for high rollers where the credit lines extended are substantial. However, wherever iris recognition might be applied, due regard must be taken of the inherent limitations. These certainly can be overcome, by for example keeping up with technological development, such as Panasonic's dual camera system, which uses face recognition with one camera allowing a second camera to zoom in on the eyes. This would theoretically allow one to do iris recognition from many meters away from the subject, potentially without the subject knowing.

Due to the complexity of detailed cost comparisons being beyond this study, a relative scale of 1 for low cost systems (guard at the gate) and 5 for very expensive systems (iris recognition) was utilised.

2.5.2 Ease of Use for the Public

Ease of use is not a traditional performance metric, but is impacted by performance-related adjustments (as shown in Figure 2. 8). Steps taken to improve performance tend to decrease the ease of use. Requiring multiple submissions, or compelling the user to submit more carefully, will each increase system performance. These will also serve to make the system more tedious and cumbersome to use.

Deceptive casinos users who have banned themselves and want to return will be non-cooperative with the system. In negative identification applications, the fraudsters will attempt to foil identification at enrolment. Consequently, enrolment supervisors will require training in detection of fraudulent techniques. In positive identification applications, high rollers will be generally cooperative with the system in an attempt

to be positively identified.

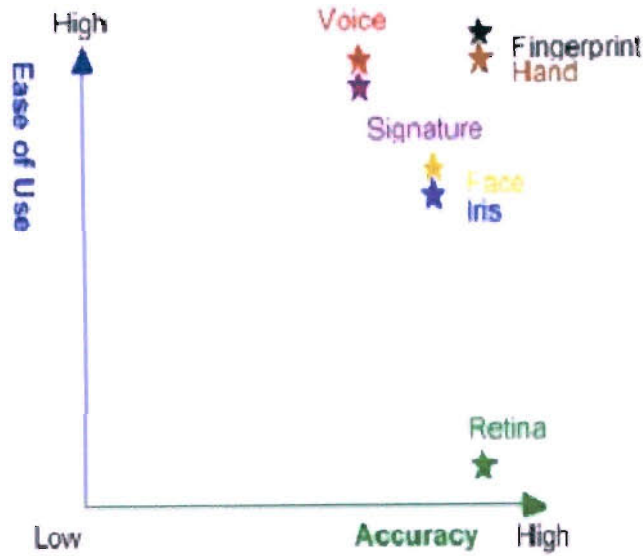


Figure 2. 8. Performance matrix by biometric technologies

A system where the user is not involved in the process at all (such as a covert system) will score 1 for ease of use while where the user has to position themselves in a certain way (as with iris recognition) will score 5.

2.5.3 Physical Contact

One of the concerns sometimes heard about biometric touch surfaces is that they can transfer infection from one person to another. A second is that they can become dirty and prevent an accurate reading. A third is that they can be damaged in a more permanent way, either by accident or intention. What if the touch surface were holographic? The concept could be used for both finger and facial positioning. Holographic contact points would permit basic positioning by the person. Numerous pixel reader beams that bathe the surface to be read, perform fine-tuning. Under this system, a holographic keypad begins with a holographic image of a real keypad, recorded by lasers on photographic film. This image is mounted on a plastic plate, which has infrared sensors behind it that can detect when the keypad is manipulated (Newkirk, G 2003, InfoSENTRY Services, Inc. www.infosentry.com, personal

communication).

While voice recognition could be hands free, the environment of a casino, with thousands of people entering the casino and the use of alcohol and late nights would prevent problem free introduction of this technology (Adcock S 2003 Voice Security Systems Inc. personal communication). The biometric techniques which, are touchless and could be applied in terms of acquisition in a casino would be face, iris and retina recognition.

An access control technique that requires the user to touch something will score poorly (5) while no contact is a preferable, scoring 1.

2.5.4 Accuracy

Biometrics are hard to make accurate, because computers do not handle people well. For example, "outliers" on the curve of possibilities, such as blind people who cannot use iris recognition, and those with a medical condition called pendular nystagmus that makes his iris move constantly. All these issues mean one should approach the selection of exclusion systems with extreme caution. It's tempting to think of biometrics as a kind of bar-coding system for people. But if the barcode on a can is misread by grocery scanners too many times, the manufacturer is told to redesign the label. With biometrics, you can't improve the people. Yet the plans for exclusion techniques never talk about outliers or alternative systems. They embrace wholly the myth of the biometric as the perfect identifier. Table 2. 6 details the misidentification rate for biometrics. Biometric system performance varies according to sample quality and the environment in which the sample is being submitted. While it is not possible to decisively state if a biometric submission will be successful, it is possible to locate factors that can reduce affect system performance.

Cards: Swiping too fast or slow, bending card, close proximity to a magnetic source, liquid, scratching.

Fingerprint: Cold finger, Dry/oily finger, High or low humidity, Angle of placement, Pressure of placement, Location of finger on platen (poorly placed core),

Cuts to fingerprint. Manual activity that would mar or affect fingerprints (construction, gardening) (Speir, M, 2003).

Method	Misidentification rate	Security
Iris Recognition	1/1,200,000	High
Fingerprinting	1/1,000	Medium
Hand Shape	1/700	Low
Facial Recognition	1/100	Low
Signature	1/100	Low
Voice printing	1 / 30	Low

Table 2. 6. Biometric Technology Comparison

Voice recognition: Cold or illness that affects voice, Different enrolment and verification capture devices, Different enrolment and verification environments (inside vs. outside), Speaking softly, Variation in background noise, Poor placement of microphone / capture device, Quality of capture device

Iris-recognition: Too much movement of head or eye, Glasses, Coloured contacts

Retina-recognition: Too much movement of head or eye, Glasses

Hand geometry: Jewellery, Change in weight, Bandages, Swelling of joints

Signature-recognition: Signing too quickly, Different signing positions (e.g., sitting vs. standing)

Facial recognition: Change in facial hair, Change in hairstyle, Lighting conditions, Adding/removing hat, Adding/removing glasses, Change in weight, Change in facial aspect (angle at which facial image is captured), Too much or too little movement, Quality of capture device, change between enrolment and verification cameras (quality and placement), ‘Loud’ clothing that can distract face location (Figure 2. 9).

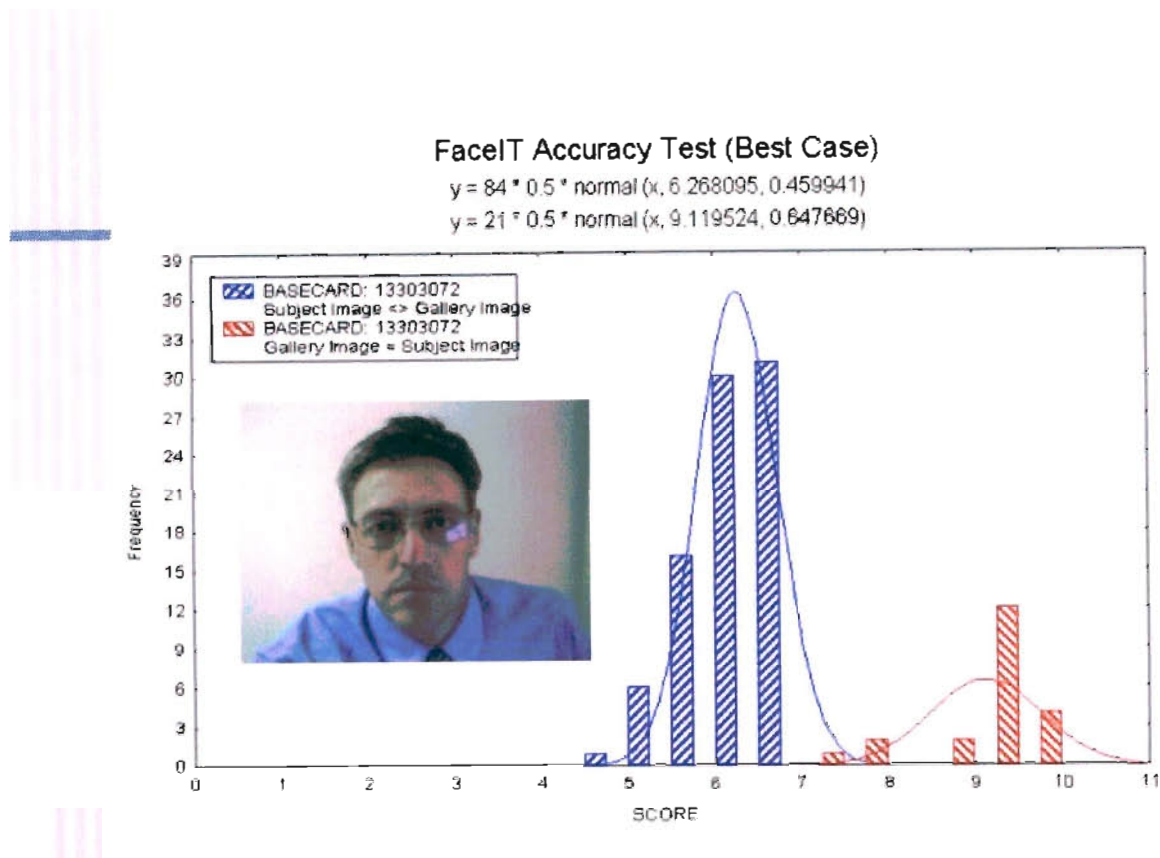


Figure 2. 9. Face recognition accuracy test

In addition, for many systems, an additional strike occurs when a long period of time has elapsed since enrolment or since the last verification. If significant time has elapsed, physiological changes can complicate verification. If time has elapsed since a user’s last verification, the user may have “forgotten” how he or she enrolled, and may place a finger differently or recite a pass phrase with different intonation. For the most part, a single strike will probably not materially affect the performance of a given system. However, as you have more and more strikes for a given submission, your chances of a successful verification diminish.

These strikes do not include inherent characteristics such as age, ethnicity, or gender, which can also affect system accuracy. The performance of many biometric systems varies for specific populations.

Iris recognition is the most accurate so scores 1, while the access control technique of the guard at the gate would be the least accurate so would score 5.

2.5.5 Response Time

Speed of recognition is important as far as the user experience goes, but compared to the time required to swipe a card, type in a name, show an identity photo, etc. biometrics are far faster with conditioned users. A proximity card that can be carried and recognised without the user doing anything is very fast (in milliseconds) and score a 1 while hand recognition where the user has to place their hand on the reader would be slower, scoring 5. The time to access the database is included in this time as it is part of the time the user would have to wait.

2.5.6 Intrusiveness

User perceptions of biometric technology are an essential element in their successful deployment. Technologies such as retinal recognition, which require significant effort on the part of the user, and which involve "sensitive" areas of the body, are perceived as being intrusive or invasive. Similarly, finger recognition technology is occasionally seen as invasive, with its connotations of criminality and police bookings. The intuitive response when considering user acceptance of facial recognition biometrics would classify it as the least problematic. After all, facial recognition facilitates human interaction as social animals.

The use of facial recognition biometrics in applications such as ATM access and network logon suggests that acceptance of the technology is high among users. Studies such as IBG's Consumer Response to Biometrics show, however, that there are some reservations, which may limit facial recognition's broader usage. Subjects who had used the technology were asked the following:

How would you feel using a finger recognition system instead of a PIN when using an

ATM?

1=Very	Comfortable
2=Somewhat	Comfortable
3=Neither	Comfortable nor Uncomfortable
4=Somewhat	Uncomfortable
5=Very Uncomfortable	

How would you feel using a facial recognition system instead of a PIN when using an ATM?

1=Very	Comfortable
2=Somewhat	Comfortable
3=Neither	Comfortable nor Uncomfortable
4=Somewhat	Uncomfortable
5=Very Uncomfortable	

Finger recognition rated 2.19, and face geometry (facial recognition) rated 2.43 - both excellent ratings, showing the viability of biometrics in this area, but markedly better for finger than face. If facial recognition is so simple to use, and so unobtrusive, why the lower rating?

There are a number of possible explanations to explain the above.

1. Many people simply do not like having their picture taken, much less having to look at their own low-resolution image on a computer screen or terminal. Both men and women expressed reservations, suggesting that the cameras being used were low quality (they were actually high-quality), insisting on wearing hats if being photographed, looking for mirrors etc. In contrast to finger recognition testing, where all subjects used the devices in spite of whatever reservations they may have had, some subjects in the face geometry testing simply refused to use the technology.
2. Despite its use in everyday life as our primary means of recognition, the face (as opposed to a signature or fingerprint) is not traditionally interpreted as an authentication mechanism. The face is almost too personal a part of the body to think of its being "scanned", broken into grids or axes, or having prominent features noted.
3. On the topic of intrusiveness, most vendors suggest that facial recognition is the least intrusive technology. In terms of ease-of-use, this is probably true - looking at a

camera and holding still momentarily is not a demanding task. However, if intrusiveness is defined in a different way, facial recognition may be among the most intrusive technologies. Aside from voice recognition, which is largely incapable of executing one-to-many searches (where the subject's identity is not known), face recognition is the only commonly used biometric which does not require cooperative subjects. A hidden camera could, indeed, take your picture, and perform one-to-many identification, without your knowledge. Without an enrolment, a one-to-many facial recognition application can not determine anything about an individual - name, customer #, etc.

User perceptions of face recognition relates directly to how people view themselves as unique individuals. As such, the issue of user acceptance must be carefully weighed in facial recognition projects, as it will have a significant impact on the project's success. Retina recognition would tend towards being intrusive scoring a 5 as the user has to position themselves in front of the sensor, while use of surveillance cameras would not be as intrusive (1).

2.5.7 Distinctiveness (Unique Identifiers)

Iris recognition has certainly the most distinct identifiers (Daugman, 1993) and scores a 1 while voice recognition has less unique identifiers and scores a 5. Other technologies fall between these two extremes.

2.5.8 Human Factor Limitations

Not all people will be able to use any exclusion system successfully every time. This implies that backup systems for exceptions will always be required. Selection of biometric in light of human factor limitation is important, since if one cannot use the biometric on the wide population it limits the success of the roll out. The effect of the emotional state and stress on voice and signature would play a significant factor in a casino environment. The availability of alcohol in casinos would have detrimental effects on keystroke but would have a lesser effect on other biometrics.

Access control based on physiological characteristics, which would be affected in a

casino environment score higher (5) and others that would not be affected would get a lower score (1).

2.5.9 Environmental Affects

It is preferable that the users be unsupervised so that they can self-ban themselves, but due to the complexity of the initial enrolment most systems would need to be supervised. The level of training required by enrolment personnel also varies over the technologies.

Face recognition would be affected by lighting (so would get a 5) while a card-based solution would not be affected by lighting (so would get a 1). If the application is to take place indoors at standard temperature, pressure, and other environmental conditions, particularly where lighting conditions can be controlled; it is considered a “standard environment” application. Outdoor systems, and perhaps some unusual indoor systems, such as the lighting generally found in casinos, are considered “non-standard environment” applications. The application will be indoors in a “standard” environment so people will not tend to cover themselves in varying and unpredictable ways however the low lighting conditions in casinos will present challenging conditions.

2.5.10 Stability of Trait

The aging of the population proves to be a challenge for some exclusion technologies, especially if the template cannot be regularly updated. Where a problem gambler or suspected thief is seen once and removed, not to reappear for many years, exclusion based on facial recognition (glasses, beard, skin tone) and hand recognition (arthritis) may prove difficult. For how long will the casino expect your enrolment images to remain usable? Template aging affects all biometric systems as a person’s physical and behavioural characteristics change. Some technologies, however, experience performance degradation more rapidly than others.

Face recognition is not stable over time, being affected by aging; shaving or growing of a beard or growth or loss of the hair on the head while Iris recognition is stable from an early age.

2.5.11 User Acceptability

Studies of user attitudes regularly show user acceptance of biometric technology to well exceed 90%. Nonetheless, there will always be a few people who object to any new technology. Use of a driver's license is familiar so would have a higher user acceptability (scoring a 1) while use of keystroke analysis would not be familiar to all (scoring a 4).

2.5.12 Market Share by Technology

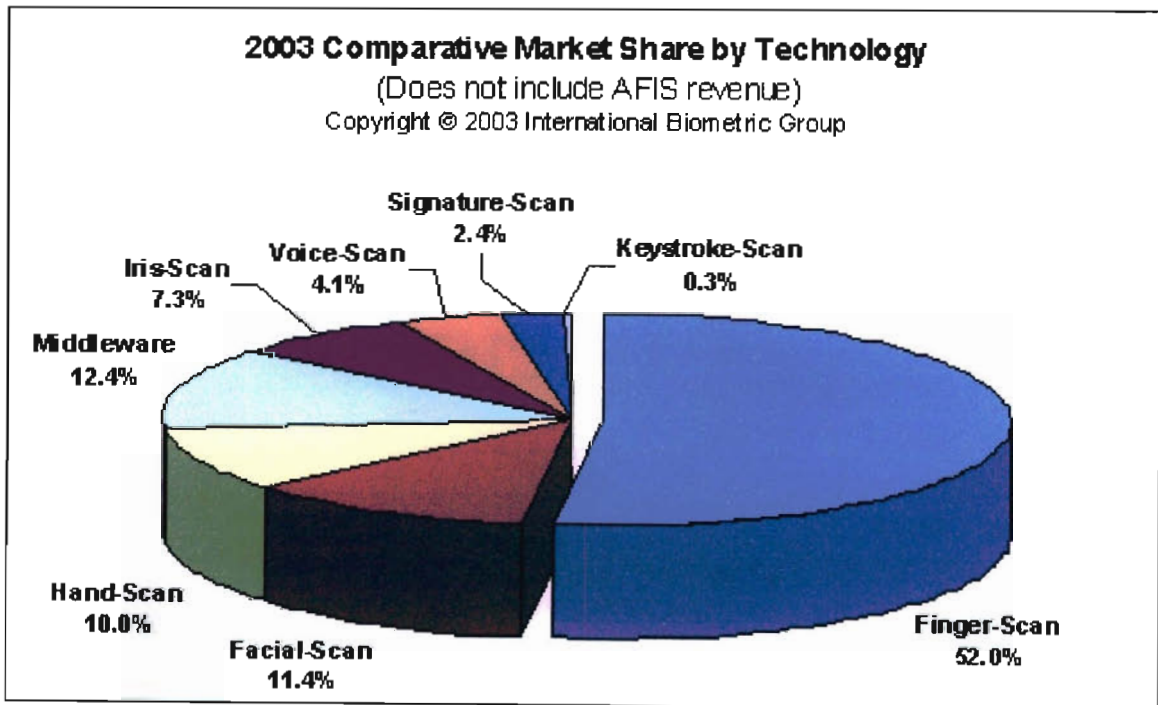


Figure 2. 10. Biometric Market Share by Technology

If one could assume that all biometric technologies were to some degree similar, which is certainly could not the case, then one could use the greater market share of finger recognition to assume that this is the appropriate technology. Other leading biometric technologies rated by market share are facial and hand recognition (Figure

2. 10). The problem with using market share is that the unique requirements of the casino environment pose serious problems solved only by the application of the correct technology.

Finger-recognition has the largest share of the access control market (so gets a 1) and Signature-recognition is not used very much at all (so gets a 5).

2.5.13 Mature Technology

Face recognition is highly rated technology, as it is familiar. However, technology has been applied to automatic face recognition only recently. Hence, face recognition is not considered a mature technology. Signature and voice are not mature technologies either, but the other biometrics are all well established, with finger recognition being the most mature. Biometric systems should not be selected based on the mature state of the technology but this continues to be one of the leading methods of selection. It is more important that the solution provider or technology provider be familiar with, and an expert in, the technology.

Fingerprint recognition is a mature technology (so gets a 1) while face recognition is still evolving (Hodosh, M, 2003), incorporating 3D features (so gets a 5).

2.5.14 False Acceptance

False acceptance, otherwise known as misidentification rate or False Non-Match Rate (FNMR), is the probability that a user's verification template will be incorrectly judged to not match that same user's enrolment template. In a 1:1 system, FNMR is the probability that User 1 will not verify against his or her own template. In a 1:N system FNMR is the probability that a user whose enrolment template located in a database will not be matched in a search (Figure 2. 11).

A guard with a file of photographs would tend to have a higher false acceptance, (letting people in who exist in the file, so would score a 5) while iris recognition has never been found to have a false acceptance (and would score a 1).

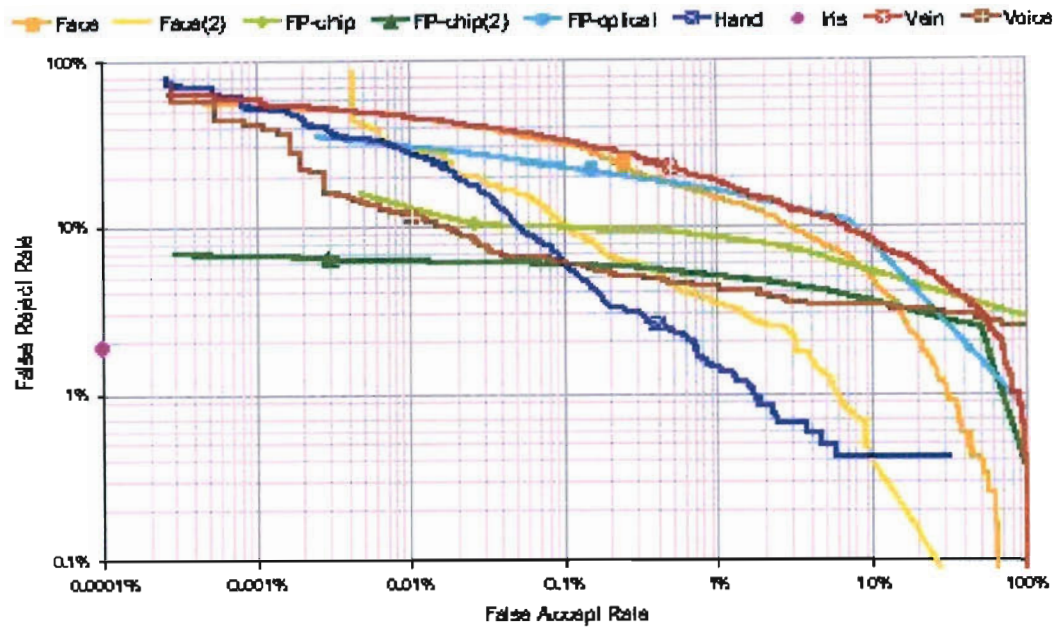


Figure 2.11. Detection error trade off: FAR VS FRR

2.5.15 False Rejection

False rejection, or (False Match Rate (FMR)), is the probability that a given user's verification template will be incorrectly judged to be a match for a different user's enrolment template (Figure 2.11). This is also referred to as false acceptance rate.

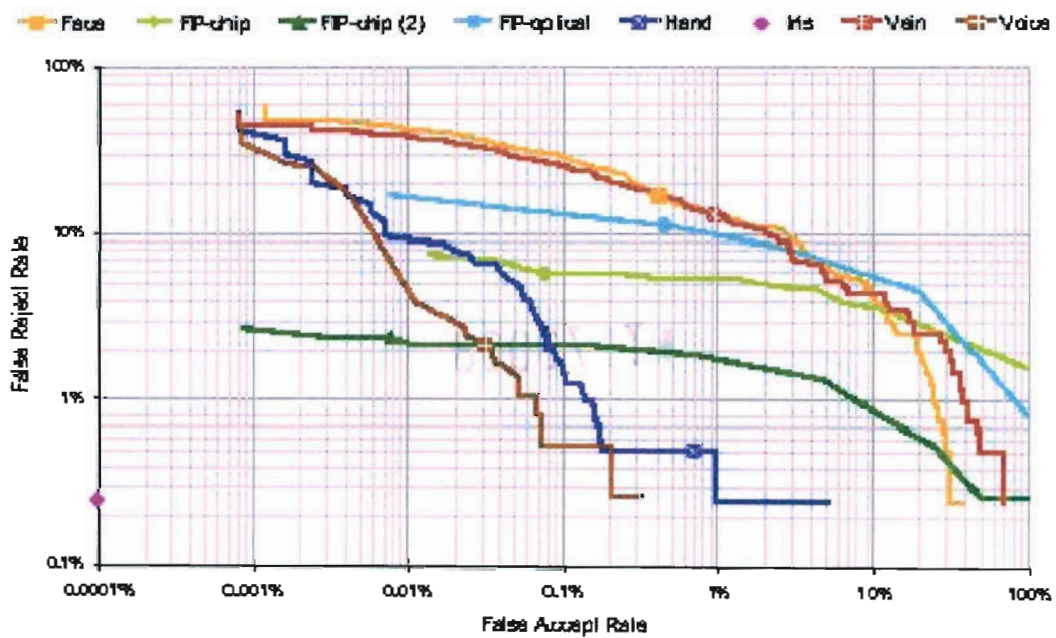


Figure 2.12. Failure to enrol rate (based on 3 attempts)

False rejection errors will require “exception handling” and will greatly decrease the throughput of the system. What number of errors per hour, day, can be tolerated? False acceptance errors will erode the perceived integrity of the system. Errors can be decreased, often at the cost of throughput rate, with more careful enrolment and more quality-control feedback to the user. Systems vary considerably in the amount of automatic quality control applied to the acquired images and the nature of the image quality information given the users.

Using a picture in an identity book to compare with the owner will have a higher false rejection (so will score a 5) than using a swipe card (which will score a 1).

Failure to enrol (FTE) rate – (not included in the study criteria). This is the probability that a given user will be unable to enrol in a biometric system due to insufficiently distinctive biometric sample(s) (Figure 2. 12).

The above three metrics must be evaluated when deploying a biometric system. Reliance on one or two metrics without the third can be highly misleading (Failure to enrol rate Available online at: <http://www.cl.cam.ac.uk/users/jgd1000/NPLsummary.gif>). The three metrics are strongly related, such that adjustment of matching or enrolment thresholds to increase security or convenience may impact each error rate (as shown in Figure 2.12). Decreasing the FMR, or making the system less susceptible to impostors, results in an increased likelihood that legitimate users will be rejected (false non-match rate). Decreasing the FTE by allowing a higher percentage of subjects to enrol successfully leads to higher FNMR, as users with low-quality biometric samples have an increased presence in the system. These metrics also change when system thresholds are adjusted.

2.5.16 Template Size (bytes)

Template sizes vary from 9 bytes to 6 Kbytes (Figure 2. 13) depending upon both vendor and technology. Not all template sizes are suitable for magnetic stripe or even smart card storage. Further more, some technologies require the storage of multiple templates for good performance.



Figure 2.13 depicts the typical template sizes for the leading biometric technologies. In some instances, specific vendors may utilise larger or smaller templates depending on the requirements of a given application. Template size can also vary depending on the size of the sample, such as the signature length and complexity, the length of a voice pass phrase, or the number of characters in a typed password (How Large Are Biometric Templates? 2003 Available online at: http://www.ibgweb.com/reports/public/reports/template_size.html).

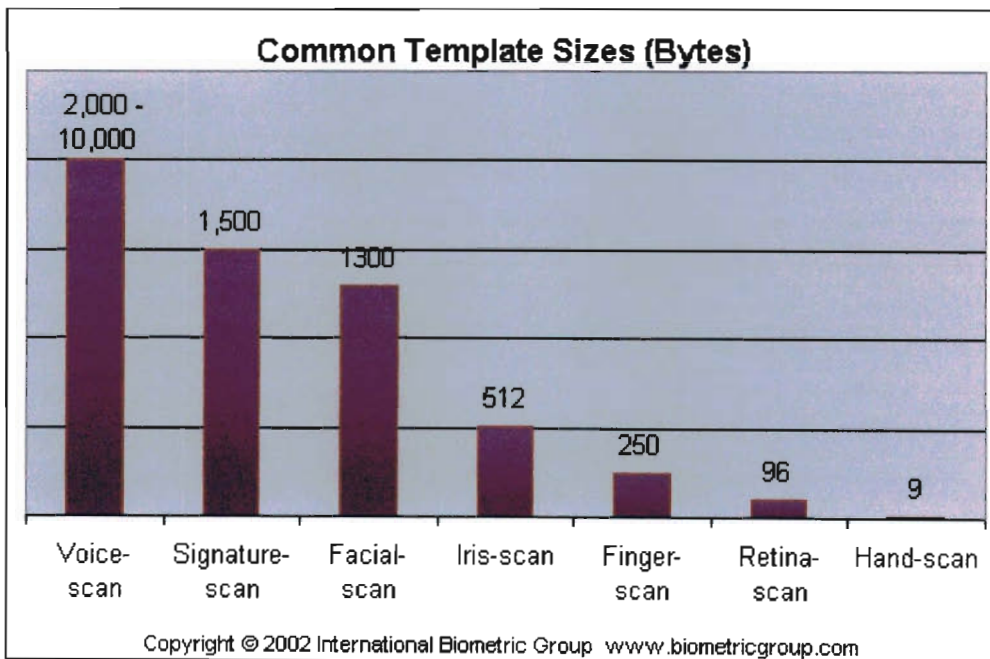


Figure 2. 13. Biometric Template size

A swipe card has a small template size (scoring a 1) while voice recognition has a much larger template (scoring a 5).

2.5.17 Remove Security Threats

Casinos have the right to ask gamblers who are too successful in their gambling to depart. A recent case from the Court of Appeal of New Zealand summarises the laws for casinos around the world, and comes down firmly on the side of the casinos. The fact that a casino is licensed "... shall not entitle any person to enter or to remain on the casino premises ... every person shall leave the casino premises when required to

do so by or on behalf of the holder of the licence [sic]." (Rose, 2002b).

The card counters and other members of the public who can increase the odds in their favour need to be identified by the casino surveillance department in order for any proposed exclusion technique to obtain full casino support.

Security threats that the casino security department would wish to exclude include bag snatchers, pickpockets and other undesirable characters, which would have a negative impact on the desirable casino patrons.

Fingerprint recognition would identify security threats if they were repeat offenders with a police history, (so would score a 1) while a swipe card (which could be transferred between persons) would not (so would score a 5).

2.5.18 Level of Impact on Existing System and Processes

The addition of exclusion techniques will inevitably lead to a change in the casino business processes. The software/hardware integration is the daunting problem of integrating the use of exclusion techniques into the existing processes. If the finished business system is not more efficient than the alternatives, the use of exclusion techniques will be regarded as a mistake.

Selection, based on ease of integration is important as a smooth transition to full functionality is desirable. The existing procedures, databases, and information need to be able to be incorporated into the proposed biometric system. There will be a period of transition where the old techniques will be used and the new biometrics will be introduced. The management of this period is crucial to the future success of the system.

Users of an access control application on a daily basis can be considered habituated after short period of time. Users who have not presented recently can be considered non-habituated. A more precise definition will be possible after better information relating system performance to frequency of use for a wide population over a wide field of devices is available. In general, all applications will be non-habituated during the first week of operation, and can have a mixture of habituated and non-habituated users at any time thereafter. Access control by the casino staff to a secure work area is

generally habituated. Access control to a casino by the public is generally non-habituated. Most users in casinos will be habituated to the technology, as they are regular visitors to the casino. That is, after a period of time, the average user will be accessing the technology regularly. Some technologies (fingerprint recognition, iris, retina and signature recognition) require greater user involvement and cooperation than others, such as facial recognition.

Face recognition would complement existing systems and processes (scoring a 1) while voice recognition would not complement any existing systems or processes (scoring a 5).

2.5.19 Compatibility with Existing Data

The system will be required to exchange data with systems operated by different casino management, i.e. be open. There are no existing standards for biometric templates, so systems from differing vendors will not necessarily be able to share templates or images, even if based upon the same biometric characteristic.

Using an identity book would complement existing records of ID numbers (scoring a 5) while hand recognition would not complement existing data (scoring a 5).

2.5.20 Identification of High Rollers (VIP's)

The casino marketing division would like to identify the high rollers so they can enhance their experience. Fingerprint sensors have been used to identify high rollers (McDonald, 2003).

A surveillance operator with a book of photographs would not be as successful in identifying VIP's (scoring a 5) while a proximity card would identify the VIP successfully (scoring a 1).

2.5.21 Verification / Identification

In applications verifying the positive claim of identity, such as with access control, the

deceptive user (“wolf” or bad guy) is cooperating with the system in the attempt to be recognised as someone s/he is not. This is a “cooperative” application. In applications verifying a negative claim to identity, the bad guy is attempting to deceptively not cooperate with the system in an attempt not to be identified. This is called a “non-cooperative” application. Users in cooperative applications may be asked to identify themselves in some way, perhaps with a card or a PIN, thereby limiting the database search of stored templates to that of a single claimed identity. Users in non-cooperative applications cannot be relied on to identify themselves correctly, thereby requiring the search of a large portion of the database. Cooperative, but so-called “PIN-less”, verification applications also require search of the entire database.

The question of maximum limits on user enrolment can be critical to large-scale systems. Limitations differ for verification and identification systems. Certain types of verification systems have no limits on potential growth. In a 1:1 system wherein matching takes place on a local PC or biometric reader, there is effectively no restriction on the number of users a system might incorporate. Spain enrolled millions of users in its TASS program, allowing users to access government-related health and social security forms from fingerprint enabled kiosks. 1:1 systems in which matching takes place at a central server are more limited - there are few examples of central-matching deployments over 1,000 users. If a large number of authentication events are taking place at the same time, a possibility in a network access environment, the response time from the central verification server may be inadequate to meet user expectations. Biometric vendors have developed products capable of performing verification across multiple servers to address this issue. Advances have been made in 1:N systems such that very large identification projects, some in the several tens of millions, are underway. These large-scale projects are generally based on fingerprint technology, although facial recognition is also capable of performing searches on large-scale databases. There are a number of steps that can be taken to increase the scalability of a 1:N system.

Binning is the process of separating biometric enrolments based on classifications inherent to the biometric data. In fingerprint systems, fingerprint templates with similar pattern types can be stored in a specific database segment, such that new templates with similar patterns only need be compared against this subset. This

reduces the overall number of comparisons that need to be made. Similar processes, such as placing fingerprint classification data in the template's header file, allow for rapid large-scale searches. Filtering is the process of using non-biometric information to limit the scope of a search. For instance, when a sample is submitted, the gender of the end user can be entered. This gender can be used as a filter to reduce the number of records that need be searched. In large-scale 1:N systems, enrolling two fingers as opposed to one can increase maximum searchable database size from the tens of thousand to the tens of millions. The system can handle more enrollees, due to the increase in user-specific data. Likewise, such a system will also increase its ability to use more distinctive classification data. Facial recognition vendors often utilise more compact templates when conducting searches against very large databases, employing a larger template only when searching against a more manageable set of users (Enrolment Limitations 2003 Available online at: http://www.ibgweb.com/reports/public/reports/enrollment_limitations.html).

Exception processing is the method of authentication employed for users incapable of successful biometric authentication. Exception processes can be secondary biometric technologies: passwords, pins, or live verifications. Casino deployments would be rendered inoperable if a large percentage of users required alternative verification. In any case, it is absolutely certain that some percentage of users – perhaps 0.5% - 10% - will be incapable of using a system successfully. Proper system design accounts for these users without reducing overall system security or penalising users for being unable to verify with a specific piece of biometric technology. The likelihood that a deployment will require a great deal of exception processing can be determined by referencing a technology's Ability to Verify (ATV) rate. This is not a commonly used metric within the biometric industry, but is very helpful in understanding real-world system performance (Ability to Verify 2003 Available online at: <http://www.ibgweb.com/reports/public/reports/atv.html>). The ATV rate represents the percentage of users who will have to be handled with a special fall-back process. The rate is simply a combination of the FTE and the FNMR:

$$ATV = (1-FTE)(1-FNMR)$$

This metric can be thought of as representing the group of users who cannot enrol

(FTE) along with users falsely rejected by the system (FRR). No system has a 100% ATV rate, but in general, a high ATV rate will make for a more effective system. When balanced with an acceptable False Match Rate, ATV can be extremely useful because it has an impact on three key aspects of biometric deployments:

1) Cost. One of the most expensive aspects of a biometric system is the cost involved with exception processing. Any user unable to be processed by the biometric needs to be processed by a fall-back procedure, meaning that dual systems must be maintained. Whether an alternate biometric, a password, or a live verification, there is a need for a separate enabling and support infrastructure.

2) Security. A low ATV means that a substantial percentage of users are not being verified by the system. The security provided by a system that can only verify 90% of its users may be acceptable for some deployments, but can be problematic in others.

3) Convenience. A low ATV may be a reflection of a difficult to use system. In situations in which user convenience is paramount, adjustments to enrolment and verification settings may be required to maximise the ATV rate.

Voice recognition can only be used for verification (scoring a 5) while using iris recognition allows for identification (scoring a 1).

2.5.22 Overt / Covert Acquisition

If the user is aware that a biometric identifier is being measured, the use is overt. If unaware, the use is covert. Deployments, in which users are aware that biometric data is being collected and used, and acquisition devices are in plain view, are less privacy-invasive than surreptitious deployments. User consent is a key principle of privacy-sympathetic deployment, and most covert systems prevent easy consent. Covert biometric systems, if deployed, should be deployed only in environments where a highly compelling interest is present.

Fingerprint recognition is naturally overt (so scores a 5) while face recognition can be done via a hidden camera (so scores a 1).

2.5.23 Behavioural / Physiological

It is a common belief that most biometric systems are capable of detecting liveness in biometric samples (Liveness Detection in Biometric Systems 2003 Available online at: <http://www.ibgweb.com/reports/public/reports/liveness.html>). Liveness detection in a biometric system ensures that only "real" fingerprints, facial images, irises, and other characteristics are capable of generating templates for enrolment, verification, and identification. From a security and accountability perspective, requiring a live biometric characteristic makes it difficult for an individual to repudiate that he or she accessed the casino (Chartrand, 2003). Although much of the biometric industry needs to go back to the drawing board to devise legitimate liveness detection capabilities, the problem of liveness detection is not unlikely to ever be fully addressed in biometric systems - nor does it need to be.

A behavioural biometric, characterised by a behavioural trait that is learnt and acquired over time, does not need to have a liveness check as it requires a live person to perform (so scores a low score). A physiological biometric, characterised by a physical characteristic rather than a behavioural trait, has to be checked for liveness (so scores higher).

2.5.24 Give / Grab Acquisition

Exclusion techniques that work only when the user gives the measurements (such as fingerprint recognition) score less (5) while techniques that can grab a measurement without user assistance (such as face recognition) score better (1).

2.5.25 Privacy Risk Rating

The users of the exclusion system will be customers of the system management and not employees. Clearly attitudes toward usage of the devices, which will directly affect their performance, vary depending upon the relationship between the end-users and system management. Public sector biometric usage can be seen as more risky than private sector usage due to the possibility of state or government abuse. Government collection of biometric data, without proper controls and restrictions is

highly problematic. On the other hand, private sector companies may be more tempted to share or link personal data for marketing or profiling purposes. Suitable protections should be developed for each type of environment. Casinos have shared information concerning people and techniques, which have threatened their profits. The exclusion system will be required, either now or in the future, to exchange data with other biometric systems run by other casinos. For instance, some casinos want to be able to exchange exclusion information with other casinos. If a system is to be open, data collection, compression and format standards are required. This encourages the abuse of the users' privacy.

Deployments in which the user maintains ownership over his or her biometric information are more likely to be privacy-sympathetic than those in which the public or private institution owns the data. User control over collection, usage, and disposal of biometric information is not possible in every deployment. A system capable of performing 1:N searches can be considered more susceptible to privacy-related abuse than a 1:1 system. A 1:N biometric system would be necessary for use in any indiscriminate large-scale searches. Protections regarding 1:N usage may need to be stricter than those employed in 1:1 usage. Biometric systems that do not retain identifiable data, such as physical access or network access systems, pose fewer privacy risks than systems that retain identifiable images. Templates cannot be readily used in law enforcement searches, and cannot be used to recreate identifiable images (BioPrivacy Impact Framework 2003 Available online at: http://www.ibgweb.com/reports_public/reports_privacy_deployment.html). Images are more sensitive data elements than biometric templates, and are more likely to lead to privacy-invasive usage.

The easier it is for someone to use the measurement to invade privacy (such as fingerprint recognition where one could compare the database against known criminals) the worse the score (5) while a measurement that has a low privacy invasion scores higher (such as hand recognition where no other records currently exist for hand recognitions (1).

Chapter 3 Role Players

3.1 Introduction

The role players were selected based on their involvement with the casino industry, the legislation or the customers of the casinos. The role players affected by controlling access to casinos have a variety of criteria they might apply to the selection of a solution.

The requirements of the various legal bodies (National Gambling Act, 1996) and provincial, which control gambling in South Africa, play a dominant role in possible casino exclusion selection, hence the inclusion of the local Gambling Boards as a key role player. The Gambling Board (<http://www.ngb.org.za>) set down guidelines for operation of casinos, which ensures the casinos do not cheat the public and that casinos follow the spirit of the law with regards to excluding problem gamblers. Neither National or provincial legislation prevent the use of exclusion techniques, and particularly biometrics in South African casinos, and all Gambling Boards approached would encourage any measure that assists casinos in identifying problem gamblers or reducing problem gambling.

Privacy issues have been found to be important in the rejection of various exclusion techniques, especially with the increase in identify theft (Vijayan, 2003), so this was included as a separate role player (Opinion Surveys 2003 by [privacyexchange.org](http://www.privacyexchange.org) available online at <http://www.privacyexchange.org/iss/surveys/surveys.html>). Is convenience (in the form of limited biometrics) or security (in the form of physical access controls) the primary driver of exclusion technique introduction? The Gambling Boards wish to prevent problem gambling while the casinos, competing for the entertainment Rand of the consumer, do not wish to inhibit public attendance while on the lookout for card counters and VIP's and appearing to appease the Gambling Board concerns.

Within the casino there are four primary departments that would be affected by the introduction of exclusion techniques (Van Wyk 2003 General Manager, Grand West Casino, personal communication). These are:

- Marketing (the attraction of users to a safe casino without any restrictions on legitimate gamblers),
- Operations management or process control (satisfying the requirements of the consumers, want as many high spenders as possible, any form of access control would not be encouraged, need to identify high rollers (VIP's)),
- Surveillance (limited to gambling within the casino, identify card counters, VIP's, known problem gamblers) and
- Security (of the casino as a whole, which is separated from gambling, concerned with remove of security threats, such as thieves & bag snatchers and identification of known problem gamblers).

Gambling Anonymous provided the viewpoint of the problem gambler to ensure that those with a gambling problem are prevented from going to casinos. The National Responsible Gambling Programme, (www.responsiblegambling.co.za) a public/private sector initiative, is the only one of its kind in Africa, and is acknowledged internationally to be exceptionally well-funded and among the most comprehensive in the world.

The public as a role player is crucial, as without them the casino would not exist. Studies have found that the public support safe access to casinos and removal of problem gamblers but have concerns over privacy, speed of access and use of information. People approve of the legalisation of gambling by a ratio of about 3:1. A similar ratio of people expressed concern about the negative affects of gambling on family life (The National Responsible Gaming Programme). The findings of a research project suggest that a third of South Africans gamble regularly (at least once a month). The initial impact of the gambling sector in 2000 amounted to just more than R3 billion with an additional spill over effect (indirect and induced impact) of R6,1 billion (Economic Impact of Legalised Gambling in South Africa, Study commissioned by the National Gambling Board of South Africa, 2002). The initial impact represents 0,38 % of the GDP of South Africa.

The following allocation between criteria was performed by the author, with input from a number of Cape casino security managers, but does not represent any specific existing or proposed casino but a universal casino.

3.2 *Marketing*

The marketing department would like to use the exclusion technique to enhance the brand building experience to the benefit of both customers and the firm. This would build customer confidence; loyalty and satisfaction, lower marketing costs, increase margins, and provide an opportunity for brand extension, rather than treating the customer as the enemy (Schrage, 2003). The exclusion technique must be able to be used to increase the loyalty of the patrons to the casino, with the ability to link it the exclusion technique to an e-mail, SMS or newsletters, etc. (which the patron would get either when they arrive at the casino or when they do not attend regularly) which will allow personalised, individual patron focus.

Exclusion techniques have some serious technological flaws. If a single false positive causes embarrassment to a customer, then one false positive per day is clearly too many. Yet exclusion systems are not capable of achieving the success rate necessary for those kinds of decisions. For the most part, biometrics appears to be a technology whose time has not yet come from the marketing viewpoint (Business Week 2003 Why Biometrics Is No Magic Bullet Available online at: http://www.businessweek.com/technology/content/jul2003/tc20030722_2846_tc125.htm).

If a casino decided to link the exclusion technique biometric to their preferred gambling cards, it would be a voluntary system, so that the casino would obtain the benefit of the system, in being able to identify high value customers, and not the problem gamblers. This may prevent some problem gamblers from gaining access, but as it is a voluntary system they could decide not to use the system. It will, however, prevent them from obtaining someone else's preferred gambling card, a problem the casinos are currently faced with. A family or circle of friends all use the same card, generating points which then allows the card holder into the high rollers

area, where free drinks and other benefits can be obtained. The partial introduction of the exclusion technique would give the major role players (the public, Gambling Boards and the casino) an opportunity to become familiar with the technology, after which it could be legislated, possibly with any changes that came about from first hand experience.

Figure 3. 1 details the weighting of selection criteria by the casino marketing division. The casino marketing division places high emphasis on ease of use for the public (20, as this is the crucial key to getting people to feel relaxed within the casino and come back), user acceptability (15, while it may improve with use, initial acceptability is crucial) and preventing false rejection (10, as one does not want to falsely accuse legitimate gamblers). Importance is placed on physical contact (8, mainly to do with hygiene factors and perceived transmission of bacteria), speed (7), removal of security threats (7, a safe environment which is not difficult to get into), identifying high rollers and privacy risk rating by marketing forces.

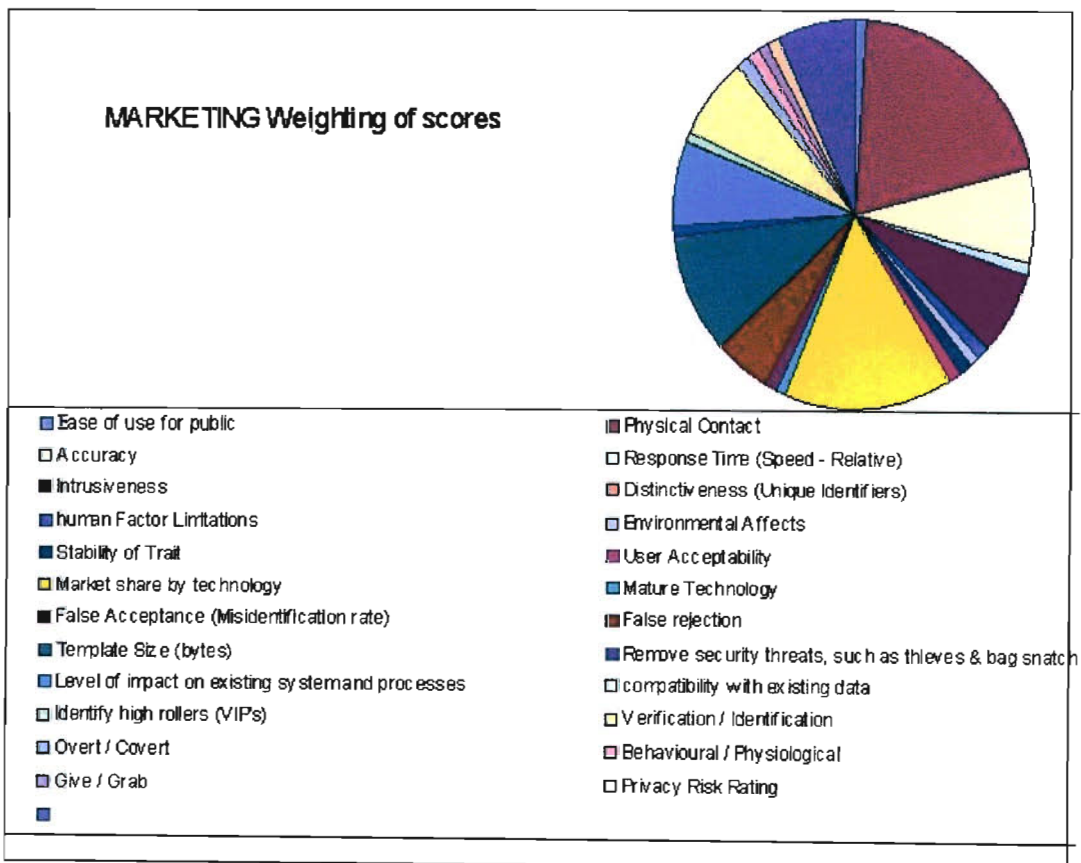


Figure 3. 1. Casino marketing - weighting of selection criteria

3.3 *Operations Management (Process control)*

Legislation is the stimulus, which could propel operations management, to become a greater strategic ingredient of the casino management. Rather than reacting to outside forces, the operations department could lead the way in solving the problem gambler issue. Tradeoffs exist among product and process choice versus the longer-term operating choices regarding quality, efficiency, schedule, and adaptability (Adam & Ebert, 2001). The first casino in South Africa to successfully apply, manage and maintain a problem gambler exclusion technique will earn the respect of all the role players. The requirements for casinos to collect information from customers with regard to the control of money laundering (Boitel, 2003) could provide weight to the use of an exclusion technique.

Throughput rate requirements for both enrolment and operation will affect the time required to enter the casino. Almost all systems require enrolment, with some techniques requiring multiple enrolments. The casino may have to provide personnel for the use of the exclusion technique during operation, to observe or operate the system and users. Non-cooperative applications will generally require supervised operation, while cooperative operation may or may not. Nearly all systems supervise the enrolment process, although some do not. In order to ensure that the exclusion technique really works it should be linked to every gambling transactions, i.e. every card hand or pull of a gambling machine, which is may be technically possible but certainly not economically feasible with the number of gambling slot machine and tables (Table 2. 6) in operation.

Operational management within the casino places a high emphasis on low cost (25, being a support activity), on speed (15, reducing crowds at the doors), ease of use for the public (10, less manpower to handle exceptions) and identifying high rollers (10, to ensure they have a good time) (Figure 3. 2). Lesser importance is placed on user acceptability (5, the public will come anyway), preventing false rejection (8, not concerned with turning legitimate gamblers away) and level of impact on existing system and processes (10) by operational management.

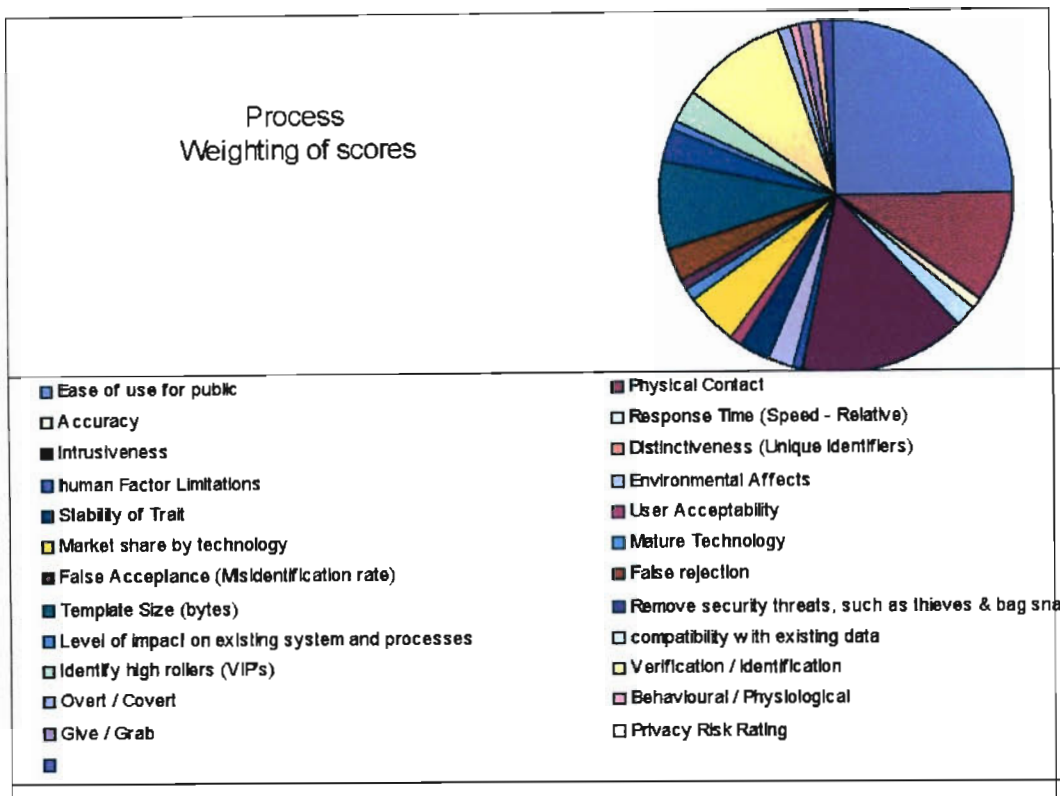


Figure 3. 2. Casino processing - weighting of selection criteria

3.4 Surveillance

The application of exclusion techniques in casinos will lead to an increase of the core competence of a casino. The surveillance department needs to grow with the use of surveillance department, is this not a subsystem and the combination of skills, processes, technologies and assets which come together within each subsystem to confer sustainable, repeatable and unique competitive advantage. Is this not essential for the casino to plan and execute new categories, which continue to build and reinforce these competences? The surveillance department has to abide by the minimal rules as set out by the relevant Gambling Board regulations (such as the Western Cape Gambling and Racing Board Rules & Regulations). However, most casinos have far higher internal requirements. Newsletters (such as Casino Surveillance Insider Tips) send out tips on how to avoid detection by the surveillance cameras (Tamburin, 2003).

The major casino syndicates have not yet started operating in South Africa (De Beer, D, Gold Reef City Casino Complex Surveillance & Security manager, Personal Communication). Images of the well know members of these syndicates have been forwarded to all South African casinos to be watchful for them. Grand West (Sun International, Cape Town) has over 1000 people on their “watch list” to be removed upon entrance come into the casino (Visagie, J, CCTV Technician, Grand West Casino, Personal Communication). Security reasons aside, preventing lawsuits like the \$1-million lawsuit by Lisa Dickert against the Ontario Lottery and Gaming Corp. for failing to enforce a self-exclusion programme, in spite of registering herself on a customers-blacklist, are prompting casinos to set up exclusion systems in place (Keeling, G, 2003).

The surveillance department within the casino places a high emphasis on accuracy (10, as they have had to enforce the exclusion policies in the past and know how important this is) (Figure 3. 3). Equal importance is placed on compatibility with existing data (10) as, for example Grand West has over 1000 images in their wanted list of problem gamblers and card counters.

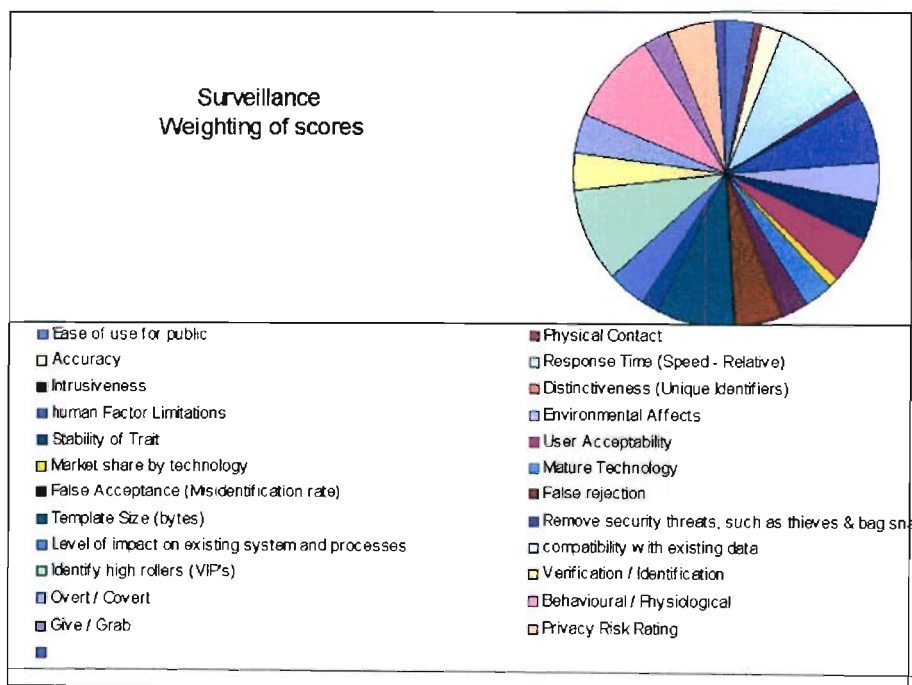


Figure 3.3. Casino surveillance - weighting of selection criteria

3.5 Security

Hemingway’s casino typifies the concerns of the security department within the casino, being the safe, responsible enjoyment of gambling. Hemingway’s casino

security official, Khayaletu

Makhotyana (Figure 3.4), is making sure all gamblers who have taken steps to bar themselves from the casino in the city are kept away.

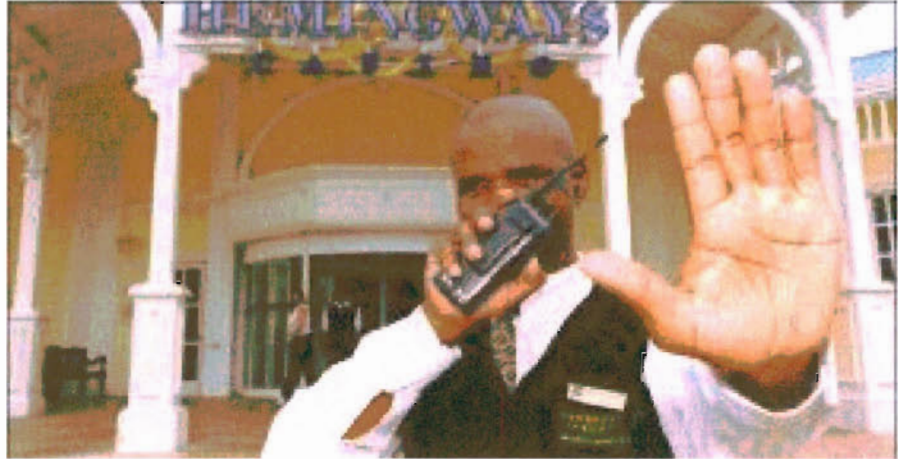


Figure 3. 4. Hemingway’s casino excluding problem gamblers.

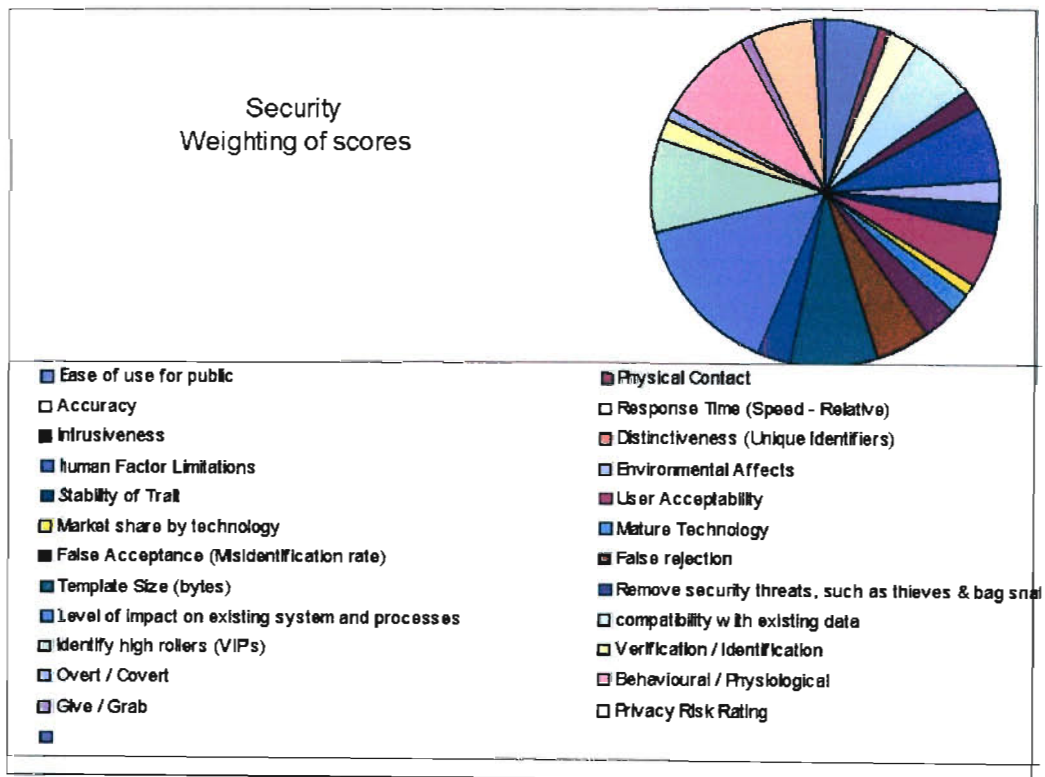


Figure 3. 5. Casino security - weighting of selection criteria

Casino management has permitted people to bar themselves. The programme was launched in September 2001 and has already seen about forty people banning themselves out of the building, "for a number of reasons -- financial, family or personal," surveillance manager Michael Fourie. The process involves the completion of a form set out by the Gaming Board, indicating from which premises the individual want to be banned. Applicants can choose whether they want to be barred for a year a few years or even for life. The applicants have their photograph taken and it is distributed to security personnel. Gaming manager, Annemie Turk, said that people who banned themselves were not necessarily "big time spenders" (Joe, W. S. 2003).

The security department within the casino places a high emphasis on the removal of security threats, such as thieves, bag snatchers and card counters (15) (Figure 3. 5). Importance is placed on compatibility with existing data (9, as they have a large number of records listing gangs who work in the area and people to watch out for) and the use of covert exclusion techniques (9, as there is a perceived need to watch these suspects without them knowing they are being observed).

3.6 *Privacy Rating*

Discussion concerning the implementation of large-scale exclusion systems always include speculation concerning public attitudes. One of the difficulties with what is said about public attitudes, on any subject, is that interest groups tend to impute their own fears, values and biases to the public. Most of the interest groups, who speak out on the subject of privacy, tend to have attitudes that are not friendly to the use of biometrics. The danger is that the more those views are repeated, the more they will tend to shape public opinion. Although there is much talk in the access control community about the public attitude, most who raise the point do so on a very superficial basis. There has been little organised dialogue or ongoing discussion concerning the subject of public attitude. It would be worthwhile study on attitudes and biases within the various segments of the biometric community, for and against large scale biometric systems. Some do not see it within their business interest for there to be rapid progress toward large systems, since they may not feel that their

technology or product is yet positioned to be competitive or dominant or are concerned that a niche they occupy or intend to occupy will be squeezed out by systems of more general application. Cf. Betamax vs. VHS; Mac OS vs. DOS vs. Windows. etc. The in depth study of the problems of privacy is beyond this thesis (see Westin, A. 2001 for more information).

New technology is boosting biometric surveillance (Grossman, 2003) and privacy may vanish forever. Just as each type of exclusion deployment can have a different impact on privacy, each exclusion technology bears a different relation to privacy. Some technologies have almost no privacy impact, and could scarcely be used in any privacy-invasive fashion. Other technologies are much more likely to be associated with privacy-invasive usage, either due to their core operation or due to extrinsic factors. It is possible that legal and political issues such as privacy and data access could hinder the application of biometrics (Lee, 2003). Most of the public polls suggest that there is nowhere near the opposition to exclusion techniques that is claimed. Very little effort has been made by the government, the press or the exclusion industry to explain, and to distinguish, exclusion techniques from the controls that ought be placed on informational databases. The result is that public concerns on the collection, use and release of data are being largely ignored.

Privacy concerns are very difficult to address, since they change over time, and differs across cultures. What is considered acceptable differs widely, and individuals are not consistent in themselves, as shown by the Internet being considered unsafe by many, but the same people will readily hand over their credit cards to a complete stranger at a restaurant or over an insure phone line. Of the biometric technologies considered, some open themselves more to privacy invasion than others. A biometric system, which stores information centrally, is clearly more capable of being abused than one in which biometric information is stored on a user's PC or even on a smart card. The privacy risks involved in biometric systems are heavily informed by the location of template storage and processing. By adhering to applicable best practices, even those technologies more capable of being misused - primarily facial recognition and fingerprint - can be deployed in a privacy-sympathetic fashion (BioPrivacy Best Practices 2003 Available online at: http://www.ilogweb.com/reports/public/reports/privacy_best_practices.html). The use of the information gathered by the casino for

exclusion purposes needs to be weighed against the possible use of the information. Fingerprint, face and iris have the highest privacy risk. It is essential that appropriate protection should be in place to ensure the technology is not misused (Mc Cullagh, D 2003). Self-reporting data would be wrapped in software or digital watermarks that guard against misuse of private information by tracking who has used the data, and where they have been moved (Roush, 2003). The manner in which proper protection occurs is beyond the scope of this study.

Identity theft, using stolen credit cards, phoney cheques, and other impostor scams to defraud casinos, is on the increase (Vijayan 2003). Until recently, the only way to way to attack the problem has been to add expensive screening and administration procedures. However, steps such as hiring security guards, maintaining accurate databases, reviewing identity documents, and asking personal questions have proven to be costly, stopgap measures that can be defeated by enterprising criminals. Compared to other methods of proving identity, biometrics are the only tools that can enhance personal privacy and still deliver effective solutions in situations that require confirmation of identity.

Privacy places a high emphasis on the privacy risk rating of the exclusion technology (19, as putting the wrong information in the wrong hands can ruin people's lives (Figure 3.6). Importance is placed on false rejection (15, as this leads to false accusations against the public) and user acceptability (10, as what might be acceptable to one person is completely unacceptable to another).

3.7 *Gambling Board*

There is an apparent lack of legal forethought, with the technology being developed at the speed of light, but the law that governs its use falling way behind. The Golden Horse Casino, that receives 2,500 visitors a day, has apparently not referred a single customer to Gamblers Anonymous for counselling since it opened its doors in 2001 (available online at: 2 June, Natal Witness, www.Witness.co.za). A compulsive gambler should be identified and banned from a casino. Gambling Anonymous say casinos are enjoying their "revenues at the expense of people's lives".

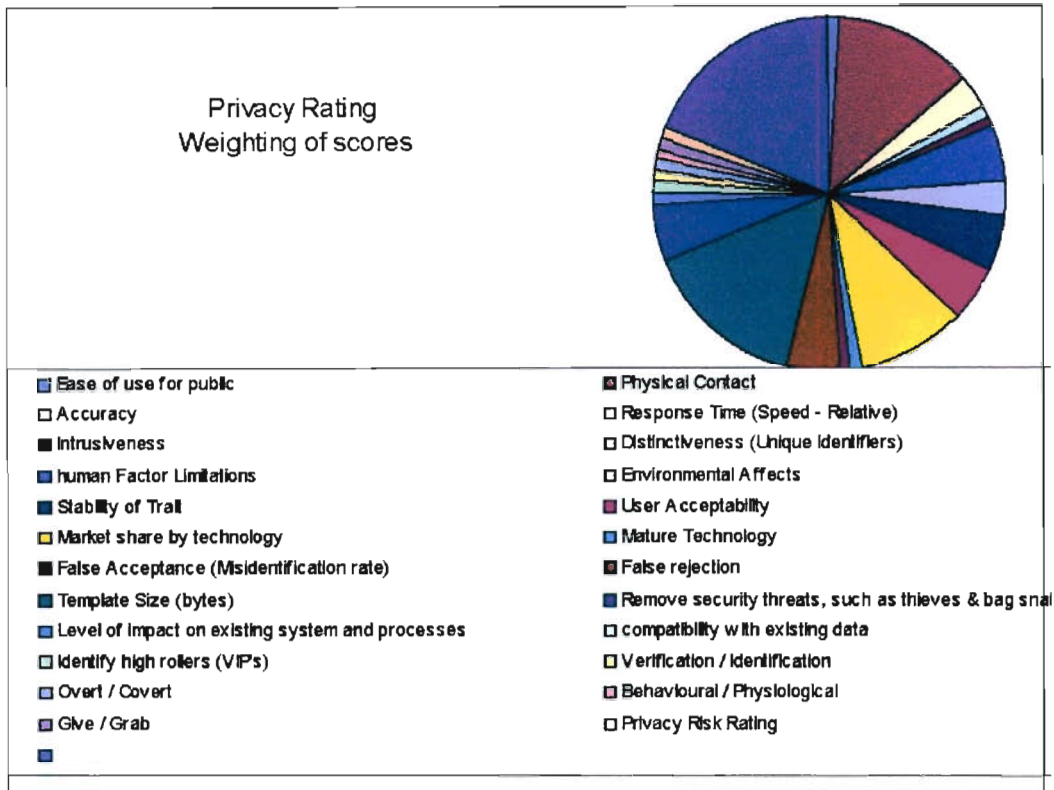


Figure 3. 6. Privacy issues - weighting of selection criteria

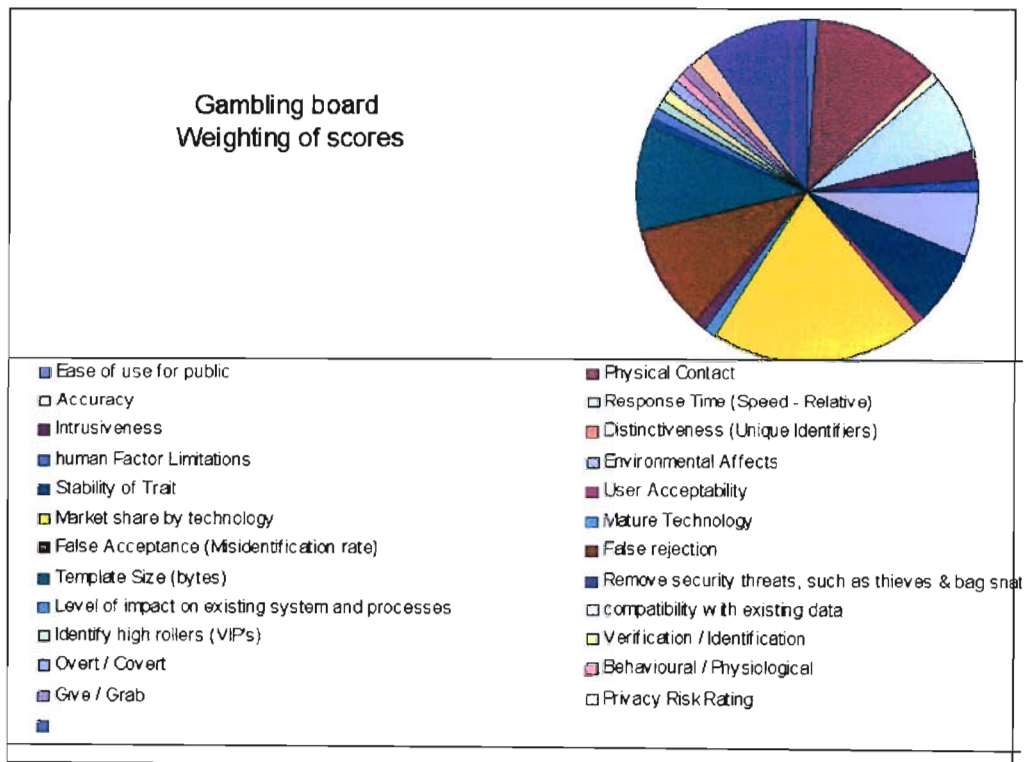


Figure 3. 7. Gambling Board - weighting of selection criteria

According to its licence agreement, the Golden Horse Casino must address negative social impact through a social responsibility programme. Since the casino opened, only six people have been reported to the Gambling Board. Casinos have three options when dealing with compulsive gamblers. The first is for the punter to ban him or herself, but according to Gambling Anonymous this is unlikely as the compulsive gambler is usually "weak". The casino does not make it easy, convenient or simple for problem gamblers to ban themselves from the gambling floor. In order to be banned from each casino the gambler is currently required to go to each casino with their identity document, where they will be photographed and logged as banned (Mayer, R 2003, Director of National gambling Problems - personal conversation).

The second option is for the casino staff to identify the compulsive gambler, which should be viable as the casino staffs are sent for training in this regard. Gambling Anonymous said this is where both the casino and the Gambling Board have fallen short in their duty to society. The third option is that families have the right to ask casinos to ban the punter. The Gambling Board has a responsibility towards the gambler, but relies on the casino to report problem gamblers (2 June, Natal Witness, available online at: www.Witness.co.za). There is no legislation preventing the use of any exclusion techniques in South African casinos. The local Gambling Boards would encourage any way to address problem gamblers (Moodley, 2003 – KZN Gambling Board, Personal conversation).

LAW ENFORCEMENT STATISTICS	TO DATE	YEAR TO DATE	JUNE 2003
Total number of closures	664	40	5
Total number of convictions	528	35	
Total number of cases withdrawn	91	2	
Total number of pending cases	24	3	
Total number of cases found not guilty	18	0	
Total number of gambling tables seized	69	0	0
Total number of slot machines seized	7.200	359	21
Total number of computers seized	210	69	0
Total number of slot machines destroyed	5.775	271	0
Total number of gambling tables destroyed	44	0	0

Table 3. 1. Law enforcement statistics

The Gambling Board would like to publish the number of problem gamblers removed from casinos under their jurisdiction, as with other law enforcement statistics (Table 3.1), which indicate the total number of illegal operators closed and machines confiscated during various raids executed by the Law Enforcement unit of the Board.

The Gambling Board places a high emphasis on user acceptability (20, as they are elected by the public and serve the interests of the public) (Figure 3. 7). Importance is placed on false acceptance (10, as problem gamblers getting into the casino defeat the object of having an exclusion technique), false rejection (10, as legitimate gamblers should not be concerned about being falsely accused as a problem gambler) and privacy rating (10, as maintaining confidential records is essential if problem gamblers are to come forward and exclude themselves).

3.8 *Gambling Anonymous*

South Africa is ranked fourteenth in the world in terms of gross gambling turnover, but 39th in terms of gross domestic product and ninety-first in terms of GDP per capita. It is estimated that the number of vulnerable problem gamblers at 5.29% of regular gamblers, and 3.8% of all adults who have easy access to gambling, which is 50% higher than in developed countries (The National Responsible Gaming Programme (NRGP) 2003 Available online at: <http://www.responsiblegambling.co.za/projects.html>).

The best approach to prevent problem gamblers entering casinos is to remove the banning responsibility from the casinos and give it to an independent body, such as Gambling Anonymous, to take over the role of coordinator to manage the collection and distribution of the biometric data to the casinos. This would ensure that the collection of the biometric was separated from the casino, as this certainly seems to be a conflict of interest scenario. Gambling Anonymous would distribute the information to the casinos who would add in their own wanted list, from international casinos, local police databases, VIP's etc. Hence the casino would have a stake in applying the biometric successfully, unlike the current situation where there are

different hard copy files of different categories of wanted people. The logs of the use of the system could be published showing that the biometric system was being used, without naming those found or removed. As they would not be required to show whom the match was, no privacy laws would be broken. The number of positive matches could then be tracked and reported as in Table 3.1.

Gambling Anonymous places a high emphasis on compatibility with existing data (20, as they have many thousands of enrolled problem gamblers as photos and identity numbers) and false acceptance (20, as once a problem gambler has taken the step to be excluded they should not be allowed back into the casino) (Figure 3. 8).

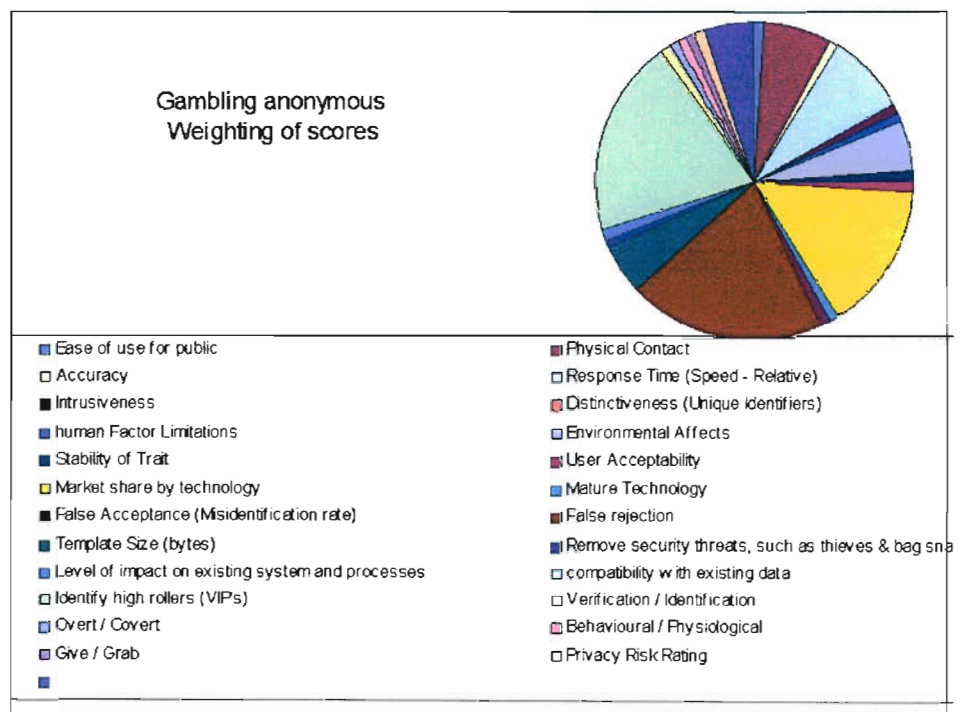


Figure 3. 8. Gambling Anonymous - weighting of selection criteria

3.9 Public

Recent news reports (Chips down forever for neglectful parents, 2003-07-01, Do gamblers not pay their municipal accounts? available online at: http://www.iol.co.za/index.php?click_id=196&art_id%20=vn20030606070354272C897629&set_id=1) highlight the concerns the public has with casinos and the lack of effort to stop problem gambling. 'Limit impact of gambling' South African's now apparently spend 5 times more on gambling products than on books (available online at:

http://www.news24.com/News24/South_Africa/Politics/0..2-7-12_1376881.00.html). Those jingling coins came out of empty pockets 19th June The Star available online at: (<http://www.thestar.co.za/index.php?fSectionId=225&fArticleId=172297>). Don't bet on gambling 10th June South Africa Statistics from South Africa show that 22% of casino gamblers are unemployed (available online at: <http://www.dailynews.co.za/index.php?fSectionId=502&fArticleId=167222>). 'The Gambling Board must come to its senses' 6th June Johannesburg & Cape Town, South Africa Source: Independent Online/Cape Times (available online at: http://www.iol.co.za/index.php?click_id=196&art_id=vn_20030606070354_272C897629&set_id=1). In a survey “Public Attitudes Toward the Uses of Biometric Identification Technologies by Government and the Private Sector” a number of relevant points are raised which will not be repeated here (available online at: http://www.search.org/policy/bio_conf/Biometricsurveyfindings.pdf).

The public places a high emphasis on ease of use (25, as a system that is difficult to use will not be adopted and the consumer will migrate to either another casino or illegal gambling) (Figure 3. 9). Importance is placed on intrusiveness (17, as if the exclusion technology is not seen it is not of the same concern) and physical contact (15, as something you touch is certainly noticeable and no matter how scientific one is about it, the lack of education of the public and events such as SARS would mean a lack of support for the exclusion technique).

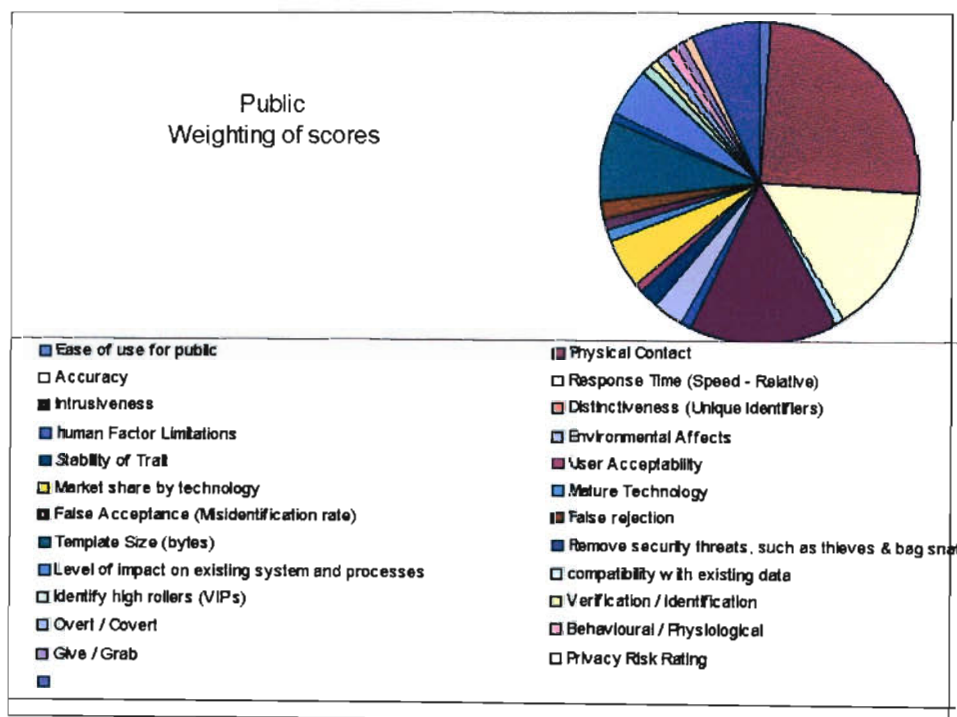


Figure 3. 9. Public - weighting of selection criteria

3.10 Weighting of Role Player Importance

In order to determine the most appropriate exclusion system for a casino the eight role players were assigned a rating ((Figure 3.10) to indicate the relative importance of each role player to the business decision process, using a weighted score system (total 100). The values were decided upon in consultation with various casino role players (Cape casino security managers, 2003 Caledon Casino, Hotel & Health Spa, personal communication) hence represent no particular casino.

All the role players in the casino are concerned about problem gamblers and the new National Gambling Act strengthens the provisions for the exclusion of problem gamblers from casinos hence Gambling Anonymous was deemed to have the highest influence, obtaining a majority weighting (30%) (Gambling Anonymous also had a substantial role in formatting the new National Gambling Act).

Due to the importance, as indicated in the introduction, of the legislative factors on casinos operating in South Africa this influenced the resulting scores considerably. The Gambling Board (both National and Provincial) obtained a 23 % weighting (Figure 3. 10). The casino surveillance department has not only had to enforce the exclusion policies, but appears, possibly in conjunction with a neutral third party, to be the way exclusions will continue to be enforced and obtained a 20% weighting. It might be concerning that privacy concerns only rated 8% if the all role players had not placed problem gamblers and their representative Gambling Anonymous as the number one concern facing casinos. The remaining departments will only increase their influence in the weighting once the concern for problem gamblers has been addressed.

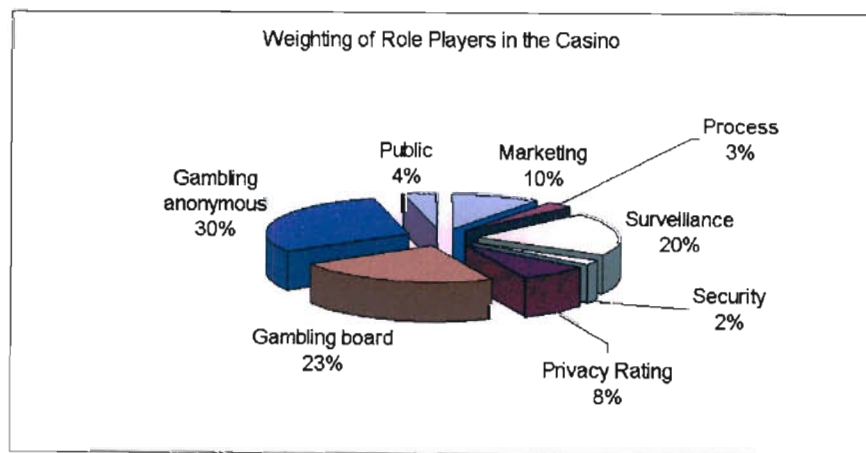


Figure 3.10. Weighting of Role Player Importance

Chapter 4 Results

The full results of the application of the proposed framework, applied to exclusion from gambling of problem gamblers, as required by the new National Gambling Bill, appear in Appendix I (Results of Role Player Evaluation) and Appendix II (Role Player Evaluation of Evaluation Techniques), where the main role players (8) in the casino industry evaluated, using a 1-5 Likert scale; with 1 being best, and 5 being worst, a number of possible exclusion techniques (13) according to a range of important criteria (25).

4.1 Role Player Rating of Exclusion Techniques

Marketing (Figure 4. 1) rates the use of the surveillance operators with a file of photographs as the most optimal exclusion technique (205) and fingerprint recognition as the least desirable (331).

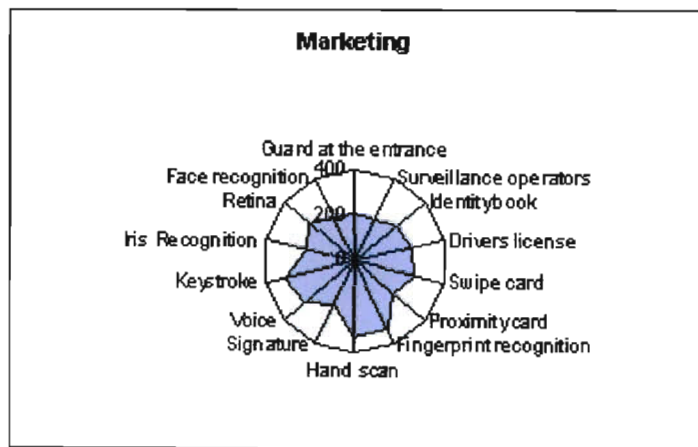


Figure 4. 1. Casino marketing department evaluation of exclusion techniques

Marketing (208) rates the use of face recognition highly as a means of combating problem gamblers (Figure 4. 2). Casino security (235) rates face recognition as being less suitable than marketing.

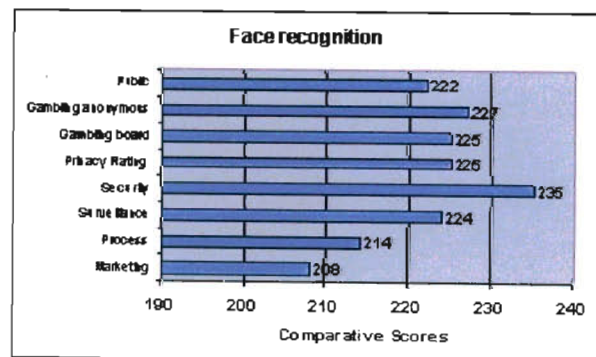


Figure 4. 2. Face recognition evaluation by casino role players

Process or casino operations (205) followed by marketing (213) rate the use of a guard at the entrance with a file of photographs as the most optimal exclusion technique (205) and retina recognition as the least desirable (321) (Figure 4. 3). Security (296) and surveillance (280) feel the use of a guard at the entrance with a file of photographs would be less desirable (Figure 4. 4).

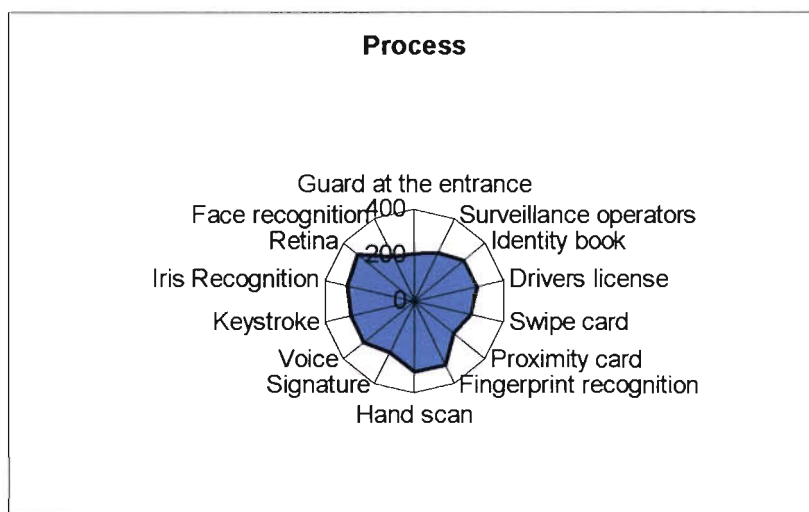


Figure 4. 3. Casino operations department evaluation of exclusion techniques

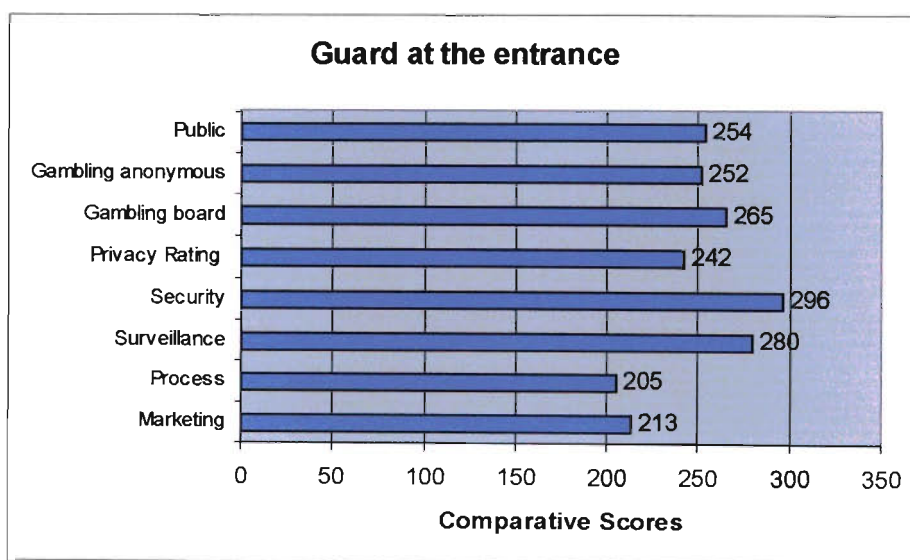


Figure 4. 4. Guard at the entrance evaluation by casino role players

Surveillance (214) and marketing (215) rate the use of iris recognition as the most optimal exclusion technique (Figure 4. 5). The process/operations department (301) and Gambling Anonymous (296) feel this would be less desirable (Figure 4. 6). Surveillance rates the use of retina recognitions as a means of combating problem gamblers highly (225) and hand recognition as the least desirable (304).

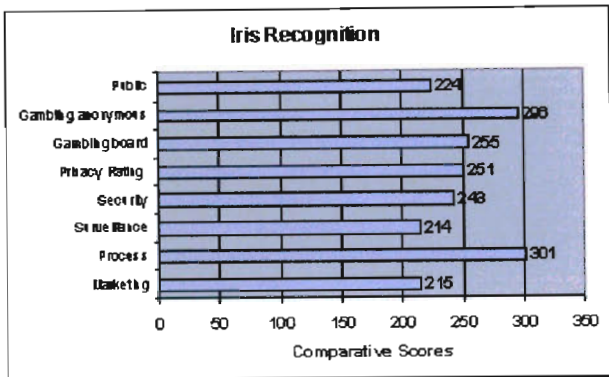


Figure 4. 5. Iris recognition evaluation by casino role players

Iris-recognition technology requires reasonably controlled and cooperative user interaction - the enrollee must remain still in a certain spot. Many users struggle to interact with the system until they become accustomed to its operations. In applications where user interaction is frequent (e.g. employee physical access), the technology becomes easier to use. However, applications in which user interaction is infrequent (e.g. gamblers who only visit the casino monthly) may encounter ease-of-use issues.

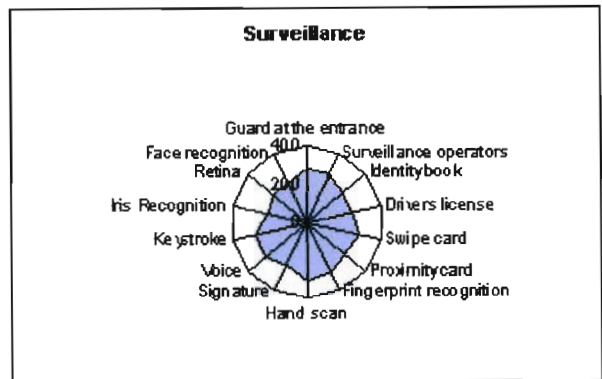


Figure 4. 6. Casino surveillance evaluation of exclusion techniques

The accuracy claims associated with iris-recognition technology may overstate the real-world efficacy of the technology. Because the claimed equal error rates are derived from assessment and matching of ideal iris images (unlike those acquired in the field), actual results may not live up to the unrealistic projections provided by leading suppliers of the technology. Lastly, since iris technology is designed to be an identification technology, fallback procedures may not be as fully developed as in a verification deployment (users accustomed to identification may not carry the necessary ID, for example). Though these issues do not reduce the effectiveness of iris recognition technology, they must be kept in mind should a casino decide to implement an iris-based solution (Iris Recognition Issues, 2003 Available online at: http://www.ibgweb.com/reports/public/reports/iris-scan_issues.html).

The security department rates the use of face recognition as the optimal exclusion technique (235) and hand recognition as the least desirable (316) (Figure 4. 7).

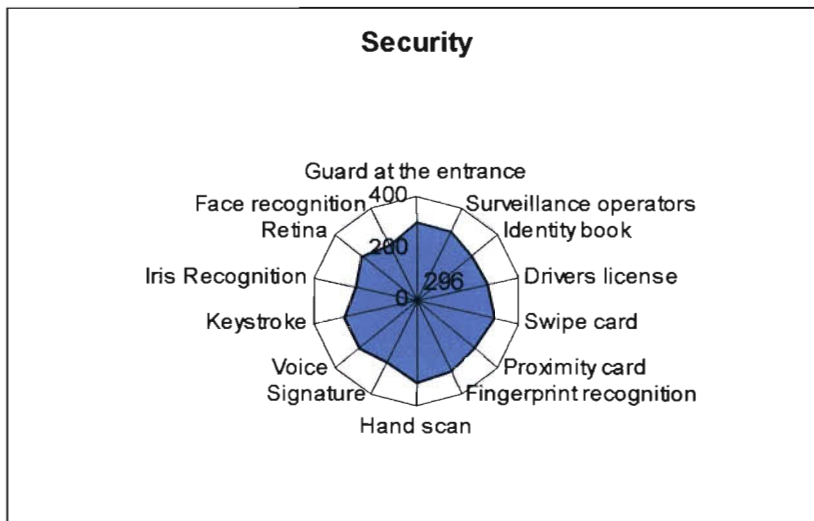


Figure 4.7. Casino surveillance department evaluation of exclusion techniques

Privacy rating dictates the use of surveillance operators with a file of photographs as the most optimal exclusion technique (222) and fingerprint recognition as the least desirable (369) (Figure 4. 8).

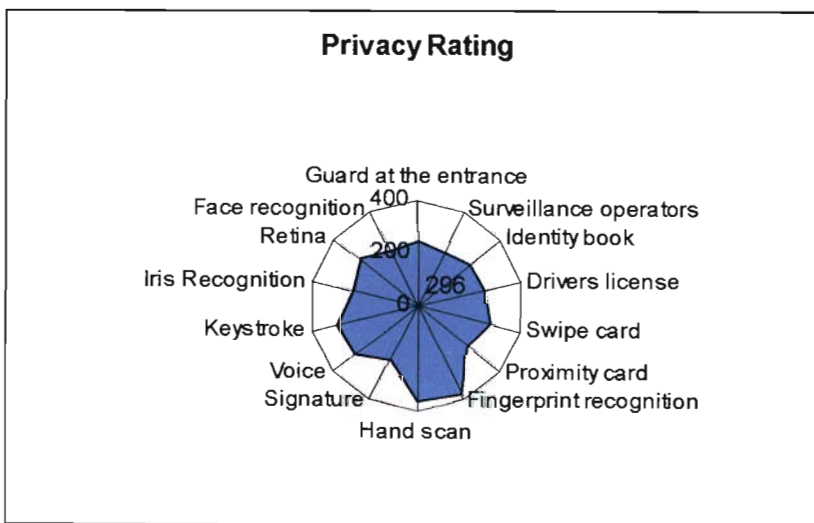


Figure 4. 8 Casino surveillance department evaluation of exclusion techniques

The Gambling Board rates the use of a proximity card as the most optimal exclusion technique (220) (Figure 4. 9) and fingerprint recognition as the least desirable (369) (Figure 4. 10). Surveillance (294) and security (296) rate the use of fingerprint recognition highly as a means of combating problem gamblers highly. The public (397) and Gambling Board (386) feel this would be less desirable.

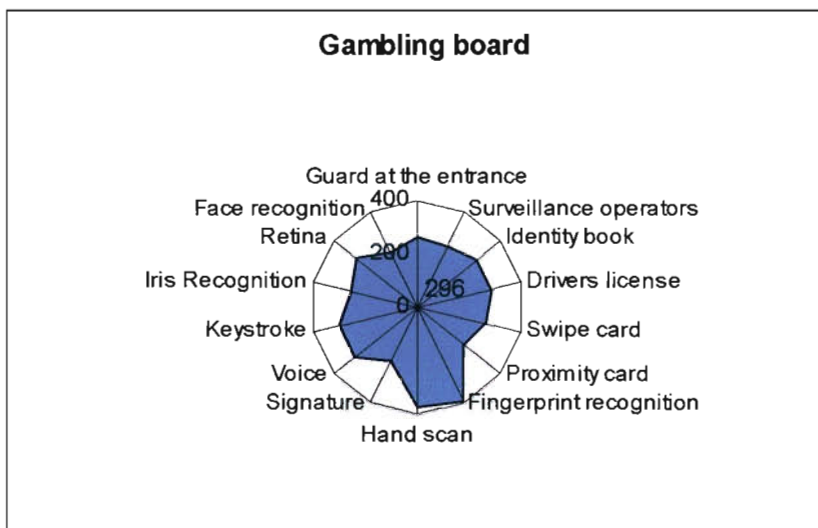


Figure 4. 9. Gambling Board evaluation of exclusion techniques

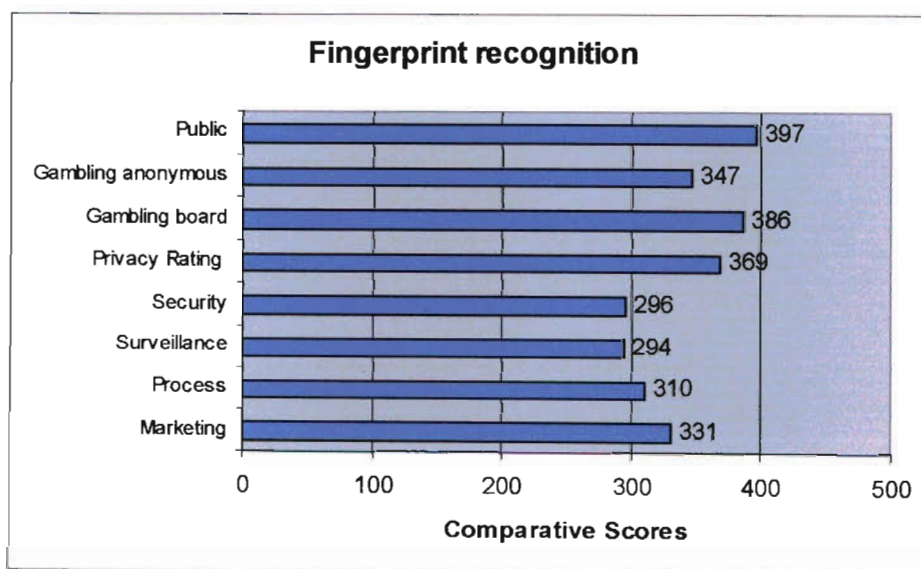


Figure 4. 10. Fingerprint recognition evaluation by casino role players

Gambling Anonymous rates the use of a swipe card as the most optimal exclusion technique (211) and fingerprint recognition as the least desirable (347) (Figure 4. 11). Gambling Anonymous (245), followed closely by surveillance (246) and then marketing (248) rate the use of an identity book photo comparison and a check of the persons ID number highly as a means of combating problem gamblers (Figure 4. 12). The public (311) feel this would be less desirable.

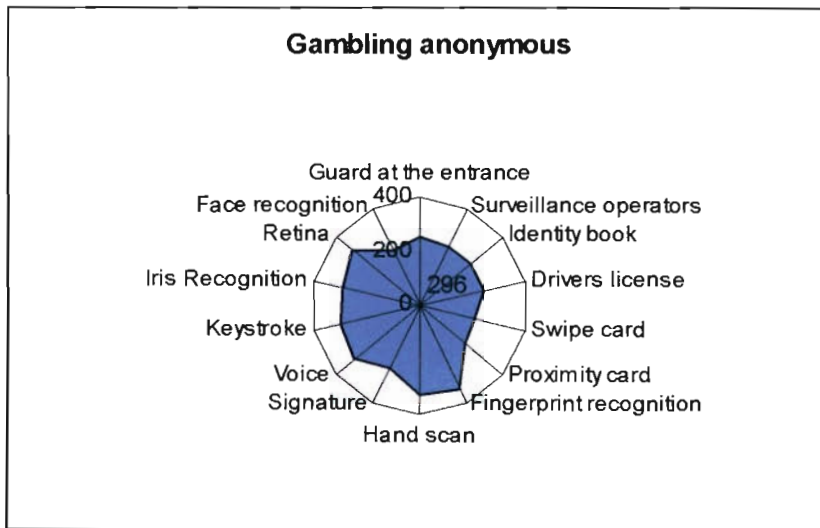


Figure 4. 11. Gambling Anonymous evaluation of exclusion techniques

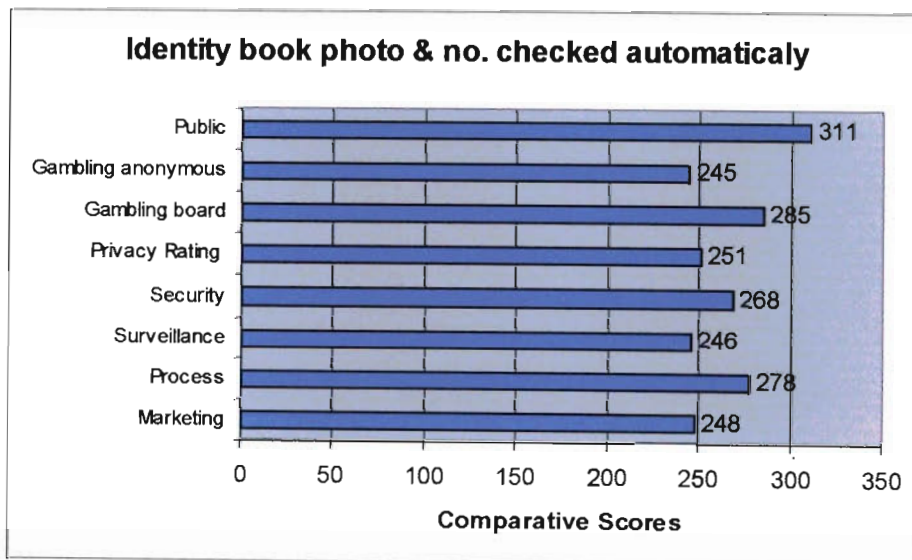


Figure 4. 12. Iris recognition evaluation by casino role players

The public rates the use of a proximity card as the most optimal exclusion technique (218) and fingerprint recognition as the least desirable (398) (Figure 4. 13).

Surveillance (282), process (283) and security (283) rate the use of voice recognition highly as a means of combating problem gamblers. The public (334) feels this would be less desirable (Figure 4. 14).

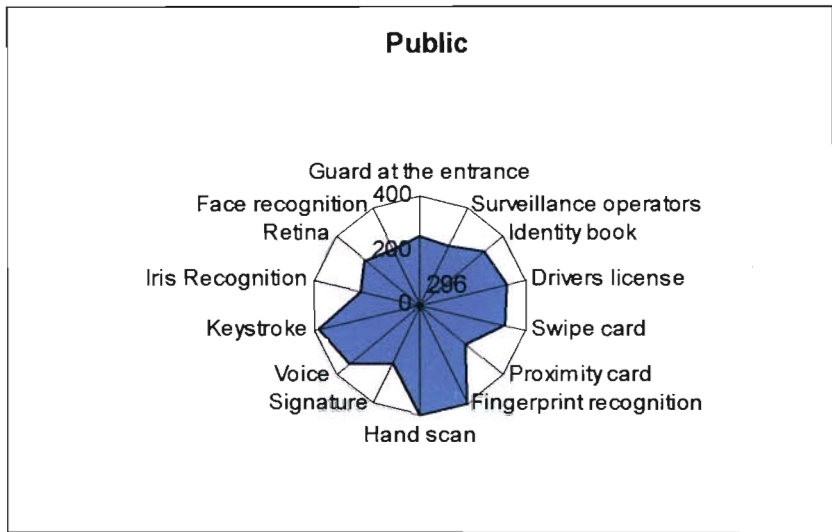


Figure 4. 13. Fingerprint recognition evaluation by casino role players

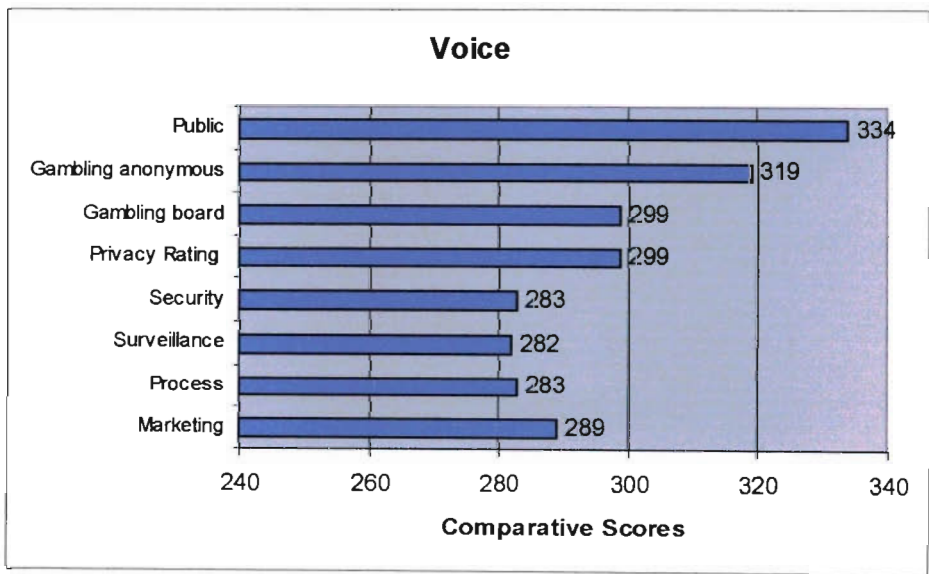


Figure 4. 14. Iris recognition evaluation by casino role players

Chapter 5 Evaluation & Recommendations

5.1 Most Acceptable Exclusion Techniques

The role player rating was applied to each exclusion technique to create a weighted score where face recognition was determined as the most accommodating (223) to all the role players, followed by proximity cards (230) with fingerprint recognition (345) as the least desirable (Figure 5.1 and 5.2)..

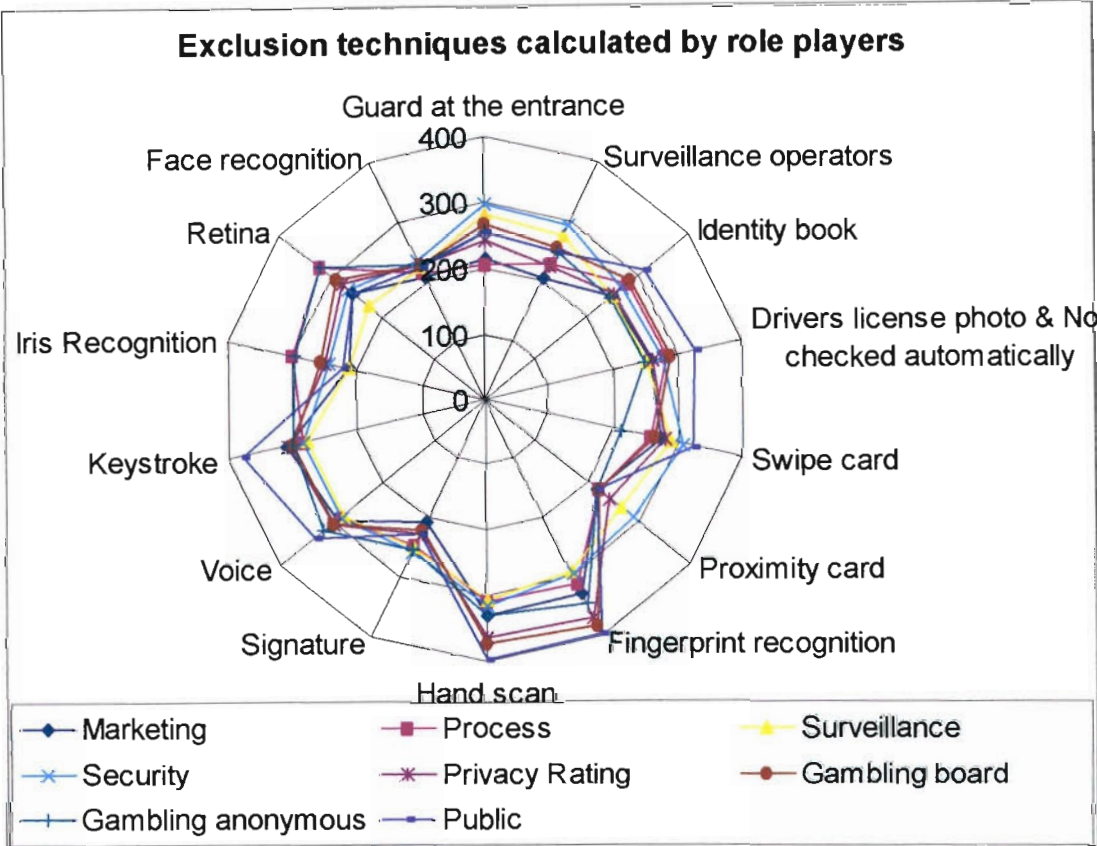


Figure 5.1. Exclusion techniques calculated by role players

It was determined that the only biometric currently available that may meet some of the most important Gambling Board, casino and public criteria, while not negatively affecting the process, marketing or privacy concerns, is face recognition (Figure 5.2). The advantages are: low cost, utilisation of existing records and infrastructure (cameras), possibility of linking to the casino Most Valuable Player cards for gradual deployment into the casino environment and, as the exclusion technology proposed is

semi-automatic, with the operator manually capturing the image of the suspected problem gambler and then the face recognition software automatically comparing the suspect to a binned database (based on sex, age, race etc.), few false rejections should occur. Statistics of problem gamblers identified and removed can then be published.

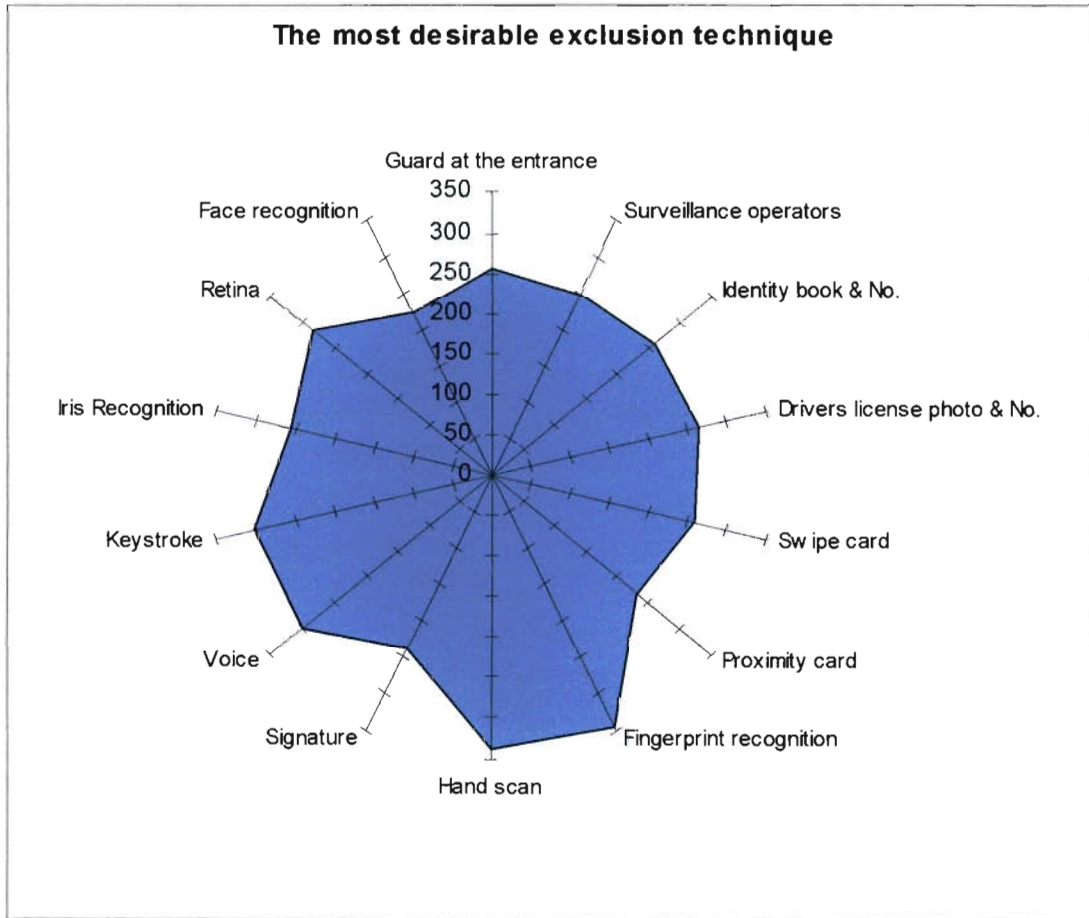


Figure 5.2. The most desirable exclusion technique for casinos

Having selected the most appropriate exclusion technique by business perspectives there remains a substantial amount of work to ensure the system is implemented correctly, widely distributed, continually updated and maintained, as without any one of these any exclusion technique will fail.



Figure 5.4. Surveillance Information Network (Sin) Report

Using face recognition the person who wishes to be banned could do the following: The person could stand in front of the face recognition PC where a software application takes the person through the required steps to self-ban themselves. A camera would take a picture and the user would add the ID no., name and casinos from which they wanted to be banned from. In this way the casino would not have to be involved with the banning. The problem gambler could then go to a number of venues other than the casino, as is the case at present, and be banned. Figure 5. 3 shows (Pepin, 2003) the type of information that might be collected along with the current photo and identity number.

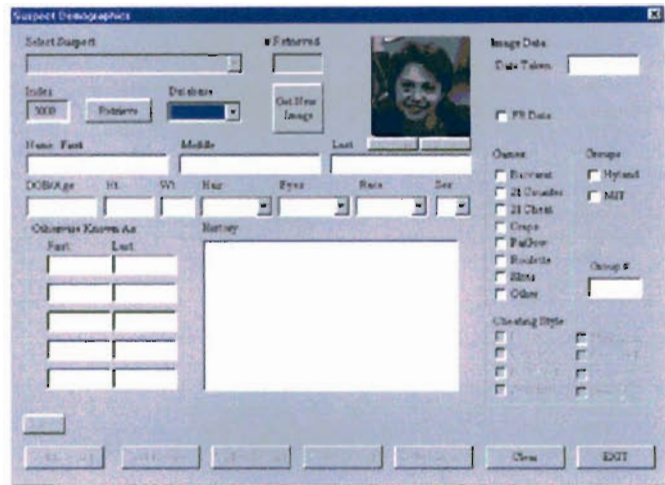


Figure 5. 3. Suspect demographics

When the person to be excluded (problem gambler or suspected thief) information is gathered from a remote station (Gambling Anonymous or another casino) the casino would received a surveillance information network (SIN) report (Pepin, 2003) (Figure 5. 4) which details which casino the person is banned from, the period of the banning, the identity number, favoured techniques or games and distinguishing marks and possibly colleagues associated with the suspect. It would then be possible to send in (via snail mail, e-mail, web form, etc.) three different pictures to be loaded into the database, detailing the name, ID number and contact number for verification. The casino or independent body would then contact the person, confirming data submitted and confirm local casino only, province or countrywide.

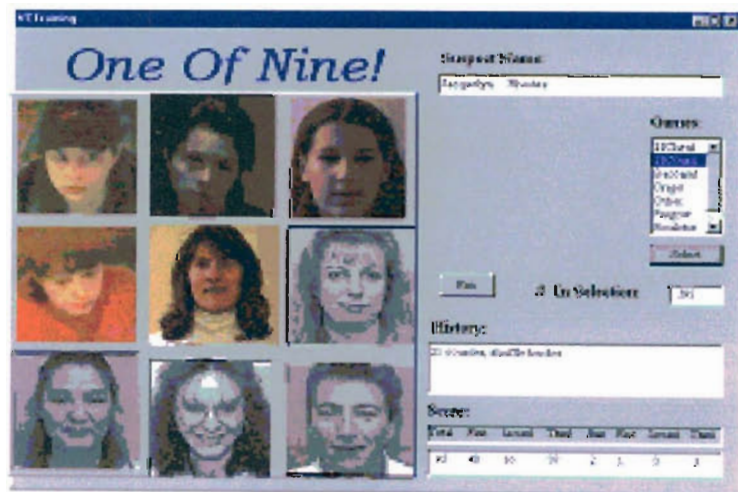


Figure 5. 5. Face recognition match - One of nine

It is proposed that an impartial 3rd party would operate the face recognition exclusion system, as currently in existence only in the Eastern Cape (Kirton, S, 2003, personal communication). The 3rd party would use the video feeds from the casino cameras, excluding those relating to back of house, gambling privileged or specific information. The face recognition system would only retain those images when a suspected problem gambler was found and discard all images of non-problem gamblers. Where a possible match was found, the operator would confirm the match, so no automatic exclusion would occur, as shown in Figure 5. 5 (Pepin, 2003). This allows the new biometrics technologies to cut down on subjectivity in photo identification. Right now, the casino security guard must decide if it is really the person in the photograph or simply someone who resembles that person.

5.2 *Multiple-Exclusion Systems*

The application of the framework allowed multimodal exclusion techniques (possibly face recognition linked to casino loyalty cards) to emerge as a promising way forward. An exclusion system that utilises more than one core technology for user authentication is referred to as multimodal (in contrast to monomodal). Multimodal systems can offer more security for the enterprise and convenience for the end user. Companies are adopting multiple authentication methods to ensure a higher confidence in an individual's identity (Shen, 2003). While face recognition was resolved to be the preferred exclusion technique among the role players there is no reason why any the other exclusion techniques could not be combined with face recognition (Figure 5. 6). It would be easy to combine some form of automatic or manual face recognition with proximity cards or identity books and preferred gambler cards.



Figure 5. 6. **Multimodal solution – face recognition linked to a swipe card**

Multiple exclusion techniques may be more accurate than a single exclusion technique however the process flow of enrolment and verification are as relevant to real-world performance as the underlying statistical bases for performance.

Bibliography

Ambrosini, V. 1998 Exploring Techniques of Analysis and Evaluation in Strategic Management Prentice Hall Harlow England

Biometrics In Human Services User Group Newsletter Volume 7 Issue 2 March 2003
Available online at: <http://www.dss.state.ct.us/digital.htm>

Brand, H. 1996 Gambling laws of South Africa : an overview of South Africa's new gambling legislation, with a focus on casinos and gambling machine activities, and selective commentary on noteworthy aspects thereof / Hendrik Brand Kenwyn : Juta

Cooper, D. R. and Schindler, P. S. 2003 Business Research Methods 8th Edition McGraw-Hill Irwin Boston

Government Biometrics Workshop, 2003 Available online at:
<http://www.biometricscatalog.org/2003GBW/read.htm>

Lynch, R. 2000 Corporate Strategy 2nd Edition Prentice Hall Harlow England

Maltoni, D. Maio, D, Jain, A. K. and Prabhakar, S. 2003 Handbook of Fingerprint Recognition Springer. Available online at:
<http://bias.csr.unibo.it/maltoni/handbook/>

Shen, M. M. 2003 Trends in Biometrics Security: Heterogeneous Product Offerings and Cost Reduction" ePolymath Consulting Firm , Available online at:
<http://www.epolymath.com/trendsinbiometrics.pdf>

Thompson, A. A. and Strickland, A. J. 2003 Strategic Management Concepts and Cases 13th Edition McGraw-Hill Irwin Boston

Wayman, J. L. 2001 Fundamentals of Biometric Authentication Technologies International Journal of Image and Graphics, Vol. 1, No. 1 (2001) 93-113. Available online at:
<http://www.worldscinet.com/ijig/01/preserved-docs/0101/S0219467801000086.pdf>

Woodward, J. Orleans, N and Higgins, P. 2003 Biometrics: Identity Assurance in the Information Age McGraw-Hill.

Wynne, H. J. 2002 Gambling and Problem Gambling in Saskatchewan, January 2002. Prepared by Harold J. , Ph.D. Canadian Centre on Substance Abuse, Ottawa, Ontario. Available online at:
http://www.health.gov.sk.ca/ps_fin_rep_prev_of_prob_gam.html

References

Ability to Verify 2003 Available online at:

<http://www.ibgweb.com/reports/public/reports/atv.html>

Adam, E. E. & Ebert, R. J. 2001 Productions and Operations Management, 4th Edition, Prentice-Hall, Pg. 19

Adcock, S. July 2003, Voice Security Systems Inc. sherrie@voice-security.com
<http://www.voice-security.com>, personal communication

Are Biometric Systems Difficult to Use? 2003 Available online at:

http://www.ibgweb.com/reports/public/reports/difficulty_of_use.html

Association for Biometrics (AfB) and International Computer Security Association (ICSA) 1999 Available online at: <http://www.afb.org.uk/docs/glossary.htm>

Bailey, B. 2003 CEO of Viisage www.viisage.com

Becker, P. 2003a Editor, The Digital ID World Newsletter - July 31, 2003 Issue, Conference: <http://www.digitalidworld.com/conference>

Becker, P. 2003b Editor, The Digital ID World Newsletter - August 7, 2003 Issue Digital Identity World, LLC. <http://www.digitalidworld.com>

Becker, P. 2003c Editor, The Digital ID World Newsletter - September 4, 2003 Issue Digital Identity World, LLC. <http://www.digitalidworld.com>

Biometrics Market Intelligence, Volume 01, issue 01 2003 Available online at: http://acuity-mi.com/?page=home_biometrics/index

Biometric Market Report 2003-2007 2003 Available online at:

http://www.biometricgroup.com/reports/public/market_report.html

BioPrivacy Impact Framework 2003 Available online at:

http://www.ibgweb.com/reports/public/reports/privacy_deployment.html

BioPrivacy Best Practices 2003 Available online at: http://www.ibgweb.com/reports/public/reports/privacy_best_practices.html

Boitel, H. J. 2003, Money laundering, Newsletter - Biometric Bits, New York BIOMETRICS-request@PEACH.EASE.LSOFT.COM

Business Week 2003 Why Biometrics Is No Magic Bullet Available online at: http://www.businessweek.com/technology/content/jul2003/tc20030722_2846_tc125.htm

Cape casino security managers, Caledon Casino, Hotel & Health Spa, July 2003, personal communication

Centre for Criminal Justice Technology 2003 Public On-Line Documentation available online at: http://www.ece.unh.edu/biometric/biomet/public_docs/

Chartrand, S. 2003, Live Scan - Patent for Verifying Human Prints NY Times, August 10, 2003 – <http://www.nytimes.com/2003/08/11/technology/11PATE.html>

Chips down forever for neglectful parents, 2003-07-01, Do gamblers not pay their municipal accounts? Available online at: http://www.iol.co.za/index.php?click_id=196&art_id%20=vn20030606070354272C897629&set_id=1

Colley, A. 2003 Customs stalls on releasing biometric passport survey 22 July, 2003 <http://www.zdnet.com.au/newstech/security/story/0,2000048600,20276460,00.htm>

Comparative Biometric Testing, Available online at: http://www.ibgweb.com/reports/public/comparative_biometric_testing.html

Daugman, J. 1993 High confidence visual recognition of persons by a test of statistical independence. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 15(11), pp. 1148-1161. Available on line at: <http://www.cl.cam.ac.uk/users/jgd1000/PAMI93.pdf>

De Beer, D. Gold Reef City Casino Complex Surveillance & Security manager, Personal Communication

Don't bet on gambling 10th June Daily News Available online at: <http://www.dailynews.co.za/index.php?fSectionId=502&fArticleId=167222>

Eastern Cape Gambling & Betting Act, 1997 (Act No. 5 of 1997) (Eastern Cape))

Economic Impact of Legalised Gambling in South Africa, Study commissioned by the National Gambling Board of South Africa, 2002 Available online at: www.ngb.co.za

Embracing New Technology in Health Care: A Case Study 2003 Available online at: http://www.emedicalfiles.com/case_study_1.shtml

Enrolment Limitations 2003 Available online at: http://www.ibgweb.com/reports/public/reports/enrollment_limitations.html

Failure to enrol rate Available online at: <http://www.cl.cam.ac.uk/users/jgd1000/NPLsummary.gif>

Gilpin, K. N. 2003 Millions Are Victimized By Identity Theft, Survey Shows <http://www.nytimes.com/2003/09/03/national/03CND-THEFT.html?hp>

Grossman, W. 2003 The Independent - August 13, 2003 <http://news.independent.co.uk/digital/features/story.jsp?story=433209>

Harrison, A. 2003 Hackers Claim New Fingerprint Biometric Attack <http://www.securityfocus.com/news/6717> By Ann <mailto:ah@well.com>, SecurityFocus Aug 13 2003

Havenga, M. 2002 Iris Recognition System Instruction Manual Revision A Release 1.0.0.110 Depth A - Orientation www.intervidtech.com, 10 May 2002 Pg A11

Hodosh, M. 2003 Chief Business Officer ID One, Inc. mhodosh@idoneinc.com www.idoneinc.com, personal communication.

How Do Identification and Verification Differ 2003 Available online at: http://www.ibgweb.com/reports/public/reports/identification_verification.html

How Large Are Biometric Templates? 2003 Available online at: http://www.ibgweb.com/reports/public/reports/template_size.html

Joe, W. S. 2003 EL casino gamblers can ban themselves Available online at: <http://www.dispatch.co.za/2003/02/20/easterncape/ACASINO.HTM>

Kirton, S. 2003 [Sharonk@ECGBB.co.za] Legal Affairs Division Eastern Cape Gambling & Betting Board, personal communication

Keeling, G. 2003 Executive Assistant to the Commissioner & Head of Communications & Technology Services Office of the Information and Privacy Commissioner/Ontario The Use Of Biometric Face Recognition Technology In Ontario Casinos http://www.ipc.on.ca/scripts/index.asp?action=31&N_ID=1&U_ID=0&P_ID=10842&LG_ID=1, personal communication.

Krause, T. W. 2003 City Unplugs Camera Software Available online at: <http://www.tampatribune.com/MGA0TF0TKJD.html> Published: Aug 20, 2003

Lee, J. 2003, Passports and Visas to Add High-Tech Identity Features <http://www.nytimes.com/2003/08/24/national/24IDEN.html?ex=1062743429&ei=1&en=4c0a678d465e4d81>

Limit impact of gambling' South African's now apparently spend 5 times more on gambling products than on books (available online at: http://www.news24.com/News24/South_Africa/Politics/0..2-7-12_1376881,00.html

Iris Recognition Issues, 2003 Available online at: http://www.ibgweb.com/reports/public/reports/iris-scan_issues.html

Liveness Detection in Biometric Systems 2003 Available online at: <http://www.ibgweb.com/reports/public/reports/liveness.html>

Mayer, R. 2003 Director of National gambling Problems personal conversation

Mc Cullagh, D. 2003 Is privacy making a comeback? Available online at: http://news.com.com/2102-1071_3-5055782.html

McDonald, N. 2003 Director of Sales EMEA & AsiaPac, Bioscrypt Inc. neil.mcdonald@bioscrypt.com www.bioscrypt.com, personal communication.

McMillan, R. 2003 The Myth of Airport Biometrics Wired News – August 9, 2003 <http://www.wired.com/news/conflict/0,2100,54418,00.html>

Miami Police Department Targets Prostitutes 2003 Available online at: <http://www.foxnews.com/story/0,2933,93749,00.html>

Minister to get powers to issue casino licences, Business Day, Thursday 21st August 2003, Pg 2

Mississippi Wants Tougher Casino Self-Ban Rules www.Casinowire.com Thursday, August 28 2003 (<http://www.casinowire.com/news.asp?id=5085>)

Moodley, S. 2003 Manager, Law Enforcement & Compliance – KZN Gambling Board, shane@kzngambling.co.za, Personal conversation

Natal Witness, 2 June 2003

National Gambling Act, No. 1098, 3 July 1996, NO. 33 OF 199

National Responsible Gambling Programme www.responsiblegambling.co.za

Newkirk, G. 2003 InfoSENTRY Services, Inc. www.infosentry.com, glenn_newkirk@infosentry.com, personal communication

Opinion Surveys 2003 by [privacyexchange.org](http://www.privacyexchange.org) available online at <http://www.privacyexchange.org/iss/surveys/surveys.html>,

Public Attitudes Toward the Uses of Biometric Identification Technologies by Government and the Private Sector” a number of relevant points are raised which will not be repeated here (available online at: http://www.search.org/policy/bio_conf/Biometricsurveyfindings.pdf

Pepin, J. 2003 *Biometrica Systems, Inc* Brochure, Biometrica Systems, Inc., 2915 West Charleston Blvd. #4A, Las Vegas, NV 89102

Reuters, 2002 Online sellers, security groups target Web ID theft <http://www.itweb.co.za/sections/internet/2003/0309030836.asp?O=E>

Rose, N. I. 2002a Court Upholds Casinos' Right To Unreasonably Exclude <http://gaming.unlv.edu/research/reading/Rose81.html>

Rose, N. I. 2002b Dealing with Card-Counters <http://gaming.unlv.edu/research/reading/Rose149.html>

Roush, W. 2003 Surveillance with Privacy -MIT Technology Review - September 2003. <http://www.technologyreview.com/articles/schrage0903.asp?p=0>

Schrage, M. 2003 The Customer as Enemy - Why constrain customers instead of creating greater choices for them? By Michael - MIT Technology Review - September 2003 <http://www.technologyreview.com/articles/schrage0903.asp?p=0>

Shen, M. M. 2003 Trends in Biometrics Security: Heterogeneous Product Offerings and Cost Reduction Available online at:
<http://www.epolymath.com/trendsinbiometrics.pdf>

Speir, M. 2003 Atmel solves fingerprint riddle. August 18, 2003 available online at:
<http://www.fcw.com/fcw/articles/2003/0818/tec-review-08-18-03.asp>

Tamburini, J. H. 2003 Casino Surveillance Insider Tips BLACKJACK INSIDER LITE. September issue 2003. , editor Blackjack Insider Newsletter www.bjinsider.com

The Gambling Board must come to its senses' 6th June Johannesburg & Cape Town, South Africa Source: Independent Online/Cape Times Available online at:
http://www.iol.co.za/index.php?click_id=196&art_id=vn_20030606070354_272C897629&set_id=1

The National Responsible Gaming Programme (NRGP) 2003 Available online at:
<http://www.responsiblegambling.co.za/projects.html>

Those jingling coins came out of empty pockets 19th June The Star Available online at: (<http://www.thestar.co.za/index.php?iSectionId=225&fArticleId=172297>)

Ursel, B. 2001 Perspective on Problem Gambling: Impulse Control Disorder and Impacts on Community Life Email: billu.cmha@accesscomm.ca
http://www.unlv.edu/centers/gaming/research/subject/Problem_gambling.html

Van Wyk, J. 2003 General Manager, Grand West Casino, personal communication

Vijayan, J. 2003 ID theft a growing problem, survey finds, Washington Post Available online at: <http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,83587,00.html>

Visagie, J. CCTV Technician, Grand West Casino, Personal Communication

Wayman, J. L. 2001 Fundamentals of Biometric Authentication Technologies International Journal of Image and Graphics. Vol. 1, No. 1 (2001) 93-113. Available online at:
<http://www.worldscinet.com/ijig/01/preserved-docs/0101/S0219467801000086.pdf>

Western Cape Gambling & Racing Board Rules & Regulations, Available online at:
www.wcgb.co.za

Westin, A. 2001 Public Attitudes Toward the Uses of Public Attitudes Toward the Uses of Biometric Identification Biometric Identification Technologies by Government Technologies by Government and the Private Sector Available online at:
http://www.search.org/policy/bio_conf/Biometricsurveyfindings.pdf

Westin, A. F. 2002 Uses of Biometric Identification Technologies by Government and the Private Sector <http://www.pandab.org/westinbiometrics.ppt>

What Are Biometrics' Basic Components and Processes 2003 Available online at: http://www.ibgweb.com/reports/public/reports/components_processes.html

Which is the Best Biometric Technology? 2003 Available online at: http://www.ibgweb.com/reports/public/reports/best_biometric.html

Willing, R. 2003 Airport anti-terror systems flub tests Face-recognition technology fails to flag 'suspects' USA TODAY <http://www.usatoday.com/usatoday/20030902/5460651s.htm>

Definitions

Active Impostor Acceptance - When an impostor submits a modified simulated or reproduced biometric sample, intentionally attempting to relate it to another person who is an enrollee, and he/she is incorrectly identified or verified by a biometric system as being that enrollee. Compare with 'Passive Impostor Acceptance'.

Algorithm - A sequence of instructions that tell a biometric system how to solve a particular problem. An algorithm will have a finite number of steps and is typically used by the biometric engine to compute whether a biometric sample and template are a match. See also 'Artificial Neural Network'.

Attempt - The submission of a biometric sample to a biometric system for identification or verification. A biometric system may allow more than one attempt to identify or verify.

Authentication - Alternative term for 'Verification'.

Automatic ID/Auto ID - An umbrella term for any biometric system or other security technology that uses automatic means to check identity. This applies to both one-to-one verification and one-to-many identification.

Behavioural Biometric - A biometric, which is characterised by a behavioural trait that is learnt and acquired over time, rather than a physiological characteristic. However, physiological elements may influence the monitored behaviour.

Biometric - A measurable, physical characteristic or personal behavioural trait used to recognise the identity, or verify the claimed identity, of an enrollee.

Biometric Application - The use to which a biometric system is put.

Biometric Data - The information extracted from the biometric sample and used either to build a reference template (template data) or to compare against a previously created reference template (comparison data).

Biometric Engine - The software element of the biometric system, which processes

biometric data during the stages of enrolment, capture, extraction and comparison.

Biometric Device - The part of a biometric system containing the sensor that captures a biometric sample from an individual.

Biometric Sample - Raw data representing a biometric characteristic of an end-user as captured by a biometric system (for example the image of a fingerprint).

Capture - The method of taking a biometric sample from the end user.

Comparison - The process of comparing a biometric sample with a previously stored reference template or templates. See also 'One-To-Many' and 'One-To-One'.

Claim of Identity - When a biometric sample is submitted to a biometric system to verify a claimed identity.

Claimant - A person submitting a biometric sample for verification or identification whilst claiming a legitimate or false identity.

Database - Any storage of biometric templates and related end user information. Even if only one biometric template or record is stored, the database will simply be "a database of one". Generally speaking, however, a database will contain a number of biometric records.

End User - A person who interacts with a biometric system to enrol or have his/her identity checked.

Encryption - The act of converting biometric data into a code so that it is unable to be read. A key is used to decrypt (decode) the encrypted biometric data.

Enrollee - A person who has a biometric reference template on file.

Enrolment - The process of collecting biometric samples from a person, subsequent preparation and storage of biometric reference templates.

Enrolment Time - The time period a person must spend to have his/her biometric reference template successfully created.

Equal Error Rate - The error rate occurring when the decision threshold of a system is set so that the proportion of false rejections will be approximately equal to the proportion of false acceptances.

Extraction - The process of converting a captured biometric sample into biometric data so that it can be compared to a reference template.

Failure to Acquire - Failure of a biometric system to capture and extract biometric data (comparison data).

Failure to Acquire Rate - The frequency of a failure to acquire.

Failure to Enrol - Failure of the biometric system to form a proper enrolment template for an end-user. The failure may be due to failure to capture the biometric sample or failure to extract template data (of sufficient quality).

Failure to Enrol Rate - The proportion of the population of end-users failing to complete enrolment

False Acceptance - When a biometric system incorrectly identifies an individual or incorrectly verifies an impostor against a claimed identity.

False Acceptance Rate/FAR - The probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. The rate given normally assumes passive impostor attempts. The False Accept Rate may be estimated as $FAR = NFA / NIJA$ or $FAR = NFA / NIVA$ where

FAR is the false acceptance rate

NFA is the number of false acceptances

NIJA is the number of impostor identification attempts

NIVA is the number of impostor verification attempts

False Rejection - When a biometric system fails to identify an enrollee or fails to verify the legitimate claimed identity of an enrollee.

False Rejection Rate/FRR - The probability that a biometric system will fail to identify an enrollee, or verify the legitimate claimed identity of an enrollee. The False Rejection Rate may be estimated as follows:

$$\text{FRR} = \text{NFR} / \text{NEIA} \quad \text{or} \quad \text{FRR} = \text{NFR} / \text{NEVA} \quad \text{where}$$

FRR is the false rejection rate
NFR is the number of false rejections
NEIA is the number of enrollee identification attempts
NEVA is the number of enrollee verification attempts

This estimate assumes that the enrollee identification/verification attempts are representative of those for the whole population of end-users. The False Rejection Rate normally excludes 'Failure to Acquire' errors

Field Test / Field Trial - A trial of a biometric application in 'real-world' as opposed to laboratory conditions.

Filtering - The process of classifying biometric data according to information that is unrelated to the biometric data itself. This may involve filtering by sex, age, hair colour or other distinguishing factors, and including this information in the database .

Goats - Biometric system end users whose pattern of activity when interfacing with the system varies beyond the specified range allowed by the system, and who consequently may be falsely rejected by the system.

Identification/Identify - The one-to-many process of comparing a submitted biometric sample against all of the biometric reference templates on file to determine whether it matches any of the templates and, if so, the identity of the enrollee whose template was matched. The biometric system using the one-to-many approach is seeking to find an identity amongst a database rather than verify a claimed identity. Contrast with 'Verification'.

Impostor - A person who submits a biometric sample in either an intentional or inadvertent attempt to pass him/herself off as another person who is an enrollee.

In-House Test - A test carried out entirely within the environs of the biometric developer, which may or may not involve external user participation.

Live Capture - The process of capturing a biometric sample by an interaction between an end user and a biometric system.

Match/Matching - The process of comparing a biometric sample against a previously stored template and scoring the level of similarity. An accept or reject decision is then based upon whether this score exceeds the given threshold.

Multiple Biometric - A biometric system that includes more than one biometric system or biometric technology.

Neural Net/Neural Network - One particular type of algorithm. An artificial neural network uses artificial intelligence to learn by past experience and compute whether a biometric sample and template are a match.

Performance Criteria - Pre-determined criteria established to evaluate the performance of the biometric system under test.

Physical/Physiological Biometric - A biometric which is characterised by a physical characteristic rather than a behavioural trait. However, behavioural elements may influence the biometric sample captured.

Population - The set of end-users for the application.

Recognition - The preferred term is 'Identification'.

Record - The template and other information about the end-user (e.g. banned)

Response Time - The time period for a biometric system to return a decision on identification or verification of a biometric sample.

Score - The level of similarity from comparing a biometric sample against a previously stored template.

Template/Reference Template - Data, which represents the biometric measurement of an enrollee, used by a biometric system for comparison against subsequently submitted biometric samples.

Template Ageing - The degree to which biometric data evolves and changes over time, and the process by which templates account for this change.

Template Size - The amount of computer memory taken up by the biometric data.

Third Party Test - An objective test, independent of a biometric vendor, usually carried out entirely within a test laboratory in controlled environmental conditions.

Threshold/Decision Threshold - The acceptance or rejection of biometric data is dependent on the match score falling above or below the threshold. The threshold is adjustable so that the biometric system can be more or less strict, depending on the requirements of any given biometric application.

Throughput Rate - The number of end users that a biometric system can process within a stated time interval.

Type I Error - In statistics, the rejection of the null hypothesis (default assumption) when it is true. In a biometric system the usual default assumption is that the claimant is genuine, in which case this error corresponds to a 'False Rejection'.

Type II Error - In statistics, the acceptance of the null hypothesis (default assumption) when it is false. In a biometric system the usual default assumption is that the claimant is genuine, so this error corresponds to a 'False Acceptance'.

User - The client to any biometric vendor. The user must be differentiated from the end user and is responsible for managing and implementing the biometric application rather than actually interacting with the biometric system.

Validation -The process of demonstrating that the system under consideration meets in all respects the specification of that system.

Verification/Verify - The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. Contrast with 'Identification'.

WSQ (Wavelet Transform/Scalar Quantisation) - A compression algorithm used to reduce the size of reference templates

(Association for Biometrics (Afb) and International Computer Security Association (ICSA) 1999).

Privacy Rating																																
1-5 scale, with 1 being best, 5 worst		Total	Ease of use	Physic. Cost	Physic. Time	Response Time	Frequency of use	Distraction	Human factors	Errors	Stress	User Acceptance	Health	Security	Privacy	Reliability	Accuracy	Flexibility	Portability	Robustness	Security	Privacy	Accuracy	Flexibility	Portability	Robustness	Security	Privacy	Accuracy	Flexibility	Portability	Robustness
Weighting of Criteria (100)																																
Current solutions																																
Owed at the entrance with a file of photographs																																
Surveillance operators with a file of photographs																																
Alternative solutions																																
Pre-existing identity based solution																																
Identity based photo & no checked automatically																																
Cross license photo & checked automatically																																
Card based solution																																
Swipe card																																
Proximity card																																
Biometrics																																
Contact biometrics																																
Physiological characteristic																																
Fingerprint recognition																																
Hand scan																																
Behavioural characteristic																																
Signature																																
Voice																																
Keystroke																																
Non-Contact biometrics																																
Overt biometric acquisition																																
Iris Recognition																																
Retina																																
Covert biometric acquisition																																
Face recognition																																

Table I. 5. Privacy rating evaluation

Gambling board																																
1-5 scale, with 1 being best, 5 worst		Total	Ease of use	Physic. Cost	Physic. Time	Response Time	Frequency of use	Distraction	Human factors	Errors	Stress	User Acceptance	Health	Security	Privacy	Reliability	Accuracy	Flexibility	Portability	Robustness	Security	Privacy	Accuracy	Flexibility	Portability	Robustness	Security	Privacy	Accuracy	Flexibility	Portability	Robustness
Weighting of Criteria (100)																																
Current solutions																																
Owed at the entrance with a file of photographs																																
Surveillance operators with a file of photographs																																
Alternative solutions																																
Pre-existing identity based solution																																
Identity based photo & no checked automatically																																
Cross license photo & checked automatically																																
Card based solution																																
Swipe card																																
Proximity card																																
Biometrics																																
Contact biometrics																																
Physiological characteristic																																
Fingerprint recognition																																
Hand scan																																
Behavioural characteristic																																
Signature																																
Voice																																
Keystroke																																
Non-Contact biometrics																																
Overt biometric acquisition																																
Iris Recognition																																
Retina																																
Covert biometric acquisition																																
Face recognition																																

Table I. 6. Gambling Board evaluation

		Gambling anonymous																												
		Ease of use	Physical factors	Response time	Distraction	Error rate	Market share	False Acceptance Rate	Security	Level of impact	Weight of criteria	Weight of criteria	Weight of criteria	Weight of criteria	Weight of criteria	Weight of criteria	Weight of criteria	Weight of criteria	Weight of criteria	Weight of criteria	Weight of criteria	Weight of criteria	Weight of criteria	Weight of criteria	Weight of criteria	Weight of criteria	Weight of criteria			
1-5 scale, with 1 being best, 5 worst																														
Weighting of Criteria (100)		100	7	1	6	12	1	5	1	15	1	1	20	5	1	15	20	1	1	1	1	1	1	1	1	1	1	1	5	
Current solutions																														
Guard at the entrance with a file of photographs		252	1	7	1	40	5	2	5	25	5	5	15	1	1	80	10	1	5	5	20	1	4	1	1	1	1	1	15	
Surveillance operators with a file of photographs		246	1	7	1	40	5	2	5	25	5	5	15	1	1	80	10	1	5	5	20	1	3	1	1	1	1	1	5	
Alternative solutions																														
Pre-existing identity based solution																														
Identity book photo & No. checked automatically		245	2	14	3	16	4	6	4	20	4	4	60	1	1	40	10	1	2	20	20	1	1	4	1	1	1	1	5	
Drivers license photo & No. checked automatically		247	2	14	4	16	4.6	4	20	4	4	60	1	1	40	10	2	2	20	20	20	1	1	4	1	1	1	1	5	
Card based solution																														
Swipe card		211	3	21	4	24	2.4	5	15	3	2	30	2	1	20	5	1	5	5	20	2	5	4	4	4	4	4	4	20	
Proximity card		217	1	28	1	16	1	2	5	10	2	2	45	2	2	20	10	1	5	5	20	2	5	4	4	4	4	4	20	
Biometrics																														
Contact biometrics																														
Physiological characteristic																														
Fingerprint recognition		347	3	21	6	32	2	8	4	20	4	2	60	1	1	80	20	2	2	10	40	2	2	2	2	2	2	2	20	
Hand scan		329	3	21	6	32	2	8	4	20	4	3	60	3	3	80	15	3	3	10	40	2	2	2	2	2	2	2	20	
Behavioural characteristic																														
Signature		258	2	14	2	24	2.2	2	10	2	2	15	3	3	60	15	3	2	15	60	2	2	2	2	2	2	2	2	10	
Voice		319	2	35	2	24	2	4	3	15	3	3	30	3	3	80	15	3	2	10	80	2	2	2	2	2	2	2	10	
Keystroke		302	2	35	5	24	2	4	3	15	3	3	30	3	3	80	15	3	2	10	60	2	2	2	2	2	2	2	10	
Non-Contact biometrics																														
Overt biometric acquisition																														
Iris Recognition		296	5	14	1	8	1.4	1	10	1	1	60	2	1	20	5	1	1	25	100	1	1	2	1	1	1	1	5	25	
Retina		321	5	21	1	8	1.4	1	10	1	1	75	2	2	20	5	2	2	25	100	1	1	2	1	1	1	1	1	5	25
Covert biometric acquisition																														
Face recognition		227	1	7	1	24	3	2	3	15	3	3	15	2	2	80	20	4	2	10	20	1	1	1	1	1	1	1	5	

Table I. 7. Gambling Anonymous evaluation

		Public																											
		Ease of use	Physical factors	Response time	Distraction	Error rate	Market share	False Acceptance Rate	Security	Level of impact	Weight of criteria	Weight of criteria	Weight of criteria	Weight of criteria	Weight of criteria	Weight of criteria	Weight of criteria	Weight of criteria	Weight of criteria	Weight of criteria	Weight of criteria	Weight of criteria	Weight of criteria	Weight of criteria	Weight of criteria	Weight of criteria	Weight of criteria	Weight of criteria	
1-5 scale, with 1 being best, 5 worst																													
Weighting of Criteria (100)		100	1	25	15	1	15	17	1	3	2	1	5	1	1	2	6	1	5	1	1	1	1	1	1	1	1	1	7
Current solutions																													
Guard at the entrance with a file of photographs		254	1	25	15	5	75	17	5	15	10	5	5	1	1	8	16	1	25	1	1	1	4	1	1	1	1	1	14
Surveillance operators with a file of photographs		246	1	25	15	5	75	17	5	15	10	5	5	1	1	8	16	1	25	1	1	1	3	1	1	1	1	1	7
Alternative solutions																													
Pre-existing identity based solution																													
Identity book photo & no. checked automatically		311	2	50	45	2	80	51	4	12	8	4	20	1	1	4	16	1	10	4	1	1	1	4	1	1	1	1	7
Drivers license photo & No. checked automatically		327	2	50	60	2	60	51	4	12	8	4	20	1	1	4	16	2	10	4	1	1	1	4	1	1	1	1	7
Card based solution																													
Swipe card		325	3	75	60	3	30	34	5	9	6	2	10	2	1	2	6	1	25	1	1	2	5	4	4	4	4	28	
Proximity card		218	3	50	15	2	15	17	5	6	4	2	10	2	2	3	6	1	25	1	1	2	5	4	4	4	4	4	28
Biometrics																													
Contact biometrics																													
Physiological characteristic																													
Fingerprint recognition		397	3	75	75	4	30	68	4	12	8	2	20	1	1	8	32	2	10	2	2	2	2	2	2	2	2	2	28
Hand scan		306	3	75	75	4	30	68	4	12	8	3	20	3	3	6	24	3	15	2	2	2	2	2	2	2	2	2	28
Behavioural characteristic																													
Signature		230	2	50	30	3	30	34	3	9	6	3	10	3	3	6	24	3	10	3	3	2	2	2	2	2	2	2	14
Voice		334	2	125	30	3	30	34	3	9	6	3	10	3	3	6	24	3	10	2	4	2	2	2	2	2	2	2	14
Keystroke		378	2	125	75	3	30	34	3	9	6	3	10	3	3	6	24	3	10	2	3	2	2	2	2	2	2	2	14
Non-Contact biometrics																													
Overt biometric acquisition																													
Iris Recognition		224	5	50	15	1	15	34	1	6	2	1	20	2	1	2	6	1	5	5	1	1	2	1	1	1	1	1	35
Retina		281	5	75	15	1	15	34	1	6	2	1	25	2	2	6	2	10	5	5	1	1	2	1	1	1	1	1	35
Covert biometric acquisition																													
Face recognition		222	1	25	15	3	45	34	3	9	6	3	5	2	2	8	32	4	10	2	1	1	1	1	1	1	1	1	7

Table I. 8. Public perception evaluation

Appendix II – Role Player Evaluation of Evaluation Techniques

	Casino				Legislative				Public		AVG	Weighted Score
	Marketing	Process	Surveillance	Security	Privacy Rating	Gambling board	Gambling anonymous	Public				
Weighted Score (total 100)	10	3	20	2	8	23	30	4		100		
Current solutions												
Used at the entrance with a file of photographs	213	205	280	296	242	265	262	254	251	246	247	256
Surveillance operates with a file of photographs	222	230	275	294	252	254	248	246	247	246	247	249
Alternative solutions												
Paper(?) based solution												
Identity book	240	270	246	260	251	205	245	311	267	311	267	259
Drivers license	257	262	260	274	299	297	247	327	273	327	273	284
Card based solution												
Swipe card	272	266	286	308	278	254	211	325	275	325	275	287
Proximity card	218	220	262	267	242	215	217	318	236	318	236	230
Biometrics												
Contact biometrics												
Physiological characteristic												
Fingerprint recognition	331	310	294	296	369	386	347	397	341	397	341	345
Hand scan	329	308	304	316	364	373	325	366	340	366	340	339
Behavioural characteristic												
Signature	299	247	260	260	227	221	260	230	228	230	228	226
Voice	289	283	282	283	299	299	319	334	299	334	299	301
Keystroke	312	283	278	283	307	301	302	379	306	379	306	300
Non-Contact biometrics												
Overt biometric acquisition												
Iris Recognition	215	301	274	243	251	255	298	224	250	224	250	255
Retina	259	321	235	266	281	290	321	261	276	261	276	282
Covert biometric acquisition												
Face recognition	200	214	224	228	226	226	227	222	221	222	221	223
MAX	331	321	304	318	369	388	347	398	341.25	398	341.25	345
MDV	205	205	214	225	222	220	211	218	222.5	218	222.5	223

KEY Indicates the lowest score

Table II. 1. Weighted evaluation of multiple exclusion techniques.

The opinions expressed in this document are the views of the author and do not necessarily reflect those of the views of Intervid, Intervid Technologies, Intervid International, the National Gambling Board, provincial gambling Board, any casino, casino management, casino employee or any other party.

THE END